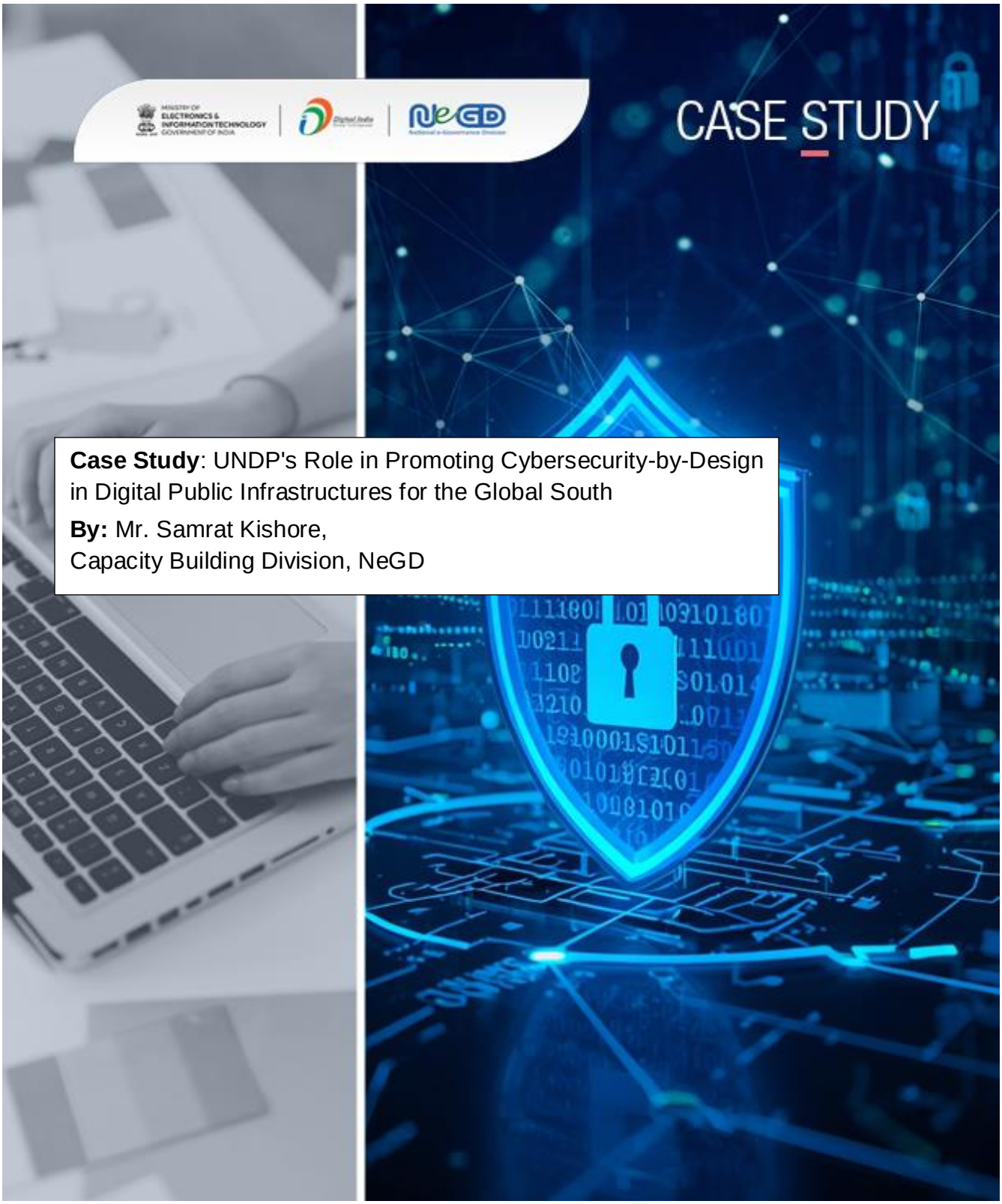

Case Study: UNDP's Role in Promoting Cybersecurity-by-Design in Digital Public Infrastructures for the Global South

By: Mr. Samrat Kishore,
Capacity Building Division, NeGD

Introduction

The National e-Governance Division (NeGD), under the Ministry of Electronics & Information Technology (MeitY), is at the forefront of realizing the Digital India vision. A cornerstone of this mission is Capacity Building (CB), which empowers government officials, creators, and stakeholders with the expertise needed to implement and sustain transformative digital initiatives.

This case study, "UNDP's Role in Promoting Cybersecurity-by-Design in Digital Public Infrastructures for the Global South," is part of UNDP's ongoing commitment to document, analyze, and share best practices in digital governance, cybersecurity, and innovation. Developed by internal experts and practitioners, this study offers a comprehensive exploration of how legal frameworks, technical systems, and stakeholder engagement are reshaping approaches to safeguarding digital systems—enhancing fairness, transparency, and inclusivity across the digital ecosystem.

As digital public infrastructures become foundational to development efforts across the Global South, the need to embed cybersecurity and privacy protections from the outset has never been more critical. This case study explores how the UNDP advances the principle of Cybersecurity-by-Design—ensuring that security, resilience, and ethical safeguards are integral to the architecture of digital systems that deliver essential services..

Our methodology combines in-depth research, analysis of legal and technical frameworks, and interviews with key stakeholders and domain experts who are shaping the Global South's approach to cybersecurity and digital public infrastructure. This ensures that the narratives are accurate and enriched with practical insights and firsthand perspectives.

The objective of this repository is to serve as a valuable knowledge asset for policymakers, program managers, technologists, and implementers at all levels. By facilitating learning and enabling the development of robust, responsive digital solutions, it supports the broader vision of citizen-centric, transparent, and sustainable digital transformation across the Global South.

Disclaimer

This case study has been developed by the National e-Governance Division (NeGD) under its Capacity Building mandate for the purpose of knowledge sharing and academic reference. The information presented herein has been compiled from official government sources, project documents, and interviews with relevant stakeholders involved.

While every effort has been made to ensure the accuracy and reliability of the information, this document is intended for educational and illustrative purposes only. It should not be interpreted as an official policy statement or a guideline for implementation. The views and conclusions expressed are those of the author and contributors based on their analysis and do not necessarily reflect the official position of the Ministry of Electronics & Information Technology (MeitY) or the National e-Governance Division (NeGD).

The commercial use of this material is strictly prohibited. This case study is meant to be used as a learning tool for government officials, trainees, and individuals interested in e-Governance and public policy.

Any reproduction or use of this material must include proper attribution to 'National e-Governance Division (NeGD).' All intellectual property rights remain with NeGD unless otherwise specified.

Acknowledgment

This case study, "UNDP's Role in Promoting Cybersecurity-by-Design in Digital Public Infrastructures for the Global South," has been developed Mr. Samrat Kishore, member of the Capacity Building Division, National e-Governance Division (NeGD), Ministry of Electronics & Information Technology (MeitY).

The content presented herein is based entirely on information available in the public domain, including official reports, published research, and publicly accessible resources. No proprietary or confidential data has been used in the preparation of this document.

The author extends gratitude to all organizations and individuals whose publicly shared knowledge and insights have contributed to the development of this study.

This case study is intended as a knowledge resource for policymakers, practitioners, and stakeholders engaged in digital public infrastructure and cybersecurity initiatives across the Global South.

Furthermore, we extend our deepest appreciation to the internal experts at NeGD who meticulously reviewed this document.

Index

Ths Case Study:

1. Introduction: The Nexus of DPI, Cybersecurity, and Global Development

1.1 Defining Digital Public Infrastructure (DPI)

Digital Public Infrastructure (DPI) represents a foundational layer of digital systems and platforms designed to facilitate the delivery of services, enable efficient data exchange, and support robust digital governance across diverse sectors. These infrastructures are characterized by components such as digital identity systems, payment platforms, and data exchange protocols, all engineered for scalability, interoperability, and broad accessibility to both governmental and private sector entities.[1] Notable examples include India's Aadhaar system for digital identity, the Unified Payments Interface (UPI) for payments, and the India Stack data exchange framework.[1] DPI serves as an intermediate layer within the digital ecosystem, enabling a wide array of applications across various public sectors and playing a crucial role in modernizing public services, including e-governance, health records management, and education.[1]

The conceptualization of digital systems as public infrastructure has evolved over several decades. Early instances, such as the Internet and GPS, were publicly funded and made universally available. However, these systems were often siloed and not initially conceived as a cohesive public infrastructure.[1] The term "digital public infrastructure" gained significant traction in the early 2020s, coinciding with a global trend of countries developing integrated digital service platforms. This evolution was notably influenced by the India Stack, which pioneered open digital payment platforms and data-sharing frameworks, conceptualized as "government-owned, non-competing" digital utilities upon which other services could be built.[1] By 2020, policymakers and thinkers increasingly adopted the infrastructure analogy, framing online services as critical and broadly accessible, akin to physical public roads.[1]

A pivotal moment for DPI occurred in 2023, during India's G20 presidency, when a global consensus on its definition emerged. World leaders agreed to describe DPI as "a set of shared digital systems that are secure and interoperable, built on open standards, to deliver equitable access to public and/or private services at societal scale".[1] This definition explicitly highlights security and interoperability as inherent and non-negotiable characteristics. The United Nations Development Programme

(UNDP) actively embraces and promotes this concept, positioning DPI as a critical enabler for digital transformation and a means to significantly improve public service delivery at scale, fostering secure and seamless interactions among people, businesses, and governments.[2] The UNDP views DPI as analogous to physical infrastructure, providing essential access to systems that shape daily life, yet recognizing that unlike physical infrastructure, access to digital systems is often fragmented and unequal.[2]

The global alignment on DPI's definition and importance signifies a profound shift from ad-hoc digital projects to a strategic, integrated approach to digital development. This formalization provides a common language and framework for international cooperation, inherently demanding a standardized approach to security across diverse international actors and national governments. This consensus sets a precedent for how digital development should be approached at a systemic level, ensuring that foundational digital systems are developed with shared principles and objectives.

1.2 The Imperative of Cybersecurity-by-Design (CbD) in DPI

Cybersecurity-by-Design (CbD), also known as Secure-by-Design, is a critical paradigm in software engineering and system development. It mandates that technology products and capabilities are built with inherent security from their foundational design, rather than security being an afterthought or a reactive measure.[3] This proactive approach necessitates anticipating malicious attacks and minimizing their potential impact from the outset, rather than merely responding to vulnerabilities after they have been exploited.[4]

Core principles of CbD include the fundamental assumption that "attacks will occur," requiring systems to be designed with resilience against anticipated malicious actions. The principle of "avoid security through obscurity" advocates for transparent and auditable designs, suggesting that security should not rely on the secrecy of the system's inner workings but rather on its inherent robustness. Furthermore, the "fewest privileges" principle dictates that all system components and individuals should operate with the absolute minimum permissions necessary to perform their designated tasks, thereby limiting the potential damage if a component is

compromised.[4] The National Institute of Standards and Technology (NIST) further elaborates on CbD with principles such as anomaly detection, commensurate protection (security measures proportional to threats), continuous protection (uninterrupted security, self-protection against tampering, and protective default states upon failure), defense in depth (multiple, coordinated lines of defense), distributed privilege (requiring agreement and coordination for critical operations), diversity, and various "least" principles (e.g., least functionality, least persistence, least privilege, least sharing).[6] These principles collectively aim to prevent vulnerabilities by limiting system exposure and potential attack surfaces.

The NIST Cybersecurity Framework complements CbD by outlining five core functions: Identify (understanding critical functions and associated risks), Protect (implementing safeguards to contain potential impacts), Detect (assessing system compromises), Respond (minimizing damage from breaches), and Recover (restoring capabilities).[7] These functions provide a structured approach for organizations to manage cybersecurity risks throughout the lifecycle of their digital assets. Similarly, the European Union Agency for Cybersecurity (ENISA) provides guidelines for national cybersecurity strategies, emphasizing a proactive stance in enhancing preparedness, conducting national risk assessments, and fostering comprehensive stakeholder involvement.[8] ENISA's role extends to fostering cooperation among Member States, strengthening resilience against cyber threats, and engaging in incident management and situational awareness at both national and EU levels.[10]

Privacy-by-Design (PbD) is a closely related and often integrated concept that shares fundamental principles with CbD. PbD mandates that privacy is embedded into the design and architecture of IT systems and business practices from the earliest stages. Its core tenets include being "proactive not reactive," ensuring "privacy as the default" setting, embedding "privacy into design" as an integral part of development, providing "end-to-end security – lifecycle protection" for data, and promoting "visibility and transparency" in data handling to build user trust.[5] PbD is not merely a best practice but a legal requirement in significant regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Protection Act (CCPA) in the US, underscoring its critical importance for any data-intensive systems.[5]

The emphasis on embedding security from the foundational design and throughout all points in the development lifecycle signifies a crucial paradigm shift from reactive

cybersecurity to a proactive, integrated approach. The substantial overlap between CbD and PbD highlights that data protection and user rights are not secondary considerations but fundamental aspects of a secure system. The UNDP's explicit "do no harm" principle within its digital standards further elevates CbD to an ethical imperative.[12] This indicates that for Digital Public Infrastructures, security is intrinsically linked to building public trust and preventing societal harm. Consequently, for DPIs operating at "societal scale" and handling sensitive personal data, CbD is indispensable for building public confidence and ensuring long-term resilience. Without this integrated approach, DPIs risk becoming vectors for harm, thereby undermining their very purpose of fostering development and inclusion.

1.3 The Global South: Context, Challenges, and Opportunities for Digital Transformation

The Global South, encompassing 88% of the world's population, faces profound digital divides that significantly impede equitable access to digital opportunities. Only 27% of the population in low-income countries has internet connectivity, a stark contrast to 93% in high-income countries.[14] Beyond mere internet access, the challenges extend to the availability of affordable devices, the prevalence of digital literacy, and the acquisition of skills necessary to navigate the internet safely and meaningfully.[15] These disparities create a complex environment for digital transformation efforts.

Cybersecurity in these regions is particularly vulnerable due to weak existing digital infrastructure, a reliance on outdated technology, and the nascent stage of cybersecurity policy frameworks.[16] Low levels of digital literacy among users exacerbate these vulnerabilities, increasing susceptibility to common cyber threats such as phishing and malware attacks.[16] Furthermore, governance challenges frequently hinder the effective development and enforcement of robust cybersecurity policies, leaving nations exposed to a rising tide of cybercrime, including data breaches and ransomware attacks. High-profile incidents, such as devastating ransomware attacks in Albania, Vanuatu, and Costa Rica, underscore the severe consequences of these vulnerabilities.[16] A critical global shortage of skilled cybersecurity professionals is acutely felt in developing countries, significantly impeding effective incident response, cybercrime prosecution, and the protection of critical infrastructure.[18]

Despite these formidable challenges, digital transformation presents substantial opportunities for the Global South. The adoption of emerging technologies, including

Artificial Intelligence (AI), blockchain, and advanced encryption, offers efficient solutions for enhancing cybersecurity capabilities where traditional protections may fall short.[16] Moreover, strategic investments in cybersecurity skills development can serve a dual purpose: directly addressing the workforce gap and simultaneously creating high-quality job opportunities, thereby driving broader socio-economic transformation.[18] The World Bank, for instance, has noted promising initiatives, often community-driven and focusing on women and youth, that are already yielding strong results in accelerating cybersecurity skills development, suggesting models for replication and scaling.[18]

The data reveals a compelling narrative of both immense opportunity and significant risk for the Global South in its digital transformation journey. While Digital Public Infrastructures offer pathways to accelerate development, enhance financial inclusion [19], and improve public service delivery, the existing vulnerabilities—weak infrastructure, pronounced skills gaps, and governance deficits [14]—mean that digitalization, if not managed with inherent security, can inadvertently deepen existing inequalities and expose populations to severe cyber threats.[15] This situation creates a heightened imperative for the integration of Cybersecurity-by-Design, as the consequences of security failures are often more severe in contexts with fewer societal and economic safety nets. Therefore, any engagement in the Global South must navigate this complex landscape by not only promoting digital access but also by proactively embedding robust CbD and comprehensive capacity-building measures to ensure that digital transformation genuinely serves as a force for equitable and secure progress, rather than a new source of vulnerability.

2. UNDP's Strategic Approach to Digital Public Infrastructure

2.1 UNDP's Digital Strategy and Foundational Principles

The United Nations Development Programme (UNDP) operates under a comprehensive Digital Strategy (2022-2025) that guides its efforts to support countries in building inclusive, ethical, and sustainable digital societies.[21] This strategy acknowledges the profound and accelerating impact of digitalization, recognizing its transformative power in addressing global challenges such as climate action and its potential to enhance the digital capacity of vulnerable and marginalized groups, including women and people with disabilities.[21]

The strategy is structured around three mutually reinforcing objectives designed to maximize development impact and organizational effectiveness. Firstly, "Digitally enabled programming" aims to embed digital technologies across all UNDP programming to amplify development outcomes, encouraging experimentation with new approaches, scaling proven solutions, and applying foresight for future preparedness.[21] Secondly, "Empowering digital ecosystems" focuses on supporting societies in creating more inclusive and resilient digital environments, assisting countries in their digital transformation journey at a societal level while prioritizing human rights protection and ensuring that no one is left behind.[21] Thirdly, "Digitally native UNDP" seeks to transform the organization itself, ensuring it possesses fit-for-purpose digital systems, processes, tools, and data, alongside a digitally competent workforce, to effectively support the first two objectives.[21]

These objectives are underpinned by a set of core guiding principles that shape UNDP's approach to digital development:

- **Human rights at the center:** Recognizing the increasing mediation of daily life by digital technologies, UNDP places human rights at the core of its digital approach, committing to a continuous understanding and mitigation of potential negative impacts.[21]
- **Inclusive and gender-sensitive approaches:** The UNDP advocates for digital transformation that is intentionally inclusive and thoughtfully designed and implemented, ensuring all processes are people-centered to build a more open, transparent, and accessible society that leaves no one behind.[21]
- **Contribution to shared global standards:** The organization ensures its digital work aligns with and supports established international standards, such as the UN Charter and the Universal Declaration of Human Rights.[21]
- **Advocacy for open digital standards and open data:** UNDP actively promotes open digital standards to unlock scale, reusability, and interoperability, leveraging digital public goods to foster a more equitable and transparent future, with a strong emphasis on protecting rights and preventing misuse.[21]
- **Strengthening local digital ecosystems:** Adopting a whole-of-society approach, UNDP collaborates with local leaders, companies, and digital innovators to cultivate thriving local digital ecosystems founded on inclusivity, sustainability, accountability, and rights.[21]
- **Leveraging strategic partnerships:** Partnerships are considered critical for catalyzing inclusive approaches to digital development, including the provision of adequate resources to implement relevant international standards and

safeguard people.[21]

- **Proactive consideration of potential risks:** UNDP takes a critical approach to selecting and applying digital solutions, anticipating and mitigating risks, particularly those pertaining to human rights.[21]

Further practical guidance is provided through UNDP's Digital Standards, which offer best practices for teams developing digital solutions. These standards include principles such as "Start with the need," "Bridge the digital divide," "Test early and often," "Do no harm," "Follow the UNDP Data Principles," and "Default to open".[12] These standards are built upon the broader Principles for Digital Development and are tailored to UNDP's unique experience and organizational breadth.[12]

UNDP's digital strategy consistently intertwines cybersecurity, human rights, and inclusivity. The "do no harm" principle, central to its digital standards [12], directly underpins Cybersecurity-by-Design by demanding proactive risk mitigation. The emphasis on "human rights at the center" and "inclusive and gender-sensitive approaches" [21] means that CbD, for UNDP, is not merely a technical exercise but a fundamental aspect of ensuring equitable access, robust data protection, and preventing digital exclusion or surveillance. This deep conceptual integration indicates that CbD serves as a means to achieve broader development and human rights objectives. For UNDP, promoting CbD in DPIs is therefore a strategic imperative that transcends the prevention of cyberattacks; it is about ensuring that digital systems are inherently designed to protect people's rights, foster trust, and contribute to a more just and equitable digital society, a consideration particularly critical in the Global South where governance and human rights protections might be less robust.

2.2 Key UNDP Frameworks and Initiatives for DPI

UNDP's commitment to promoting secure and inclusive Digital Public Infrastructures (DPIs) in the Global South is operationalized through several key frameworks and initiatives, each embedding principles of Cybersecurity-by-Design (CbD) and ethical development.

2.2.1 Universal DPI Safeguards Framework

The Universal DPI Safeguards Framework, launched in September 2024 (version 1.0) by the UN's DPI Safeguards Initiative, represents a multi-stakeholder collaborative effort to ensure that DPI implementations effectively mitigate risks at both individual and societal levels. Its core mission is to advance the Sustainable Development Goals (SDGs) and cultivate trust and equity across all countries.[23]

This framework outlines nine foundational principles that serve as the building blocks for safe and inclusive DPI: "Do No Harm," "Do Not Discriminate," "Do Not Exclude," "Reinforce Transparency and Accountability," "Uphold the Rule of Law," "Promote Autonomy and Agency," "Foster Community Engagement," "Ensure Effective Remedy and Redress," and "Focus on Future Sustainability".[23] These principles are not merely aspirational; they are translated into actionable recommendations applicable across the entire DPI lifecycle, from initial conception and scoping to implementation and ongoing evolution.[25] The framework's approach is designed to minimize risks across technical, normative, and organizational layers of digital transformation, thereby ensuring DPI implementation is secure, inclusive, practical, and adaptable.[24]

The Universal DPI Safeguards Framework is explicitly designed to mitigate risks and foster trust and equity.[23] Its foundational principles, particularly "Do No Harm," "Uphold the Rule of Law," and "Promote Autonomy and Agency," directly operationalize CbD and broader ethical considerations. The framework's comprehensive approach, addressing risks across technical, normative, and organizational layers [24], demonstrates a CbD strategy that extends beyond mere technical controls to encompass governance and human-centric design. This framework serves as UNDP's primary policy tool for embedding security and ethical considerations into DPI from the outset. This provides a standardized yet adaptable blueprint for countries in the Global South to build DPIs that are not only technologically advanced but also inherently secure, private, and respectful of human rights, directly addressing the unique vulnerabilities prevalent in these contexts.

2.2.2 Model ID Governance Framework

Developed by UNDP, the Model ID Governance Framework is a strategic resource specifically designed to support countries in the design, implementation, and governance of their digital legal identity systems, a critical component of DPI.[2] The primary objective of this framework is to ensure that all efforts to digitalize legal identity are accompanied by robust protections for human rights, personal data, and privacy.[26] It represents a deliberate shift in discourse from focusing solely on technological solutions to emphasizing the crucial governance of technology itself.[26]

The framework advocates for a rights-based and inclusive approach to digital ID governance, comprising nine key components. These include robust legal and regulatory frameworks, principles of non-discrimination, ensuring access to information, establishing clear legal accountability, building capable institutions, prioritizing user value, transparent procurement processes, and anti-corruption measures.[27] The framework is designed not as a rigid checklist but as a set of important questions for policymakers, civil society organizations, and citizens to consider when improving digital legal identity governance within their unique national contexts.[26]

The Model ID Governance Framework's explicit focus on the "governance of technology" over technology itself [26] highlights a crucial understanding: even perfectly coded systems can fail if governance is weak or absent. By emphasizing human rights, data protection, and privacy within the governance structure [26], UNDP integrates CbD principles at the policy and regulatory level. This framework functions as a meta-CbD, ensuring that the rules governing the DPI are as secure and trustworthy as the underlying technology. For digital identity systems, which are foundational to many DPIs, robust governance is a prerequisite for effective CbD. This framework guides Global South nations in building not just technically secure IDs but also legally and ethically sound systems that protect citizens' rights and prevent the misuse of sensitive data, thereby building public trust and ensuring long-term sustainability.

2.2.3 Open Source Ecosystem Enabler (OSEE)

The Open Source Ecosystem Enabler (OSEE) is a collaborative initiative between

the International Telecommunication Union (ITU) and UNDP, supported by the European Commission. Its purpose is to strengthen national digital capacity by fostering the establishment and growth of Open Source Programme Offices (OSPOs) within countries.[2] OSEE aims to enhance knowledge and action regarding the effective use of open-source technologies for delivering public services.[28]

The initiative champions open-source technologies and Digital Public Goods (DPGs) as vital enablers for government digital transformation. A key benefit highlighted is their role in reducing vendor lock-in, which is a significant vulnerability for many Global South nations, and promoting digital sovereignty by allowing governments greater control over their technological infrastructure.[28] OSEE also acknowledges the inherent challenges associated with deploying and maintaining open-source solutions in government, such as the need for new skill sets, continuous training, and sustainable business models for system maintenance.[28] The initiative works to collect insights from experts, analyze successful open-source initiatives, and document best practices to create an Open Source Ecosystem Enablement Framework, alongside developing training and advocacy materials.[28]

UNDP's promotion of open-source through OSEE directly aligns with CbD principles such as "avoid security through obscurity".[4] Open-source software, by its very nature, allows for greater transparency, community scrutiny, and collective identification and remediation of vulnerabilities, which can significantly enhance overall security. Crucially, it addresses the risk of "vendor lock-in" [28], a pervasive challenge for Global South nations that can lead to dependency and reduced control over critical digital infrastructure. By fostering digital sovereignty and local capacity to maintain and adapt systems, open-source becomes a strategic CbD decision that builds resilience through transparency and collaborative development. By supporting open-source, UNDP empowers Global South countries to build DPIs that are more auditable, adaptable, and less dependent on external proprietary solutions, thereby enhancing their long-term cybersecurity posture and fostering local innovation and self-reliance.

2.2.4 Digital Public Goods Alliance (DPGA)

The Digital Public Goods Alliance (DPGA) is a multi-stakeholder initiative co-hosted

by UNDP, UNICEF, and Norad, established in 2019.[31] Its overarching mission is to accelerate the attainment of the Sustainable Development Goals (SDGs) in low- and middle-income countries by facilitating the discovery, development, use, and investment in digital public goods (DPGs).[31]

DPGs are specifically defined as open-source software, open data, open AI systems, and open content collections that adhere to privacy and other applicable laws and best practices, explicitly "do no harm," and contribute to the SDGs.[31] The DPGA actively advocates for DPGs as key enablers for advancing both the SDGs and Digital Public Infrastructure. A significant achievement in this advocacy was the strong reference to DPGs in the UN's Global Digital Compact, which was adopted by UN Members in September 2024, underscoring their importance in global digital cooperation.[31] The DPGA Secretariat plays a crucial role in stewarding and maintaining the DPG Standard and Registry, advocating for DPG implementation, and convening experts and communities to advance core topics such as AI, DPGs for DPI, and climate action.[32]

The DPGA's definition of DPGs explicitly mandates adherence to "privacy and other applicable laws and best practices" and the "do no harm" principle.[31] This means that any digital public good promoted by the alliance is inherently designed with CbD and Privacy-by-Design principles embedded from its inception. By facilitating the use of these pre-vetted, open-source components, UNDP, through its active involvement in the DPGA, ensures that the foundational elements of DPIs are secure and ethical by design. This partnership streamlines the adoption of secure and ethical digital components for Global South nations, reducing the burden of independent security vetting and promoting a consistent, responsible approach to DPI development at scale. This approach ensures that digital solutions are not only effective but also trustworthy and protective of user rights.

3. Core Principles of Cybersecurity-by-Design for DPI

3.1 Foundational Concepts of Secure and Privacy-Enhancing Design

The effective implementation of Cybersecurity-by-Design (CbD) in Digital Public Infrastructures (DPIs) relies on a robust integration of technical, strategic, and ethical design principles. Various international frameworks and standards provide comprehensive guidance for achieving this.

NIST Principles for Trustworthy Security Development:
The National Institute of Standards and Technology (NIST) offers a foundational framework for designing secure systems, emphasizing proactive measures to minimize vulnerabilities. Key principles include:

- **Anomaly Detection:** Systems must possess the capability to collect and interpret self-awareness data, comparing it against a predefined model of correct behavior to identify deviations or anomalies.[6] This enables early detection of potential security breaches.
- **Commensurate Protection:** Security measures should be scaled proportionally to the most significant threats and the potential adverse effects that could arise from a security failure. Higher potential impact necessitates a higher degree of security.[6]
- **Continuous Protection:** System components must provide uninterrupted protection throughout their operation. This includes the ability of components to protect themselves against tampering and to default into a protective, fail-safe state if a failure occurs.[6]
- **Defense in Depth:** This principle advocates for implementing multiple, coordinated lines of defense, utilizing several types of loss control, and maintaining diversity across these components to prevent data loss.[6] This layered approach ensures that if one security measure fails, others are in place to mitigate the threat.
- **Least Principles:** A cornerstone of secure design, these principles limit the functionality and access of system components to prevent unintended vulnerabilities. This includes:
    - *Least Functionality:* A system component should only accomplish its required functions and nothing more.[6]
    - *Least Persistence:* Components should only be available and accessible to fulfill their required operation for the minimally necessary duration.[6]

    - *Least Privilege:* Components should possess only the privileges absolutely necessary to perform their appointed tasks, and no more.[6]
    - *Least Sharing:* Resources should be shared between components only as minimally necessary to support operations and with as few components as possible.[6]
- **Protective Defaults:** The default configuration of any component should inherently provide maximum protective effectiveness based on its intended operations within the system.[6]

Beyond these granular principles, the broader NIST Cybersecurity Framework outlines five core functions critical for managing cybersecurity risk: Identify (understanding critical functions and associated risks), Protect (implementing safeguards to contain potential impacts), Detect (assessing system compromises), and Respond (minimizing damage from breaches).[7]

ENISA Guidelines:
The European Union Agency for Cybersecurity (ENISA) provides National Cybersecurity Strategies Guidelines aimed at enhancing cybersecurity preparedness across Member States.8 These guidelines recommend establishing a clear vision, scope, objectives, and priorities for national strategies, conducting thorough national risk assessments, and integrating cybersecurity awareness into national policies.8 ENISA's mandate extends to fostering cooperation among cybersecurity stakeholders, strengthening resilience against cyber threats, and engaging in incident management and situational awareness at both national and EU levels.10 These guidelines emphasize a proactive and collaborative approach to national cybersecurity.
ISO Standard (Privacy by Design - ISO 31700-1:2023):
While primarily focused on privacy, the ISO standard for Privacy by Design (PbD) includes principles that are intrinsically critical for CbD, particularly for data-intensive DPIs. These principles include:

- **Proactive not reactive; preventative not remedial:** This principle advocates for actively building processes and procedures to prevent privacy risks or invasions from occurring, rather than reacting to them after the fact.[5]
- **Privacy as the default:** Users should automatically receive the highest level of data protection throughout their experience with a product or service, without needing to take explicit action.[5]
- **Privacy embedded into design:** Privacy should be an integral part of the development process, with each design stage explicitly accounting for user privacy checks, rather than being an afterthought.[5]
- **End-to-end Security – Lifecycle protection:** From the moment user data is

collected until it is ultimately destroyed, it must be secured at every stage of its lifecycle.[5]

- **Visibility and transparency:** Organizations must be open and clear with users about how their data is handled, fostering trust through clear documentation and communication.[5]

The consistent integration of these principles across various international standards underscores a shared understanding that security and privacy are not optional features but fundamental requirements for trustworthy digital systems.

The interdependence of technical, strategic, and ethical design principles for DPI security is evident in these frameworks. The NIST principles offer granular technical instructions for building secure systems, detailing *how* to implement CbD. ENISA's guidelines provide the strategic and policy-level *what* and *why* for national cybersecurity, emphasizing the importance of a coordinated national approach. The ISO PbD standard introduces the crucial ethical and human-centric *who* and *for whom* aspects, prioritizing data protection and user rights. For DPIs, which operate at a societal scale and handle sensitive personal data, effective CbD requires the seamless integration of all three dimensions: a technically sound architecture, a supportive national policy environment, and an unwavering commitment to privacy and human rights. A deficiency in one area can compromise the entire system, highlighting the necessity of a holistic approach.

Table 1: Key Cybersecurity-by-Design Principles and Their Relevance to DPI

Principle Category	Specific Principle	Source(s)	Relevance to DPI
Foundational Security	Anomaly Detection	NIST [6]	Essential for real-time monitoring of DPIs (e.g., payment systems, identity verification) to detect unusual or malicious activities, protecting against fraud and unauthorized

			access.
	Commensurate Protection	NIST [6]	Ensures that security investments in critical DPI components (e.g., digital ID databases) are proportional to the high impact of their failure, especially in contexts where public trust is fragile.
	Continuous Protection	NIST [6]	Mandates uninterrupted security for always-on DPI services, requiring self-protection against tampering and graceful degradation to a protective state upon failure, crucial for essential public services.
	Defense in Depth	NIST [6]	Implies layered security for DPIs, where multiple controls (e.g., network, application, data) protect against various threats, preventing single points of failure in identity or payment systems.

	Least Functionality	NIST [6]	Limits the attack surface of DPI components by ensuring they perform only their core required functions, reducing potential vulnerabilities in complex digital ecosystems.
	Least Privilege	NIST [6]	Restricts access rights for users and system components within DPIs to the bare minimum necessary, mitigating the impact of compromised accounts or malicious insiders.
	Protective Defaults	NIST [6]	Ensures that DPI systems are secure by default, providing maximum protection out-of-the-box, which is vital for widespread adoption and trust, particularly for non-technical users in the Global South.
Data Protection & Privacy	Proactive not reactive; preventative not remedial	ISO 31700-1:2023 [5]	Requires anticipating and designing against data privacy risks from the outset in

			DPIs, preventing breaches rather than merely responding to them, crucial for sensitive personal data.
	Privacy as the default	ISO 31700-1:2023 [5]	Ensures that DPIs automatically provide the highest level of data protection to users, simplifying privacy management for citizens and building inherent trust in digital services.
	Privacy embedded into design	ISO 31700-1:2023 [5]	Integrates privacy considerations into every stage of DPI development, ensuring that data protection is a core feature, not an afterthought, for digital identity and payment systems.
	End-to-end Security – Lifecycle protection	ISO 31700-1:2023 [5]	Guarantees that personal data within DPIs is secure from collection through processing, storage, and eventual destruction, maintaining integrity and confidentiality across its entire lifecycle.

	Visibility and transparency	ISO 31700-1:2023 [5]	Demands clear communication to users about how their data is handled within DPIs, fostering trust and accountability, particularly important for public acceptance and engagement.
Operational Resilience	Identify (NIST CSF)	NIST [7]	Involves understanding the critical functions of DPIs (e.g., identity verification, payment processing) and identifying potential cybersecurity risks that could disrupt these functions.
	Protect (NIST CSF)	NIST [7]	Focuses on implementing safeguards to ensure the secure operation of DPIs, including access controls, data security procedures, and personnel training, to contain the impact of cyber incidents.
	Detect (NIST CSF)	NIST [7]	Aims to enable rapid discovery of cybersecurity events within DPIs

			through continuous monitoring and analysis, allowing for timely action against compromises.
	Respond (NIST CSF)	NIST [7]	Outlines actions to take following a detected cybersecurity incident in a DPI, focusing on minimizing damage and promoting rapid recovery of essential services.
Governance & Ethics	Do No Harm	UNDP Digital Standards [12], Universal DPI Safeguards Framework [23]	A foundational ethical principle requiring DPIs to be designed to prevent severe negative consequences, including unintended social or economic harms, particularly for vulnerable populations.
	Do Not Discriminate	Universal DPI Safeguards Framework [23]	Ensures DPIs provide unbiased access and equal opportunity, mitigating risks of exclusion for marginalized groups based on identity or circumstance.

	Uphold the Rule of Law	Universal DPI Safeguards Framework [23]	Mandates that DPIs are introduced with a clear legal basis and that legal and regulatory aspects are embedded into their design, ensuring compliance and accountability.
	Promote Autonomy and Agency	Universal DPI Safeguards Framework [23]	Empowers individuals to control their data and exercise choice within DPI systems, fostering trust and preventing coercive or mandatory participation.
	Default to open	UNDP Digital Standards [12]	Encourages the use of open standards and open-source solutions for DPIs, promoting transparency, collaboration, and reducing vendor lock-in, which enhances long-term security and sustainability.

3.2 Integrating Human Rights, Ethics, and "Do No Harm" in CbD for Development

The UNDP's foundational commitment to placing human rights at the center of its

digital approach is paramount, transforming Cybersecurity-by-Design (CbD) from a purely technical concern into an ethical and developmental imperative.[21] This commitment is concretely manifested in the Universal DPI Safeguards Framework, which explicitly embeds human rights principles directly into the design and implementation of Digital Public Infrastructures (DPIs).[23]

Key principles within this framework, such as "Do No Harm," "Do Not Discriminate," "Do Not Exclude," "Uphold the Rule of Law," and "Promote Autonomy and Agency," are not merely aspirational statements. They are intended to be integrated throughout the entire DPI lifecycle – from initial conception and scoping to ongoing operation – to proactively anticipate, assess, and mitigate potential human rights harms and power differentials.[23] This means that DPIs are designed to prevent outcomes such as digital exclusion, surveillance, or the exacerbation of existing inequalities, which could arise from poorly implemented or misused digital systems. For instance, the "Do Not Exclude" principle emphasizes providing individuals with a choice of channels (digital/non-digital) to access services, ensuring that access is never limiting, conditional, or mandatory, either explicitly or in practice.[23] This directly addresses the risk of marginalization in contexts where digital access is unequal.

The framework further calls for democratic participation, robust public oversight, and transparent governance mechanisms. These elements are crucial for preventing issues like vendor lock-in, promoting fair market competition, and ultimately ensuring that DPI serves the broader public good rather than narrow commercial or political interests.[23] Transparency and accountability are reinforced through requirements for clear legal bases for DPI, with necessary legal and regulatory aspects embedded into the design, supported by adequate capacity for implementation, oversight, and regulation.[23] This comprehensive approach ensures that the legal and ethical dimensions are as rigorously considered as the technical ones.

An innovative and critical aspect of this integration is the concept of "obligations in code".[34] This approach suggests that compliance with human rights and privacy principles can be automatically embedded directly into the system's architecture. By making these principles inherent features of the software and protocols, they become fundamental to the system's operation, rather than external policy requirements that might be overlooked or circumvented. This deep embedding ensures that privacy, security, and human rights are protected by the very design of the digital infrastructure. For example, secure coding practices, data minimization by default, and cryptographic controls can be built into the system to enforce privacy

and security rules automatically.

This integration means that UNDP's CbD efforts in the Global South are inherently focused on building DPIs that are not only resilient against cyberattacks but also trustworthy, equitable, and designed to empower individuals. This is particularly crucial for contexts where digital systems might otherwise be leveraged for control or to exacerbate existing inequalities. By embedding human rights and ethical considerations from the earliest design stages, UNDP aims to ensure that digital transformation genuinely contributes to inclusive and sustainable development, fostering public trust and safeguarding the fundamental rights of all citizens.

4. Cybersecurity-by-Design in UNDP-Supported DPI Blueprints in the Global South

4.1 India Stack (Aadhaar & UPI): Architecture, Embedded Security, and Lessons Learned

Overview and Impact:
India Stack stands as a pioneering and highly influential example of Digital Public Infrastructure, serving as a blueprint for digital transformation in the Global South. It comprises a set of open APIs and digital public goods designed to unlock economic primitives of identity, data, and payments at a population scale.36 Key components include Aadhaar, a biometric digital identity system launched in 2009, and the Unified Payments Interface (UPI), a real-time cashless payment system introduced in 2016.1 The India Stack's implementation has yielded remarkable results in financial inclusion and public service delivery. Aadhaar has facilitated rapid and cost-effective electronic Know Your Customer (eKYC) processes, significantly reducing the cost of customer verification for banks.36 UPI has emerged as a leading global payment system, processing over 15 billion transactions per month as of November 2024, and accounting for more than three-quarters of India's digital retail transactions.20 This infrastructure has dramatically boosted financial inclusion, with bank account ownership doubling between 2011 and 2021, reaching 78% of the population, and enabling efficient direct benefit transfers to hundreds of millions, saving the government billions.20
Embedded Security Features:
The design of India Stack components incorporates several Cybersecurity-by-Design (CbD) principles. UPI, for instance, was engineered with interoperability and an open, technology-agnostic architecture at its core, allowing various third-party applications to build upon it.38 For secure transactions, it employs a separate UPI PIN for second-factor authentication and utilizes Virtual Payment Addresses (VPAs) in addition to traditional identifiers, enhancing both flexibility and security.39 The system adheres to a "defense in

depth" strategy, incorporating multiple independent security layers. These layers include velocity analysis (rate limiting transactions), behavioral analytics (identifying unusual payment patterns), optional geo-location verification, and robust API security through request signing with the Payment Service Provider's private key.40 Additional defensive measures include annual CERT-In audits to identify vulnerabilities, certificate pinning to prevent Certificate Authority-based attacks, code signing verification to detect tampered app updates, and Runtime Application Self-Protection (RASP) to detect exploitation attempts.40 Despite handling an immense volume of transactions, UPI has maintained remarkably low fraud rates, reportedly below 0.01%.40 Aadhaar, as the identity layer, relies on biometric authentication (fingerprints) for identity verification, aiming to provide a unique and secure identifier for each individual.37

Challenges and Lessons Learned Regarding Security:

Despite its successes and embedded security features, India Stack, particularly Aadhaar, has faced significant cybersecurity challenges. Public reports indicate major data breaches affecting the personal information of millions, with sensitive data such as Aadhaar numbers, passport details, phone numbers, and addresses appearing on the dark web.41 Initial suspicions regarding the root causes of these breaches point to third-party data leaks (e.g., from companies selling SIM cards), undisclosed database vulnerabilities, weak security procedures, insider threats, and a notable lack of systematic and regular auditing.41 The consequences of these breaches have been far-reaching, leading to widespread identity theft, financial fraud, and a significant erosion of public trust in the digital system.42 Furthermore, issues of mandatory linking have surfaced; despite a Supreme Court ruling that mandatory linking of Aadhaar to banking services is unconstitutional, some banks have continued to require it, leading to exclusion for vulnerable individuals who cannot or choose not to comply.43

Beyond Aadhaar, an academic study in 2020 identified multi-factor authentication design flaws in UPI 1.0. These flaws, when combined with attacker-controlled applications, could potentially lead to unauthorized registration and transactions, even for users who had never used a UPI app.[44] These vulnerabilities were responsibly disclosed to relevant authorities, including CERT India, and were subsequently addressed in UPI 2.0.[44]

The experience of India Stack demonstrates the paradox of scale and the continuous nature of CbD. Its success highlights the transformative power of DPI in achieving unprecedented financial inclusion and streamlining public services. However, the Aadhaar data breaches and identified UPI vulnerabilities reveal a critical reality: the larger the scale and interconnectedness of a DPI, the greater the potential impact of security failures. The occurrence of breaches despite robust technical measures and strict regulations underscores that CbD is not a one-time implementation but an ongoing, dynamic process. It requires continuous vigilance against evolving threats,

rigorous oversight of third-party integrations, proactive management of insider risks, and adaptive governance frameworks. The necessity for constant auditing and rapid adaptation to address newly discovered vulnerabilities, even those arising from non-technical factors, is paramount. For UNDP and other Global South nations, India Stack serves as a powerful case study, illustrating that while CbD can build highly effective and secure systems, its long-term success demands a dynamic approach that includes continuous threat intelligence, stringent third-party oversight, adaptive governance, and a commitment to addressing vulnerabilities as they emerge, ensuring enduring trust and resilience.

4.2 Sierra Leone Digital Transformation Project: Cybersecurity Capacity Building and Policy Frameworks

Overview and Cybersecurity Focus:
Sierra Leone has embarked on an ambitious Digital Transformation Project (SLDTP), significantly supported by a $50 million grant from the World Bank.45 The project's broad objectives include expanding access to broadband internet, enhancing digital skills across the population, and improving the efficiency and reach of digital public services.45 A central pillar of the SLDTP is the strengthening of national cybersecurity capabilities. This involves a multi-faceted approach, including the development and implementation of a national public education and awareness campaign on cybersecurity, the creation of a comprehensive national cybersecurity skills strategy and action plan, and initiatives to boost local technical capabilities.45
National Cybersecurity Strategy (2021-2025):
The country's commitment to a secure digital future is articulated in its National Cybersecurity Strategy (2021-2025). This comprehensive framework aims to establish a secure and resilient cyberspace for Sierra Leone, aligning with national development goals while robustly safeguarding citizens' rights and privacy.47 The strategy's strategic goals are multi-dimensional:

- Establishing institutional, legal, and regulatory frameworks for effective governance of cybersecurity.
- Promoting public education, awareness, child online protection, digital rights, and privacy.
- Protecting critical digital infrastructure through enhanced response readiness.
- Developing cyber capabilities by integrating cybersecurity into formal education, offering professional training, and fostering local cybersecurity industries, thereby promoting innovation and research.
- Strengthening national, regional, and international cooperation on cybersecurity

matters.[47]

The implementation approach for this strategy involves establishing key governance structures, such as a National Cybersecurity Advisory Council and a technical working group, and proposing a National Cyber Security Center to centralize efforts. It also mandates the enactment of a National Cybercrime Bill and data protection laws, alongside equipping the criminal justice system with the necessary skills and tools for investigating and prosecuting cybercrime.[47] Public awareness campaigns and educational programs are key elements to enhance public understanding of digital hygiene and promote trust in secure internet use.[47]

Challenges and Gaps:

Despite these comprehensive policy efforts, Sierra Leone faces significant challenges in its cybersecurity posture. The International Telecommunication Union (ITU) Global Cybersecurity Index for 2024 ranks Sierra Leone in Tier 3 out of five, indicating a basic level of commitment to cybersecurity.46 While the country scores relatively well in legislative frameworks (17.29/20) and organizational measures (18.81/20), substantial weaknesses persist in technical measures (1.39/20), capacity building (6.95/20), and international cooperation (12.02/20).46 This indicates a notable gap between policy formulation and practical implementation. Furthermore, the country's telecom infrastructure remains a significant hurdle, with a low internet penetration rate of just 30.4%, which inherently limits the reach and impact of any digital security initiatives.46

UNDP's Engagement:

UNDP plays a supportive role in Sierra Leone's digital transformation. Sierra Leone is a founding Board member of the Digital Public Goods Alliance (DPGA) and has been designated as a "First-Mover" country in the 50-in-5 campaign, signifying its commitment to accelerating the adoption of safe and interoperable DPI.48 UNDP explicitly supports countries in strengthening local digital ecosystems and advocating for human rights and safeguards in digital transformation, aligning with the strategic goals outlined in Sierra Leone's national strategy.49

The robust National Cybersecurity Strategy of Sierra Leone and its relatively strong scores in legislative and organizational measures indicate a clear policy commitment to Cybersecurity-by-Design. However, the low scores in technical measures and capacity building highlight a critical implementation gap. This suggests that while the *design* of cybersecurity policies may be sound and comprehensive, the practical embedding of these principles through tangible technical safeguards and the development of a skilled workforce faces significant real-world challenges in resource-constrained environments. The low internet penetration further complicates the widespread adoption and security of digital services. Therefore,

UNDP's support in Sierra Leone must intensely focus on translating policy into practice, prioritizing direct and sustained investments in technical infrastructure, digital literacy, and human capital development. This involves not only advocating for CbD principles but also providing hands-on support for their technical implementation and the creation of a resilient local cybersecurity ecosystem capable of addressing the identified gaps.

4.3 Sri Lanka's Civil Registration and Vital Statistics (CRVS) System (OneRegistry): Security and Privacy Integration

Overview and Objectives:

Sri Lanka is undergoing a significant digital transformation initiative to modernize its traditional paper-based Civil Registration and Vital Statistics (CRVS) system into a digital platform known as "OneRegistry." This ambitious project is supported by the United Nations Development Programme (UNDP) and the World Health Organization (WHO), and it is strategically aligned with the nation's broader digital transformation agenda.50 The primary objectives of "OneRegistry" are to make civil registration processes faster, more accessible, and fully digital, thereby eliminating bureaucratic delays and removing barriers to essential services for marginalized communities.50 A key feature of the initiative is its aim to connect the digital CRVS system with other critical government databases, ensuring a functioning and interoperable CRVS database linked with at least three government institutions. This interoperability is designed to facilitate smoother and more reliable public services, such as healthcare, pensions, and government assistance.50

Embedded Security and Privacy Integration:

The integration of CRVS with Digital Public Infrastructure (DPI) is explicitly recognized for its potential to not only improve service delivery but also to safeguard human rights.51 CRVS systems, when designed with interoperability in mind, can significantly reduce identity fraud and corruption by enabling secure and responsible data exchanges for identity verification processes.51 UNDP emphasizes that the implementation of DPI must be carefully managed to ensure inclusivity, robust security, and long-term sustainability.52

A core tenet of this approach is that "Privacy-by-Design principles should be non-negotiable".[52] This mandates the incorporation of essential privacy-enhancing measures such as encryption, anonymization, and robust data governance policies from the very outset of the system's design. Furthermore, cybersecurity is prioritized through the implementation of stringent security standards and continuous audits, recognizing the dynamic nature of cyber threats.[52] Inclusive governance is also

deemed crucial, requiring collaborative frameworks among civil society, regulators, and the private sector to uphold digital rights and ensure fair competition within the digital ecosystem.[52] These measures aim to prevent the misuse of sensitive personal data and build public trust in the digital system.

Challenges:

The transition from a legacy paper-based system presents inherent challenges. The traditional system is characterized by its slowness, outdated processes, and susceptibility to errors, leading to prolonged delays and potential exclusion for vulnerable communities who struggle to obtain critical documents.50 Moreover, the very act of centralizing such sensitive data, as envisioned by "OneRegistry," raises significant concerns about data privacy and cybersecurity. Centralized systems, by their nature, become attractive targets for cyberattacks and surveillance.52 Without robust regulatory safeguards and continuous vigilance, there is a substantial risk that DPI, despite its transformative potential, could inadvertently become a tool for exclusion or control rather than empowerment.52 The need to address these risks proactively is paramount to ensure the system genuinely serves all citizens.

The "OneRegistry" initiative highlights CRVS as a foundational DPI, directly impacting legal identity and access to essential services. The push for "interoperability" is crucial for achieving efficiency and seamless service delivery, but it simultaneously introduces new security complexities, as sensitive data must be securely exchanged across multiple government systems. The explicit call for "Privacy-by-Design principles" and "stringent security standards and continuous audits" demonstrates a clear recognition that digitizing such foundational and sensitive data requires inherent security and privacy controls from the very outset. The acknowledged risk of centralized systems becoming attractive targets for cyberattacks underscores the critical need for a robust Cybersecurity-by-Design approach. For UNDP's work in Sri Lanka and similar contexts, CbD for foundational DPIs like CRVS means not only ensuring technical resilience but also designing systems that actively prevent the misuse of sensitive personal data across interconnected platforms. This necessitates a strong regulatory framework, continuous oversight, and a steadfast commitment to user rights and data protection throughout the entire data lifecycle, ensuring that the digital transformation truly benefits all citizens equitably and securely.

4.4 Other UNDP Engagements: Brief examples from Togo, Ethiopia, and Zambia

UNDP's commitment to promoting Cybersecurity-by-Design (CbD) within Digital Public Infrastructures (DPIs) extends across various countries in the Global South, demonstrating adaptive strategies tailored to diverse developmental contexts.

Togo:

In Togo, UNDP has provided significant support to the establishment and operationalization of the National Operational and Emergency Center (CNOU). This center is integral to the country's multi-hazard early warning and emergency management system, designed to strengthen national emergency response capabilities. UNDP's involvement included equipping the center with necessary technology, developing Standard Operating Procedures (SOPs) for emergency response, and providing comprehensive training for staff. A strong emphasis was placed on ensuring the CNOU's interoperability with regional systems, which is critical for coordinated disaster response efforts across borders.53 The resilience and efficiency of Togo's digital systems were notably demonstrated during the COVID-19 pandemic, when the country successfully leveraged its fully digital social assistance program to swiftly and accurately disburse cash transfers to informal workers, showcasing the practical benefits of robust digital infrastructure in crisis situations.54 Togo's proactive engagement in digital development is further evidenced by its designation as a "First-Mover" country in the 50-in-5 campaign, an initiative to accelerate DPI adoption globally, and its endorsement of the Digital Public Goods Charter.34 These efforts underscore a commitment to building digital systems that are not only functional but also resilient and responsive to national needs, reflecting an embedded CbD approach in crisis management and public service delivery.

Ethiopia:

Ethiopia is another nation recognized as a "First-Mover" country in the 50-in-5 campaign and has formally endorsed the Digital Public Goods Charter, indicating a strategic alignment with global best practices in digital development.34 UNDP's broader engagement in Ethiopia includes initiatives focused on empowering women in digital leadership.22 While specific details on CbD in DPI blueprints for Ethiopia are not extensively detailed in the provided materials, the emphasis on inclusive digital development and adherence to the Digital Public Goods Charter implies an inherent commitment to principles of security, privacy, and open standards. The focus on women's digital leadership also suggests an understanding that digital transformation must address social inequalities and ensure equitable participation, which implicitly requires secure and trustworthy digital environments.

Zambia:

Zambia also stands as a "First-Mover" country in the 50-in-5 campaign and has endorsed the Digital Public Goods Charter.34 UNDP, in a significant partnership with Japan and the Japan International Cooperation Agency (JICA), is investing over $5.4 million in the

development of climate-smart, inclusive, and gender-responsive infrastructure for displaced persons and host communities.57 While this project primarily focuses on physical infrastructure, its alignment with UNDP's broader vision for sustainable development and its emphasis on "inclusive" and "gender-responsive" design suggests an implicit integration of principles that would necessitate secure and equitable digital access where digital components are involved. UNDP works closely with the Zambian government to achieve its Vision 2030 and Sustainable Development Goals, with programmatic areas encompassing governance, gender, poverty reduction, and health systems strengthening.57 These broader engagements, particularly in governance and social protection, often involve underlying digital systems that would benefit from and increasingly integrate CbD principles to ensure data protection, service reliability, and public trust. The focus on "Leave No One Behind" 57 further reinforces the need for secure and inclusive digital solutions that protect vulnerable populations.

UNDP's adaptive application of CbD principles across these diverse development contexts is evident. In Togo, the emphasis on interoperability and rapid, secure digital payments during crises demonstrates CbD's role in operational resilience. For Ethiopia and Zambia, their participation in global initiatives like the 50-in-5 campaign and endorsement of the DPG Charter signify a commitment to building digital infrastructure with inherent security and ethical considerations, even if specific technical details are not fully elaborated. The consistent thread across these engagements is UNDP's holistic approach to digital development, where CbD is not a standalone technical requirement but an integrated component of broader efforts to achieve the SDGs, foster inclusion, and build resilient societies in the Global South. This approach recognizes that effective CbD must be tailored to the unique socio-economic and infrastructural realities of each country, while upholding universal principles of human rights and security.

5. Conclusions and Recommendations

The comprehensive analysis of UNDP's role in promoting Cybersecurity-by-Design (CbD) within Digital Public Infrastructures (DPIs) for the Global South reveals a multi-faceted and strategically integrated approach. DPIs are increasingly recognized as foundational for achieving sustainable development, offering unparalleled opportunities for financial inclusion, efficient public service delivery, and economic growth in developing nations. However, their implementation in the Global South is fraught with significant challenges, including pronounced digital divides, weak existing infrastructure, critical skills gaps, and evolving cyber threats. The imperative

for CbD is therefore amplified, as security failures in these contexts can have devastating socio-economic consequences, eroding public trust and exacerbating existing inequalities.

UNDP's strategic framework, particularly its Digital Strategy (2022-2025), consistently positions CbD not merely as a technical requirement but as an ethical and developmental imperative. The organization's commitment to placing human rights at the center of its digital approach, manifested through principles like "Do No Harm," "Do Not Discriminate," and "Promote Autonomy and Agency" within the Universal DPI Safeguards Framework, signifies that DPIs must be inherently designed to protect individual rights and foster equitable access. This approach extends to advocating for open digital standards and open-source solutions through initiatives like the Open Source Ecosystem Enabler (OSEE) and the Digital Public Goods Alliance (DPGA), which promote transparency, reduce vendor lock-in, and build local capacity—all crucial elements of a resilient CbD posture. The Model ID Governance Framework further underscores the understanding that robust governance is an indispensable layer of CbD, ensuring that the rules governing DPIs are as secure and trustworthy as the technology itself.

The case studies of India Stack, Sierra Leone's Digital Transformation Project, and Sri Lanka's "OneRegistry" CRVS system offer valuable lessons. India Stack demonstrates the immense potential of DPI at scale but also highlights the continuous nature of CbD, where even robust systems face persistent threats from third-party vulnerabilities, insider risks, and the need for constant auditing and adaptation. Sierra Leone's experience illustrates the critical policy-implementation gap, where strong strategic frameworks must be matched by tangible investments in technical measures, digital literacy, and human capital development. Sri Lanka's CRVS modernization underscores the dual imperative of interoperability and inherent security for foundational data systems, emphasizing that digitizing sensitive personal data requires non-negotiable Privacy-by-Design principles and continuous oversight to prevent misuse. The broader UNDP engagements in countries like Togo, Ethiopia, and Zambia further demonstrate the adaptive application of CbD principles across diverse contexts, emphasizing operational resilience, inclusive development, and the protection of vulnerable populations.

The overarching conclusion is that for DPIs to truly serve as a force for good in the Global South, CbD must be comprehensively embedded across all layers—technical, policy, governance, and ethical. This requires a holistic and dynamic

approach that anticipates risks, prioritizes human rights, fosters local ownership, and adapts to evolving challenges.

Recommendations:

Based on this analysis, the following recommendations are put forth to further strengthen UNDP's role in promoting Cybersecurity-by-Design in DPIs for the Global South:

1. **Prioritize Capacity Building and Technical Implementation:** While policy frameworks are crucial, sustained investment in technical measures and human capital development is paramount. UNDP should intensify efforts to translate CbD policies into practical, on-the-ground implementation, focusing on training local cybersecurity professionals, establishing national incident response capabilities, and supporting the adoption of secure coding practices and robust technical safeguards within government agencies. This directly addresses the policy-implementation gap observed in contexts like Sierra Leone.
2. **Strengthen Third-Party Risk Management and Oversight:** The vulnerabilities exposed in India Stack underscore the critical need for rigorous due diligence and continuous oversight of third-party vendors and partners involved in DPI development and operation. UNDP should advocate for and support the implementation of stringent contractual obligations, security audits, and transparency requirements for all external entities interacting with DPIs, ensuring that security is maintained across the entire ecosystem.
3. **Advance "Obligations in Code" and Open Standards:** UNDP should continue to champion the embedding of human rights and privacy principles directly into the technical architecture of DPIs through "obligations in code." This involves promoting the use of open standards and open-source solutions, which enhance transparency, auditability, and foster digital sovereignty, reducing reliance on proprietary systems that can create vendor lock-in and reduce accountability.
4. **Enhance Participatory Governance and Accountability Mechanisms:** To build and maintain public trust, DPI governance frameworks must be genuinely inclusive, involving civil society, affected communities, and diverse stakeholders from the design phase through implementation and oversight. Robust, accessible, and transparent redress mechanisms for individuals impacted by security or privacy failures are essential to ensure accountability and reinforce trust in digital systems.
5. **Foster Regional and South-South Cooperation for Knowledge Exchange:**

Leveraging the experiences of "First-Mover" countries and successful DPI implementations, UNDP should further facilitate peer-to-peer learning and knowledge exchange platforms among Global South nations. This includes sharing best practices in CbD, lessons learned from security incidents, and strategies for overcoming common challenges in digital transformation, thereby accelerating collective progress and building regional resilience.

6. **Integrate Foresight and Adaptive Security Strategies:** Recognizing the rapidly evolving cyber threat landscape, UNDP should advocate for and support the integration of strategic foresight into DPI planning and continuous adaptive security strategies. This involves regularly assessing emerging risks, anticipating future vulnerabilities (e.g., from AI advancements), and proactively adjusting CbD measures to ensure long-term resilience and sustainability of DPIs.

By rigorously pursuing these recommendations, UNDP can further solidify its critical role in enabling the Global South to harness the transformative power of Digital Public Infrastructures, ensuring that these systems are not only innovative and inclusive but also inherently secure and trustworthy, ultimately contributing to a more equitable and resilient digital future for all.

Works cited

1. Digital public infrastructure - Wikipedia, accessed July 26, 2025, https://en.wikipedia.org/wiki/Digital_public_infrastructure
2. Digital Public Infrastructure (DPI) - United Nations Development Programme, accessed July 26, 2025, https://www.undp.org/digital/digital-public-infrastructure
3. www.cisa.gov, accessed July 26, 2025, https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf
4. Secure by design - Wikipedia, accessed July 26, 2025, https://en.wikipedia.org/wiki/Secure_by_design
5. 7 steps to comply with ISO 31700-1:2023 (standard on Privacy by Design) - OneTrust, accessed July 26, 2025, https://www.onetrust.com/blog/7-steps-to-comply-with-iso-31700-12023-standard-on-privacy-by-design/
6. What Are NIST Principles for Trustworthy Secure Design?, accessed July 26, 2025, https://continuumgrc.com/what-are-nist-principles-for-trustworthy-secure-design/
7. NIST Cybersecurity Framework: 5 Essential Phases for Optimal ..., accessed July 26, 2025, https://sopa.tulane.edu/blog/NIST-cybersecurity-framework
8. ENISA National Cybersecurity Strategies Guidelines - Secureframe, accessed July 26, 2025, https://secureframe.com/frameworks-glossary/enisa-national-cybersecurity-strategies-guidelines
9. What is the ENISA framework? | Answers - 6clicks, accessed July 26, 2025, https://www.6clicks.com/resources/answers/what-is-the-enisa-framework
10. What we do | ENISA - European Union, accessed July 26, 2025, https://www.enisa.europa.eu/about-enisa/what-we-do
11. ENISA: Fit for Purpose? - Stiftung Neue Verantwortung, accessed July 26, 2025, https://www.interface-eu.org/publications/enisa-fit-for-purpose
12. Digital Standards | United Nations Development Programme, accessed July 26, 2025, https://www.undp.org/digital/standards
13. UNDP Digital Guides, accessed July 26, 2025, https://digitalguides.undp.org/
14. How do we build for the Global South? - Data Privacy Brasil

Research, accessed July 26, 2025, https://www.dataprivacybr.org/en/how-do-we-build-for-the-global-south/
15. Global South pushes for digital inclusion | Digital Watch Observatory, accessed July 26, 2025, https://dig.watch/updates/global-south-pushes-for-digital-inclusion
16. Cybersecurity and Cyber-Resilience in the Global South - FACTS Asia, accessed July 26, 2025, https://www.factsasia.org/blog/cybersecurity-and-cyber-resilience-in-the-global-south
17. Effects of socioeconomic and digital inequalities on cybersecurity in a developing country, accessed July 26, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10122089/
18. "Hacking" the cybersecurity skills gap in developing countries - World Bank Blogs, accessed July 26, 2025, https://blogs.worldbank.org/en/digital-development/hacking-cybersecurity-skills-gap-developing-countries
19. Assessing infrastructure readiness for scaling digital cash transfers toward ending poverty, accessed July 26, 2025, https://www.brookings.edu/articles/assessing-infrastructure-readiness-for-scaling-digital-cash-transfers-toward-ending-poverty/
20. Approaches to Digital Public Infrastructure in the Global South - CSIS, accessed July 26, 2025, https://www.csis.org/analysis/approaches-digital-public-infrastructure-global-south
21. Digital Strategy 2022-2025 | United Nations Development Programme, accessed July 26, 2025, https://www.undp.org/digital/Digital-Strategy
22. Digital | United Nations Development Programme, accessed July 26, 2025, https://www.undp.org/digital
23. How Mojaloop Embraces the UN's DPI Safeguards Framework, accessed July 26, 2025, https://mojaloop.io/how-mojaloop-embraces-united-nations-dpi-safeguards-framework/
24. UN Universal Safeguards for Inclusive Digital Public Infrastructure, accessed July 26, 2025, https://www.dpi-safeguards.org/
25. Universal DPI Safeguards Framework, accessed July 26, 2025, https://www.dpi-safeguards.org/framework
26. Why Legal Digital ID Matters - Digital Legal ID Governance, accessed

July 26, 2025, https://www.governance4id.org/why
27. UNDP on digital ID governance framework, accessed July 26, 2025, https://dig.watch/updates/undp-on-digital-id-governance-framework
28. Open Source Ecosystem Enabler - ITU, accessed July 26, 2025, https://www.itu.int/en/ITU-D/ICT-Applications/Pages/Initiatives/OSEEPSI/home.aspx
29. Expression of Interest: Open Source Ecosystem Enabler, accessed July 26, 2025, https://ee-eu.kobotoolbox.org/x/WsignT7f
30. UN's DPI Day: Elizabeth Garber on standards as safeguards - OpenID, accessed July 26, 2025, https://openid.net/uns-dpi-day-elizabeth-garber-on-standards-as-safeguards/
31. 2024 STATE OF THE DIGITAL PUBLIC GOODS ECOSYSTEM - Unicef, accessed July 26, 2025, https://www.unicef.org/digitalimpact/media/826/file/DPG-Ecosystem-2024.pdf.pdf
32. 2024 STATE OF THE DIGITAL PUBLIC GOODS ECOSYSTEM, accessed July 26, 2025, https://www.bmz-digital.global/wp-content/uploads/2025/02/DPG-Ecosystem-2024.pdf
33. Digital Public Goods Alliance - DPGA - Policy Commons, accessed July 26, 2025, https://policycommons.net/orgs/digital-public-goods-alliance/
34. Digital Public Infrastructure: A Practical Approach for Africa, accessed July 26, 2025, https://carnegieendowment.org/research/2025/02/digital-public-infrastructure-a-practical-approach-for-africa?lang=en
35. Digital Public Infrastructure: Orientation Matters - Centre for International Governance Innovation (CIGI), accessed July 26, 2025, https://www.cigionline.org/articles/digital-public-infrastructure-orientation-matters/
36. India Stack, accessed July 26, 2025, https://indiastack.org/
37. India Stack - Wikipedia, accessed July 26, 2025, https://en.wikipedia.org/wiki/India_Stack
38. The organisation of digital payments in India - lessons from the Unified Payments Interface (UPI) - Bank for International Settlements, accessed July 26, 2025, https://www.bis.org/publ/bppdf/bispap152_e_rh.pdf
39. Payments - India Stack, accessed July 26, 2025,

https://indiastack.org/payments.html
40. How UPI Works: A Technical Deep Dive into Its Architecture, Data Flow, - Akshansh Jaiswal, accessed July 26, 2025, https://blog.akshanshjaiswal.com/the-upi-architecture-a-security-look
41. Aadhaar Data Leak: Risks and Solutions Uncovered - CertPro, accessed July 26, 2025, https://certpro.com/aadhaar-data-leak/
42. Aadhaar Data Breach: An In-Depth Analysis of One of India's Most Pervasive Data Breaches, accessed July 26, 2025, https://digialert.com/index.php/resources/blog/blog/others/aadhaar-data-breach-an-in-depth-analysis-of-one-of-india-s-most-pervasive-data-breaches
43. A human rights-centered approach to digital public infrastructure - Access Now, accessed July 26, 2025, https://www.accessnow.org/guide/digital-public-infrastructure/
44. Security Analysis of Unified Payments Interface and Payment Apps in India - USENIX, accessed July 26, 2025, https://www.usenix.org/system/files/sec20summer_kumar_prepub.pdf
45. Sierra Leone Digital Transformation Project - World Bank, accessed July 26, 2025, https://projects.worldbank.org/en/projects-operations/procurement-detail/OP00321503
46. Sierra Leone Strengthens Cybersecurity to Drive Digital Transformation - Ecofin Agency, accessed July 26, 2025, https://www.ecofinagency.com/telecom/2403-46533-sierra-leone-strengthens-cybersecurity-to-drive-digital-transformation
47. Sierra Leone's National Cybersecurity Strategy (2021–2025) | Digital Watch Observatory, accessed July 26, 2025, https://dig.watch/resource/sierra-leones-national-cybersecurity-strategy-2021-2025
48. Sierra Leone Joins Global Digital Public Infrastructure Ecosystem For The Launch Of The 50in5 Campaign - DSTI, accessed July 26, 2025, https://www.dsti.gov.sl/sierra-leone-joins-global-digital-public-infrastructure-ecosystem-for-the-launch-of-the-50in5-campaign/
49. Digital Public Infrastructure (DPI) | United Nations Development ..., accessed July 26, 2025, https://www.undp.org/srilanka/dpi
50. One Registry, Endless Potential: How Sri Lanka is Modernizing Civil

Registration, accessed July 26, 2025, https://unsdg.un.org/latest/stories/one-registry-endless-potential-how-sri-lanka-modernizing-civil-registration

51. Civil registration and vital statistics (CRVS) and digital public infrastructure (DPI): Why their integration is important for digital transformation | United Nations Development Programme, accessed July 26, 2025, https://www.undp.org/digital/blog/civil-registration-and-vital-statistics-crvs-and-digital-public-infrastructure-dpi-why-their-integration-important-digital
52. Charting Sri Lanka's Digital Future Through Inclusive Digital Public Infrastructure, accessed July 26, 2025, https://www.undp.org/srilanka/blog/charting-sri-lankas-digital-future-through-inclusive-digital-public-infrastructure
53. UNDP Togo - CIMA Research Foundation, accessed July 26, 2025, https://www.cimafoundation.org/en/project/undp-togo/
54. UNDP Inclusive by Design: Accelerating Digital Transformation for the Global Goals - Agora, accessed July 26, 2025, https://agora-parl.org/sites/default/files/agora-documents/UNDP-Inclusive-by-Design-Accelerating-Digital-Transformation-for-the-Global-Goals.pdf
55. Togo | United Nations Development Programme, accessed July 26, 2025, https://www.undp.org/tag/togo
56. Digital Public Infrastructure - United Nations Development Programme, accessed July 26, 2025, https://www.undp.org/sites/g/files/zskgke326/files/2023-12/undp-accelerating-the-sdgs-through-digital-public-infrastructure-v2.pdf
57. Zambia, Japan and UNDP Breaks Ground on a USD 5.4 Million Infrastructure Investment for Displaced Persons and Host Communities, accessed July 26, 2025, https://www.undp.org/zambia/press-releases/zambia-japan-and-undp-breaks-ground-usd-54-million-infrastructure-investment-displaced-persons-and-host-communities

*****End of the document*******