INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2025-2028

SG20-TD1348
STUDY GROUP 20
Original: English

Question(s): 6/20 Geneva, 12-21 May 2026

TD

Source: Co-Rapporteurs Q6/20

Title: Initial text for proposed draft new Recommendation ITU-T Y.sf-dpi-ssc "Security Framework of Digital Public Infrastructure for Smart Sustainable Cities", Q6/20 meeting (Geneva, 12-21 May 2026)

Contact: Jie CHENG
China Mobile Communications Co. Ltd.
China
Tel: +86 13811723151
E-mail: chengjiewl@chinamobile.com

Contact: Xiongwei Jia
China Unicom
China
Tel: +86 156 1109 2296
E-mail: jiaxw9@chinaunicom.cn

Abstract: This TD contains initial text for proposed draft new Recommendation ITU-T T Y.sf-dpi-ssc "Security Framework of Digital Public Infrastructure for Smart Sustainable Cities", based on contribution SG20-C411R1 and reflected the discussion at Q6/20 meetings (Geneva, 12-21 May 2026).

The following table shows discussion results for contributions.

Contribution. No.	Contribution title	Agreements & Comments
SG20-C411	Proposes a new work item on "Security Framework of Digital Public Infrastructure for Smart Sustainable Cities"	Accepted as a draft new Recommendation.

Draft new Recommendation ITU-T Y.sf-dpi-ssc

Security Framework of Digital Public Infrastructure for Smart Sustainable Cities

Table of Contents

1 Scope ..... - 5 -

2 References ..... - 5 -

3 Definitions ..... - 5 -
3.1 Terms defined elsewhere ..... - 5 -
3.2 Terms defined in this Document ..... - 5 -

4 Abbreviations and acronyms ..... - 5 -

5 Conventions ..... - 5 -

6 Overview ..... - 6 -
6.1 Introduction of Digital Public Infrastructure ..... - 6 -
6.2 DPI in Smart Sustainable Cities ..... - 6 -
6.3 Components of DPI in SSC ..... - 7 -

7 Security Threat and risk analysis for DPI in SSC ..... - 9 -
7.1 Threat Landscape for DPI in SSC ..... - 9 -
7.1.1 Common Cybersecurity Threats ..... - 9 -
7.1.2 Threats on Data Security and Privacy ..... - 10 -
7.1.3 Emerging Threats ..... - 11 -
7.2 Risk analysis for DPI in SSC ..... - 14 -

8 Security Framework for DPI in SSC ..... - 15 -
8.1 Lifecycle-embedded security framework for DPI in SSC ..... - 15 -
8.2 Security Control Classification Across the DPI lifecycle ..... - 17 -

9 Security Guidelines for DPI in SSC ..... - 18 -
9.1 Architectural & Technical Measures ..... - 19 -
9.1.1 Defense-in-Depth Architectural Model ..... - 19 -
9.1.2 Zero Trust Architecture (ZTA) ..... - 21 -
9.1.3 Secure Integration Protocols ..... - 21 -
9.1.4 Resilient Infrastructure Models ..... - 22 -
9.2 Data Protection & Privacy Preserving ..... - 22 -
9.2.1 Data Protection Mechanisms ..... - 22 -
9.2.2 Privacy-Preserving Mechanisms ..... - 24 -

9.3 Security Operation & Continuous Monitoring ..... - 25 -
9.3.1 Continuous Monitoring & Threat Detection ..... - 25 -
9.3.2 Incident Response & Crisis Management ..... - 26 -
9.3.3 Disaster Recovery & Business Continuity Planning ..... - 26 -
9.4 Countering Emerging & Future Threats ..... - 27 -
9.4.1 AI-Posed Security Threats & Mitigations ..... - 27 -
9.4.2 Countermeasures for Post-Quantom Cryptography threats ..... - 28 -

Appendix I ..... - 29 -

Best Practices of Secure DPI Implementation ..... - 29 -

References ..... **Error! Bookmark not defined.**

List of figures

<to be revised>

P20 Figure 1 High-level conceptual cybersecurity framework for DPI

P23 Figure 2 Security-embedded DPI-Specific lifecycle

List of tables

<to be revised>

P11 Table 1 Common Cybersecurity Threats to DPI

P12 Table 2 Threats to Data Security and Privacy

P14 Table 3 External AI-Enabled Threats to DPI

P15 Table 4 Threats to AI-Integrated DPI Systems

P17 Table 5 Cyber Threats Posed by Quantum Computing

P23 Table 6 PPT approaches mapping into the phases of DPI lifecycle

P29 Table 7 A Layered Defense-In-Depth Model for DPI Architecture

P38 Table 8 AI Security Governance Recommendations for DPI

P40 Table 9 Best Practices of Secure DPI Implementation Globally

Summary

Digital Public Infrastructure (DPI) has emerged as a foundational digital layer for smart sustainable cities (SSCs), enabling essential functions such as digital identity, secure payments, data exchange, and public service delivery. These city-scale systems form the backbone of urban digital transformation, supporting millions of citizens in their daily interactions with public services, financial systems, and government institutions.

While DPI has traditionally been conceptualized and implemented at the national level, its deployment in SSC introduces distinct characteristics that fundamentally alter its technical architecture, operational requirements, and risk profile. The unique features of DPI for SSC include: Urban Density and Edge Distribution, Real-Time Operational Dependencies, Deep Physical-Digital Convergence, Multi-Stakeholder Complexity, Sustainability-Driven Data Intensity, Rapid Innovation and Pilot-to-Scale Dynamics.

The characteristics of DPI for SSC generate security challenges that exceed the boundaries of conventional cybersecurity frameworks developed for national-scale DPI or enterprise IT systems. The unique convergence of scale, speed, physicality, multiplicity, and innovation demands a framework that is simultaneously comprehensive and specific, providing actionable guidance for securing DPI in SSC.

This document establishes a Security Framework of Digital Public Infrastructure for Smart Sustainable Cities. The framework integrates threat and risk analysis, lifecycle-embedded security architecture, and actionable technical guidelines tailored to the SSC context. It provides city leaders, DPI architects, security practitioners, and technology vendors with a common reference for building and operating DPI that maintains confidentiality, integrity, and availability while sustaining the public trust essential for digital transformation.

Keywords

Internet of things (IoT), digital public infrastructure (DPI) for smart sustainable cities and communities, security framework, smart sustainable city (SSC).

1 Scope

This document provides a security framework and a technical guidance to secure Digital Public Infrastructure (DPI) deployed in smart sustainable cities (SSC).

The scope of this document includes:

- Security threat and risk analysis relevant to DPI in SSC environments;
- Security framework applicable to DPI for SSC;
- Technical security guidelines for protecting DPI systems.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Artificial intelligence [ITU-T F.749.13]: An interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning.

3.1.2 Digital Public Infrastructure [OECD]: shared digital systems that are secure and interoperable and that can support the inclusive delivery of and access to public and private services across society.

[TBD]

3.2 Terms defined in this Document

< to be added>

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

AI	Artificial Intelligence
DPI	Digital Public Infrastructure
PKI	Public Key Infrastructure
SSC	Smart Sustainable City

[TBD]

5 Conventions

This document uses the following conventions:

- The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.
- The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement needs not be present to claim conformance.

6 Overview

6.1 Introduction of Digital Public Infrastructure

Digital Public Infrastructure (DPI) refers to a set of foundational digital systems that provide common, reusable capabilities supporting the delivery of public and private digital services at scale. It forms a shared digital layer that enables interoperability, secure data exchange, identity verification, payment processing, and trusted interactions across sectors.

DPI is characterized by its openness, modularity, and focus on enabling ecosystem innovation rather than providing end-to-end solutions. Unlike traditional digitization efforts that often result in siloed, proprietary systems, DPI emphasizes the creation of shared, reusable infrastructure that can support multiple use cases across different sectors and jurisdictions. The global significance of DPI has been recognized across multiple international forums, including the G20 New Delhi Leaders' Declaration (2023) and the United Nations Global Digital Compact (2024), which acknowledge DPI's potential to deliver services at scale and increase social and economic opportunities for all.

6.2 DPI in Smart Sustainable Cities

While DPI has traditionally been conceptualized and implemented at the national level, its deployment in SSC introduces distinct characteristics that fundamentally alter its technical architecture, operational requirements, and risk profile. These urban-scale systems exhibit six defining features that differentiate them from generic national DPI implementations:

- **Urban Density and Edge Distribution**: Cities concentrate large populations within geographically bounded areas, necessitating highly distributed, edge-heavy infrastructure. Unlike national DPI systems that rely primarily on centralized cloud data centers, DPI for SSC deploys tens or hundreds of thousands of edge nodes—including IoT sensors, smart cameras, autonomous vehicle roadside units, and building automation systems—across the urban fabric. This density creates a massively distributed attack surface where physical proximity to devices becomes a viable attack vector, and the sheer scale of endpoints makes uniform security enforcement technically challenging.
- **Real-Time Operational Dependencies**: Urban DPI systems must support time-critical functions that directly affect public safety and city operations. Traffic signal control, emergency response coordination, smart grid frequency regulation, and autonomous public transport systems operate at millisecond-to-second latencies. This real-time imperative contrasts sharply with national DPI systems and traditional security controls—such as deep packet inspection, behavioral analysis, or multi-hop authentication—may not be applicable due to the latency they introduced.
- **Deep Physical-Digital Convergence**: DPI for SSC directly interfaces with physical infrastructure: Supervisory Control and Data Acquisition (SCADA) systems controlling water treatment and distribution, industrial control systems managing district heating and cooling, building management systems regulating energy consumption, and automated environmental monitoring networks. This convergence transforms DPI from a purely information system into a cyber-physical system where cybersecurity incidents can cause physical impacts such as contaminated water supplies, building lockdowns, transportation gridlock, or environmental hazards.
- **Multi-Stakeholder Complexity**: National DPI is characterized by relatively simple stakeholder topology—government providers and citizen users—with security responsibilities concentrated in sovereign institutions Urban DPI, by contrast, functions within a complex ecosystem of municipal agencies, regulated utilities, private platform operators, academic research institutions, and citizens themselves. A single urban data exchange may involve data flows between city transportation departments, ride-sharing platforms, electric grid operators, weather services, and navigation applications. This multiplicity complicates trust establishment, liability allocation,

and security governance, as no single entity maintains comprehensive visibility or control over the entire data lifecycle.

- **Sustainability-Driven Data Intensity**: DPI for SSC is explicitly designed to measure, optimize, and verify progress toward environmental and social sustainability goals. This purpose drives the collection of unprecedented volumes and varieties of data: real-time energy consumption at building and district levels, multimodal transportation patterns, air quality and noise pollution measurements, waste generation and recycling flows, and social service access patterns. ensuring robust data security and privacy protection is essential to safeguard sensitive urban data, maintain public trust, and enable the responsible use of large-scale data for sustainable decision-making and long-term city resilience.
- **Rapid Innovation and Pilot-to-Scale Dynamics**: Cities increasingly function as innovation testbeds for emerging technologies. DPI for SSC frequently incorporates experimental deployments—autonomous delivery robots, AI-driven predictive maintenance, digital twins for urban planning, blockchain-based energy trading—that transition from pilot to production scale within compressed timelines. These technical innovations may create security issue since systems may achieve functional deployment before comprehensive security architecture review, and the experimental nature of components may preclude mature security validation.

6.3 Components of DPI in SSC

DPI in SSC comprises a complex ecosystem of services, stakeholders, and assets that together enable the delivery of digital services at urban scale. Figure 1 illustrates this ecosystem, showing the three components and their interrelationship.

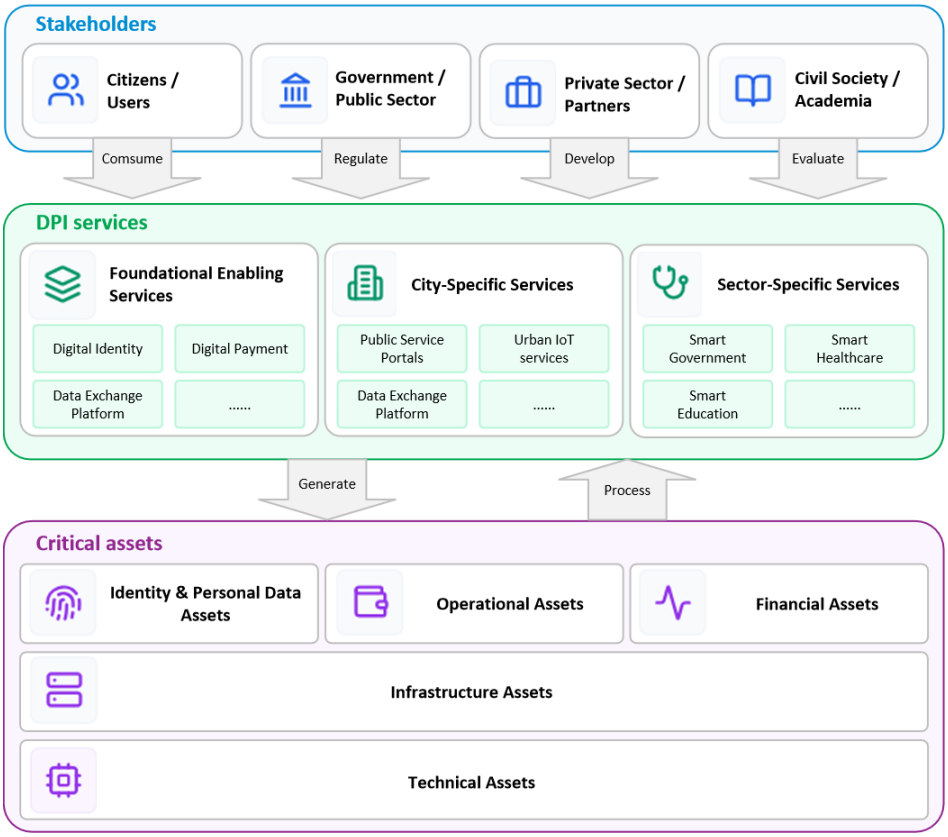

Figure 1 – Ecosystem of DPI for SSC

- **Key DPI Services in SSC**

DPI services form the functional layer of DPI, supporting the daily lives of residents, the operations of businesses, and the functioning of government. Key DPI services in SSC can be categorized into 3 types:

- **Foundational Enabling Service**s: Foundational enabling services provide common, reusable capabilities that underpin all other digital services. Key services include but are not limit to: Digital Identity, Digital Payments, and data exchange platform.
- **City-Specific Services**: City-specific services are the application-layer DPI services directly for urban management and the daily life scenarios of citizens. Key services include but are not limit to: Public Service Portals, Urban IoT Services, and Smart transportation.
- **Sector-Specific Services**: Sector-specific services are the specialized DPI services designed for particular vertical domains. Key services include but are not limit to: Smart Government, Smart Healthcare, and Smart Education.

- **Involved Stakeholders**

Stakeholders form the governance and participation dimension of DPI for SSC. Typical stakeholders include:

- **Citizens/users**: Citizens and users are the ultimate beneficiaries and primary service objects of city DPI. They are consumers of public services, generators of data, and participants in urban life.
- **Government/Public Sector**: The government and public sector are the primary stewards, regulators, and service providers of city DPI. They are responsible for policy formulation, infrastructure investment, service delivery, and ensuring that DPI serves the public interest.
- **Private Sector/Partners**: The private sector and partners are essential collaborators in building, operating, and innovating upon DPI. They bring technical expertise, investment capital, operational efficiency, and market-driven innovation.
- **Civil Society/Academia**: Civil society and academia provide independent expertise, ensuring that DPI development remains responsive to societal needs and values.

- **Critical assets**

Assets are the digital resources that DPI systems depend on to function, which need to be protected and managed effectively. Critical assets for DPI in SSC includes:

- **Identity & Personal Data Assets**: Identity and personal data assets comprise all digital information that can be linked to identified or identifiable individuals. Examples include citizen identity records, biometric data, health and social data, location and mobility data, and service usage history.
- **Operational Assets**: Operational assets are the digital systems, data, and algorithms that directly control, monitor, and manage city operations. Examples include traffic control systems, emergency response systems, environmental monitoring systems, and public safety systems.
- **Financial Assets**: Financial assets encompass the digital systems, accounts, and data involved in managing, processing, and recording financial transactions related to city services. Examples include payment processing systems, government financial accounts, billing and collection data, and tax administration systems.
- **Infrastructure Assets**: Infrastructure assets are the foundational digital systems and platforms upon which other DPI services are built. Examples include core identity systems, data exchange platforms, city portals and websites, development environments, audit and logging systems, and digital twin platforms.

- **Technical Assets**: Technical assets are the specialized digital components that enable security, intelligence, and functionality within DPI systems. Examples include encryption keys, AI models, APIs, source code, and algorithms.

7 Security Threat and risk analysis for DPI in SSC

7.1 Threat Landscape for DPI in SSC

7.1.1 Common Cybersecurity Threats

Cybersecurity threats pose a persistent challenge to the stability and trustworthiness of DPI deployed in SSCs. While many of these threats—such as ransomware, phishing, supply chain attacks, and insider risks—are common across digital ecosystems, their impacts on city DPI are particularly critical, as these urban-scale systems underpin the delivery of essential services to millions of citizens. The interconnected nature of city DPI, spanning multiple administrative domains, physical infrastructure, and citizen-facing services, increases exposure and amplifies the consequences of even routine cyber incidents.

The commonly seen cybersecurity threats within city DPI contexts and examples of the city DPI services that may be affected are summarized in Table 1.

Table 1 – Common Cybersecurity Threats to city DPI

Threat	Description	Affected Security Attribite	Affected city DPI services
Ransomware Attacks	Attackers encrypt critical DPI data and demand ransom, disrupting essential public services and operations	Availability	- Public service portals - Digital identity systems - Payment platforms - Smart healthcare systems
Supply Chain Vulnerabilities	Insecure third-party vendors or providers can compromise core DPI components due to interdependencies	Confidentiality Integrity Availability	- All city DPI services (systemic risk across the ecosystem)
DDoS Attacks	Large-scale botnet attacks overwhelming DPI resources, causing service disruptions or complete outages	Availability	- Public service portals - Identity authentication services - Payment gateways - Emergency response systems
Espionage and Privileged Access Compromise	Attackers intercept communications or target privileged individuals to gain unauthorized access	Confidentiality Integrity	- All city DPI services (compromised privileges enable access across the ecosystem)
Legacy System Vulnerabilities	Outdated infrastructure components lacking modern security are	Confidentiality Integrity	- Legacy city service platforms - Legacy databases

Threat	Description	Affected Security Attribite	Affected city DPI services
	more susceptible to exploitation	Availability	- Old IoT devices - Legacy industrial control systems
Insider Threats	Negligent or malicious insiders can damage or expose DPI systems and data	Confidentiality Integrity Availability	- All city DPI services (insiders with sufficient privileges can access any system within their authorized scope)
Complexity & Interdependency	The interconnected, layered nature of DPI can obscure vulnerabilities and make systems harder to secure	Availability	- Cross-agency integrated services - Multi-vendor service ecosystems - City data sharing platforms

7.1.2 Data Security and Privacy-Oriented Threats

Data security and privacy are foundational to DPI deployed in SSCs, which manages vast amounts of sensitive personal, governmental, and operational data. Threats such as unauthorized access, data breaches, and manipulation not only compromise individual privacy but can also disrupt the availability of essential public services. As city DPI systems often serve as the backbone for identity, healthcare, financial, and communication services, ensuring data confidentiality, integrity, and availability is critical to their reliability, resilience, and public trust essential for sustainable urban development.

The main security threats that endanger core data assets and the privacy within city DPI contexts and examples of the city DPI services that may be affected are summarized in Table 2.

Table 2 – Threats to Data Security and Privacy

Threat	Description	Affected Security Attribite	Affected city DPI services
Unauthorized Access & Credential Compromise	Exploiting weak authentication, misconfigured access controls, or stolen credentials to gain unauthorized access to DPI data	Confidentiality	- Digital identity services - Administrative portals - Healthcare systems - Social service databases
Data Breaches & Exfiltration	Unpatched vulnerabilities, legacy system exploits, or Advanced Persistent Threats leading to large-scale breaches, exposing sensitive information	Confidentiality	- City data platforms - Health record systems - Social service databases - Financial transaction systems - Identity registries

Threat	Description	Affected Security Attribite	Affected city DPI services
Sophisticated Phishing & Social Engineering	Using advanced phishing techniques and social engineering to deceive users into revealing credentials, installing malware, or granting unauthorized access	Confidentiality	- Citizen-facing service portals - Administrative dashboards - Vendor access interfaces - Help desk systems
Excessive Data Aggregation & Profiling	Over-collection of personal data from multiple sources leading to privacy breaches and unauthorized surveillance	Confidentiality	- Urban IoT systems - Mobility tracking platforms - Public Wi-Fi systems - Video surveillance systems
Data Tampering & Injection Attacks	Injecting malicious code or altering data streams to manipulate DPI data and undermine the reliability and accuracy	Integrity	- Financial transaction systems - Traffic management systems - Public records databases

These data-centric risks may arise from traditional cyberattacks as well as from emerging technologies such as AI-driven analytics misuse or future quantum-enabled decryption capabilities, which are further elaborated in 7.1.3.

7.1.3 Technology-Driven Emerging Threats

Emerging threats refer to novel or rapidly evolving cybersecurity risks driven by the development and integration of cutting-edge technologies—such as AI, quantum computing, and advanced automation—that introduce new attack vectors and system vulnerabilities. For DPI deploed in SSCs, the stakes are high: emerging threats can disrupt service continuity, exploit unanticipated weaknesses in newly deployed systems, and undermine trust. As DPI increasingly adopts innovative tools to improve scale and efficiency, proactive risk assessment and adaptive defense mechanisms become essential to safeguard its security.

7.1.3.1 **Threats Posed by AI to DPI for SSC**

With the rapid development of Agentic AI systems, AI-driven attacks are becoming increasingly autonomous, coordinated, and goal-oriented. Such systems can independently plan attack paths, coordinate multiple attack tools, and continuously adapt to defensive measures, posing unprecedented challenges to DPI in SSC. Additionally, the growing adoption of edge AI, hybrid AI architectures, and multimodal perception-reasoning-action pipelines within city DPI will introduce new attack surfaces. These threats are particularly relevant in smart city, digital mobility, and public service scenarios, and must be incorporated into city DPI threat model.

7.1.3.1.1 External AI-Enabled Threats to DPI for SSC

AI technologies are now being exploited by malicious actors to enhance the sophistication, scale, and effectiveness of cyberattacks targeting city DPI. These threats include AI-driven malware, deepfake-enabled social engineering, and automated data harvesting. AI significantly expands the cyberattack surface, enabling more convincing deception and accelerating attack cycles.

The main external AI-enabled security threats that endanger city DPI and examples of the city DPI services that may be affected are summarized in Table 3.

Table 3 – External AI-Enabled Threats to DPI

Threat	Description	Affected Security Attribite	Affected city DPI services
AI-Powered Cyber Attacks	AI-driven malware and automated attacks that can learn, adapt, and evade traditional security defences	Confidentiality Integrity Availability	- Traffic management systems - Public service portals - City data platforms
Privacy Invasion & Data Extraction	AI's ability to analyze vast datasets can be misused to extract sensitive information	Confidentiality	- Urban IoT networks - City data platforms - Healthcare systems
Deepfake-Based Social Engineering	Creation of realistic fake audio or video to impersonate trusted individuals and deceive targets	Confidentiality	- Financial services - Digital identity systems

7.1.3.1.2 Threats to AI-Integrated DPI Systems

The deployment of AI within city DPI can inadvertently introduce security threats and vulnerabilities due to the complexity and opacity of AI models. In the urban context, these risks are magnified as AI systems increasingly underpin critical city functions, from predictive traffic management to AI-assisted emergency dispatch.These systems may be susceptible to data poisoning, adversarial attacks, and other forms of manipulation that compromise security.

The main threats to AI-integrated DPI systems in SSC and examples of the city DPI services that may be affected are summarized in Table 4.

Table 4 – Threats to AI-Integrated DPI Systems

Threat	Description	Affected Security Attribite	Affected city DPI services
Data Poisoning	Injection of malicious data into AI training sets, leading to corrupted model outputs	Confidentiality Integrity	- Traffic management systems - Smart grid systems - City analytics platforms
Adversarial Attacks	Input of specially crafted data designed to mislead AI models into making incorrect decisions	Confidentiality Integrity	- Autonomous vehicle systems - Facial recognition systems - Smart surveillance systems

Threat	Description	Affected Security Attribite	Affected city DPI services
			- Traffic signal control systems
Model Inversion	Extraction of sensitive information from AI models by analyzing their outputs	Confidentiality	- Healthcare AI systems - Digital identity systems - City data platforms
Model Vulnerabilities in DPI Systems	Inherent vulnerabilities in AI models used in DPI systems that can be exploited for malicious purposes	Confidentiality Integrity Availability	- All AI-integrated city DPI services (systemic vulnerability across the ecosystem)
AI and Unintended Consequences in DPI Decisions	AI-powered DPI decisions causing unintended impacts on data privacy, system fairness, or integrity	Confidentiality Integrity	- Predictive policing systems - Smart city resource allocation - Traffic management systems
Unsafe Content Generation and Propagation	AI systems generating, amplifying, or propagating false, manipulated, or malicious content	Integrity Availability	- Public information portals - Emergency alert systems

7.1.3.2 **Threats Posed by Quantum Computing to DPI**

Quantum computing holds immense promise for revolutionizing industries by solving complex problems at unprecedented speeds. However, this technology also poses unique challenges to the cybersecurity landscape for SSCs. As quantum computing advances, it could potentially undermine traditional cryptographic systems that are fundamental to the security of DPI. Cryptographically Relevant Quantum Computers may be capable of breaking existing encryption protocols, putting sensitive data at risk and threatening the confidentiality, integrity, and availability of critical city DPI systems. While practical quantum computing is still in its early stages, the potential for these risks necessitates forward-looking security strategies to ensure that cit DPI can withstand the disruptive power of this emerging technology.

The main threats posed by quantum computing to DPI in SSC and examples of the city DPI services that may be affected are summarized in Table 5.

Table 5 – Cyber Threats Posed by Quantum Computing

Threat	Description	Affected Security Attribite	Affected city DPI services
Compromise of asymmetric Cryptography	Quantum computers can break RSA and ECC encryption, threatening	Confidentiality, Integrity	- Digital identity systems - Payment platforms - Data exchange platforms

Threat	Description	Affected Security Attribite	Affected city DPI services
	data confidentiality and integrity		- Public Key Infrastructure (PKI) systems
Halving the security of symmetric Cryptography	Quantum computing can reduce the complexity of exhaustive search by halving the security of a symmetric encryption algorithm	Confidentiality Integrity	- Encrypted data storage systems - City databases - Backup systems
Undermining of Digital Signatures	Quantum computing could allow attackers to forge digital signatures, bypassing authentication mechanisms	Integrity	- Digital identity systems - Government authorization systems - Financial transaction systems
'Harvest Now, Decrypt Later' Attacks	Adversaries collect encrypted data today, planning to decrypt it once quantum computing advances	Confidentiality	- Citizen identity records - Health information systems - Historical archives
Hybrid Threat Scenarios	AI-augmented quantum computing accelerates vulnerability discovery and cyber exploitation	Confidentiality Integrity Availability	- All city DPI services (systemic risk acceleration)

7.2 Risk analysis for DPI in SSC

In the context of DPI for SSC, risk arises when identified threats exploit existing vulnerabilities, leading to consequences that disrupt city services, compromise citizen data, or undermine public trust. Given the distributed, multi-stakeholder, and highly interconnected nature of SSC environments, to ensure analytical clarity and to support the development of targeted security controls, risks to DPI in SSC are classified into three domains.

- **Governance risk** refers to the possibility that inadequate security policies, unclear accountability structures, insufficient regulatory alignment, or weak oversight mechanisms may result in ineffective implementation of security requirements.
- **Operational risk** refers to the risk that inadequate processes, poor coordination, weak monitoring, or ineffective incident response will enable threats to disrupt city services..
- **Technical Risk** refers to the possibility that vulnerabilities within software components, infrastructure platforms, cryptographic implementations, AI models, integration interfaces, or edge devices may be directly exploited to compromise system security properties.

Table 6 maps the threats identified in Clause 7.1 to these three risk domains, illustrating how each threat manifests across governance, operational, and technical dimensions, and indicating the primary stakeholder groups affected by each category.

Table 6– Cyber Threats Posed by Quantum Computing

Threat Category	Governance Risk	Operational Risk	Technical Risk	Stakeholder Impact
Common Cybersecurity Threats (ransomware, DDoS, supply chain, etc.)	Weak accountability, insufficient third-party oversight	Service interruption, delayed incident response	Exploitation of infrastructure and credential vulnerabilities	- Government agencies - Service operators - Citizens
Data Security and Privacy-Oriented Threats (unauthorized access, breaches, tampering, etc.)	Inadequate data governance and policy enforcement	Improper access control and monitoring failures	Compromise of identity systems, databases, encryption mechanisms	- Citizens - Government data controllers - Regulated entities
AI-Driven and AI-Integrated Threats	Insufficient AI oversight and security validation	Weak lifecycle management of AI systems	Model poisoning, adversarial attacks, AI-enabled exploitation	- Government decision systems - Citizens - Private AI operators
Quantum-Related Cryptographic Threats	Delayed cryptographic transition governance	Inadequate migration planning and key lifecycle control	Compromise of digital signatures, PKI, secure communications	- All stakeholders dependent on identity, payment, and data exchange systems

8 Security Framework for DPI in SSC

8.1 Lifecycle-embedded security framework for DPI in SSC

DPI deployed in SSC supports critical and large-scale systems such as digital identity services, payment platforms, urban IoT infrastructures, public service portals, and data exchange platforms. These systems are characterized by high interconnectivity across administrative and functional domains, real-time operational dependencies, large-scale aggregation and exchange of sensitive citizen data, and strong interdependencies between cyber and physical infrastructures. Given these characteristics, security considerations is required to be embedded across the entire DPI lifecycle.

Figure 2 illustrates the lifecycle-embedded security framework for DPI in SSC. Security mechanisms shall be integrated into each phase of a typical lifecycle of DPI— conception & scoping, strategy & design, development, deployment, and operations & maintenance to ensure resilience, integrity, availability, confidentiality, and traceability in SSC environments.

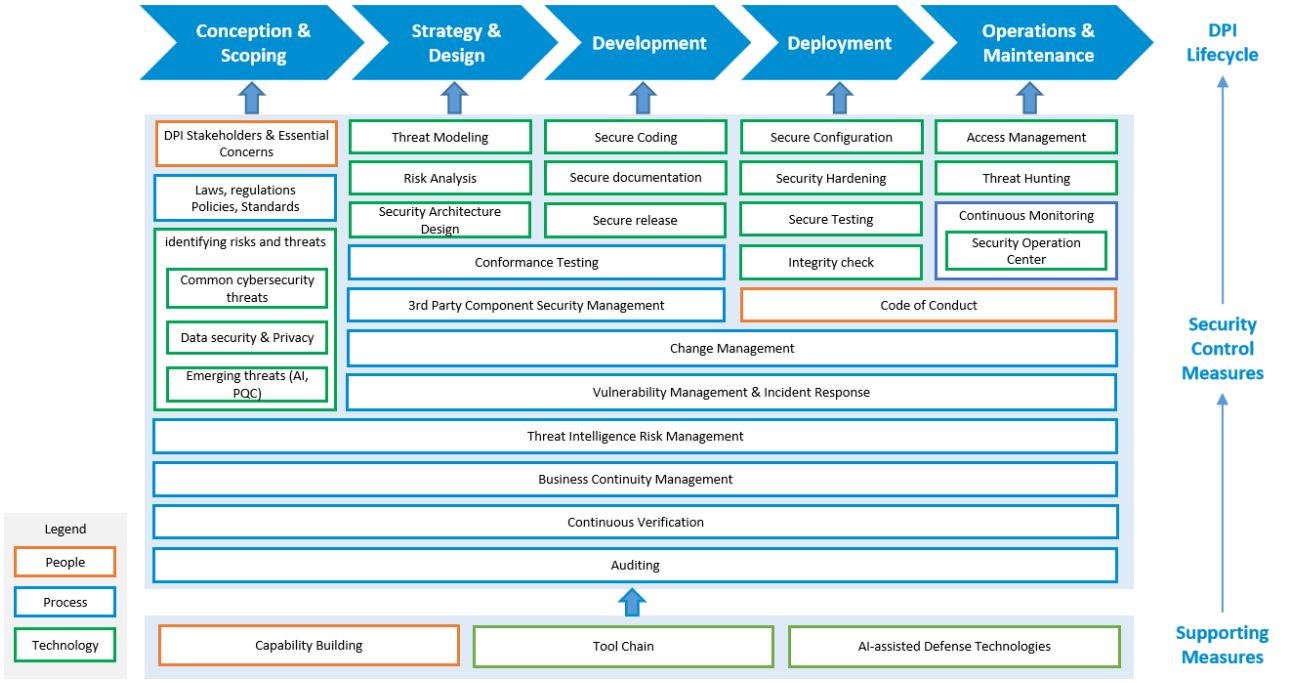

Figure 2 – Lifecycle-embedded security framework for DPI in SSC

- In **Conception and Scoping phase,** the purpose, goals, constraints, and boundaries of DPI is required to be established, guiding decisions and aligning with city strategic objectives and needs. Key security activities include setting security goals and objectives for city stakeholders, considering linkages to urban sustainability goals; analyzing applicable legal, regulatory, and standards requirements for city DPI; and identifying security risks and threats within the urban context while assessing potential impacts on city service continuity and citizen trust..
- In **Strategy and Design phase,** a comprehensive plan is required to be developed to meet city DPI functional and performance objectives through actionable steps. Abiding by the principle of security-by-design, key security activities include conducting threat modeling and risk analysis tailored to urban service scenarios; performing security architecture design; setting out phase spanning activities such as conformance testing, 3rd party component management, change management, vulnerability management and incident handling process; and utilizing risk-based strategies to effectively mitigate design-related and architectural risks specific to city DPI.
- In **Development phase,** prototype systems conforming to city service specifications is required to be built, ensuring functionality, reliability, and scalability. The main objective of the phase is to implement the secure design while preventing the introduction of additional engineering security risks. Therefore, key security activities include secure coding, secure verification including white-box, grey-box and black-box testing, documentation of the city DPI security specifications, and secure releasing.
- In **Deployment phase,** the implementation of DPI systems in the actual urban operational environment is required to ensure successful large-scale adoption while maintaining city service security and resilience. Key security activities include secure configuration, security hardening, security testing, and integrity check of the release. The objective is to ensure the integrity of the delivered systems, and make the installed hardware, software, and networking components are secure-by-default. Standardized code of conduct for system operators is essential because security responsibility is transferred within the phase.
- In **Operations and Maintenance phase,** the ongoing performance, stability, and efficiency of city DPI is required to be ensured. Key security activities include access management, threat hunting, continuous monitoring, and incident response to ensure security and resilience of the

urban system. This phase typically triggers continuous improvement of security capabilities to address emerging threats arising from ongoing urban digital transformation..

In addition ~~the~~ the security activities for specific phase specified above, to address evolving security risks in smart sustainable cities, a set of security activities shall span the entire DPI lifecycle. Security activities such as threat intelligence risk management, incident response, vulnerability management, business continuity management, continuous verification and auditing should be included to stay aligned with the evolving security risks, protect the assets from the harm from cyber-attack or physical disasters, and inspect the effectiveness of the security control measures in each phase.

Particularly, Vulnerability Management and Incident Response are essential as lifecycle-spanning security processes due to their critical role in maintaining continuous protection and resilience across all phases of city DPI lifecycle. Vulnerability Management systematically identifies, assesses, and remediates weaknesses from design through maintenance, reducing the attack surface proactively rather than reactively. Similarly, Incident Response ensures preparedness, rapid detection, containment, and recovery from security incidents throughout the lifecycle, minimizing operational disruption and learning from incidents to strengthen urban defenses capabilities.

To effectively execute these functions, it is recommended for cities to establish dedicated security teams, such as city-level Computer Emergency Response Team, Computer Security Incident Response Team, or Product Security Incident Response Team, which provide centralized expertise, ensure consistent response coordination, and maintain oversight of ongoing security activities.

Furthermore, adopting collaborative approaches like coordinated vulnerability disclosure and collaborative incident response builds trust among city stakeholders, promotes transparency, and enhances collective ability to respond to evolving threats—strengthening the overall security posture of the DPI ecosystem in an interconnected urban operational environment.

Acting as supporting measures to the framework, capability building equips city administrators, operators, and citizens with essential cybersecurity competencies, while a digitized tool chain enhances operational consistency and traceability. Furthermore, the integration of state-of-the-art AI-assisted defense technologies significantly improves threat detection accuracy, accelerates response times, and reduces reliance on manual intervention—thereby strengthening overall resilience and minimizing human error across the DPI ecosystem.

8.2 Security Control Classification Across the DPI lifecycle

To ensure completeness and traceability of security controls, the lifecycle-embedded framework shall classify security measures across three control dimensions:

- Organizational Controls: accountable stakeholders and responsibilities;
- Procedural Controls: repeatable and auditable processes;
- Technical Controls: enforceable technical mechanisms.

Security controls defined in each lifecycle phase is required to be mapped to at least one of these dimensions to ensure balanced implementation. Table 6 illustrates the mapping of control dimensions to DPI lifecycle phases.

Table 7 – Security control dimensions mapping into DPI lifecycle phases

<Editor's Note: city specific security activities are to be included.>

DPI Lifecycle phases	Organizational Controls	Procedural Controls	Technical Controls
Conception & Scoping	- Identify key stakeholders, e.g., city agencies, private sector, civil society. - Define security accountability across multiple city agencies and operators	- Establish security objectives, risk appetite, and compliance frameworks. - Conduct risk assessments against urban threat landscape.	- Define security architecture principles for city-scale systems, e.g., secure-by-design, privacy-by-design. - Plan for interoperability and resilience.
Strategy & Design	- Conduct security awareness training for DPI architects and policymakers. - Build cross-sector collaboration for security best practices.	- Integrate secure development lifecycle principles. - Perform threat modelling and security validation.	- Design system architecture with encryption, IAM, and Zero Trust models. - Implement access control and secure coding practices.
Development	- Train developers on secure coding and security testing. - Conduct regular security drills and simulations.	- Establish change management and secure software development policies. - Require machine-readable Software Bill of Materials (SBOM) for all digital components. - Implement continuous risk assessments.	- Automate security testing, e.g., CI/CD security checks, vulnerability scanning. - Integrate automated vulnerability correlation against SBOM inventories. - Use container security and endpoint protection tools.
Deployment	- Provide security awareness programs for operational staff. - Conduct phishing and social engineering attack simulations.	- Implement compliance checks before go-live. - Conduct penetration testing and red teaming.	- Enforce secure configuration baselines. - Deploy monitoring and logging solutions (SIEM, IDS/IPS).
Operations & Maintenance	- Maintain continuous cybersecurity training for city DPI operators. - Foster a security-first culture within organizations.	- Conduct periodic security audits and compliance reviews. - Implement an incident response and recovery framework.	- Deploy real-time threat intelligence and anomaly detection systems. - Use AI/ML for predictive cybersecurity threat management.

9 Security Guidelines for DPI in SSC

<Editor's Note: city specific details are to be included.>

Addressing the cybersecurity challenges of DPI systems requires comprehensive, multi-layered approaches that integrate robust technical controls, sound governance frameworks, proactive risk management, and privacy-preserving measures. The following recommendations provide a structured approach to safeguard the confidentiality, integrity, and availability of DPI—enabling governments, developers, operators, and auditors to design, implement, and maintain secure digital public infrastructure in a rapidly evolving threat landscape. By addressing both current and future challenges through a layered defense strategy, DPI can remain resilient, trustworthy, and effective in delivering essential public services.

9.1 Architectural & Technical Measures

<Editor's Note: mission critical infrastructures are to be included. Examples of mission critical infrastructures are needed>

DPI must be architected with security as a foundational principle, incorporating modern paradigms and layered defenses to protect against evolving threats. This involves a strategic combination of layered defenses, a fundamental shift in trust assumptions, secure interoperability, and inherent resilience to ensure the confidentiality, integrity, and availability of critical services.

9.1.1 Defense-in-Depth Architectural Model

To ensure the security and resilience of DPI, a **layered defense-in-depth model** offers a systematic and robust foundation to ensure that breaches in one layer do not compromise the entire system. The approach spans physical environment up through networks, identity controls, applications, data, operational monitoring and auditing. Each layer implements a unique set of security controls designed to address specific threat vectors, creating a synergistic barrier that significantly raises the cost and complexity for an attacker. The model enables DPI architects, integrators, auditors, and operators to address specific concerns such as intrusion detection, identity assurance, and regulatory compliance with precision.

Table 8 A Layered Defense-In-Depth Model for DPI Architecture

Layer	Security Concern	Controls / Technologies	Reference Standards & Frameworks
Audit & Compliance Layer	Ensure traceability, non-repudiation, regulatory compliance	Immutable, blockchain-based logging systems; Automated compliance checking and reporting (e.g., via SOAR playbooks); Centralized audit trails.	ISO/IEC 27001:2022 (Clause 9), NIST SP 800-92, NIST SP 800-53 (AU Family), ITU-T X.1051, GDPR Art. 30
Operations, Monitoring &Orchestration Layer	Detect, respond to, and autonomously contain incidents; monitor behavior and automate security operations	Security Information and Event Management (SIEM) with integrated threat intelligence; Security Orchestration, Automation, and Response (SOAR) platforms; User and Entity Behavior Analytics (UEBA); Endpoint Detection and	NIST CSF 2.0 (Detect/Respond), ISO/IEC 27035, NIST SP 800-137, MITRE ATT&CK®

		Response (EDR); Network Detection and Response (NDR).	
Data Layer	Preserve confidentiality, integrity, privacy	Encryption (AES-256, RSA-2048) for data at rest and in transit; Hardware Security Modules (HSMs) for key management; Data Loss Prevention (DLP) tools; Privacy-Enhancing Technologies (PETs) like differential privacy and secure multi-party computation (MPC).	ISO/IEC 27018, ISO/IEC 20889, NIST SP 800-175B, NIST FIPS 140-3, GDPR Art. 32
Application Layer	Prevent exploits, injection, insecure code execution	Web Application Firewalls (WAF); Static and Dynamic Application Security Testing (SAST/DAST); Machine-readable SBOM; Runtime Application Self-Protection (RASP); Secure coding practices following OWASP Top 10.	ISO/IEC 27034, OWASP ASVS, NIST SSDF (SP 800-218), OWASP Top 10
Access & Identity Layer	Enforce authentication, authorization, least privilege	Multi-Factor Authentication (MFA) with phishing-resistant methods (e.g., FIDO2); Zero Trust Network Access (ZTNA); Role-Based and Attribute-Based Access Control (RBAC/ABAC); Privileged Access Management (PAM) solutions.	NIST SP 800-63B, ISO/IEC 29146, NIST SP 800-207 (Zero Trust), ENISA Zero Trust Reference Architecture
Network Layer	Prevent eavesdropping, DDoS, lateral movement	Next-Generation Firewalls (NGFW) with deep packet inspection; Microsegmentation; Software-Defined Networking (SDN) for policy enforcement; Intrusion Prevention Systems (IPS); DDoS mitigation services.	ISO/IEC 27033, NIST SP 800-41, CIS Critical Security Control 12, ITU-T X.1036
Physical Layer	Prevent unauthorized physical access,	Biometric access controls; Video surveillance with AI-powered analytics; Environmental	ISO/IEC 27002:2022 (9.1), NIST SP 800-53

	tampering, sabotage	monitoring (temperature, humidity); Hardware root of trust (e.g., TPM); Tamper-evident seals on critical infrastructure.	(PE Family), SOC 2 Type II

9.1.2 Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) operates on the core principle of "never trust, always verify," explicitly assuming that threats exist both inside and outside the traditional network perimeter. Implementing ZTA involves a comprehensive approach beyond simple network changes:

- **Strong, Phishing-Resistant Authentication:** Verifying every user, device, and service identity attempting to access resources. This mandates the use of multi-factor authentication (MFA), prioritizing phishing-resistant methods like FIDO2 security keys over weaker SMS-based codes.
- **Explicit Least Privilege Access:** Dynamically restricting access rights to only the data and applications necessary for a specific session or task, minimizing the attack surface. This is often enforced through Just-In-Time (JIT) and Just-Enough-Access (JEA) policies.
- **Microsegmentation & Software-Defined Perimeters:** Dividing the network into fine-grained, isolated segments based on workload identity to prevent lateral movement by malicious actors. This extends beyond the network layer to application and data layers.
- **Continuous Validation and Authorization:** Re-evaluating trust based on changing context (user location, device health, behavior analytics) for all access requests and connections, not just at initial login.
- **Comprehensive Visibility and Analytics:** Implementing robust logging and monitoring across all assets to feed the continuous validation engine and provide visibility into all access attempts.

Adopting ZTA enhances security by eliminating implicit trust and enforcing strict access controls based on identity and context, thereby drastically reducing the risk of unauthorized access and lateral movement.

9.1.3 Secure Integration Protocols

Ensuring secure and trusted communication between DPI systems and external platforms is essential for maintaining a coordinated security architecture. These protocols safeguard interoperability across distributed components such as cloud controllers, network policy engines, and threat intelligence platforms. Critical measures include:

- **Inter-System Authentication and Secure Channels:** Implementing certificate-based mutual authentication (mTLS) and secure tunneling protocols (e.g., IPsec, TLS 1.3) to ensure trusted connections between DPI systems and external management or orchestration services. All certificates must be managed through a robust Public Key Infrastructure (PKI).
- **API Security Controls:** Deploying authenticated and encrypted API communication using standards such as OAuth 2.0 with mTLS and OpenID Connect, especially for dynamic policy updates and telemetry sharing. API gateways should be employed to enforce rate limiting, schema validation, and threat detection at the API layer.

- **Orchestration and Automation Security:** Adopting secure automation protocols such as NETCONF/YANG with SSH or TLS for secure network configuration management and DPI policy distribution. All automation scripts and credentials must be securely stored and managed, ideally within a privileged access management (PAM) solution.
- **Unified Access Control Across Domains:** Enforcing consistent access policies through federated identity systems (e.g., using SAML 2.0 or OpenID Connect) to prevent privilege escalation and lateral movement via integrated interfaces. A central identity provider (IdP) should serve as the single source of truth for authentication.

These protocols ensure that DPI systems interoperate securely within broader network and cloud environments, creating a seamless yet secure fabric that prevents threat actors from exploiting integration interfaces to bypass inspection, exfiltrate data, or disrupt traffic analysis.

9.1.4 Resilient Infrastructure Models

Building reliable and fault-tolerant DPI systems requires foundational infrastructure practices that maintain operation during failures, attacks, or peak load. Resilience is measured by the ability to maintain availability and performance under stress. Essential methods include:

- **Redundant, Geographically Distributed Deployment:** Using multiple, active-active instances of DPI systems across different availability zones or regions to ensure continuous traffic inspection if one node fails and to survive regional disasters.
- **Elastic Load Balancing and Scalability:** Distributing network traffic evenly across DPI nodes and automatically scaling resources up or down to prevent overloading and maintain performance during high-volume periods, such as during a DDoS attack.
- **Regular Backups and Rapid, Verified Restoration:** Frequently backing up DPI configurations, policy sets, and critical state data. Backups must follow the 3-2-1 backup rule and be regularly tested via restoration drills to ensure they are uncorrupted and service can be quickly restored after an outage.
- **Failure Testing and Automated Updates:** Periodically testing system response to failures through chaos engineering practices and applying security patches via automated, orchestrated rollout procedures with rollback capabilities to strengthen resilience against known vulnerabilities.
- **Stateless Design Where Possible:** Designing DPI components to be stateless, pushing stateful sessions to an external, resilient data store. This simplifies failover and allows any node to handle any request, improving horizontal scalability.

These practices help DPI systems continue operating effectively under stress or partial failure, ensuring uninterrupted network monitoring and protection even in adverse conditions, which is critical for maintaining trust in public infrastructure.

9.2 Data Protection & Privacy Preserving

Protecting data throughout its lifecycle is critical to fulfilling regulatory obligations and maintaining public trust, requiring both foundational security and advanced privacy techniques.

1 9.2.1 Data Protection Mechanisms

Implementing comprehensive measures that provide baseline protection for data confidentiality and integrity, and help prevent unauthorized access and potential misuse of resources.

1.1.1.1 9.2.1.1 Data Encryption & Secure Storage

<Editor's Note: security measures are need to be PQC-secured.>

Protecting data confidentiality and integrity is paramount. Effective measures include:

- **Data Encryption**: Utilizing robust encryption protocols (e.g., AES-256 for data at rest, TLS 1.3 for data in transit) to prevent unauthorized access. A well-defined encryption strategy, including regular key rotation and cryptographically secure random number generation, is essential for maintaining long-term security.
- **Secure Storage Solutions**: Implementing storage systems with built-in security features, such as automatic encryption, immutable backups, and fine-grained access controls, to safeguard sensitive information. Solutions should be evaluated against industry standards (e.g., FIPS 140-3) to ensure they meet stringent security requirements.
- **Hardware Security Modules (HSMs):** Deploying certified hardware security modules to provide a hardened, tamper-resistant environment for cryptographic key storage and operations. HSMs ensure that encryption keys are generated, stored, and used never leaving the protected hardware boundary, significantly raising the security bar against key extraction and misuse. They are fundamental for protecting root encryption keys and managing the entire cryptographic key lifecycle in a secure and compliant manner.

These practices ensure that even if data is intercepted or accessed without authorization, it remains unintelligible and secure.

1.1.1.2 9.2.1.2 Data Integrity & Cryptographic Verification

Maintaining the accuracy and trustworthiness of data is a critical security objective. This is achieved through:

- **Cryptographic Hashing:** Employing secure hash algorithms (e.g., SHA-256, SHA-3) to generate unique digital fingerprints (cryptographic digests) for datasets. These digests are stored separately from the data itself. Any alteration to the data, however minor, will result in a completely different hash value upon re-calculation, immediately indicating tampering. This is critical for verifying the integrity of software updates, configuration files, and evidence logs.
- **Digital Signatures:** Implementing asymmetric cryptography (e.g., using ECDSA or RSA-based digital certificates) to sign critical data. This not only verifies integrity but also provides non-repudiation, confirming the data's origin and authenticity. The private keys used for signing must be protected to the highest standard, ideally using an HSM (as outlined in 4.3.1.1), to prevent forgery in the verification process.
- **Cryptographic Data Lineage:** For federated data exchange platforms, incorporating tamper-evident provenance mechanisms (e.g., hash chaining, Merkle-tree-based attestations, or signed metadata) to ensure verifiable data lineage across distributed systems. Such mechanisms strengthen integrity guarantees and reduce the risk of undetected data tampering or malicious dataset manipulation.

These measures guarantee that data has not been modified in an unauthorized manner, ensuring its reliability throughout its lifecycle.

1.1.1.3 9.2.1.3 Identity & Access Management (IAM)

Effective IAM is crucial for controlling user access within DPI systems:

- **Multi-Factor Authentication (MFA)**: Requiring multiple independent forms of verification (e.g., a password combined with a time-based one-time token (TOTP) or a hardware security key) to authenticate users, thereby drastically reducing the risk of account compromise due to credential theft.
- **Role-Based Access Control (RBAC)**: Assigning permissions strictly based on user roles and responsibilities to enforce the principle of least privilege (PoLP). Access policies should be clearly defined, regularly reviewed, and automatically enforced across all system components to minimize the attack surface.
- **Continuous Monitoring & Auditing**: Implementing a comprehensive logging and monitoring solution that records all access attempts, privilege changes, and data transactions. Regularly auditing and updating access rights is essential to adapt to organizational changes and emerging threats. This audit trail is vital for forensic analysis and demonstrating compliance.

Implementing robust IAM policies helps prevent unauthorized access and potential misuse of resources, creating a secure and accountable operational environment.

2 9.2.2 Privacy-Preserving Mechanisms

Safeguarding user privacy is paramount for DPI. Key privacy-preserving mechanisms include:

2.1.1.1 9.2.2.1 Data Anonymization & Pseudonymization Techniques

- **Data Anonymization**: This process involves removing or modifying personal identifiers to prevent the association of data with specific individuals. Common techniques include data generalization and data permutation. The goal is to irreversibly prevent re-identification, though this can sometimes reduce the data's usefulness for analysis. Advanced methods exist to better balance privacy protection with data utility.
- **Pseudonymization**: This technique replaces real identifiers with artificial ones, or pseudonyms, reducing the linkability of a dataset with the original identity of an individual. Unlike anonymization, pseudonymization does not remove all identifying information but makes it more challenging to identify individuals without additional information. It is a vital tool for secure data processing and analytics. The "key" that can re-identify individuals must be stored separately and guarded with strong security controls, such as encryption and strict access limits.

2.1.1.2 9.2.2.2 Secure Multi-Party Computation & Homomorphic Encryption

- **Secure Multi-Party Computation (MPC)**: MPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. This ensures that no individual party can see the other parties' data, maintaining data privacy during collaborative computations. This enables valuable collaborations—like multiple banks jointly detecting fraud patterns or research institutions conducting combined health studies—without any participant having to expose their raw, sensitive data to the others.

- **Homomorphic Encryption**: This form of encryption permits computations to be performed directly on encrypted data without the need for decryption. The result, when decrypted, matches the outcome as if the operations had been performed on the original data, thereby preserving data confidentiality during processing. This powerful technology allows data to be processed securely in untrusted environments, like a public cloud, without ever decrypting it. While performance is improving, it is often used for specific, targeted operations.

2.1.1.3 **9.2.2.3 Privacy-Enhancing Technologies (PETs)**

Implementing privacy-preserving mechanisms in DPI helps ensure data protection and privacy by design, facilitating efficient integration and delivery of digital services while addressing ethical considerations associated with emerging technologies.

- **Differential Privacy**: By introducing controlled random noise to data queries, differential privacy ensures that the presence or absence of a single individual's data does not significantly affect the outcome, thus protecting individual privacy. It is a robust standard for releasing public aggregate data (e.g., traffic patterns, health statistics) while mathematically guaranteeing that no individual's information can be learned from the results.
- **Trusted Execution Environments (TEE)**: TEEs provide isolated environments within hardware where sensitive data can be processed securely, preventing unauthorized access or tampering during execution. TEEs are ideal for securing data while it is being used, enabling "confidential computing" where even the cloud provider cannot see the data.
- **Zero-Knowledge Proofs**: These cryptographic methods allow one party to prove to another that a statement is true without revealing any information beyond the validity of the statement itself. This is particularly useful in scenarios requiring verification without data exposure. This is revolutionary for enabling trust and verification without compromising privacy. For example, a user can prove they are over 18 without revealing their exact birthdate, or prove a transaction is valid without revealing any details about it.

9.3 Security Operation & Continuous Monitoring

Proactive security operations and planning are essential to anticipate, withstand, and recover from disruptions, ensuring continuous DPI operation amid cyber threats. This requires a shift from a reactive posture to a continuous, intelligence-driven security cycle, integrating people, processes, and technology.

3 **9.3.1 Continuous Monitoring & Threat Detection**

Proactive monitoring is vital for early threat detection:

- **Security Information and Event Management (SIEM)**: Aggregating and analyzing logs from various sources (network traffic, endpoints, servers, applications) to identify anomalies. Modern SIEM platforms integrate with threat intelligence feeds to correlate internal events with known global attack indicators (IOCs), providing critical context for alerts and reducing false positives.
- **AI-Driven Security Solutions:** Leveraging artificial intelligence and machine learning (ML) to detect subtle, evolving patterns indicative of advanced persistent threats (APTs) and zero-

day attacks that traditional signature-based tools might miss. These systems continuously learn from new data, improving their detection capabilities over time.

- **Extended Detection and Response (XDR):** Implementing XDR solutions provides a more unified view across multiple security layers (email, endpoint, cloud, network). By automatically correlating data from these integrated sources, XDR enables faster threat hunting and more comprehensive investigation and response capabilities.
- **Threat Intelligence Integration:** Consuming and leveraging curated threat intelligence is crucial for contextualizing internal alerts. Understanding the tactics, techniques, and procedures (TTPs) of relevant threat actors allows security teams to proactively hunt for signs of these specific behaviors within their DPI environment.

Continuous monitoring enables organizations to detect and respond to security incidents in a timely manner, drastically reducing mean time to detect (MTTD) and mean time to respond (MTTR).

4 **9.3.2 Incident Response & Crisis Management**

Effective incident response and crisis management are vital for minimizing the impact of cyber incidents:

- **Develop Comprehensive Incident Response Plans:** Establish clear procedures for detecting, analyzing, containing, eradicating, and recovering from security incidents. Plans should be aligned with established frameworks like NIST SP 800-61 and must include clear communication protocols for internal stakeholders, regulators, and law enforcement. Regularly update and test these plans through tabletop exercises and simulations to ensure effectiveness.
- **Crisis Management & Communication:** Developing strategies for managing large-scale cyber incidents with cross-organizational impact. This includes establishing a dedicated crisis command structure, preparing pre-approved communication templates for customers and the public, and managing public relations to protect the organization's reputation.
- **Conduct Regular Training and Simulations:** Equip staff with the necessary skills and knowledge through continuous training and simulated cyber-attack exercises to ensure preparedness. These exercises should test technical responses and decision-making under pressure, ensuring the entire team, from technical staff to executive management, understands their role during a crisis.
- **Staff Training and Awareness:** Equipping personnel with necessary skills through continuous training programs. Beyond the security team, all employees should receive regular awareness training to recognize and report potential security threats, such as phishing attempts, which are a common initial attack vector.

5 **9.3.3 Disaster Recovery & Business Continuity Planning**

Preparing for potential disasters ensures that DPI systems can quickly recover and maintain essential functions:

- **Develop Disaster Recovery Plans:** Create detailed strategies to restore hardware, applications, and data promptly after a disaster. This includes defining Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical systems, regular data backups, and establishing alternative data centers or cloud-based failover sites.

- **Establish Business Continuity Plans:** Outline procedures to continue critical business operations during and after a disaster, ensuring that essential functions remain operational. BCPs focus on the people and processes, ensuring that even if primary technical systems are unavailable, the organization can continue to serve its users and meet its obligations through predefined manual or alternative workflows.
- **Resilience Testing:** Regularly testing recovery and continuity capabilities through simulated outage scenarios. This includes conducting full-scale disaster recovery drills to fail over to backup systems and verifying that data can be restored from backups without corruption. The lessons learned from these tests must be used to continuously refine and improve the plans.
- **Geographic Redundancy:** For maximum resilience, critical DPI components should be deployed across geographically dispersed availability zones or regions. This mitigates the risk of a natural disaster or regional outage causing a complete service failure.

Implementing these guidelines will strengthen the resilience of DPI systems, ensuring their ability to withstand and recover from various challenges and threats.

9.4 Countering Emerging & Future Threats

DPI systems must be designed to adapt to and mitigate evolving threat landscapes, including those posed by emerging technologies like AI and quantum computing.

6 9.4.1 AI-Posed Security Threats & Mitigations

As AI becomes deeply integrated into DPI—including digital ID systems, public service delivery, health platforms, and financial services—there is a growing need to mitigate the security and safety risks that AI may pose. Global efforts like the EU AI Act, U.S. Executive Order on Safe, Secure, and Trustworthy AI, NIST AI Risk Management Framework, and China's Generative and Synthetic Content Labeling Measures offer valuable models for governance.

Table 8 AI Security Governance Recommendations for DPI

Measure	Description
Risk-Based Categorization of AI Systems	Classify AI systems used in DPI (e.g., biometric ID, predictive analytics, chatbots) into **risk tiers** (minimal, limited, high, and unacceptable), with stricter governance for high-risk applications.
Secure-by-Design Development	Enforce AI systems in DPI to be developed using **secure-by-design** and **privacy-by-design** principles. Mandate testing against adversarial attacks, model poisoning, and bias vulnerabilities.
Transparency and Explainability Standards	Require **model interpretability**, decision traceability, and audit logs for AI-enabled DPI services. Provide public disclosure for high-impact systems.

Measure	Description
Human Oversight & Accountability	Implement clear human-in-the-loop mechanisms and **accountability structures** for decision-making in critical DPI functions (e.g., public benefits adjudication or law enforcement applications).
Synthetic Content & Deepfake Governance	Apply **synthetic content identification** and watermarking in DPI media and communications to prevent misinformation and maintain public trust.
Cross-border Regulatory Alignment	Harmonize DPI AI governance with global best practices and support **international regulatory interoperability** through bilateral and multilateral frameworks.
AI Auditing & Certification	Mandate **regular independent audits**, red-teaming exercises, and certification of AI systems deployed in DPI environments. Create national registries for high-risk AI models.
Public Engagement & Redress Mechanisms	Include public consultations and grievance redress mechanisms for citizens affected by automated DPI decisions. Promote civic education on AI in public infrastructure.
Mitigation of Agentic AI Threats	Establish detection and response mechanisms for agentic AI-driven attacks, including behavioral analytics, anomaly detection, and dynamic policy adaptation.
Secure Federated Learning	Require robustness mechanisms (e.g., Byzantine-robust aggregation, gradient validation, secure parameter exchange) for distributed AI training.

7 9.4.2 Countermeasures for Post-Quantom Cryptography threats

Proactive planning and early adoption of quantum-resistant measures are crucial to protect DPI from the evolving threats posed by quantum technologies. The "Harvest Now, Decrypt Later" attack model, where adversaries collect encrypted data today for decryption once a quantum computer is available, makes immediate action imperative. A structured migration plan is essential to future-proof critical digital public infrastructure.

- **Transition to Post-Quantum Cryptography (PQC):** Develop and implement a phased strategy for adopting cryptographic algorithms resistant to quantum attacks. This begins with conducting a cryptoinventory to catalogue all systems using public-key cryptography (e.g., TLS, digital signatures, key exchange). Prioritize the migration of systems protecting highly sensitive data with long-term confidentiality requirements. Embrace Cryptographic Agility in system design—the ability to swiftly swap out cryptographic algorithms without overhauling entire systems—to facilitate smoother future transitions. Organizations should begin assessing their systems and planning migrations to PQC standards as defined by leading bodies like the U.S. NIST, which is finalizing its PQC Standardization Project.
- **Data Inventory and Classification:** Identify and prioritize the protection of sensitive data that requires long-term confidentiality, ensuring that critical information is safeguarded against future quantum threats. Data with a shelf-life extending beyond the anticipated advent of cryptographically-relevant quantum computers (CRQCs) is at greatest risk. This includes national identification data, health records, long-term legal documents, and classified government information. Encryption of this data must be upgraded to PQC standards at the earliest opportunity.
- **Infrastructure Assessment:** Evaluate existing DPI components (e.g., HSMs, root CA certificates, VPN concentrators, key management systems) to determine their vulnerabilities to quantum attacks and upgrade systems accordingly to support quantum-resistant protocols. Assessment must include evaluating dependencies on third-party vendors and service providers for their PQC migration roadmaps. Procuring new hardware and software should include contractual requirements for PQC readiness and support.
- **Collaboration and Standardization:** Engage with international cybersecurity bodies (e.g., ENISA, NIST), governmental agencies, and industry partners to stay informed about emerging PQC standards and best practices. Participation in industry consortia and information-sharing forums is critical for aligning national DPI strategy with global developments. This collaborative approach helps avoid fragmented solutions and ensures interoperability across borders and systems.
- **Workforce Training:** Invest in training programs to equip cybersecurity professionals, developers, and system architects with the knowledge and skills necessary to implement and manage quantum-resistant technologies. Building internal expertise on PQC concepts, migration challenges, and new API integrations is vital for a successful long-term strategy. Furthermore, supporting academic and industry initiatives to develop and vet PQC solutions will strengthen the overall security ecosystem.

Implementing a quantum-resistant strategy is not a one-time project but a long-term, ongoing process that must be integrated into the organization's overall cybersecurity and risk management lifecycle.

Appendix I

Best Practices of Secure DPI Implementation

<Editor’s Note: technical implementation details are to be included. Dedicated case studies of cities are needed.>

(This appendix lists some leading global cases of securing DPI implementations in smart cities.)

Governments and organizations worldwide have implemented best-in-class security frameworks to protect their DPI. Table I.1 shows a summary of some leading global cases showcasing secure, resilient, and scalable DPI implementations for smart cities:

Table I.1 Best Practices of Secure DPI Implementation Globally

Country – DPI Implementation	Best Practices	Impact
Estonia – X-Road (Secure Data Exchange Platform)	**- Decentralized Architecture:** Uses a distributed and federated model to ensure security and resilience. **- End-to-End Encryption (E2EE):** Ensures secure communication between government agencies and private sector entities. **- Blockchain for Integrity:** Uses KSI blockchain for tamper-proof logging of transactions. **- Zero-Trust Model:** Only authenticated and authorized entities can access data. **- Automated Threat Monitoring:** AI-driven cybersecurity measures detect and mitigate risks in real time.	- Zero major cyber breaches since its inception. - Secure interoperability among 1,000+ organizations while protecting citizen data privacy.
India – Aadhaar & UPI (Identity & Payment DPI)	**- Biometric & Multi-Factor Authentication (MFA):** Aadhaar uses fingerprint, iris, and OTP-based authentication to prevent identity fraud. **- Tokenization & Privacy Safeguards:** Virtual IDs replace Aadhaar numbers in transactions to enhance data security. **- Regulatory Frameworks:** Strong legal backing (Aadhaar Act, Personal Data Protection Bill) for data privacy and security compliance. **- AI-Based Fraud Detection:** Continuous monitoring of transactions using machine learning algorithms to detect anomalies. **- Resilient Digital Payment Infrastructure (UPI):** Secure and real-time interoperable digital payment system with fraud detection mechanisms.	- Over 1.3 billion registered users securely use Aadhaar for authentication. - UPI processes over 16 billion transactions monthly as of early 2025.
Brazil – Pix (Secure Real-Time Payment System)	**- Centralized and Federated Security Model:** The Brazilian Central Bank enforces strict cybersecurity protocols for participants. **- ISO 27001 Compliance:** Ensures secure handling of financial transactions. **- Multi-Layered Fraud Prevention:** Uses behavioral biometrics and AI-driven fraud detection. **- Instant Transaction Monitoring:** Real-time flagging and blocking of suspicious transactions. **- Secure API-Driven Interoperability:** Banks and fintechs integrate securely with Pix's encrypted APIs.	- Processes over 6 billion monthly transactions in Q4 2024. - AI-driven fraud prevention has reduced customer friction by 89%.
Singapore – Singpass (Secure Digital Identity)	**- Multi-Factor & Passwordless Authentication:** Uses FIDO2-based biometric authentication for secure logins.	- Over 4.2 million users actively use the Singpass app.

Country – DPI Implementation	Best Practices	Impact
	- Decentralized Data Storage: Minimizes risks of single-point failures and mass data breaches. **- Privacy by Design:** Users control what data is shared with government and third parties. **- End-to-End Encryption (E2EE):** Ensures confidentiality of identity-related transactions. **- Cybersecurity Threat Intelligence Sharing:** Proactive threat monitoring & national-level security collaboration.	- Facilitates over 41 million transactions monthly. - Singpass Digital Identity has never suffered a major breach.
Japan – My Number System (Secure Digital Identity)	**- Centralized Digital Identity with Privacy Safeguards:** The My Number system assigns a unique 12-digit identifier to residents, integrating personal data securely across government services under the Act on Protection of Personal Information (APPI). **- Multi-Factor Authentication (MFA):** Uses IC chip-enabled cards with PINs and biometric options for secure access to services. **- End-to-End Encryption (E2EE):** Ensures secure data transmission between government agencies and citizens. **- Regulatory Framework:** Strict compliance with APPI and oversight by the Personal Information Protection Commission (PPC) to protect citizen data. **- Cybersecurity Measures:** Collaboration with the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) for threat monitoring and incident response.	- Over 70% of Japan's population (approximately 90 million people) registered with My Number cards by 2024. - Enables secure access to public services, tax filing, and healthcare, streamlining administrative processes. - No major data breaches reported
European Union – eIDAS & GDPR Compliance	**- Strong Regulatory Frameworks (GDPR & eIDAS):** Defines security & privacy mandates for DPI across all EU nations. **- Cross-Border Digital Identity Authentication:** Secure mutual recognition of national digital identities. **- End-to-End Encryption & Secure Digital Signatures:** Uses PKI-based cryptography to ensure data security. **- Zero-Knowledge Proofs (ZKP):** Enables privacy-preserving authentication for digital ID verification. **- Cyber Resilience Strategy:** Includes regular cybersecurity stress testing & incident response drills.	- 27 EU nations securely interoperate using eIDAS-compliant digital services. - GDPR has strengthened legal compliance in DPI security.

Country – DPI Implementation	Best Practices	Impact
United States – Login.gov (Secure Digital Identity)	**- Single Sign-On (SSO) with Strong Authentication:** Provides a unified, secure login for accessing federal services using multi-factor authentication (MFA), including biometrics and security keys. **- Privacy by Design:** Adheres to NIST 800-63-3 guidelines, ensuring user data is not centralized and is only shared with explicit consent. **- End-to-End Encryption (E2EE):** Secures data transmission between users and government systems. **- Interoperability and Open Standards:** Built on open protocols (e.g., SAML, OpenID Connect) to ensure compatibility across federal agencies. **- Continuous Security Monitoring:** Leverages CISA's cybersecurity guidance and regular audits to maintain system integrity.	- Used by over 50 million users across 200+ federal and state services as of 2024. - Reduces credential sprawl, lowering risk of phishing and identity theft. - No major breaches reported.
China –eID & WeChat Pay/Alipay (Secure Digital Identity & Secure Fintech DPI)	**- Unified Digital Identity System:** eID (Electronic ID) is integrated into China's Resident Identity Card and used for secure authentication. **- Multi-Factor Authentication & AI-Based Fraud Detection:** Uses biometric authentication (facial recognition & fingerprint scanning) for transactions. **- Privacy & Data Encryption:** Implements homomorphic encryption and zero-knowledge proof (ZKP) to enhance user data privacy. **- Cybersecurity Law & Data Protection Compliance:** Strict legal mandates under the China Cybersecurity Law and Personal Information Protection Law (PIPL) enforce DPI security. **- Secure Digital Payments Ecosystem (WeChat Pay & Alipay):** Uses real-time fraud detection, AI-based risk analysis, and advanced tokenization to prevent cyber threats.	- 1 billion+ users securely access digital public services via eID authentication. - WeChat Pay & Alipay process trillions of dollars in secure transactions annually. - Minimal fraud incidents due to AI-driven monitoring and secure payment protocols.

To conclude, the world's best practices of secure DPI implementations focus on privacy, encryption, multifactor authentication, fraud prevention, and resilience. Countries that adopt a multi-layered cybersecurity approach, AI-driven threat detection, and regulatory enforcement are better positioned to protect their DPI against cyber threats, fraud, and privacy risks.

Bibliography

[Editor's Note: Bibliography Section to be checked and formatted according to Author's guide for drafting ITU-T Recommendations]

1. Cybersecurity Framework Version 2.0, National Institute of Standards and Technology (NIST), https://www.nist.gov/cyberframework
2. Regulation (EU) 2024/1689 on Artificial Intelligence Act (EU AI Act), Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
3. General Data Protection Regulation (EU) 2016/679 (GDPR), European Parliament and Council, https://gdpr-info.eu/
4. eIDAS Regulation (2024). Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 on Electronic Identification and Trust Services, Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183
5. Global Cybersecurity Outlook 2025, World Economic Forum, https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
6. ENISA Threat Landscape Report 2024. European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
7. Digital public infrastructure for digital governments, OECD, https://www.oecd.org/en/publications/digital-public-infrastructure-for-digital-governments_ff525dc8-en.html
8. UIDAI Annual Report 2023-2024. Unique Identification Authority of India.URL: https://www.uidai.gov.in/en/2024-report-uidai-annual
9. Annual Report 2024, Central Bank of Brazil (BCB), https://www.bcb.gov.br/content/publications/Annual_Report_docs/AR-2024.pdf
10. Singpass Service Metrics 2024, Infocomm Media Development Authority (IMDA Singapore), https://www.imda.gov.sg/business
11. Riding the Wave of Digital Transformation: Insights from Japan's Journey, World Bank Group, https://documents1.worldbank.org/curated/en/099352305232428567/pdf/P177977145b03308b19ef61f321c4e404f4.pdf
12. Transition to Post-Quantum Cryptography Standards, NIST, https://csrc.nist.gov/pubs/ir/8547/ipd
13. Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, NIST, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf
14. NISTIR 8105 Report on Post-Quantum Cryptography, NIST, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
15. Malaysia Cyber Security Strategy 2020-2024, https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf
16. The Singapore Cybersecurity Strategy 2021, https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf