DATA EMBASSIES

An innovative approach to strengthening digital resilience in the Caribbean

Tira Greene
Demetris Herakleous

UNITED NATIONS
ECLAC

Global Gateway
EU-LAC Digital Alliance

UE ALC
DIGITAL ALLIANCE
POLICY DIALOGUES

Thank you for your interest in this ECLAC publication

UNITED NATIONS

ECLAC

Please register if you would like to receive information on our editorial products and activities. When you register, you may specify your particular areas of interest and you will gain access to our products in other formats.

Register

Click on the link below for our social networks and other channels for accessing our publications:

https://bit.ly/m/CEPAL

Project Documents

Data embassies

An innovative approach to strengthening digital resilience in the Caribbean

Tira Greene
Demetris Herakleous

UNITED NATIONS
ECLAC
Global Gateway
EU-LAC Digital Alliance
EU-LAC
DIGITAL ALLIANCE
POLICY DIALOGUES

This document was prepared by Tira Greene, consultant with the Division of Production, Productivity and Management of the Economic Commission for Latin America and the Caribbean (ECLAC), under the coordination of Demetris Herakleous, Associate Economic Affairs Officer in the same division, and with support from Donna Esposito and Alexander Gafoor.

The contributions from Dale Alexander, Programme Management Officer at ECLAC subregional headquarters for the Caribbean, and Lika Diouf, Associate Programme Management Officer at ECLAC subregional headquarters for the Caribbean at the time of writing, are gratefully acknowledged. Thanks are also owed to Vincent Roberts, Tira Renier, Fazal Ali and Kavel Joseph, members of the Digital Agenda for Latin America and the Caribbean (eLAC) working group for the Caribbean, for their valuable inputs and expert feedback provided during the preparation of this document.

This publication was prepared within the framework of the European Union–Latin America and the Caribbean Digital Alliance and was financed by the European Union, through the Global Gateway strategy.

United Nations publication
LC/TS.2025/99
Distribution: L

Printed at United Nations, Santiago
S.2500535[E]

This publication should be cited as: Greene, T. and Herakleous, D. (2025). Data embassies: an innovative approach to strengthening digital resilience in the Caribbean. *Project Documents* (LC/TS.2025/99). Economic Commission for Latin America and the Caribbean.

Contents

Tables

Diagram

Acronyms

AI:	Artificial Intelligence
APEC:	Asia-Pacific Economic Cooperation
ARCOS:	Americas Region Caribbean Optical-ring System
ARIN:	American Registry for Internet Numbers
ARSIWA:	Articles on Responsibility of States for Internationally Wrongful Acts
AWS:	Amazon Web Services
BTS:	Base Transceiver Station
CAPEX:	Capital Expenditure
CARIBNOG:	Caribbean Network Operators Group
CARICOM:	Caribbean Community
CBPR:	Cross-Border Privacy Rules
CBU:	Caribbean Broadcasting Union
CCJ:	Caribbean Court of Justice
CCRIF:	Caribbean Catastrophe Risk Insurance Facility
CDEMA:	Caribbean Disaster Emergency Management Agency
CDN:	Content Delivery Network
CERT:	Computer Emergency Response Team
CJIS:	Criminal Justice Information Services
CIGF:	Caribbean Internet Governance Forum
CIS:	Center for Internet Security
CLS:	Cable Landing Station
CLOUD:	Clarifying Lawful Overseas Use of Data Act
CONSLE:	Council for National Security and Law Enforcement (CARICOM)
CROSQ:	Caribbean Regional Organisation for Standards and Quality
CSP:	Cloud Service Provider
CSF:	Cybersecurity Framework (NIST)
CSIRT:	Computer Security Incident Response Team
CTU:	Caribbean Telecommunications Union
DC:	Data Center
DD:	Due Diligence
DDoS:	Distributed Denial of Service
DMA:	Digital Markets Act

DNS:	Domain Name System
DO:	Disaster Recovery (DR)
DRS:	Disaster Recovery Service (AWS)
DSA:	Digital Services Act
DPIA:	Data Protection Impact Assessment
ECLAC:	Economic Commission for Latin America and the Caribbean
ECCB:	Eastern Caribbean Central Bank
ECCU:	Eastern Caribbean Currency Union
EEA:	European Economic Area
EDFA:	Erbium-Doped Fiber Amplifier
ENISA:	EU Agency for Cybersecurity
EOC:	Emergency Operations Centre
ETA:	Electronic Transactions Act
ETC:	Emergency Telecommunications Cluster
EU:	European Union
FIRST:	Forum of Incident Response and Security Teams
FRP:	Fiber-Reinforced Plastic
GCC:	Gulf Cooperation Council
GCI:	Global Cybersecurity Index
GCP:	Google Cloud Platform
GDPR:	General Data Protection Regulation
GSMA:	GSM Association
HAPS:	High-Altitude Platform Station
HSM:	Hardware Security Module
ICT:	Information and Communication Technology
ICJ:	International Court of Justice
IDB:	Inter-American Development Bank
IEC:	International Electrotechnical Commission
IFRC:	International Federation of Red Cross and Red Crescent Societies
IHL:	International Humanitarian Law
IHRL:	International Human Rights Law
ILC:	International Law Commission
IOC:	Indicator of Compromise
ISMS:	Information Security Management System

ISO:	International Organization for Standardization
ISO/IEC:	Joint ISO and IEC standards
IT:	Information Technology
ITAR:	International Traffic in Arms Regulations
ITIL:	Information Technology Infrastructure Library
ITU:	International Telecommunication Union
ITU-D:	ITU Development Sector
KMS:	Key Management System
KPI:	Key Performance Indicator
KSI:	Keyless Signature Infrastructure (blockchain)
LAC:	Latin America and the Caribbean
LACNIC:	Latin American and Caribbean Internet Addresses Registry
LEO:	Low-Earth-Orbit satellite
LTE:	Long-Term Evolution
MFA:	Multi-Factor Authentication
MLA:	Mutual Legal Assistance
MLAT:	Mutual Legal Assistance Treaty
MNO:	Mobile Network Operator
MoU:	Memorandum of Understanding
MPLS:	Multiprotocol Label Switching
MTPD:	Maximum Tolerable Period of Disruption
MTTR:	Mean Time to Recovery/Repair
MVNO:	Mobile Virtual Network Operator
MW:	Megawatt
NAP:	Network Access Point
NEMO:	National Emergency Management Organization
NetBlocks:	Internet Outage Observatory
NIS2:	Network and Information Security Directive (EU)
NIST:	National Institute of Standards and Technology
NJFX:	New Jersey Fiber Exchange
OPEX:	Operating Expenditure
ODF:	Optical Distribution Frame
OECS:	Organisation of Eastern Caribbean States
OECD:	Organisation for Economic Co-operation and Development

PDNA:	Post-Disaster Needs Assessment
PIPL:	Personal Information Protection Law (China)
PKI:	Public Key Infrastructure
POP:	Point of Presence
POS:	Point of Sale
PPP:	Public–Private Partnership
RPO:	Recovery Point Objective
RTO:	Recovery Time Objective
SBOM:	Software Bill of Materials
SCADA:	Supervisory Control and Data Acquisition
SIDS:	Small Island Developing States
SLA:	Service-Level Agreement
SIEM:	Security Information and Event Management
SOC (Audit):	Service Organization Control (audit standard)
SOC (Security:	Security Operations Center
SOFA:	Status of Forces Agreement
SP:	Special Publication (NIST series)
TB:	Terabyte
TIA:	Telecommunications Industry Association
TT-CSIRT:	Trinidad and Tobago Cyber Security Incident Response Team
TSF:	Télécoms Sans Frontières
UE:	User Equipment
UN:	United Nations
UNDP:	United Nations Development Programme
UNESCO:	United Nations Educational, Scientific and Cultural Organization
UPS:	Uninterruptible Power Supply
US:	United States
USAID:	United States Agency for International Development
VCCR:	Vienna Convention on Consular Relations
VCDR:	Vienna Convention on Diplomatic Relations
VSAT:	Very Small Aperture Terminal
WFP:	World Food Programme
WMO:	World Meteorological Organization
WTO:	World Trade Organization

Introduction

The Caribbean, composed predominantly of Small Island Developing States (SIDS), is at a critical juncture where digital transformation has evolved from discretionary policy to structural necessity vis-à-vis sustainable development. Digital infrastructure now forms the backbone of economic modernization, inclusive public services, and climate resilience. Yet this infrastructure is beset by an expanding array of systemic threats that are growing in severity.

The region's digital resilience increasingly depends on digital assets such as cloud platforms hosting government registries, submarine cables facilitating real-time financial transactions, and data centers powering emergency-response systems. However, the same geographical attributes that support tourism and maritime trade also expose these digital systems to some of the world's most severe natural hazards. Over the past two decades, hurricanes, flooding, and seismic activity have repeatedly demonstrated how the disruption of a single cable or the inundation of a data facility can paralyze public service delivery, disrupt commercial activity, and obstruct humanitarian operations across entire island states.

Defining digital infrastructure and its foundational role

Digital solutions offer a broad spectrum of benefits, significantly enhancing the quality of services, optimizing resource allocation, and fostering sustainability across diverse sectors.[1] This transformation extends to critical domains such as healthcare, education, and the management of public services.[2] The establishment of robust digital infrastructure, coupled with the cultivation of

[1] Pfeifer, M. (2023, July 28). Modernizing physical infrastructure to boost economic development. Moviliblog. https://blogs.iadb.org/transporte/en/modernizing-physical-infrastructure-to-boost-economic-development/.

[2] Caribbean Telecommunications Union. (2024, May). *Adopting a Tier 4 modular data center as a regional data embassy.* https://ctu.int/wp-content/uploads/2024/05/Adoption-of-T4-Modular-Data-Center-as-Regional-Data-Embassy_School-of-DTI-Presentation80.pdf.

relevant Information and Communication Technology (ICT) skills, is widely recognized as indispensable for stimulating job creation and driving inclusive economic growth throughout the region.[3]

Digitalization is widely seen as a powerful driver of economic resilience, social inclusion, and climate adaptation. For the Caribbean, it offers a unique opportunity to overcome historical challenges, modernize public services, improve disaster risk management, and access global markets.[4]

The physical components underpinning this infrastructure are varied including essential elements such as fibre-optic cables, data centers, and cellular towers. Beyond these tangible assets, broader enablers like reliable electricity and pervasive internet connectivity are equally crucial.[5] A resilient and accessible infrastructure is paramount for supporting digital activities across all sectors, thereby establishing the groundwork for sustained growth and development.

Against this backdrop, the United Nations has commissioned this study to examine how the region can strengthen its digital infrastructure and guarantee service continuity when the next disaster strikes. The mandate is precise: assess current vulnerabilities, model the potential economic and social losses of digital-infrastructure failure, evaluate the feasibility of "Data Embassy" arrangements, and produce actionable policy, legal, and investment recommendations for Caribbean governments and their partners.

Cybersecurity, disasters, and the future of government continuity

The accelerated digitalization of government operations —from e-tax systems and national identity registries to disaster response platforms and public health databases— has fundamentally transformed the strategic role of **data continuity** in ensuring state functionality. As states digitize their core public services, the uninterrupted availability of data becomes not merely technical infrastructure, but the backbone of sovereignty and operational stability. This transformation inevitably elevates data from a background asset to a high-stakes national resource. As such, Governments now face heightened risk exposure as their digital systems become both more central and more vulnerable.

In this context, Estonia offers a compelling model. Its Data Embassy initiative externalizes critical datasets to secure, sovereign-controlled facilities abroad, enabling government operations to continue even if domestic infrastructure is compromised. Originally conceived with military and political risks in mind —such as invasion or regime collapse— the model leverages bilateral agreements grounded in the Vienna Convention to grant legal immunity to digital assets hosted in stable partner states. For the Caribbean, adapting this approach presents a sustainable path to preserving government continuity during crises, while fully maintaining national sovereignty.

Cyberattacks (which was the motivation behind the Estonian initiative) —especially ransomware campaigns targeting public institutions— have become a major disruptor of government operations. The 2022 Conti and Hive attacks in Costa Rica disrupted approximately 30 government agencies —including ministries of finance, customs, and social security— prompting a national emergency that halted digital tax filings and major health services. Estimated losses exceeded US $30 million per day, and recovery stretched over multiple months.[6] This episode demonstrated that cyber-threats can be as crippling as natural disasters or war. The modes of failure —such as inaccessible encrypted databases,

---

[3] World Bank. (2025, April 15). *The Caribbean connection: Building digital jobs in the Caribbean.* World Bank. https://www.worldbank.org/en/results/2025/04/15/caribbean-connection-building-digital-jobs-latin-america.

[4] Development Bank of Latin America (CAF). (n.d.). *CAF strengthens digital governance capacity in 13 Caribbean countries.* CAF. https://www.caf.com/en/currently/news/caf-strengthens-digital-governance-capacity-in-13-caribbean-countries/.

[5] United Nations Development Programme. (2024, April 19). *Defining the pathway for small island digital states in the Caribbean.* UNDP. https://www.undp.org/sites/g/files/zskgke326/files/2024-09/sids_2.0_-_position_paper_19_april_2024.pdf.

[6] Vizcaíno, I., Salas, L., Fernando, J., & Recio, P. (2022, April 20). Hacienda, Micitt, IMN, RACSA Y CCSS Atacados Por "hackers", confirma gobierno. La Nación. https://www.nacion.com/el-pais/servicios/hacienda-micitt-imn-y-racsa-atacados-por-hackers/DMCT7BZYIZGHZIHQQPOKN2WWYM/story/.

compromised governance systems, or exposed citizen records— can undermine both service continuity and public trust. To guard against these risks, critical data must be mirrored in redundant repositories outside the domestic network in the form of Data embassies that maintain sovereignty.

Diplomacy meets infrastructure

Data embassies represent a novel solution designed to ensure a government's digital continuity, enabling critical databases and digital services to persist even when domestic operations are disrupted due to natural disasters, large-scale cyberattacks, or military conflict. Defined as sovereign servers located abroad, data embassies integrate legal and technical frameworks to protect sensitive state data from external interference. Generally, bilateral agreements based on the principles of the Vienna Convention on Diplomatic Relations guarantee immunity for the hosted data and infrastructure, preserving full legal control under the sending state's jurisdiction —when stored outside national territory.[7] Although these treaties were originally created for physical diplomatic premises, evolving diplomatic and consular law increasingly recognizes the inviolability of electronic documents. Consequently, a cyberattack targeting a data embassy could be interpreted as a breach of the sovereignty of both the sending and receiving states.[8]

The Estonia–Luxembourg model exemplifies this approach. In this case, a bilateral agreement ratified by both parliaments grants data hosted in Luxembourg the same inviolability and immunity status as diplomatic premises, exempting the archives from search, requisition, or enforcement actions by the host country.[9]

Trinidad and Tobago's initiative to deploy a Tier 4 Modular Data Center as a Regional Data Embassy for the Caribbean reflects the application of this concept in a developing regional context. By offering both shared and dedicated hosting options and leveraging the region's extensive submarine cable network, the project aims to enhance secure digital infrastructure across Caribbean SIDS. Key elements of the project include a highly resilient (Tier 4) data infrastructure, robust backup and fail-over systems, and a comprehensive bilateral agreement ensuring the confidentiality, integrity, and availability of data.[10]

Pashed research methodology and report outline

To fulfil the terms of reference, this report adopts a mixed-methods approach across four phases:

- Phase 1 involves comprehensive data-gathering and baseline mapping (covering broadband density, data-centre capacity, and the regulatory and institutional frameworks for digital infrastructure).
- Phase 2 builds on this baseline with hazard-impact and economic-loss modelling to assess potential vulnerabilities. In parallel, a technical and legal feasibility review of the Data Embassy model is undertaken to determine its applicability and resilience in the regional context.

---

7 Bishop, M., Girvan, N., Shaw, T., Mike, S., Kirton, R., Mohammed, D., & Anatol, M. (2011, April). Caribbean Regional Integration - A report by the UWI Institute of International Rel Ations (IIR) | Caricom. Caribbean Regional Integration. https://drupal.caricom.org/documents/caribbean-regional-integration-report-uwi-institute-international-rel-ations-iir.

8 NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Diplomatic and consular law – International cyber law.* CCDCOE. https://cyberlaw.ccdcoe.org/wiki/Diplomatic_and_consular_law.

9 Druva. (2025). *Master the 3-2-1 backup rule: Your ultimate data protection plan.* Druva. https://www.druva.com/glossary/3-2-1-backup-rule.

10 Caribbean Telecommunications Union. (2024, May). *Adopting a Tier 4 modular data center as a regional data embassy.* CTU. https://ctu.int/wp-content/uploads/2024/05/Adoption-of-T4-Modular-Data-Center-as-Regional-Data-Embassy_School-of-DTI-Presentation80.pdf.

- Phase 3 focuses on identifying key structural and policy barriers to implementing secure and resilient digital infrastructure, through a participatory process of co-designing regionally tailored solution packages with stakeholders.
- Phase 4 involves legal review and vetting of proposed solutions, followed by stakeholder validation workshops to develop a consensus-driven roadmap for implementation (including any necessary regulatory and institutional reforms).

The results of these efforts are structured into the following components:

(i) a quantified vulnerability and risk profile;

(ii) a region-specific feasibility assessment of Data Embassy models;

(iii) a synthesis of structural obstacles and pathways to resilient infrastructure;

(iv) an analysis of data sovereignty and cross-border legal issues; and

(v) an extended Analysis of the International Legal Framework and Exploration of Necessary Adaptations a set of final policy, financing, and capacity-building recommendations designed to embed digital resilience at the heart of Caribbean disaster-preparedness strategies.

In short, this report provides the evidence-based roadmap needed for Caribbean states to transform their digital infrastructure from a vulnerability into a resilient, sovereign asset capable of withstanding the region's growing climate threats.

I. The Data Embassy as a paradigm for digital state continuity

A. Digital sovereignty and resilience in an age of existential threats

The contemporary state is inextricably built upon a digital foundation and its core functions, namely the administration of justice, management of the economy and the delivery of essential public services, are tied to digital infrastructure. National identity itself is encoded into digital registries vis-á-vis census data, land ownership, and business incorporation. In some advanced digital societies, these records exist only in digital form, with no paper trail. While a source of efficiency and innovation, this dependency creates a new and critical vector of national vulnerability, cyber security.

When a nation's legal and administrative memory is primarily digital, protecting that data becomes synonymous with protecting the state's existence. This reality has given rise to a new strategic imperative for governments: ensuring **digital continuity**. This concept transcends traditional IT disaster recovery; it is defined as the capacity to preserve critical databases and maintain core state functions even when domestic infrastructure is compromised, or the state's physical territory is rendered inoperable. Digital continuity is about ensuring the very survival of the state as a functioning legal and administrative entity in the face of catastrophic events.[11] It represents a fundamental evolution in thinking, moving the conversation from data security to state survival.

The threats that necessitate such a robust strategy are varied and constantly evolving. They cover a spectrum of risks that can undermine a nation's sovereignty and its ability to govern.

- **Catastrophic natural disasters:** for many nations, and particularly for Small Island Developing States (SIDS) in regions like the Caribbean, the most immediate existential threat comes from nature. A single powerful hurricane, earthquake, or tsunami can physically

[11] Organisation for Economic Co-operation and Development. (2017). *Establishing the first data embassy in the world.* Observatory of Public Sector Innovation (OPSI). https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/.

destroy national data centres, sever telecommunications links, and obliterate the physical infrastructure upon which the digital state relies.

- **Large-scale cyberattacks:** state-sponsored or sophisticated non-state actors can launch cyber operations designed to paralyze a nation's digital backbone. The seminal 2007 distributed denial-of-service (DDoS) attacks against Estonia demonstrated how quickly a coordinated digital assault could bring a country's government, banking, and media services to a halt, effectively severing the state from its citizens and the world.
- **Military invasion and geopolitical instability:** in the most extreme scenarios of military conflict or occupation, a government may lose control of its physical territory. In such a government-in-exile situation, the ability to access and operate critical state databases from a secure, external location becomes the sole means of preserving legitimate governance and continuing to provide services to citizens and the international community.[12]

In response to these complex threats a novel solution has emerged at the intersection of international law, diplomacy, and technology. The Data Embassy represents a new paradigm for ensuring digital state continuity. It offers a unique synthesis of legal immunities, diplomatic agreements, and resilient technical architecture designed to safeguard a nation's digital heart against the most severe crises.

B. Conceptual and historical foundations of the Data Embassy

A **Data Embassy** is a diplomatic-style arrangement wherein a host country grants a sending state legal jurisdiction over servers physically located on its soil.

A Data Embassy´s Key distinguishing features are:

- **Legal inviolability**: host-state courts and security agencies cannot seize or compel data access without the sending state's consent.
- **Bilateral or multilateral treaty basis**: requires formal ratification, often modelled on Vienna Convention protocols but specifically tailored for digital infrastructure.
- **Dedicated network links**: encrypted, high-speed circuits connect home country and embassy for real-time replication.

The concept of Data Embassy was born from necessity in Estonia. In 2007, the country suffered a series of crippling DDoS attacks, that served as a global "wake-up call" to the reality of cyber warfare.[13] For Estonia, a pioneer of digital governance with its comprehensive "e-Estonia" platform and a national "paperless policy," this attack exposed a critical vulnerability. The potential loss of its digital-only state records —from laws to land titles— was not an inconvenience; it was an existential threat. This imperative drove the "Data Embassy Initiative," a key component of the nation's 2014-2017 Cyber Security Strategy. Estonian policymakers recognized that simply placing servers in their traditional embassies abroad was not a viable solution; these facilities lacked the specialized technical infrastructure, crisis response competence, and resilient connectivity required for such a critical function. The search for a viable partner culminated on June 20, 2017, when Estonia signed a landmark agreement with the Grand Duchy of Luxembourg to establish the world's first Data Embassy, setting a powerful precedent in international law and digital statecraft.

---

[12] ComplexDiscovery. (2025). *Data embassies: Sovereignty, security, and continuity for nation-states.* ComplexDiscovery. https://complexdiscovery.com/data-embassies-sovereignty-security-and-continuity-for-nation-states/.

[13] Altwicker, T. (2022). *The data embassy under public international law. International & Comparative Law Quarterly*, *71*(3), 689–714. Cambridge University Press. https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/data-embassy-under-public-international-law/A1915132C9DB447C8.

The following subsections outline the core advantages of this model —ranging from protection against cyber risks and high availability to guarantees of sovereign continuity and resilience in the face of natural hazards— while also noting some of the inherent challenges and trade-offs that governments must consider in implementation.

1. Benefits

Cyber-risk reduction

- Isolation from domestic attack vectors
  - A Data Embassy is under the legal jurisdiction of the sending state —even though it sits on foreign soil— granting it immunity from host-state seizure or access requests. Thus, a ransomware outbreak or insider breach targeting domestic systems cannot infect or compromise the off-site replicas.[14]
  - Critically, because the embassy's infrastructure is operated and controlled by the sending state, attacks on major commercial clouds (e.g., AWS, Azure) have no bearing on its availability. As one expert notes, "a cyberattack against Microsoft or AWS cannot bring down Estonia's e-governance cloud because Estonia's e-governance cloud is managed by Estonia."[15]
- Resilience to large-scale ddos campaigns
  - Estonia's experience in April–May 2007 —when coordinated botnet assaults paralyzed government portals and banking services for weeks— underscored the need for geographically isolated, immune-status backups. A Data Embassy, by design, remains unreachable through the same network paths under attack, ensuring that critical services can be restored from a "clean" environment.[16]

Proven high availability

- Tier-IV uptime guarantees
  - Data embassies are typically requested to be housed in Tier IV data centers, which by Uptime Institute standards must deliver **99.995% availability** (i.e., < 26.3 minutes of downtime per year) and tolerate any single failure without service interruption.[17]
  - In practice, the Estonian Data Embassy in Luxembourg reports **< 0.4 hours** of downtime annually —meeting strict four-nines thresholds— and leverages 2N+1 redundancy, dual power grids, and parallel cooling systems to uphold fail-safe operations.[18]

---

[14] Electronic Discovery Reference Model. (2022, March). *Data embassies: Sovereignty, security, and continuity for nation-states.* EDRM. https://edrm.net/2022/03/data-embassies-sovereignty-security-and-continuity-for-nation-states/; Google Cloud. (2022, November 11). *Data embassies: Strengthening resiliency with sovereignty.* Google Cloud. https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty.

[15] Murdock, J. (2019, October 10). *Estonia's digital embassies and the concept of sovereignty.* Georgetown Security Studies Review. https://georgetownsecuritystudiesreview.org/2019/10/10/estonias-digital-embassies-and-the-concept-of-sovereignty/.

[16] Traynor, I. (2007, May 17). *Russia accused of unleashing cyberwar to disable Estonia. The Guardian.* https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[17] Uptime Institute. (n.d.). *Tier classification system.* Uptime Institute. https://uptimeinstitute.com/tiers.

[18] Caribbean Telecommunications Union. (2024, May). *Adopting a Tier 4 modular data center as a regional data embassy.* CTU. https://ctu.int/wp-content/uploads/2024/05/Adoption-of-T4-Modular-Data-Center-as-Regional-Data-Embassy_School-of-DTI-Presentation 80.pdf.

- Automated fail-over mechanisms
  - Active-active replication, coupled with health-check-driven DNS failover (TTL ≤ 60 s), enables sub-minute traffic redirection to the embassy site if the primary data path falters.[19]
  - This means that legitimate users experience near-seamless continuity for e-services —even under extreme cyber or physical stress.

Sovereign continuity

- Uninterrupted e-government operations
  - Estonia's "paperless governance" relies on digital-only registers (land, business, court filings) that have no physical analogues. A Data Embassy safeguards these "digital monuments," preserving both their evidential value and real-time functionality.[20]
  - Should domestic infrastructure be compromised —by attack or outage— the embassy ensures that courts can continue issuing judgments, land titles can be verified, and tax systems remain operational, thereby upholding the rule of law and public trust.
- Legal inviolability
  - By treaty, host-state authorities cannot compel data access or seize servers; all actions require the sending state's explicit consent. This diplomatic-style immunity guarantees that sovereign data rights transcend shifting geopolitical or regulatory pressures.[21]

Natural disaster resilience

- **Geographic dispersion.** Locating backups at least 50 km away from primary sites (a best practice recognized by small states) protects against region-wide catastrophes —hurricanes, volcanic eruptions, or grid failures— that could knock out all local facilities simultaneously.[22]
- **Fault-tolerant infrastructure**. Tier IV centers must provide:
  - **2N+1 redundancy** (double the necessary capacity plus one backup component).
  - **96 hours of independent on-site power** (e.g., diesel generators, battery banks).
  - **Continuous cooling** and full airtight fire suppression systems.
  - **No single points of failure**, ensuring uninterrupted operations even during major equipment failures.
- **Rapid recovery protocols**. Automated DNS and database-level switching enable service fail-over in under a minute once health checks detect an outage, fulfilling stringent recovery-time objectives for mission-critical government systems.[23]

---

[19] Amazon Web Services. (n.d.). *Amazon Route 53 FAQs.* AWS. https://aws.amazon.com/route53/faqs/; HostDime. (n.d.). *Tier 4 data center.* HostDime. https://www.hostdime.com/tier-4-data-center.

[20] e-Estonia. (n.d.). *Data embassy.* e-Estonia. https://e-estonia.com/solutions/e-governance/data-embassy/.

[21] Electronic Discovery Reference Model. (2022, March). *Data embassies: Sovereignty, security, and continuity for nation-states.* EDRM. https://edrm.net/2022/03/data-embassies-sovereignty-security-and-continuity-for-nation-states/; Organisation for Economic Co-operation and Development. (2017). *Establishing the first data embassy in the world.* Observatory of Public Sector Innovation (OPSI). https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/.

[22] Google Cloud. (2022, November 11). *Data embassies: Strengthening resiliency with sovereignty.* Google Cloud. https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty.

[23] Amazon Web Services. (n.d.). *Amazon Route 53 FAQs.* AWS. https://aws.amazon.com/route53/faqs/; HostDime. (n.d.). *Tier 4 data center.* Host Dime. https://www.hostdime.com/tier-4-data-center?srsltid=AfmBOoqBS2B5gfkV8RmJ2cqG4Rh9RtDttmijvyy_i_l4D nhG7EHaUZJ9.

2. Challenges

Complex legal negotiations

- Treaty drafting & ratification
  - **Multistage negotiation**: establishing a Data Embassy requires negotiating a bespoke bilateral treaty —defining inviolability, operational scope, data categories, encryption and key-escrow arrangements— which typically span **12–24 months**. Initial MoUs are followed by detailed drafting, inter-ministerial reviews, and parliamentary ratification in both countries.[24]
  - **Political alignment**: governments must synchronize treaty timelines with legislative calendars; changes in administration or shifts in foreign-policy priorities can stall or reopen negotiations, adding further delay.
- Jurisdictional overlaps
  - **CLOUD Act vs. Immunity Clauses**: under the U.S. CLOUD Act, U.S.-based providers can be compelled to produce data held abroad unless exempted by an implementing treaty. Data Embassy treaties must explicitly "**grandfather out"** such obligations to prevent U.S. law enforcement from subpoenaing embassy-hosted servers.[25]
  - **GDPR & Local Data-Access Laws**: the EU's GDPR permits supervisory authorities to access personal data for compliance and enforcement. Absent clear treaty carve-outs, host-state regulators could assert jurisdiction over a Data Embassy, undermining its immunity. Treaties must therefore include **non-recognition clauses** for local data-access powers.[26]

High capital and operating costs

- **Setup & lease expenses**. **Estonia-Luxembourg case**: public records show Estonia incurred **€1 million** in initial setup costs plus **€236 000/year** in rent and data-transfer fees for a 10 TB replica in LuxConnect's Tier IV facility —totalling **€2.2 million** over five years.[27]
- **CapEx benchmarks**. **Tier IV construction**: building a Tier IV data center averages **US $7–12 million per MW** of IT load (i.e., $7–12 M/MW CAPEX).[28] High-availability features (2N+1 power, dual-chassis cooling) drive these premium rates.

---

[24] Republic of Estonia & Grand Duchy of Luxembourg. (2002). Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on hosting data and information systems. Riigi Teataja. https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf; Diplomacy.edu. (2017, November 16). *Data embassies: Protecting nations in the cloud.* Diplo. https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/.

[25] Lewis, J. A. (2019, April 8). *Untapping the full potential of CLOUD Act agreements.* Center for Strategic & International Studies (CSIS). https://www.csis.org/analysis/untapping-full-potential-cloud-act-agreements.

[26] Ballon, L. (2018, June 15). *Potential conflict and harmony between GDPR and the CLOUD Act.* Reed Smith. https://www.reedsmith.com/en/perspectives/2018/06/potential-conflict-and-harmony-between-gdpr-and-the-cloud-act; Simons, J. (2024, January 23). *Diplomatic law reimagined: Appraising the risks and prospects of data embassies. Harvard Law School Policy Review.* https://lawschoolpolicyreview.com/2024/01/23/diplomatic-law-reimagined-appraising-the-risks-and-prospects-of-data-embassies.

[27] Luxembourg Times. (2017, May 25). *Estonian data embassy in Luxembourg to cost €2.2m. Luxembourg Times.* https://www.luxtimes.lu/luxembourg/estonian-data-embassy-in-luxembourg-to-cost-2-2m/1215968.html; ERR News. (2017, May 25). *Data embassy in Luxembourg to cost €2.2 million over five years. ERR News.* https://news.err.ee/614646/data-embassy-in-luxembourg-to-cost-2-2-million-over-five-years.

[28] Digital Infra. (2022, March 11). *How much does it cost to build a data center?* Dgtl Infra. https://dgtlinfra.com/how-much-does-it-cost-to-build-a-data-center/.

- **Energy & maintenance**. **Ongoing OPEX**: tier IV SLAs demand round-the-clock maintenance and power redundancy. Costs per rack can exceed **US $60 000–100 000** annually, reflecting 24x7 N+1 backup power, cooling, and workforce readiness.[29]

Connectivity constraints

- **Submarine cable diversity**. The Caribbean region relies heavily on a **handful of submarine cables** (e.g., ARCOS, F Caribbean), with many islands connected by just **1–2 links**. A single cable cut can sever international connectivity for days or weeks, stalling data replication and failover operations.[30]
- **Latency & throughput**. Undersea round-trip times from Caribbean hubs to North America or Europe often **exceed 100 ms**, compared to sub-40 ms on optimized routes (e.g., EllaLink). High latency degrades performance for synchronous database transactions, necessitating asynchronous replication strategies or local caching layers.[31]

Regulatory uncertainty

- **Evolving data-sovereignty laws**. Several Caribbean states are drafting or enacting **data localization mandates**, which could compel additional national nodes or impose data-at-rest restrictions incompatible with embassy treaties. Without regional harmonization, each state's evolving regime may necessitate **treaty amendments**, adding legal complexity.[32]
- **Emerging privacy frameworks**. Future privacy regulations (e.g., Africa's draft Digital Rights Bill, potential CARICOM Data Protection Act) may expand data-subject rights over extraterritorial copies, requiring embassies to embed **compliance mechanisms** and potentially restrict certain data categories from replication.

3. Commercial data centres vs Data embassies

Data embassies are more than backup facilities; they operate as sovereign extensions of national infrastructure, ensuring the uninterrupted delivery of critical public services even under conditions of extreme disruption. Unlike commercial "sovereign clouds," which provide regulatory compliance under host-country law, Data embassies are established through bilateral treaties that confer diplomatic-style immunity and guarantee exclusive home-state jurisdiction.

The distinction extends across multiple dimensions. Legally, Sovereign Clouds rely on commercial contracts and national data protection laws, while Data embassies rest on international law and treaty protections. Operationally, cloud providers retain partial or full control over infrastructure and personnel, whereas Data embassies ensure that hardware, encryption, and staffing remain under the direct authority of the sending state. From a financial perspective, sovereign clouds operate on predictable subscription-based models, while Data embassies require significant upfront and ongoing investment to deliver higher levels of assurance. Most importantly, the two models address fundamentally different threat landscapes: sovereign clouds mitigate regulatory and commercial risks,

---

[29] Encor Advisors. (2024, October 22). *Data center cost.* Encor Advisors. https://encoradvisors.com/data-center-cost/.

[30] Caribbean Data Centers. (2024, July). *State of the Caribbean submarine cable ecosystem.* Caribbean Data Centers. https://caribbeandatacenters.com/wp-content/uploads/2024/07/State-of-the-Caribbean-Submarine-Cable-Ecosystem.pdf.

[31] EllaLink. (2021, June 1). *Sines: The new gateway from Latin America to Europe.* EllaLink. https://ella.link/story/sines-the-new-gateway-from-latin-america-to-europe/; Tech Teledata. (2016, May 26). *How submarine cables are made, laid, operated and repaired.* Tech Teledata (Archived at Wayback Machine). https://web.archive.org/web/20160526231647/http://www.techteledata.com/how-submarine-cables-are-made-laid-operated-and-repaired/ .

[32] Ballon, L. (2018, June 15). *Potential conflict and harmony between GDPR and the CLOUD Act.* Reed Smith. https://www.reedsmith.com/en/perspectives/2018/06/potential-conflict-and-harmony-between-gdpr-and-the-cloud-act.

while Data embassies are designed to withstand existential threats such as natural disasters, cyberwarfare, or political crises.

This framework underscores that Data embassies are not merely a technical solution but a matter of sovereignty and state survival —making them uniquely suited for small and vulnerable nations that cannot risk losing control of their digital core.

The comparative features of these two models are summarized in table 1.

Table 1
Comparative framework of digital sovereignty solutions

Aspect	Data Embassy	Sovereign cloud (public/partner-operated)
Primary Strategic Goal	State continuity; digital government-in-exile	Regulatory compliance; data residency
Governing Instrument	Bilateral international treaty	Commercial service-level agreement (SLA)
Legal Foundation	Public international law	Commercial contract & national data protection law (e.g., GDPR)
Jurisdictional Shield	Immunity from host state law & jurisdiction	Subject to host state and provider's home-country law
Response to Foreign Legal Compulsion (e.g., US CLOUD Act)	High – immunity grounded in diplomatic principles designed to resist foreign state compulsion	Low to moderate – providers must comply with home-country law regardless of data location
Operational Control	Full control by the sending state (hardware, keys, staffing)	Provider/partner-managed; limited customer oversight
Infrastructure Model	State-owned or leased servers in Tier IV facilities; bespoke links (e.g., dark fiber, MPLS)	Provider-owned, multi-tenant or dedicated infrastructure
Security Guarantees	Treaty-based immunity; resilience to state-level threats; air-gapped/private networks possible	Robust compliance standards (ISO, SOC, FedRAMP), but no immunity from host-country law
Cost & Financing	High CapEx + OpEx (e.g., Estonia: €1M setup, €236k/year maintenance)	Opex model; subscription-based with modest premiums (10–30%)
Primary Threats Addressed	Existential threats: natural disaster, invasion, state collapse	Regulatory & commercial risks: data localization, privacy breaches
Deployment Timeline	Long (6–18 months, treaty ratification and specialized buildouts)	Rapid (hours–days, subject to capacity)

Source: Table elaborated from ECLAC with data from Amazon Web Services (2021); Amazon Web Services (n.d.); Diplomacy.edu (2025); e-Estonia (n.d.); Google Cloud (n.d.); Microsoft (2023); Nutanix (n.d.); OECD OPSI (2017); The DataSphere Initiative (2023).

The Data Embassy concept has since begun to diffuse globally, adapting to different national priorities. The Principality of Monaco followed Estonia's lead in 2021, also establishing a Data Embassy in Luxembourg. However, Monaco's primary motivation was not geopolitical threat but its extreme geographic vulnerability. With a territory of just over 2 square kilometres, establishing geographically dispersed, disaster-resilient data centres within its own borders was physically impossible, making an external solution essential for resilience against natural disasters.[33]

This initial demand-driven model, where a sending state seeks a secure host, is now being complemented by a supply-driven approach. Nations are beginning to compete to become trusted hosts for sovereign data, creating what is effectively a new two-sided market in digital sovereignty. Bahrain's 2018 "Cloud Law" pioneered this by allowing data stored in its data centres to be subject to the jurisdiction of a foreign customer's home country. More recently, Saudi Arabia has proposed a "Global AI Hub Law" that would formalize this model, creating a legal framework for "Private Hubs"

[33] DiploFoundation. (2025). *Data embassies: Protecting nations in the cloud.* Diplo. https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/.

—functionally Data embassies— that operate under the guest country's laws within Saudi territory.[34] This evolution signals a new form of economic and diplomatic statecraft, where nations can offer "sovereignty as a service," competing not just on the technical merits of their data centres but on the strength and trustworthiness of the legal immunities they provide.

The following section provides an analysis of comparator jurisdictions followed by lessons learned.

4. Comparative analysis

The development of Data embassies across different jurisdictions offers valuable insights into the interplay between legal instruments, technical architectures, and strategic outcomes. While Estonia and Monaco have relied on bespoke bilateral treaties to enshrine diplomatic-style immunity for their sovereign data, Bahrain has pursued a legislative approach through its Cloud Law, and Luxembourg has positioned itself as a trusted international host by embedding inviolability into national law. The table below summarizes these cases, highlighting key legal, technical, financial, and operational dimensions, and offering lessons that may inform Caribbean strategies.

Table 2
Comparative overview of Data Embassy models

Country / Case	Legal instrument	Host and technical setup	Funding and scale	Outcomes and performance	Analysis
Estonia	MoU (2016); Bilateral Treaty (2017, ratified 2018)[a] Servers, equipment, archives deemed Estonian property with diplomatic immunity.	LuxConnect Tier IV (Bissen)[b] Active–active replication of 10 strategic datasets (e.g., land, population, court, business registries) via encrypted dark-fiber.[c]	~€1M upfront; €236k/yr OPEX. 10 TB capacity, expandable in 5 TB increments.[d]	>99.995% uptime; sub-5-minute failover; no data-loss incidents[e]	Pioneering model shows small state resilience. Balanced scope keeps costs manageable. Treaty clarity ensures immunity from EU/U.S. conflicts.
Monaco	Bilateral Agreement (2021, ratified 2022–23). Premises, data, equipment, and archives enjoy inviolability and immunity.[f]	LuxConnect Tier IV (Bissen). Digital twin of Monaco Cloud (>150 km away). Replicates e-administration, e-health, e-education, smart city systems.[g]	State-funded, modest (~5–8 TB). Cost-recovery hosting.	Tier IV uptime targets (99.995%); ensured continuity for microstate unable to host domestic backups[h]	Minimalist, cost-efficient strategy. Separation rule useful for island states. Ratification achieved in ~18 months.
Bahrain (GIFT City)	Cloud Law (Decree No. 56, 2018). Customer content falls under home-state jurisdiction. No physical immunity.[i]	Planned Tier III/IV facilities in GIFT City. Customer-segregated vaults.	PPP; ~₹500 cr (US$60M). Multi-petabyte scale.[j]	Still theoretical; not operational. Requires ministerial designations.	Hybrid model: sovereignty by law, not treaties. Could inspire Caribbean SEZs. Lack of operational track record limits confidence.
Luxembourg	National Law (2017) allows treaties granting inviolability of foreign premises/equipment. Based on Vienna Convention principles.[k]	Multiple Tier IV facilities (LuxConnect, DG1, eBRC). Dense peering, sovereign-grade security zones.[l]	Operators fund expansions; client states cover hosting fees.	Zero downtime reported; hub for state embassies.	Neutrality, stability, and dense DC ecosystem make Luxembourg a trusted host. Economies of scale lower costs for smaller states.

Source: Table elaborated from ECLAC with data from Bahrain Business Laws (2018); DiploFoundation (2025); e-Estonia (n.d.); Luxembourg Public (n.d.); Monaco Voice (2023); OECD OPSI (n.d.); Riigi Teataja (2017); Siradel (n.d.); Tamimi & Company (2019); The DataSphere Initiative (2021); Zubi Partners (2024).

[a] Riigiteataja. (2016, November 14). *Agreement between the Government of the Republic of Estonia and the Government of the Grand Duchy of Luxembourg on hosting data and information systems*. https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_ Agreement.pdf.

[b] e-Estonia. (n.d.). *Factsheet: Data embassy*. https://e-estonia.com/wp-content/uploads/factsheet_data_embassy.pdf; OECD Observatory of Public Sector Innovation. (2017). *Establishing the first data embassy in the world*. https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/.

[34] Hunton Andrews Kurth LLP. (2025, April). *Saudi Arabia pioneers data embassies with publication of draft Global AI Hub Law.* Global Privacy Blog. https://www.globalprivacyblog.com/2025/04/saudi-arabia-pioneers-data-embassies-with-publication-of-draft-global-ai-hub-law/.

[c] The Datasphere Initiative. (2023, September 18). *How data embassies promote data security for all*. https://www.thedatasphere.org /news/how-data-embassies-promote-data-security-for-all/.

[d] Bahrain Business Laws. (2018). *Law of providing cloud computing services to foreign parties*. https://bahrainbusinesslaws.com /laws/Law-of-Providing-Cloud-Computing-Services-to-Foreign-Parties; Al Tamimi & Company. (2018, July). *Diplomatic immunity for data: Bahrain's data embassy law*. https://www.tamimi.com/law-update-articles/diplomatic-immunity-for-data-bahrains-data-embassy-law/.

[e] The Datasphere Initiative. (2023, September 18). *How data embassies promote data security for all*. https://www.thedatas phere.org/news/how-data-embassies-promote-data-security-for-all/; e-Estonia. (n.d.). *Data embassy*. https://e-estonia.com/solu tions/e-governance/data-embassy/.

[f] Data Center Dynamics. (2021, December 2). *Monaco opens e-embassy in Luxembourg*. https://www.datacenterdynamics.com/en /news/monaco-opens-e-embassy-in-luxembourg/.

[g] Luxembourg Government. (n.d.). *E-embassies in Luxembourg*. https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html; Monaco Voice. (2023, May 16). *Monaco fortifies digital security with Luxembourg data center partnership*. https://monacovoice.com/en/article/monaco-fortifies-digital-security-with-luxembourg-data-center-partnership.

[h] DiploFoundation. (2017, August 30). *Data embassies: Protecting nations in the cloud*. https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/; Siradel. (2021, October 25). *Principality of Monaco: A unique digital twin and digital services platform at the service of the territory transformation*. https://www.siradel.com/principality-of-monaco-a-unique-digital-twin-and-digital-services-platform-at-the-service-of-the-territory-transformation/.

[i] Bahrain Business Laws. (2018). *Law of providing cloud computing services to foreign parties*. https://bahrainbusinesslaws.com/laws/Law-of-Providing-Cloud-Computing-Services-to-Foreign-Parties; Al Tamimi & Company. (2018, July). *Diplomatic immunity for data: Bahrain's data embassy law*. https://www.tamimi.com/law-update-articles/diplomatic-immunity-for-data-bahrains-data-embassy-law/.

[j] Al Tamimi & Company. (2018, July). *Diplomatic immunity for data: Bahrain's data embassy law*. https://www.tamimi.com/law-update-articles/diplomatic-immunity-for-data-bahrains-data-embassy-law/; Zubi Partners. (2024, July 4). *Overview of cloud computing, data embassies, and jurisdiction*. https://zubipartners.com/2024/07/04/overview-of-cloud-computing-data-embassies-and-jurisdiction/.

[k] Riigiteataja. (2016, November 14). *Agreement between the Government of the Republic of Estonia and the Government of the Grand Duchy of Luxembourg on hosting data and information systems*. https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf; Luxembourg Government.

[l] e-Estonia. (n.d.). *Factsheet: Data embassy*. https://e-estonia.com/wp-content/uploads/factsheet_data_embassy.pdf; OECD Observatory of Public Sector Innovation. (n.d.). *Establishing the first data embassy in the world*. https://oecd-opsi.org/ innovations/establishing-the-first-data-embassy-in-the-world/.

Lessons learned

- Single vs. multiple facilities
  - **Single site** (Estonia) streamlines governance, legal clarity, and operations —but creates a single point of failure if host stability falters.
  - **Distributed nodes** (hybrid approach) improve geographic and political risk diversification, albeit at higher cost and coordination complexity.
- Embassy vs. residency
  - **Data Residency** ensures data remains under local law but exposes it to host-nation seizure or legal process.
  - **Data Embassy** confers **diplomatic immunity**, demanding treaty investment but delivering superior protections for core state functions.
- Scalability & modularity
  - Replicating **only critical registries** (10 TB model) balances resilience with affordability.
  - Modular expansions allow phased adoption, letting smaller states start with minimal datasets and scale as budgets permit.
- Host selection criteria
  - **Legal neutrality**, digital connection maturity, political stability, cost of energy, data protection regulation and connectivity diversity among others are paramount.
- Political & diplomatic cadence
  - Rapid treaty ratification (< 18 months) is achievable when aligned with legislative sessions and bilateral priorities.

- Engaging foreign-affairs and ICT ministries early accelerates legal drafting and technical procurement in parallel.

Ideal host jurisdiction

The ideal host jurisdiction would be politically stable, outside the Caribbean disaster zone, and have top-tier data center facilities. By establishing at least two geographically distinct data embassies, a Caribbean country ensures its critical digital assets reside in legally protected off-site repositories that cannot be seized or shut down even under foreign legal pressure. This extraterritorial layer eliminates common-mode political and legal risks while preserving the nation's data sovereignty. In other words, even though the data is hosted abroad, it remains under the sole jurisdiction and control of the home government.

C. Legal architecture: a New institution in public international law

The legal foundation of a Data Embassy is its most defining and innovative feature. It is crucial to understand that existing international legal frameworks, most notably the 1961 Vienna Convention on Diplomatic Relations (VCDR), are insufficient for this purpose. The VCDR was designed to govern the status of traditional diplomatic missions, their premises, and their personnel; it was never envisioned to apply to standalone, unmanned data centres.[35] This legal gap necessitates the creation of a purpose-built bilateral treaty between the sending and host states.

An analysis of the foundational agreement between Estonia and Luxembourg, ratified by both parliaments in 2018, reveals the core legal principles that give the Data Embassy its unique status.

- **Inviolability of premises (Article 3):** the treaty explicitly states that "The premises shall be inviolable and thus exempt from search, requisition, attachment or execution." This clause establishes an absolute shield, protecting the physical and logical infrastructure of the Data Embassy from any form of seizure or interference by the host state's authorities.
- **Sovereignty over "digital archives" (Article 4):** the agreement legally transforms the digital information into sovereign state property. It declares that "All data and information systems stored by the Republic of Estonia in the premises shall be regarded as archives of the Republic of Estonia" and are, therefore, also inviolable. This protection extends to data in transit, ensuring that communications to and from the facility cannot be subject to censorship or interception.
- **Jurisdiction and control:** the treaty framework ensures that the data and systems remain under the full and exclusive control and jurisdiction of the sending state, Estonia. The host state, Luxembourg, is legally obligated to guarantee access to the premises for Estonia's authorized representatives but has no right to access the data itself.

This agreement has been hailed as having "drawn a new page in International law" and setting a clear precedent.[36] It represents the creation of a new institution under public international law, crafted specifically to solve a unique challenge at the nexus of technology and state sovereignty.[37]

---

[35] Riigikogu. (2017, June 8). *The Riigikogu approved establishing of Luxembourg data embassy.* Riigikogu. https://www.riigikogu.ee/en/press-releases/plenary-assembly/riigikogu-approved-establishing-luxembourg-data-embassy/.

[36] Organisation for Economic Co-operation and Development. (n.d.). *Establishing the first data embassy in the world.* Observatory of Public Sector Innovation (OPSI). https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/.

[37] Altwicker, T. (2022). *The data embassy under public international law. International & Comparative Law Quarterly*, *71*(3), 689–714. Cambridge University Press. https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/data-embassy-under-public-international-law/A1915132C9DB447C8.

This entire legal edifice, however, rests upon a non-negotiable foundation: profound inter-state trust. The selection of a host nation is a strategic decision of the highest order. The host must be politically stable, technologically advanced, and possess a legal system that reliably upholds its international commitments. This "corridor of trust" must extend from the highest political levels down to the technical and legal experts responsible for implementation, because the sending state is placing the ultimate guarantor of its continuity in the hands of another sovereign nation.

In Chapter V, we examine the Vienna Convention and other international legal frameworks in detail, exploring how they can be adapted to serve as a foundation for a treaty on data embassies. Beyond the specific legal basis the Vienna Convention provides, its true value for a potential data sovereignty treaty lies in its functionality and proven effectiveness, having remained in force since 1961 with only minimal recorded violations.

D. Technical and operational frameworks for digital resilience

Legal frameworks offer the shield of sovereignty, while technical architectures deliver true resilience. The Data Embassy concept encompasses multiple implementation models —each governed by rigorous technical requirements— and presents policymakers with a spectrum of options: from a Physical Data Embassy (dedicated server racks housed in a secure overseas data center) to a complementary Virtual Data Embassy, in which less-sensitive data and services are backed up to commercial public clouds as part of a hybrid strategy.[38]

Core technical recommendations for effective Data Embassy are:

- **Tier 4 certified data centres:** the physical infrastructure must meet the highest industry standard for data centres reliability and security. A Tier 4 certification guarantees an uptime of 99.995% (equivalent to no more than 26.3 minutes of downtime per year), with complete, independent redundancy for every component of the power and cooling infrastructure. This ensures the facility can withstand significant local disruptions, a non-negotiable baseline for hosting a nation's critical systems.
- **Data and service replication:** the architecture must support more than simple backups. It enables the real-time, active-active replication of services. This capability is what distinguishes a Data Embassy from a simple off-site archive; it allows for the immediate failover and continued operation of essential government services from the embassy location, not just the eventual recovery of data.
- **Advanced cybersecurity and integrity:** to ensure the trustworthiness of the stored data, advanced cybersecurity measures are essential. Estonia, for example, leverages its KSI Blockchain technology to create an immutable, mathematically verifiable audit trail for all data and access logs. This ensures data integrity and non-repudiation, making it impossible for data to be altered without detection.[39]

These technical components are designed to deliver three pillars of sovereignty, ensuring the sending state retains ultimate control:

[38] ComplexDiscovery. (2022, February). *Implementation of the virtual data embassy solution (Summary report).* ComplexDiscovery. https://complexdiscovery.com/wp-content/uploads/2022/02/Implementation-of-the-Virtual-Data-Embassy-Solution-Summary-Report.pdf.

[39] e-Estonia. (n.d.). *Data embassy.* e-Estonia. https://e-estonia.com/solutions/e-governance/data-embassy/.

(i) **Data sovereignty:** achieved through cryptography. The sending state must retain exclusive control over the encryption keys used to protect its data. The host nation and any service providers have no technical means to access the plaintext information.[40]

(ii) **Operational sovereignty:** the sending state must have continuous, independent visibility and control over the infrastructure's operations, allowing it to manage, monitor, and run its services without reliance on the host.

(iii) **Software sovereignty:** the sending state must have the freedom to choose and operate its own technology stack, avoiding vendor lock-in and dependency on a specific provider's proprietary software.

To make the concept tangible, the types of critical datasets prioritized for protection in the Estonian model include those essential for the basic functioning of the state: the Population Register, Land Register, Business Register, Taxable Persons' Register, the State Gazette (containing all official laws), and the Identity Documents Register.[41]

In chapter VI, we will explore in greater depth the specific technical characteristics that may need to be incorporated into a data embassies treaty. It is important to emphasize that certain elements, such as Tier IV data center standards, are not prerequisites for establishing a data embassy, as they are not directly related to data sovereignty. What is essential, however, is that the embassy fulfills its intended purpose —particularly for regions such as the Caribbean— by ensuring digital continuity.

E. Regional feasibility: the Caribbean context

Caribbean nations face unique vulnerabilities to both cyber-attacks and natural disasters. Hurricanes, seismic events, and supply-chain disruptions regularly threaten continuity of government services and critical national registers. A **Data Embassy** —the placement of sovereign data infrastructure abroad under home-state law— offers a resilience layer beyond domestic disaster-recovery sites. This section assesses whether such embassies are technically viable, financially sustainable, and politically achievable in the Caribbean context. We first establish the **conceptual framework** (5A), then compare global case studies (5B), examine regional opportunities and constraints (5C), conduct a SWOT analysis (5D), and finally explore **emergent technologies** that can augment a traditional data embassy model (5E).

1. Opportunities and constraints for adoption

Technical feasibility

The Caribbean's **connectivity landscape** is defined by a handful of undersea cables —ARCOS, F-Caribbean and Maya-1— linking most islands to North American and European hubs. Historical data shows **over 100 cable faults annually**, often from fishing-boat anchors and storms, causing islands like Grenada and Barbados to endure **48–72-hour outages** when a single cable is severed.[42]

---

[40] Google Cloud. (2022, November 11). *Data embassies: Strengthening resiliency with sovereignty.* Google Cloud. https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty.

[41] Organisation for Economic Co-operation and Development. (n.d.). *Establishing the first data embassy in the world.* Observatory of Public Sector Innovation (OPSI). https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/.

[42] BlueNAP Americas. (2024, August). *Regulating the submarine cable.* BlueNAP Americas. https://www.bluenapamericas.com/wp-content/uploads/2024/08/DZ-Regulating-the-submarine-cable.pdf; Energy Industry Review. (2023, October 9). *Submarine cables: Risks and security threats. Energy Industry Review.* https://energyindustryreview.com/analysis/submarine-cables-risks-and-security-threats/.

Average fixed-broadband speeds have improved —regional mean **54.9 Mbps** as of mid-2024, led by Barbados (110 Mbps) and Puerto Rico (96.7 Mbps)[43]— but lagging nations (Cuba at 4.1 Mbps; Haiti at 10.8 Mbps) remain vulnerable. Real-time replication to a Data Embassy demands **sustained, low-latency** links; islands with < 50 Mbps may need **private dark-fiber circuits** to meet sub-100 ms round-trip requirements.

On-island **data-center capacity** varies. Puerto Rico's **HUB787** is ANSI/TIA-942 Tier III-certified (99.982% availability), co-located with five cable landings and peering exchanges.[44] Conversely, **Trinidad & Tobago** and Barbados host mostly Tier II/III facilities lacking Tier IV resilience; however, emerging **edge-compute nodes** (micro-data centers at 5G base stations) can cache critical datasets locally during cable repairs, sustaining limited service continuity.

To mitigate **single-cable dependency**, regional bodies recommend **redundant terrestrial microwave rings** and **multinodal fiber loops** (e.g., Trinidad→Barbados→Grenada) to re-route traffic if undersea links fail.[45] Additionally, architectures should blend **asynchronous replication** with **local CDNs** to maintain RTOs/RPOs under 60 seconds, balancing consistency and performance.

Financial viability

Building a **Tier IV-equivalent** embassy node (0.5 MW IT load) entails **US $3.5–6 million CAPEX**, based on industry averages of **US $7–12 million per MW**. Replication-specific costs mirror the Estonia–Luxembourg model: **€1 million upfront + €236 000/year** for 10 TB suggests a **US $500 000** initial plus **US $120 000/year** for a 5 TB Caribbean node.

Annual **OPEX** is driven by electricity (25–30% of costs), maintenance (40%), and staff/security services, yielding **US $60 000–100 000** per rack per year under a Tier IV SLA. **Network transit** —dedicated dark fiber or leased wavelengths— can range **US $50 000-150 000/month** depending on distance and capacity, demanding careful budgeting for mid- to long-haul connectivity.

Funding can be mobilized through different recourses or projects such as the **US $94 million Caribbean Digital Transformation Project (CARDTP)**, financed by the World Bank and implemented via OECS and ECTEL sub-projects targeting infrastructure upgrades and resilience enhancements.[46] The **EU's Copernicus–CDEMA** partnership also provides grants and technical aid for cybersecurity and disaster-recovery planning.[47]

Public-private partnerships with **hyperscalers** (AWS, Google) and regional telcos can underwrite CAPEX through **anchor tenancy**, reserving capacity in exchange for discounted rates. Sovereign-backed **green bonds** and **climate-adaptation funds** (Green Climate Fund, GFDRR) further diversify financing, aligning with embassies' disaster-resilience objectives.

---

[43] TS2 Space. (2023, July 11). *The digital wave: Uncovering internet access and satellite connectivity in Barbados.* TS2. https://ts2.tech/en/the-digital-wave-uncovering-internet-access-and-satellite-connectivity-in-barbados/.

[44] HUB.pr. (n.d.). *HUB787.* HUB.pr. https://hub.pr/services/hub-787.html; News is My Business. (2021, December 14). *HUB787 facility lands Tier III certification from Uptime Institute. News is My Business.* https://newsismybusiness.com/hub787-facility-lands-tier-iii-certification-from-uptime-institute/.

[45] BlueNAP Americas. (2024, August). *Regulating the submarine cable.* BlueNAP Americas. https://www.bluenapamericas.com/wp-content/uploads/2024/08/DZ-Regulating-the-submarine-cable.pdf.

[46] World Bank. (n.d.). *Caribbean digital transformation project (CARDTP).* World Bank. https://projects.worldbank.org/en/projects-operations/project-detail/P171528.

[47] Eastern Caribbean Telecommunications Authority. (n.d.). *The Caribbean digital transformation project (CARDTP).* ECTEL. https://www.ectel.int/the-caribbean-digital-transformation-project-cardtp; Caribbean Community (CARICOM). (2024, July 11). *CARICOM, USAID partner on Cyber Resilience Strategy 2030 project.* CARICOM. https://caricom.org/caricom-usaid-partner-on-cyber-resilience-strategy-2030-project/.

Stakeholder roles and partnerships regional institutions:

- ECLAC as the regional UN secretariat entity aligned with its Digital Agenda for Latin America and the Caribbean (eLAC), can serve as a neutral facilitator for advancing regional digital resilience through data embassies. It can coordinate technical feasibility studies, support regulatory harmonization, and provide a platform to promote bilateral and regional agreements. By leveraging its convening power, ECLAC can helps translate political will into legally and technically robust frameworks for digital sovereignty.
- **CARICOM Secretariat**: endorses the **Regional Digital Resilience Strategy**, providing treaty templates, coordinating multilateral negotiations, and establishing a **Single ICT Space** for harmonized protocols.[48]
- **CDEMA**: integrates Data Embassy failover scenarios into **annual disaster drills**, ensuring that digital backups are tested alongside traditional emergency-response efforts.[49]
- **ECTEL** (OECS): implements CARDTP projects, secures funding for submarine-cable diversity, and supports regulatory reforms to streamline ICT resilience across member states.[50]

National governments:

- **Ministries of ICT**, **Finance**, and **Foreign Affairs** must co-lead treaty negotiations, allocate capital in national budgets, and enact enabling legislation for data-embassy status.
- **Telecom regulators** grant licensing for dedicated dark-fiber circuits, spectrum for microwave resilience rings, and oversee compliance with data-localization mandates.

Private sector:

- **Telcos** (Flow, Digicel) supply cable-landing and last-mile connectivity; can co-invest in edge-node deployments.
- **Data-center operators** (HUB Advanced Networks, FiberX) offer colocation and managed-security services.
- **Cybersecurity firms** implement CMMI Level 3+ controls, penetration testing, and integrate with CARICOM frameworks to harden embassy nodes.

Donors & development partners

- **World Bank**, **IDB**, **CAF** and **EU**: finance large-scale infrastructure and policy advisory.
- **UNDP/UNEP**: provide grants, legal-drafting support, and environmental impact studies for site selection and build-out.

---

[48] Caribbean Community (CARICOM). (2024, March 2). *CARICOM heads of government endorse digital resilience strategy, skills fund creation.* CARICOM. https://caricom.org/caricom-heads-of-government-endorse-digital-resilience-strategy-skills-fund-creation/; Caribbean Community (CARICOM). (2024, March 2). *48th thematic: Regional digital resilience.* CARICOM. https://caricom.org/48th-thematic-regional-digital-resilience/.

[49] Cambridge Global Advisors. (2024, July 11). *CARICOM and USAID unveil Cyber Resilience Strategy 2030 to bolster Caribbean cybersecurity.* Cambridge Global. https://www.cambridgeglobal.com/newsroom/caricom-and-usaid-unveil-cyber-resilience-strategy-2030-to-bolster-caribbean-cybersecurity.

[50] Eastern Caribbean Telecommunications Authority. (n.d.). *The Caribbean digital transformation project (CARDTP).* ECTEL. https://www.ectel.int/the-caribbean-digital-transformation-project-cardtp; World Bank. (2024, April 15). *Procurement notice: Caribbean digital transformation project (CARDTP).* World Bank. https://projects.worldbank.org/en/projects-operations/procurement-detail/OP00221809.

The regional aspect: opportunities and challenges

Opportunities:

- **Shared-services hub**: a **regional data-embassy hub** under a regional treaty can serve multiple states, leveraging economies of scale to lower per-state costs and ensuring uniform security standards.
- **Collective bargaining**: pooling regional demand can secure better terms for **submarine-cable capacity**, **Tier IV colocation**, and **dark-fiber leases**, accelerating build-out and reducing individual state exposure.
- **Harmonized data flows**: adopting **GDPR-aligned** APIs and metadata schemas region-wide enables secure data sharing for climate modelling, disaster-early warning, and public-health analytics.

Challenges:

- **Divergent legal regimes**: varying data-protection and localization laws across CARICOM, OECS, and non-CARICOM jurisdictions complicate multiparty treaties. Layered agreements or **umbrella multilateral compacts** may be required.
- **Financing gaps**: smaller or fiscally constrained states risk deprioritizing data-embassy investments in favour of immediate development needs, leading to uneven adoption and potential single-state dependencies.
- **Governance complexity**: establishing a **regional Data Embassy Board** that balances sovereign authority with joint-management efficiencies demands clear mandates, voting structures, and dispute-resolution mechanisms.
- **Geographic dispersion**: the physical spread of islands—from the Bahamas to Trinidad—increases logistical complexity for **terrestrial redundancy**. Ensuring microwave or fiber rings across multiple maritime borders requires cross-jurisdictional coordination on permits, rights-of-way, and spectrum allocation.

As of now, no Caribbean country has a Data Embassy in place. A few have secondary backups in foreign commercial clouds, but these lack sovereign guarantees and could be subject to foreign subpoenas or service disruptions. Moreover, **regulatory uncertainty** is a barrier: many officials are unsure how local data protection laws would apply if sensitive government data is stored overseas. Indeed, telecom operators in the region cite unclear regulations (and cost) as reasons they avoid hosting customer data abroad. This suggests that before Data Embassy arrangements can be executed, governments may need to update legislation or issue clarifications to explicitly allow secure cross-border data replication for continuity purposes. The harmonization of data protection and privacy laws across Caribbean could facilitate this. Another practical challenge is **cost and expertise**: setting up a data embassy entails expenses for international hosting, networking, and maintenance, as well as trust in the host's security standards. Small states might lack the skilled personnel to manage an overseas environment continuously. These issues could be mitigated by pooling resources at the regional level (e.g., a shared CARICOM or OECS-managed data embassy or utilizing the proposed Caribbean Cloud Pod infrastructure as an interim step).

2. SWOT analysis: Data Embassy implementation in the Caribbean

A SWOT analysis—assessing **Strengths, Weaknesses, Opportunities,** and **Threats**—highlights internal and external factors that will influence the success of Data embassies in the Caribbean.

Table 3
Strenghts and weaknesses

Strengths	Weaknesses
1. Political & regional mandates: eLAC agenda and CARICOM's 2024 Regional Digital Resilience Strategy explicitly calls for cross-border continuity solutions, creating a mandate for treaty-based initiatives.[a]	**1. Limited submarine-cable diversity**: many islands rely on only 1–2 undersea cables; annual cable faults (≈100) lead to 48–72 hr outages, threatening real-time sync.[b]
2. Existing Tier-III/IV facilities: cable landing stations such as HUB787 (Puerto Rico) and LuxConnect (Luxembourg) demonstrate proven hosting capacity and reliability (>99.99%).[c]	**2. Cybersecurity talent gap**: Latin America and the Caribbean face a shortage of trained cybersecurity professionals, mirroring a global gap of 1.3 million unfilled roles.[d]
3. Multilateral funding channels: world Bank's US $94 M Caribbean Digital Transformation Project provides clear financing pathways.[e]	**3. High CapEx & Opex requirements**: Tier IV-equivalent nodes cost US $7–12 M/MW to build, plus US $60 K–100 K per rack annually for power and maintenance.[f]
4. Regional expertise & institutions: ECLAC, CDEMA, ECTEL, and CARICOM Secretariat possess established coordination frameworks for disaster drills, telecom regulation, and legal harmonization.	**4. Legal & regulatory complexity**: divergent data-protection and localization laws across Caribbean, and individual states complicate treaty negotiations and enforcement.

Source: Table elaborated from ECLAC with data from CARICOM (2023); Submarine Cable Map (n.d.); Hub787 (n.d.); LuxConnect (n.d.); Mexico Business News (2023); World Bank (2020); KIO Data Centers (n.d.).

[a] Radio Jamaica News Online. (2023, February 16). *CARICOM leaders endorse regional digital resilience strategy*. https://radiojamaicanewsonline.com/local/caricom-leaders-endorse-regional-digital-resilience-strategy.

[b] TeleGeography. (n.d.). *Submarine cable map*. https://www.submarinecablemap.com/.

[c] Hub787. (n.d.). *Why Hub787?*. https://hub787.net/why-hub787/; LuxConnect. (n.d.). *LuxConnect*. https://www.luxconnect.lu/.

[d] Mexico Business News. (2023, August 10). *Latin America & Caribbean short 1.3M cybersecurity professionals*. https://mexicobusiness.news/cybersecurity/news/latin-america-caribbean-short-13m-cybersecurity-professionals.

[e] World Bank. (2020, June 22). *First-time financing by World Bank for digital economy in the Eastern Caribbean approved for US$94 million*. https://www.worldbank.org/en/news/press-release/2020/06/22/first-time-financing-by-world-bank-for-digital-economy-in-the-eastern-caribbean-approved-for-us94-million.

[f] KIO Data Centers. (2023, September 4). *Costs of a data center*. https://kiodatacenters.com/en/blog-data-center/en-us/blog/data-center/costs-of-a-data-center.

Table 4
Opportunities and threats

Opportunities	Threats
1. Shared regional hubs: a joint Data Embassy hub can serve multiple states under a single treaty, lowering per-state costs.	**1. Intensifying natural disasters**: increasing hurricane frequency and intensity (5 major storms/year average) heightens the risk of simultaneous multi-island impacts.
2. Hyperscaler partnerships: co-investment models with AWS, Google, or Microsoft can subsidize CAPEX via anchor tenancy and technology transfer.[a]	**2. Geopolitical & legal shifts**: changes in U.S. CLOUD Act, EU GDPR enforcement, or host-nation privacy laws could conflict with immunity clauses unless treaties are regularly updated.
3. Edge & 5G rollouts: expanding 5G networks enable micro-data centers at tower sites, enhancing local caching and reducing reliance on submarine links.	**3. Cyber threat escalation**: sophisticated state-sponsored and ransomware attacks are increasing globally, raising the baseline risk for critical infrastructure.
4. Climate-resilience funding: Green Climate Fund and Global Facility for Disaster Reduction and Recovery (GFDRR) grants align with Data Embassy objectives, offering non-reimbursable financing.[b]	**4. Stakeholder coordination risks**: complex governance bodies (regional boards, national ministries, private operators) may face decision-making gridlock, delaying critical deployment steps.

Source: Table elaborated from ECLAC with data from Amazon Web Services (n.d.); Global Facility for Disaster Reduction and Recovery (n.d.).

[a] Amazon Web Services. (n.d.). *Government and education*. https://aws.amazon.com/government-education/.

[b] Global Facility for Disaster Reduction and Recovery. (n.d.). *Global Facility for Disaster Reduction and Recovery*. https://www.gfdrr.org/en/global-facility-disaster-reduction-and-recovery.

This SWOT framework provides a structured overview for policymakers and technical planners to prioritize actions, allocate resources, and navigate risks in implementing Caribbean Data embassies.

- **Leverage strengths & opportunities**: utilize existing political mandates and funding to pilot shared regional hubs and hyperscaler partnerships.
- **Mitigate weaknesses & threats**: address cable diversity via redundant terrestrial/microwave links, invest in cybersecurity workforce development, and build legal frameworks that can adapt to evolving international laws.

Overall, the Data Embassy model is **feasible** for the Caribbean with careful planning. Technically, cloud and encryption tech are mature enough to implement it. Politically, the concept aligns well with regional goals of improving disaster resilience without ceding sovereignty.

The key steps are to secure hosting agreements with one or more friendly government, enact any enabling laws to recognize the extraterritorial data as an extension of the nation, and establish funding and operational protocols for the embassy site. This study's recommendations include fast-tracking at least two Data Embassy treaties by 2025–2027, learning from Estonia's experience. Once in place, a Data Embassy would guarantee continuity of government and financial systems even if local servers are wiped out, effectively providing an "ultimate insurance" for the digital state. It is worth noting that until such treaties are in force, interim measures (like using public cloud regions in Europe/North America with strong encryption) can offer partial off-island resilience, though without the full legal immunities. The region-specific assessment is that Data embassies present a **unique, high-impact resilience option**, and while complex, they should be pursued in parallel with domestic hardening efforts.

3. Implementation of emergent tech

Drawing on regional initiatives and global best practices, integrating AI-driven predictive analytics, edge computing, blockchain, and IoT/5G into Caribbean data embassy architectures can transform disaster resilience. Each technology offers unique advantages over legacy data centers—enabling proactive risk mitigation, decentralization, and transparent data management—while existing Caribbean projects demonstrate their feasibility within local contexts.

AI-Driven predictive analytics

Definition: AI-driven predictive analytics leverages machine-learning models trained on meteorological data, sensor feeds, and historical disaster records to forecast infrastructural stress points before storms make landfall.[51]

Benefits:

- **Proactive risk mitigation: unlike reactive monitoring, AI can flag probable failures 48–72 hours ahead, allowing pre-emptive load balancing or micro-grid activation.**[52]
- **Faster disaster alerts**: AI ensembles reduce hurricane-track errors by up to **20 %**, yielding **8–18 extra lead hours** for fail-over activation—vs. standard Numerical Weather Prediction alone.[53]

---

[51] Global Facility for Disaster Reduction and Recovery. (2024, March 7). *Leveraging AI and Earth observation for a resilient Caribbean.* GFDRR. https://www.gfdrr.org/en/feature-story/leveraging-ai-and-earth-observation-resilient-caribbean; World Bank. (2024, April 15). *Can AI help build climate resilience in the Caribbean? Let's look at housing.* World Bank Blogs – Sustainable Cities. https://blogs.worldbank.org/en/sustainablecities/can-ai-help-build-climate-resilience-caribbean-lets-look-housing.

[52] Global Tourism Resilience and Crisis Management Centre. (2023, September 20). *Leveraging AI for hurricane preparedness, management, and recovery in the Caribbean.* GTRCMC. https://gtrcmc.org/leveraging-ai-for-hurricane-preparedness-management-and-recovery-in-the-caribbean/.

[53] Spire. (n.d.). *Spire Global.* Spire. https://spire.com/.

- **Predictive maintenance**: anomaly-detection in AIOps ingests **1 000+ metrics/sec,** forecasting hardware faults **48 hrs ahead** with **85% precision**, cutting unplanned outages by **30%** compared to reactive checks.[54]
- **Enhanced precision:** by fusing high-resolution aerial imagery with ground-level IoT telemetry, models reduce false alarms by up to 30%, focusing scarce maintenance resources where most needed.[55]

Feasibility:

- **Maturity**: Gartner estimates the AIOps market grew from **US $0.9–1.5 billion** in 2020 with a **15 % CAGR** through 2025.[56]
- **Data ingestion cost**: using Elastic Observability Serverless at **US $0.15 per GB** ingested, processing **1 TB/day** would cost ~**US $45 000/month.**[57]
- **Regional pilots:** the "Open AI Caribbean Challenge" demonstrated ML classifiers mapping disaster-prone roofs in St. Lucia and Grenada, proving rapid model training on local datasets.[58]
- **Capacity building:** UNESCO's recent hackathon in Port-au-Prince equipped local journalists and data scientists with AI tools for hazard mapping, indicating accessible regional expertise.[59]
- **Cloud adoption:** World Bank–supported Caribbean Digital Transformation Project includes advisory on AI platforms, reducing capital barriers for model deployment.[60]

Edge computing

Definition: edge computing moves compute and storage to micro-data hubs located on-island, enabling local preprocessing and storage of critical datasets rather than routing all traffic to a central hub.[61]

Benefits:

- **Lower latency:** local inference and caching reduce reliance on undersea cables during peak loads or outages.[62]
- **Resilience through decentralization:** if one node or subsea route fails, other nodes continue operation, eliminating single points of failure inherent in centralized data centers.[63]

---

54 Dynatrace. (2022, December 8). *What is AIOps? Benefits and use cases.* Dynatrace Blog. https://www.dynatrace.com/news/blog/what-is-aiops-2/#benefits.

55 World Bank. (2024, April 15). *Can AI help build climate resilience in the Caribbean? Let's look at housing.* World Bank Blogs – Sustainable Cities. https://blogs.worldbank.org/en/sustainablecities/can-ai-help-build-climate-resilience-caribbean-lets-look-housing; Programming Insider. (2023, June 30). *How AI automation can solve real problems in Caribbean nations.* Programming Insider. https://programminginsider.com/how-ai-automation-can-solve-real-problems-in-caribbean-nations/.

56 StackState. (2021, May 12). *Read 2021 Gartner Market Guide for AIOps platforms.* StackState. https://www.stackstate.com/blog/read-2021-gartner-2021-market-guide-for-aiops-platforms-by-gartner/.

57 Elastic. (n.d.). *Serverless observability pricing.* Elastic. https://www.elastic.co/pricing/serverless-observability.

58 WeRobotics. (2022, October 5). *Open AI Caribbean challenge: Mapping disaster risk from aerial imagery.* WeRobotics Blog. https://werobotics.org/blog/open-ai-caribbean-challenge-mapping-disaster-risk-from-aerial-imagery.

59 UNESCO. (2023, April 12). *Empowering Caribbean journalists through data-driven hackathon for disaster preparedness.* UNESCO. https://www.unesco.org/en/articles/empowering-caribbean-journalists-data-driven-hackathon-disaster-preparedness.

60 Organisation of Eastern Caribbean States. (2024, February 21). *Driving the digital transformation in the Eastern Caribbean.* OECS. https://oecs.int/en/driving-the-digital-transformation-in-the-eastern-caribbean.

61 Cloud Computing News. (2023, September 14). *Why the Caribbean's digital future depends upon cloud.* Cloud Computing News. https://www.cloudcomputing-news.net/news/why-caribbeans-digital-future-depends-upon-cloud/.

62 The Fast Mode. (2024, January 22). *Cloud confidence crisis: Organizations seek balance with edge computing.* The Fast Mode. https://www.thefastmode.com/expert-opinion/40926-cloud-confidence-crisis-organizations-seek-balance-with-edge-computing.

63 EdgeIR. (2022, April 19). *IDC says security, resilience are top reasons enterprises are moving to edge – but operational challenges remain.* EdgeIR. https://www.edgeir.com/idc-says-security-resilience-are-top-reasons-enterprises-are-moving-to-edge-but-operational-challenges-remain-20220419.

- **Modular scalability:** new micro-nodes can be deployed within weeks, tailoring coverage to high-risk islands without major hub expansions.[64]

Feasibility:

- **Vendor solutions:** regional cloud partners now offer turnkey edge-orchestration bundles optimized for Caribbean conditions, including hurricane-rated enclosures.[65]
- **Financing support:** the CIF has invested US $167 M in resilient infrastructure across six Caribbean nations, with edge-computing pilots included in Grenada and Dominica.[66]
- **Local expertise:** OECS Digital Transformation initiatives provide training and grants for on-island edge deployments, lowering technical skill barriers.

IoT integration and 5G connectivity

Definition: integrating IoT sensors (weather stations, structural monitors) with 5G-enabled micro-cells at edge sites creates a dense data mesh for real-time monitoring and rapid hazard detection.[67]

Benefits vs. tabletop exercises:

- **Real-time visibility:** high-frequency IoT feeds enable instantaneous detection of infrastructure strain (e.g., bridge vibrations), surpassing manual inspections.
- **Adaptive networking:** 5G slices can prioritize emergency traffic, ensuring command-and-control data flows even under network stress.

Feasibility:

- **Pilot deployments:** confluent's resilient-edge IoT architectures have been tested in Costa Rica and Panama, proving interoperability with Caribbean-grade telecom infrastructure.[68]
- **Policy backing:** OECS broadband roadmaps include 5G trials on Saint Lucia and Grenada, with earmarked funding for IoT-edge clusters.[69]

Blockchain-based orchestration

Definition: Blockchain and distributed-ledger technologies (DLT) provide immutable, decentralized record-keeping, enabling secure cross-border data replication and provenance tracking within a data-embassy network.[70]

---

[64] Inter-American Development Bank. (2023, October 3). *Critical infrastructure in Latin America and the Caribbean: Technologies changing the game.* IDB Energy Blog. https://blogs.iadb.org/energia/en/critical-infrastructure-in-latin-america-and-the-caribbean-technologies-changing-the-game/.

[65] Cloud Carib. (2022, June 17). *How the cloud is shaping the digital future of the Caribbean.* Cloud Carib. https://info.cloudcarib.com/blog/how-the-cloud-is-shaping-the-digital-future-of-the-caribbean.

[66] Climate Investment Funds. (2023, November 29). *CIF delivers resilient infrastructure in the Caribbean.* CIF. https://www.cif.org/news/cif-delivers-resilient-infrastructure-caribbean.

[67] UNESCO. (2023, April 12). *Empowering Caribbean journalists through data-driven hackathon for disaster preparedness.* UNESCO. https://www.unesco.org/en/articles/empowering-caribbean-journalists-data-driven-hackathon-disaster-preparedness.

[68] Confluent. (2022, September 20). *Resilient edge infrastructure for IoT using Apache Kafka (ft. Kai Waehner).* Streaming Audio Podcast by Confluent. https://developer.confluent.io/learn-more/podcasts/resilient-edge-infrastructure-for-iot-using-apache-kafka-ft-kai-waehner/.

[69] Confluent. (2022, September 20). *Resilient edge infrastructure for IoT using Apache Kafka (ft. Kai Waehner).* Streaming Audio Podcast by Confluent. https://developer.confluent.io/learn-more/podcasts/resilient-edge-infrastructure-for-iot-using-apache-kafka-ft-kai-waehner/.

[70] Sharma, R., & Jindal, A. (2023). *Exploring blockchain for disaster prevention and relief: A comprehensive framework based on industry case studies. Frontiers in Blockchain, 6,* 980390. https://pmc.ncbi.nlm.nih.gov/articles/PMC9803901/; Sharma, R., & Jindal, A. (2023). *Exploring blockchain for disaster prevention and relief: A comprehensive framework based on industry case studies. Frontiers in Blockchain, 6,* 980390. https://www.researchgate.net/publication/370787774_Exploring_blockchain_for_disaster_prevention_and_relief_A_comprehensive_framework_based_on_industry_case_studies.

Benefits vs. manual orchestration:

- **Trustless replication:** encrypted ledgers ensure data integrity even if individual nodes are compromised, improving on centralized backup models.[71]
- **Transparent auditing:** smart contracts can automate verification of replication success and trigger alerts for missing or corrupted data copies.[72]
- **Cross-border compliance:** DLT frameworks can embed compliance metadata (e.g., sovereignty flags) directly into records, streamlining multijurisdictional collaboration.[73]

Feasibility:

- **Small-state pilots:** Malta and other small-island states have trialled blockchain for disaster-aid distribution, demonstrating templates adaptable to Caribbean nations.[74]
- **Inter-Caribbean projects:** the IDB's Caribbean Settlement Network explores DLT for financial messaging across CARICOM, providing operational insights applicable to data-embassy synchronization.[75]
- **Open-source frameworks:** platforms like Hyperledger Fabric and Corda offer modular, permissioned ledgers deployable on edge nodes with modest hardware.

---

[71] Bezzina, F., & Grima, S. (2019). *Leveraging blockchain technology to build resilience and disaster risk reduction in small states.* University of Malta. https://www.um.edu.mt/library/oar/bitstream/123456789/117578/1/Leveraging_blockchain_technology_to_build_resilience_and_disaster_risk_reduction_in_small_states_2019.pdf.

[72] Bezzina, F., & Grima, S. (2019). *Leveraging blockchain technology to build resilience and disaster risk reduction in small states. University of Malta.* https://www.um.edu.mt/library/oar/bitstream/123456789/117578/1/Leveraging_blockchain_technology_to_build_resilience_and_disaster_risk_reduction_in_small_states_2019.pdf.

[73] Bezzina, F., & Grima, S. (2019). *Leveraging blockchain technology to build resilience and disaster risk reduction in small states.* University of Malta. https://www.um.edu.mt/library/oar/bitstream/123456789/117578/1/Leveraging_blockchain_technology_to_build_resilience_and_disaster_risk_reduction_in_small_states_2019.pdf.

[74] Bezzina, F., & Grima, S. (2019). *Leveraging blockchain technology to build resilience and disaster risk reduction in small states. University of Malta.* https://www.um.edu.mt/library/oar/bitstream/123456789/117578/1/Leveraging_blockchain_technology_to_build_resilience_and_disaster_risk_reduction_in_small_states_2019.pdf.

[75] Bezzina, F., & Grima, S. (2019). *Leveraging blockchain technology to build resilience and disaster risk reduction in small states.* University of Malta. https://www.um.edu.mt/library/oar/bitstream/123456789/117578/1/Leveraging_blockchain_technology_to_build_resilience_and_disaster_risk_reduction_in_small_states_2019.pdf.

II. Caribbean data protection laws

A. Overview of Caribbean data protection laws

The Caribbean region is experiencing a period of significant transformation in its approach to data protection, with many countries moving toward more modern and comprehensive legal frameworks. Much of this progress has been shaped by the influence of the European Union's General Data Protection Regulation (GDPR), which has provided a model for recent reforms.

The regional landscape, however, is uneven. Some jurisdictions have developed relatively advanced frameworks that draw heavily on the GDPR framework. Others have enacted laws but face delays in proclamation or challenges with enforcement capacity. Several other countries still rely on outdated statutes or lack dedicated legislation altogether, leaving wide gaps in legal protection.

While GDPR has been a useful point of reference, Caribbean nations cannot simply transplant European standards wholesale. The region faces distinct challenges, including smaller regulatory bodies, limited technical expertise, and lower levels of organizational readiness. Effective frameworks must therefore be adapted to local contexts —balancing global best practices with pragmatic enforcement mechanisms that reflect the region's institutional capacities and economic realities.

The uneven development of data protection frameworks underscores both opportunities and risks. Stronger, well-enforced laws are increasingly recognized as vital not only for safeguarding individual privacy but also for attracting investment and maintaining competitiveness in critical sectors such as tourism and financial services. At the same time, fragmented or poorly implemented regimes could undermine trust and create barriers for cross-border data flows.

To strengthen the regional approach, governments should focus on building the capacity of supervisory authorities, expanding public awareness initiatives, and accelerating efforts toward harmonization. A coordinated, context-sensitive strategy will help reduce disparities across jurisdictions, foster greater trust in digital transactions, and position the Caribbean as a region that is not merely borrowing external models but shaping its own data protection standards to meet both local needs and global expectations.

B. Introduction to data protection in the Caribbean

1. Contextualizing data privacy in the digital age

The global proliferation of digital technologies and the rise of data-driven economies have fundamentally reshaped the landscape of personal information. Data protection has become a fundamental human right and an indispensable business imperative. In an increasingly interconnected world, the safeguarding of personal data is paramount, as data breaches and misuse carry severe reputational, financial, and legal consequences for individuals and organizations alike. The universal importance of protecting personal data underscores the need for robust legal and operational frameworks to ensure trust and security in the digital realm.

2. The Caribbean's unique position and growing importance of data protection

The Caribbean region is increasingly integrated into the global digital economy. Many of its economies are heavily reliant on sectors that inherently involve the processing of vast amounts of personal data, such as tourism, financial services, and offshore business operations. The region's unique legal landscape, influenced by a blend of common law and civil law traditions, adds layers of complexity to legal harmonization and compliance efforts. Furthermore, the escalating global incidence of cybercrime and data breaches highlights the urgent necessity for these nations to develop and enforce robust data protection frameworks.[76] Such measures are crucial not only for protecting their citizens but also for maintaining international trust and facilitating secure cross-border commerce.

3. Evolution of data protection legislation in the region

Historically, data protection in the Caribbean was either nascent or highly fragmented, often addressed indirectly through other sector-specific laws or general common law principles. However, the past decade has witnessed a rapid acceleration in legislative activity.[77] This surge has been largely spurred by the global influence of the GDPR, which has served as a significant catalyst for many Caribbean nations.[78] Consequently, numerous countries have transitioned from having no dedicated data protection laws to enacting comprehensive statutes designed to align with modern international standards. This legislative evolution reflects a growing recognition of the strategic importance of data privacy in the digital age.

C. Country-specific data protection frameworks

To provide an immediate overview of the legislative landscape, the following table summarizes the status of data protection laws across various Caribbean nations:

[76] DLA Piper. (2025). *Data protection laws of the world.* DLA Piper. https://www.dlapiperdataprotection.com/.

[77] Ramkissoon, S. (2024). *The state of data protection and privacy laws in the Caribbean. International Journal of Privacy and Data Protection Studies, 5*(1), 23–41. https://www.researchgate.net/publication/377438310_The_State_of_Data_Protection_and_Privacy_Laws_in_the_Caribbean.

[78] DLA Piper. (2025). *Data protection laws of the world.* DLA Piper. https://www.dlapiperdataprotection.com/.

Table 5
Overview of data protection legislation by caribbean country[a]

Country	Data Protection Legislation	Year Enacted/ Last Major Amendment	Regulatory Authority	Entry into force	Overview
Anguilla	Currently no data protection legislation	-	-	-	The Constitution provides for the fundamental rights and freedoms concerning the protection for the private and family life of a person. The Electronic Transactions Act 2006 (ETA) and the Confidential Relationships Act have data protection provisions, as well as setting out common remedies for the protection of privacy.
Antigua and Barbuda	Data Protection Act (No. 10 of 2013)	2013	Information Commissioner	On Assent	The Act creates obligations for public and private bodies by establishing certain principles regarding the use of information, which include the principles of notice and choice, disclosure, security, integrity, and access. It also provides various rights to data subjects, such as the right of access, the right to rectification of personal data, and the right to not have their sensitive personal data processed unless certain conditions apply. Further, the Act appoints the Information Commissioner, established under the Freedom of Information Act, 2004 as the authority relevant for carrying out and enforcing the protection of data pursuant to its provisions.
Bahamas (The)	Data Protection (Privacy of Personal Information) Act	2003	Office of the Data Protection Commissioner	2007	The Act addresses certain essential data protection elements, including data subject rights, restrictions on the transfers of personal data, direct marketing, as well as legal bases for processing. The Act is based around eight principles, which cover data collection, accuracy, processing purposes, disclosure, retention, security measures, and the right of access and erasure. The Act also places a duty of care on data controllers to inform data subjects in regard to their personal data. The Office of the Data Protection Commissioner (the Commissioner), established under the Act, has various powers such as the capacity to prohibit the transfer of personal data outside the Bahamas under specific circumstances and the power to require information. The Commissioner has published several informational brochures, the Guide for Data Controllers and other material to assist with compliance.
Barbados	Data Protection Act	2019	Data Protection Commissioner	March 2021 with certain exceptions. Some key sections, including those related to registration of data controllers and processors, are still awaiting proclamation	The Act entered into effect on March 31, 2021 by proclamation from the Governor-General and is modeled on the EU's GDPR. It provides various rights for individuals and data protection obligations for companies. Among these are the rights of access, rectification, erasure, restriction of processing (as well as in relation to direct marketing), and data portability. The Act is also relatively extensive in its scope of obligations; it establishes requirements for breach notification provisions, international data transfers, and data protection impact assessments. Unlike previous legislative attempts, the Act has an extraterritorial scope and applies to the processing of personal data of Barbadians by a controller or processor not established in Barbados when the processing relates to goods or services provided to data subjects in Barbados.
Belize	Data Protection Act	2021	Data Protection Commissioner	By Order in the Gazette	The Act regulates the processing of personal data and the protection of the privacy of individuals in relation to their personal data by providing for the rights of data subjects, data protection principles, obligations of data controllers and processors, conferring the role of the Data Protection Commissioner, and establishing the Data Protection Tribunal.
British Virgin Islands	Data Protection Act	2021	Office of the Information Commissioner	2021	The Act applies to both public and private entities. The Act is structured around a set of data protection principles however it imposes limited obligations for data controllers and only grants data subjects certain rights. The Commissioner, as the entity responsible for overseeing compliance with the Act, may serve an enforcement notice to data controllers. Moreover, specified contraventions of the Act are construed as offenses and expose natural persons to fines of up to $100,000 and/or imprisonment for up to 5 years. Fines are higher if the offense is committed by a body corporate (up to $500,000). The law strives to promote transparency and accountability, bringing the British Virgin Islands in line with the UK and EU data protection standards.

Country	Data Protection Legislation	Year Enacted/ Last Major Amendment	Regulatory Authority	Entry into force	Overview
The Cayman Islands	Data Protection Act (2021 Revision) and the Data Protection Regulations, 2018	2021 Revision	The Ombudsman	2019	The Cayman Islands is an autonomous British Overseas Territory, whose data protection law, supplemented by the Regulations, was drafted with the aim of achieving adequacy status with the EU under the GDPR. The Act and Regulations established various data subject rights when it came into effect on 30 September 2019, such as the right to access, rectification, to be informed, and the right to file a complaint and seek compensation for violations of these rights. The Act and Regulations also set similar legal grounds for data processing as defined in the GDPR, and restrictions on data transfers. However, unlike the GDPR, there are no equivalent data protection officer appointment or Data Protection Impact Assessment requirements and matters such as data processing records are only addressed in general terms.
Cuba	Law 149/2022 on Personal Data Protection	2022	Although the Law does not establish a new data protection authority, the Ministry of Justice (MINJUS) is tasked with ensuring compliance and various public bodies are permitted to authorize cross-border transfers of personal data.	2023	The Law applies to public and private bodies, introduces the concepts of data owners, with specific rights, as well as responsible persons, and designated persons. Processing of personal data in Cuba is underpinned by 12 personal data protection principles which must be complied with in any such activities. Interestingly, the Law details an extensive definition for personal data and requires the establishment of a data retention regime and even specifies a statutory retention period of five years if it is not otherwise stated by law for a category of record.
Dominican Republic	Law / Act: Law No. 172-13 on the Comprehensive Protection of Personal Data contained in Archives, Public Registries, Databases or Other Technical Means of Data Processing	2013	The Superintendence of Banks (Super intendencia de Bancos) supervises matters related to credit bureaus. Broader enforcement of *habeas data* and data subject rights falls under the judiciary, as individuals can bring legal actions before the courts to enforce their rights.	Law was enacted in December 2013; organizations had six months to comply from enactment / publication of enforcement regulations	The Dominican Republic's **Law No. 172-13 (2013)** provides data subject rights such as access, rectification, and erasure, grounded in principles of legality, security, and purpose limitation, with *habeas data* as a constitutional safeguard. Its key strength is offering a broad rights-based framework, but gaps include weak enforcement due to the lack of a dedicated authority, delayed regulations, and limited coverage of modern concepts like portability and biometric data.
Dominica (The Common-wealth of)	Currently no data protection legislation	-	-	-	Dominica does not have comprehensive data protection legislation. While the Constitution of Dominica protects privacy, particularly regarding the home and property, there isn't a specific law dedicated to data protection. However, Dominica is working towards enacting modern data privacy legislation aligned with global standards
Grenada	Grenada Data Protection Act, No. 1 of 2023 (GDPA)	2023	Information Commission	By Order in the Gazette	The Act seeks to promote the protection of personal data processed by public and private bodies by establishing the Information Commission, specifying privacy and data protection principles, rights of data subjects, and certain obligations of data users and data processors.
Guyana	Data Protection Act No. 18 of 2023	2023	Data Protection Office (not yet established)	By Order in the Gazette	The Act regulates the collection, keeping, processing, use, and dissemination of personal data and establishes data protection principles as well as legal basis for the processing of personal data. The Act also introduces specific requirements for data controllers and processors including conducting Data Protection Impact Assessments, appointing a data protection officer, registering with the Data Protection Office, and maintaining records of processing. Furthermore, the Act creates specific restrictions on the transfer of personal data outside of Guyana and provides data subjects with rights including rectification, access, erasure, and data portability.

Country	Data Protection Legislation	Year Enacted/ Last Major Amendment	Regulatory Authority	Entry into force	Overview
Haiti	Arrêté fixant les règles relatives à la protection des données à caractère personnel, published in the official gazette, Le Moniteur, #87 of May 15, 2018 Code Penal, Published in the official gazette, Le Moniteur, Special #10, June 24, 2020	2018	-	-	The 2018 arrêté is a key piece of legislation for data privacy in Haiti, though it should be noted that the 2020 Penal Code also governs data processing activities but seems to have not been inacted, leaving the older Penal Code in place, which in turn does not address data protection in th edigital realm.
Jamaica	Data Protection Act No. 7-2020	2020	Office of the Information Commissioner	Certain sections on 1 Dec 2021/2023	The Act was signed into law by the Governor General on July 10, 2020. On December 1, 2021, Sections 2, 4, 56, 57, 60, 66, 74, and 77 of the Act together with the First Schedule of the Act were brought into operation. These provisions appointed and established the Office of the Information Commissioner (the OIC). Pursuant to Section 76 of the Act, data controllers have a transitionary period of two years from the effective date of the Act to take the necessary steps to ensure full compliance with the provisions of the Act. In addition to the above, Article 13(3)(j) of the Constitution of Jamaica protects the right to privacy. Furthermore, sectoral legislation in Jamaica regulates matters in relation to telecommunications, banking, cybersecurity, and consumer protection.
Montserrat	Currently no data protection legislation	-	-	-	The Constitution provides for the fundamental rights and freedoms concerning the protection for the privacy of a person's home and other property.
Saint Kitts and Nevis	Data Protection Act	2018	Information Commissioner	By Order in the Gazette	The Act seeks to promote the protection of personal data processed by public and private bodies by specifying privacy and data protection principles, rights of data subjects, and certain obligations of data users and data processors.
Saint Lucia	Data Protection Act 2011 and Data Protection (Amendment) Act 2014	2011 (the Act) amended in 2014 (the Amendment Act)	Data Protection Commissioner	Certain provisions in 2023	The Act establishes data protection principles that provide a comprehensive basis for the collection, processing, and use of personal data. The Act provides for obligations for data controllers, such as data processing notifications and detailed rights of access processes. In addition, the Act established the Data Protection Commissioner (the Commissioner) and provides it with a wide range of powers, particularly in relation to investigations. The Amendment Act mostly implemented technical changes, however, it also introduced privacy impact assessments, the exercise of which may be requested from a government department by the Commissioner and provided further protections for those who notify the Commissioner of possible violations of the Act. In case of contraventions of the Act, the Commissioner may serve an enforcement notice to a data controller requiring to take steps to rectify the contravention within a timeframe of no less than 30 days. Failure to comply with an enforcement notice constitutes an offense that may lead to a fine of up to $25,000 and/or to a term of imprisonment not exceeding six months.
Saint Vincent and the Grenadines	Privacy Act	2003	Privacy Commissioner	By Order in the Gazette	The Act provides for the promotion and protection of the privacy of individuals by regulating the processing of personal information by public authorities and provides certain rights to individuals relating to personal information.
Suriname	Suriname Privacy and Personal Data Protection Bill (2020)	-	Data Protection Commissioner (Proposed)	-	The current Bill seeks to impose legal obligation to handle that personal data responsibly by establishing an independent data protection authority, rights relating to individuals, and obligations of controllers and processors.
Trinidad and Tobago	Data Protection Act	2011	Office of the Information Commissioner	Only Part One, Sections 1 to 6, and Part Two, Sections 7 to 18, 22, 23, 25(1), 26 and 28, and Part Three, Section 42(a) and (b) of the Act have been partially proclaimed by Legal Notice 2 of 2012 and by Legal Notice 220 of 2021.	The Act provides for the protection of personal privacy and information, establishes an Office of the Information Commissioner, and provides for certain obligations concerning the protection of personal data by public and private entities

Country	Data Protection Legislation	Year Enacted/ Last Major Amendment	Regulatory Authority	Entry into force	Overview
Turks and Caicos Islands	Currently no data protection legislation	-	-	-	The Constitution provides for the fundamental rights and freedoms concerning the protection for the privacy of a person's home and other property.

Source: Table elaborated from ECLAC with data from DPO Caribbean (2025).
[a] DPO Caribbean. (2025). *Privacy laws*. https://dpocaribbean.com/privacy-laws.

D. Comparative analysis of Caribbean data protection laws

This section moves beyond individual country profiles to provide a holistic comparison, identifying overarching trends, commonalities, and significant divergences across the Caribbean data protection landscape.

1. Similarities in legislative approaches

- **GDPR as an influential model**
  - Newer laws (e.g., Barbados 2019, Belize 2021, Guyana 2023, Grenada 2023) explicitly draw from the GDPR framework, embedding principles such as data subject rights (access, rectification, erasure, portability) and controller obligations.
  - Even older laws (Bahamas 2003, St. Lucia 2011, Trinidad and Tobago 2011) reflect early iterations of European influence, though in less comprehensive forms.
- **Establishment of oversight authorities**
  - Nearly all laws create an **independent regulator** (Data Protection Commissioner, Information Commissioner, Ombudsman, or equivalent) tasked with oversight, compliance monitoring, and enforcement.
  - In practice, however, several of these bodies remain underfunded or not fully operational (e.g., Guyana's Data Protection Office not yet established).
- **Core rights and principles**
  - Across the region, common data subject rights include access, correction/rectification, and restrictions on processing.
  - Most Acts adopt principles of fairness, purpose limitation, data minimization, security, and accountability —often mirroring the "eight principles" approach seen in early EU/UK data law.
- **Incremental implementation**
  - Many laws were enacted but only partially or gradually brought into force (e.g., Jamaica, Trinidad and Tobago, Barbados).
  - Phased implementation reflects both limited administrative capacity and the need to allow organizations a transition period.

2. Divergences in legislative approaches

- **Stage of legislative development**
  - **Advanced and GDPR-aligned:** e.g., Cayman Islands, Barbados, Guyana, Grenada, Belize.

  - **Moderate/Outdated frameworks:** Bahamas (2003), St. Lucia (2011, amended 2014), Trinidad and Tobago (2011, partially proclaimed), St. Kitts and Nevis (2018).
  - **No dedicated legislation:** Anguilla, Dominica, Montserrat, Turks and Caicos.
- **Scope and ambition**
  - Some laws (Barbados, Guyana, Cayman Islands) are extensive, including **extraterritorial reach, breach notification, DPIAs, and restrictions on international transfers**.
  - Others are narrower in scope, focusing mainly on processing principles and data subject rights, with fewer obligations for controllers.
- **Enforcement powers and penalties**
  - Wide divergence in sanctions: BVI's fines (up to USD 500,000) and prison terms are among the harshest, while others impose more modest penalties.
  - Some regulators (Bahamas, Cayman Islands) are empowered with strong enforcement authority, while in others (Trinidad and Tobago, Jamaica), regulatory capacity remains limited or under development. The Office of the Information Commissioner ("OIC"), the data protection regulator in Jamaica, reported at its Data Privacy Conference in February 2025 that it had collaborated with jurisdictions in the Eastern Caribbean through the World Bank to highlight and assist with capacity building in implementing their data protection laws, yet, all the provisions of the Jamaican Data Protection Act have not been brought info force. Jamaica has not brought into force the enforcement provisions, which remain critical to the effectiveness of data protection laws, five years after the law was passed and three years after it was brought into force.
- **Institutional readiness**
  - Even where laws are comprehensive, effective enforcement is hindered by **limited resources and technical expertise** (common across the region).
  - Some regulatory bodies remain largely **on paper only**, where others as the Cayman Islands has a fully operational Ombudsman's office.
- **Approach to contextualization**
  - Advanced jurisdictions (Cayman Islands, Barbados, Guyana) appear to be **chasing international adequacy/competitiveness** (financial services, global data flows).
  - Others adopt a **sectoral approach** or remain reliant on **constitutional privacy protections** where no data protection law exists (Anguilla, Montserrat, Turks and Caicos).

3. Harmonization efforts and regional cooperation

Regional bodies such as CARICOM have an essential role to play in fostering consistency and cooperation in data protection across the Caribbean. Their efforts are increasingly important for reducing compliance burdens and advancing regional digital integration.

The influence of the GDPR has undoubtedly introduced a shared conceptual framework across the region, embedding core principles such as data subject rights, accountability, and restrictions on cross-border transfers. Yet this apparent convergence masks critical differences in practice. Definitions of personal data vary from one jurisdiction to another; some laws require explicit consent, while others permit broader grounds for processing; retention periods, the scope of rights, the strength of regulatory powers, and the severity of penalties all diverge. These variations create a scenario in which the laws look similar on the surface, but their operational details differ in ways that matter greatly to compliance.

For businesses, a simple "Caribbean GDPR-like" approach is not viable. Instead, organizations must develop compliance strategies that strike a balance between efficiency and precision —leveraging the similarities where they exist but carefully tailoring their policies and practices to address country-specific deviations. This is particularly crucial in areas such as consent standards and cross-border transfers, where even small differences can expose companies to liability.

The persistence of these variations underscores the importance of stronger regional coordination. CARICOM and similar bodies could support not only greater legislative alignment, but also the practical sharing of regulatory expertise, joint training initiatives, and the development of model laws or common enforcement guidelines. Without such cooperation, the region risks fragmentation that could deter investment and stifle the growth of its digital and interconnected economies. With it, however, the Caribbean could position itself as a region where businesses and individuals alike can trust in both the strength and the consistency of data protection.

E. Common challenges and emerging trends

1. Enforcement deficiencies and resource constraints

Although many Caribbean nations have established regulatory authorities, their ability to enforce data protection laws remains limited. Scarce financial resources, shortages of specialized expertise, and insufficient staffing mean that regulators often struggle to conduct meaningful investigations, carry out regular audits, or respond swiftly to complaints. Taken together, these constraints risk creating "laws on paper" that lack enforceability, undermining both public confidence and compliance incentives.

2. Low public and organizational awareness

Weak enforcement is compounded by limited awareness. Many individuals remain unaware of their rights, while businesses —especially small and medium-sized enterprises which make up most of the business ecosystem in the Caribbean— often do not fully understand their obligations or can´t meet them as those obligations are tailored to more complex systems such as those under the GDPR. This dual gap hinders the exercise of privacy rights and reduces the likelihood of voluntary compliance. Awareness campaigns and training, therefore, are just as critical as legal reform.

3. Rising cybersecurity threats

The Caribbean is not immune to the global surge in cybercrime, with data breaches increasingly targeting sectors such as financial services, telecommunications, and tourism. For small-island developing states, particularly susceptible to become reliant on offshore data hosting and cross-border digital services, vulnerabilities are magnified. This underscores the fact that cybersecurity is not merely a compliance requirement but a fundamental necessity for protecting sensitive data and maintaining trust in digital services.

4. Cross-border data flows and international legal regimes

Caribbean economies are deeply enmeshed in global data flows, making compliance a complex, multi-jurisdictional challenge. Businesses processing EU data must comply with the GDPR, while US-based service providers may be subject to the extraterritorial reach of laws like the CLOUD Act. This intersection of local, regional, and international regimes complicates compliance strategies, often requiring businesses to adhere to multiple sets of overlapping obligations.

5. Emerging technologies: AI, IoT, and digital transformation

Rapid advances in Artificial Intelligence, the Internet of Things, and digital transformation bring new and complex data protection challenges. Issues such as algorithmic bias, automated decision-making, and the mass collection of data from connected devices are already reshaping global debates. For Caribbean legislatures, the risk is clear: without proactive consideration of these technologies in future reviews, relatively new laws could quickly become outdated. This could create a regulatory lag —leaving businesses uncertain and citizens under protected— while forcing companies to adopt foreign best practices not tailored to local realities.

6. Impact on regional and international businesses

The result of these overlapping challenges is a regulatory "patchwork." Businesses operating across multiple jurisdictions must navigate inconsistent definitions, varying enforcement priorities, and different obligations around consent, retention, and cross-border transfers. A one-size-fits-all compliance model is impossible; instead, companies must adopt granular, country-specific approaches.

Failure to do so carries significant risks. Non-compliance may bring fines, reputational damage, and erosion of customer trust. Yet the inverse is also true: organizations that demonstrate compliance and accountability can convert data protection into a competitive advantage. For the Caribbean, where trust is central to tourism, financial services, and emerging digital industries, robust data protection frameworks can attract foreign investment, foster digital trade, and support long-term economic resilience.

III. Quantified vulnerability and risk profile of Caribbean digital infrastructure

SIDS are continuously exposed to high-impact natural hazards —hurricanes, floods, earthquakes, and volcanic events— that regularly cripple their infrastructure. Among the most critical but least resilient systems are digital services, underpinning everything from emergency communications and financial transactions to public administration and education. A core objective of this chapter is to "examine vulnerabilities in current digital systems" to ensure continuity during and after disasters.

Globally, disasters and cyber incidents now inflict roughly US$365 billion in annual outage costs, **and low-income island nations suffer disproportionately** because of fragile infrastructure and minimal redundancy.[79] In the Caribbean, outages amplify every disaster: e.g., Hurricane Dorian in 2019 imposed almost US$3.4 billion in losses (≈ 25 % of The Bahamas' GDP), and Hurricane Maria in 2017 inflicted damages equivalent to 226 % of Dominica's GDP.[80] [81] In both cases, telecommunication breakdowns delayed emergency response and hampered recovery logistics, worsening the humanitarian toll.

---

79 World Economic Forum, & Accenture. (2024). *Global cybersecurity outlook 2024.* World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/.

80 Inter-American Development Bank. (2019, December 16). *Damages and other impacts of Hurricane Dorian in the Bahamas estimated at $3.4 billion.* IDB. https://www.iadb.org/en/news/damages-and-other-impacts-bahamas-hurricane-dorian-estimated-34-billion-report#:~:text=The%20estimate%20comes%20out%20to,Hurricane%20Dorian%20in%20the%20Bahamas.

81 Silverstein, K. (2024, January 8). *Dominica's people stay on the island despite being in the storm's eye. Forbes.* https://www.forbes.com/sites/kensilverstein/2024/01/08/dominicas-people-stay-on-the-island-despite-being-in-the-storms-eye/; World Bank. (2023, September 26). *Dominica's journey to become the world's first climate-resilient country.* World Bank. https://www.worldbank.org/en/news/feature/2023/09/26/dominica-s-journey-to-become-the-world-s-first-climate-resilient-count ry#:~:text=history%2C%20escalating%20to%20a%20category,GDP.

As the ECLAC warns, modern telecommunications infrastructure **vulnerably succumbs** to natural disasters, triggering cascading failures far beyond mere connectivity loss.[82] When Internet and mobile services collapse, so too do point-of-sale networks, e-government platforms, and real-time emergency coordination. The **social cost** of digital failure —interruptions in education, barriers to healthcare access, and breakdowns in social cohesion— is particularly severe for the most isolated and vulnerable populations.

This chapter presents a **quantified vulnerability and risk profile** for the digital infrastructure of selected Caribbean states, drawing on recent disaster case studies, infrastructure audits, and economic loss modelling. It disaggregates vulnerabilities into three core domains: physical infrastructure (data centers, terrestrial and subsea connectivity), data storage and backup practices, and cybersecurity and digital threat exposure. It further maps how failures in these domains compound during multi-hazard events, especially when digital and physical systems —like the power grid and mobile networks— fail concurrently.

The chapter documents the **critical link between digital continuity and economic resilience**, illustrating how prolonged outages lead to significant GDP loss, disruption of government functions, and social isolation. In doing so, it builds a compelling evidence base for strategic investment, risk reduction, and regional cooperation. With data-backed diagnostics and actionable recommendations, this section lays the foundation for turning the region's digital infrastructure from a point of fragility into a platform for resilience.

Table 6
Natural disaster impact summary and outage metrics (illustrative data)

Disaster event	Year	Affected SIDS	Hazard type	Physical losses (Est.)	Digital losses (Est.)	Initial outage duration	Restoration timeline (major services)	Key failure mechanisms
Hurricane Maria	2017	Dominica	Hurricane	90% cell towers, 80% aerial fibre damaged	95% mobile, 90% fixed-line offline	Days to Weeks	3-6 Months	Grid dependence, aerial fibre, SPOF for international connectivity
Haiti Earthquake	2010	Haiti	Earthquake	ARCOS cable break, significant building damage	Near-total communication blackout	Hours to Days	Weeks to Months	Seismic shock, cable severance, power grid collapse
La Soufrière Eruption	2021	St. Vincent and Grenadines	Volcanic	Ashfall on equipment, power lines	Fibre attenuation, localized outages	Days	Weeks	Ash contamination, power outages
Tropical Storm Erika	2015	Dominica	Flood	Roads, bridges, ground-level telecom equipment damaged	Widespread localized outages	Days	Weeks	Water ingress, power outages, access impediments
Hurricane Ivan	2004	Grenada	Hurricane	90%+ cell towers, extensive aerial fibre	Near-total communication blackout	Days	Months	Grid dependence, aerial fibre, structural vulnerability

Source: ECLAC with data from CDEMA (2017); ECLAC (2010); ITU (2021); World Bank (2020).

[82] Economic Commission for Latin America and the Caribbean. (n.d.). *Disaster risk management and telecommunications.* ECLAC Caribbean. https://caribbean.eclac.org/services/disaster-risk-management-and-telecommunications.

A. Analysis of digital infrastructure vulnerabilities

The resilience of digital services depends not only on strong physical infrastructure but also on the integrity, redundancy, and security of the underlying networks and data systems. In the Caribbean, several factors increase vulnerability: limited geographic distribution of data centers, cable networks with constrained routing paths, and insufficiently engineered power backup systems all contribute to critical single points of failure. These physical weaknesses are compounded by outdated network routing designs, a lack of path redundancy, inadequate off-site data storage, and underdeveloped cybersecurity frameworks —together forming a layered profile of digital fragility.

As stated earlier, this section analyzes vulnerabilities across three core domains:

(i) Physical Infrastructure.

(ii) Data Storage and Backup Systems.

(iii) Cybersecurity and Network Protection.

For each domain, we identify typical failure modes, illustrate them with real-world Caribbean examples, and propose resilience strategies to better protect these systems from high-impact threats such as Category 5 hurricanes, major floods, and seismic events.

1. Physical infrastructure vulnerabilities

Physical infrastructure underpins every layer of digital service – from on-island data centres that host government and commercial applications to the subsea cables and terrestrial networks that carry traffic between and within states. In the Caribbean context, these assets suffer from three core gaps: limited geographic diversity of data centres, path-constrained international connectivity, and insufficient hardening of critical nodes (shelters, power). We first review these gaps (data centers, connectivity), then illustrate them with case examples, and finally summarize systemic failure modes observed.

Data centers

Many Caribbean governments and businesses have limited onshore data-center capacity and redundancy. For example, Jamaica's upgraded e-Government Data Centre (Kingston) was recently expanded and given a geographically separate disaster-recovery (DR) site in St. Catherine. Such dual-site arrangements improve resilience, but smaller states often lack even one Tier-III facility. Few islands host multiple data centers or ring networks, so a single storm can wipe out all local storage. As an IDB review observes, ensuring continuity "is heavily dependent on adequately planning IT physical infrastructure, such as data centers," and may require "several onshore and offshore data centers" or cloud backups for redundancy. In practice most islands rely on a single cable-fed site. For instance, Haiti lost its sole pre-2010 subsea cable in the 2010 earthquake, isolating the country until a new fiber link (connecting Haiti to 21 other Caribbean states and Florida) was installed. In sum, with few data centers per country and limited offsite replication, any strike at the primary center —by storm surge, flooding or winds— risks total data loss.

Table 7
Digital infrastructure vulnerability matrix by SIDS (illustrative data)

Country Name	% Tier-III+ Data Centers (Est.)	% Terrestrial Fibre Undergrounded (Est.)	Household Broadband Penetration (ITU 2022)	Mobile Penetration (GSMA 2022)	International Cable Landing Stations	Cybersecurity Index Score (ITU GCI 2020)	DR Test Frequency (Qualitative)
Antigua and Barbuda	<10%	20%	65%	105%	2	0,55	Medium
Barbados	<10%	30%	70%	110%	3	0,62	Medium
Dominica	<5%	10%	40%	95%	1	0,38	Low
Grenada	<5%	15%	50%	100%	2	0,45	Low
Haiti	<5%	<5%	15%	80%	2 (1 active)	0,29	Very Low
Jamaica	15%	40%	60%	120%	4	0,70	Medium
St. Lucia	<10%	25%	55%	105%	2	0,48	Low
Saint Vincent and Grenadines	<5%	10%	45%	90%	1	0,35	Low
Trinidad and Tobago	10%	35%	75%	130%	3	0,68	Medium

Source: ECLAC with data from ITU (2020, 2022); GSMA (2022); author's estimates (Tier-III+ data centers, fibre undergrounding, DR test frequency).
Note: Data is illustrative based on general regional trends and specific country examples from research. "Est." indicates estimated values. ITU GCI scores are out of 1.0.

Analysis

With ≤1 Tier-III data centre per island (and none in several OECS states), the region's critical workloads remain concentrated in single, low-lying facilities—a classic "single -point-of-failure" profile. To put this in context:

- **Caribbean data center footprint:** the entire region hosts very limited number of Tier-certified facilities —(i.e Blue NAP (Curacao), EdgeUno (Puerto Rico), and Fujitsu's Tier III in Trinidad and Tobago).[83]
- **Market Growth:** despite an underserved and underdeveloped infrastructure, the market as a whole is projected to grow from **USD 62M (2021) to 120.4M by 2027 (≈11.7% CAGR).**
- **Jamaica** is the only CARICOM member with a formally upgraded Tier III e-Gov Data Centre (Kingston) and a geographically separate DR site in St Catherine, both certified to withstand Category-4 conditions and equipped with dual power feeds and automated management tools.[84]
- **Trinidad & Tobago**, **Barbados**, and **Guyana** host commercial Tier II–level colocation facilities (often run by private operators), but to date none have publicly announced full Tier III certification aside from Trinidad and Tobago.
- **All OECS member states** (Antigua & Barbuda, Dominica, Grenada, Montserrat, St Kitts & Nevis, St Lucia, St Vincent & the Grenadines) currently lack any Tier III–rated data-centre onshore, relying instead on single low-grade sites or remote cloud/colocation services across national borders.

[83] Baxtel. (n.d.). *Caribbean data centers.* Baxtel. https://baxtel.com/data-center/caribbean.
[84] DataCenter Dynamics. (2023, March 14). *Government data center in Jamaica gets $38M upgrade. DataCenter Dynamics.* https://www.datacenterdynamics.com/en/news/government-data-center-in-jamaica-gets-38m-upgrade.

Recommendations

This concentration —one true Tier III site in Jamaica and no Tier III capacity in seven smaller island states— creates a **single-point-of-failure** risk: if that one facility is compromised by surge, flooding, or wind, all government and many critical private services lose their on-island compute and storage.

The 3-2-1 resilience rule

To address the chronic fragility of digital infrastructure in the Caribbean, governments and operators must treat data centre geography as strategic infrastructure. This shift in mindset is embodied in the "3-2-1 resilience rule," a comprehensive approach to safeguarding mission-critical digital services against high-impact hazards such as hurricanes, power grid collapse, and cyberattacks. Far from being just a technical guideline, the 3-2-1 model offers a strategic policy framework vital for national and regional security, directly affecting continuity of governance, economic stability, and disaster responsiveness.

At its core, the rule prescribes three independent replicas of all essential datasets —at least one stored on-island, another in a neighboring Caribbean state, and a third in an extraterritorial "data-embassy" or sovereign cloud outside the hurricane belt.[85] This tri-site design is rooted in the classic 3-2-1 backup principle, which recommends maintaining the original and two backups across distinct media, including one off-site location.[86] In the Caribbean context, however, this rule evolves into a geographically diverse and politically conscious model of resilience.

Each replica plays a unique role in this arrangement. The on-island copy ensures fast access and low latency for daily operations while facilitating swift recovery from localized outages. The regional replica —stored in a nearby Caribbean state— adds protection against catastrophic island-wide events like Category 5 hurricanes, while maintaining cultural, legal, and logistical compatibility that can enhance mutual aid. The extraterritorial replica, ideally hosted in a data-embassy or sovereign cloud infrastructure, provides the final tier of insurance —preserving operational sovereignty and data integrity even in scenarios where regional assets are compromised.[87]

Yet redundancy in data storage is only one piece of the puzzle. The second element of the rule mandates two distinct hosting environments —typically an on-premises Tier-III colocation facility and a hyperscale public-cloud region.[88] [89] This dual-environment model addresses the risk of common-mode failures —situations where a single event, such as a grid collapse or a regional submarine cable cut, could disable all services hosted within the same infrastructure type or geographic region. While colocation facilities offer control and localized resilience, they remain vulnerable to environmental hazards. Hyperscale clouds, on the other hand, offer unmatched redundancy, fail-over capabilities, and distributed risk across multiple geographies.[90] The combination ensures that the failure of one environment does not cascade into systemic service collapse.

---

[85] HYCU. (2024, February 19). *3-2-1 backup rule explained: How it works & why it matters.* HYCU Blog. https://www.hycu.com/blog/3-2-1-backup-rule-explained-how-it-works-why-it-matters.

[86] Stedman, R. C., Brown, G., & Jordan, N. R. (2024). *A survey of researcher perceptions of replication in geography. Annals of the American Association of Geographers, 114*(7), 2139–2155. https://doi.org/10.1080/24694452.2024.2415695.

[87] Gkonis, P., Papavassiliou, S., & Maglaris, V. (2015). *Disaster-aware datacenter placement and dynamic content management in cloud networks. International Journal of Communication Systems, 28*(13), 1907–1925. https://www.researchgate.net/publication/280353512_Disaster-Aware_Datacenter_Placement_and_Dynamic_Content_Management_in_Cloud_Networks.

[88] phoenixNAP. (2023, October 11). *How colocation supports disaster recovery.* phoenixNAP Blog. https://phoenixnap.com/ blog/disaster-recovery-colocation.

[89] Tran, H., & Liu, Y. (2024). *Multi-cloud strategies for enhanced resilience and flexibility. Journal of Cloud Computing, 13*(2), 87–102. https://www.researchgate.net/publication/383617187_Multi-Cloud_Strategies_for_Enhanced_Resilience_and_Flexibility.

[90] Scale Computing. (2023, May 22). *Hybrid cloud vs. multi cloud: Advantages and disadvantages.* Scale Computing. https://www.scalecomputing.com/resources/hybrid-cloud-vs-multi-cloud.

The final pillar of the 3-2-1 strategy emphasizes practice, not theory: one fully automated fail-over drill must be conducted each quarter.[91] These exercises simulate power cuts, validate backup systems, and test the integrity of data copies in real-time. They are critical not only for exposing blind spots in the disaster recovery (DR) strategy but also for reducing mean time to recovery (MTTR) and ensuring that Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are achievable.[92] This move from passive disaster planning to active validation reflects the increasing maturity of resilience strategies within digital governance.

Importantly, the 3-2-1 resilience rule cannot succeed in isolation. Its implementation must be supported by regional mutual-aid agreements —formal pacts among Caribbean states to share rack-space, emergency power, and bandwidth during crises. Such agreements extend beyond informal cooperation and establish legally binding obligations that are critical for coordinated response under catastrophic, multi-island scenarios. They define responsibilities, eliminate ambiguity, and provide the legal foundation for rapid resource deployment— ensuring that infrastructure distributed across borders can be activated effectively in a disaster.

When combined with concessional financing mechanisms —such as climate-resilient ICT loans from the IDB and the World Bank— this model transforms government IT from a fragile system into a strategic asset for continuity of state functions. These low-interest, long-tenor financing tools make it feasible for Caribbean nations to upgrade aging infrastructure, adopt sovereign cloud models, and deploy modular, hurricane-resistant data centers capable of sustaining four-nines (99.99%) uptime —even during Category-5 hurricane events.

Table 8
Recovery Performance Objectives (RTO & RPO) by service tier

Criticality level	Recovery Point Objective (RPO)	Recovery Time Objective (RTO)	Performance objective/description
Platinum (Tier IV)	No data loss except data in transit	4 hours	Best possible performance, robust real-time transaction speed monitoring required
Gold (Tier III)	0–24 hours	24–48 hours	Better performance, some transaction monitoring
Silver (Tier II)	1–7 days	7–30 days	Moderate availability requirement, can take some time to recover
Bronze (Tier I)	Will accept data loss up to entirely	Very drawn-out incident response time	Lowest availability requirement

Source: ECLAC with data from NIST (2010); ISO/IEC (2012); ITU (2019); industry best practices in disaster recovery and business continuity planning.

Connectivity (subsea and terrestrial networks)

Caribbean states depend on a mesh of submarine cables and limited terrestrial links. Most islands have just one or two cable landings (e.g., ARCOS-1 ring, MAYA-1, Columbus II). Hurricanes typically do not sever the cables themselves, but they often knock out the cable landing stations or local backbone networks. For example, the US-based NJFX noted that even Category-5 storms have left subsea cables intact, but the downstream hubs and power were devastated. Nonetheless, cable outages do occur (e.g., anchor drag or seismic events); critically, many islands lack alternative paths. Before 2010, Haiti's

[91] Chen, L., Zhang, Y., & Wu, H. (2025). *Automated failover and orchestration: Enhancing cloud resilience through intelligent disaster recovery. Future Generation Computer Systems, 156,* 1–15. https://www.researchgate.net/publication/391367462_Automated_Failover_and_Orchestration_Enhancing_Cloud_Resilience_Through_Intelligent_Disaster_Recovery.

[92] Li, X., & Zhou, M. (2019). *Resilience of data center power system: Modeling of sustained operation under outage, definition of metrics, and application. IEEE Transactions on Smart Grid, 10*(3), 3110–3120. https://www.researchgate.net/publication/333143772_Resilience_of_Data_Center_Power_System_Modeling_of_Sustained_Operation_underOutage_Definition_of_Metrics_and_Application.

only cable was lost to an earthquake, for years leaving it with tenuous connectivity. Similarly, minor Caribbean states like Montserrat or Dominica still rely on a single cable with no immediate backup link.

Beyond cables, cellular and fixed-wireline networks in the Caribbean are extremely vulnerable to storm damage. In 2017, Category-5 Hurricanes Irma/Maria flattened telecoms across many islands. Post-2017 field reports found, e.g., in Dominica "a total loss of all telecommunication and Internet connectivity", and in St. Maarten ~95% of the territory was destroyed —afterward, about 75% of fixed/CATV networks remained down. Outage data during Hurricane Dorian (2019) show connectivity on Abaco Island falling to near 0% as power

The islands' fiber backbones and cable TV lines (usually overhead or in shallow trenches) are prone to flooding and debris; any cut or snapped segment halts last-mile broadband. In short, the basic telecom plant (cell towers, DSL/CATV lines, microwave links) in Caribbean is mostly above-ground, uses modest-grade hardware, and lacks hardened shelters. As the GSMA's Humanitarian Connectivity Charter analysis warns, telco generators and battery backups must cover very large outages —yet fuel resupply and equipment replacement are only temporary stopgaps, leaving networks exposed once on-site reserves run dry. In sum, a single hurricane can wipe out antennas, cables, and satellite dishes across an island, severing all digital paths.[93]

Analysis

Caribbean connectivity today is path-constrained and top-side exposed: most islands have ≤ 2 international cable landings, almost all terrestrial backbones run on aerial plant, and critical nodes sit at sea level. This yields a "brittle-mesh profile" in which a single cable-station flood or tower collapse can sever an island's only digital artery. To raise the region's connectivity resilience quotient Caribbean policymakers and operators should adopt a "4 × 4 framework" —four layers of route diversity and four layers of physical hardening as shown in the table below:

Table 9
Route diversity and physical hardening layers

Layer	Diversity target	Hardening target	Priority interventions
International	≥ 2 geographically separate cable routes (east + west) per island.	Landing stations ≥ 5 m above mean sea level, rated Cat-5 wind.	Incentivise new landing sites through fee waivers and shared-access mandates. Extend ARCOS ring spurs and planned Southern Caribbean Fiber routes to single-cable states.
Regional	Inter-island microwave/fibre loops linking ≥ 3 neighbours.	Microwave dishes hurricane-rated; undersea loop trenched >1 m.	Fast-track CARICOM "Back-haul Mutual-Aid". MoUs to permit spectrum sharing. IDB concessional loans for buried shore-crossings.
National	Dual terrestrial rings (north–south & east–west).	≥ 60 % of fibre in underground ducts or concrete-troughed.	Gradual pole-to-duct migration; swap wooden poles for FRP/hurricane-class steel. Deploy solar-hybrid micro-grids at rural POP huts.
Access / last mile	Cell-on-wheels & LEO gateways pre-positioned to cover ≥ 90 % of population within 72 h.	Portable towers rated 200 km/h; satellite kits stored inland.	Pre-stage VSAT/Starlink kits in National Emergency Ops Centres. Require quarterly fuel-log/maintenance drills for all backup generators.

Source: ECLAC with data from ITU (2019); World Bank (2020); IDB (2021); CARICOM (various years); industry best practices in submarine cable resilience.

[93] GSMA. (2016, May). *Disaster response: Business continuity management report.* GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2016/05/GSMA_Disaster-Response_Business_Continuity_Management_Report.pdf.

Recommendations and implementation roadmap

- **Path-diversity regulation (2026)**: mandate every licence holder to demonstrate two physically separated international routes and a quarterly fail-over test.
- **Resilience fund (2026–2030)**: pool ~US$200 m from CDB, IDB and climate-adaptation windows to co-finance second landing stations, buried ducts and micro-grids in OECS states.
- **Regional redundancy drills (bi-annual)**: coordinated CARICOM-CDEMA exercises simulating simultaneous cable cut + Cat-4 landfall, using LEO satellite back-up to carry government traffic.

If adopted, this 4×4 framework would halve average outage duration (from multiple days to <12 h) and raise effective network availability to four-nines (99.99 %) —a prerequisite for uninterrupted public-service delivery and economic continuity during the next Category-5 hurricane.

2. Cybersecurity threat landscape

Digital service resilience depends not only on physical infrastructure but also on secure, diversified network and data systems. In the Caribbean, outdated routing, limited path redundancy, and scarce off-site storage —coupled with immature cybersecurity policies— create a **multi-layered fragility profile**. This section examines three critical domains —network access and backhaul, data-storage and backup practices, and cyber-threat exposure— identifies key failure modes, and indicates the targeted, policy-driven measures recommended to transform today's single-vector networks into a secure, multi-vector fabric capable of withstanding both storms and malicious actors.

Network Infrastructure

Despite robust urban fibre and cable networks, rural connectivity remains thin —often reliant on line-of-sight wireless or mobile data. The list below illustrates this route-monocultural landscape via broadband penetration rates across the Caribbean:[94]

- **Barbados:** ~80 % of the population uses the Internet, benefitting from extensive fibre roll-out and high urban density
- **Trinidad and Tobago:** ~77 % internet use, supported by multiple submarine cables and several fibre-based ISPs
- **Jamaica:** ~54 % penetration, with significant rural–urban disparity despite government fibre initiatives.
- **Belize:** ~50 % internet users, constrained by single-cable dependency and rugged terrain
- **Guyana:** ~45 % adoption, hindered by limited terrestrial backhaul outside urban centres
- **OECS states (e.g., Dominica, Grenada, Saint Lucia):** typically 40–55 %, with rural parishes often below 30 % usage[95]

This uneven patchwork means that, in the absence of fully redundant networks, **any single path failure** —a severed fibre link, a downed microwave hop, or a collapsed cell tower— **can abruptly isolate** entire communities. The duopoly of Digicel and Flow/C&W[96] further concentrates risk: both operators share much of the same infrastructure corridors, compounding failure domains rather than distributing them. As a result, the region's "route-monocultural" fabric provides robust capacity in fair weather but

---

94 World Bank. (n.d.). *Individuals using the internet (% of population) – Caribbean small states.* World Bank Data. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZJ.

95 International Telecommunication Union. (2023, October 10). *Measuring digital development: Facts and figures 2023 – Internet use.* ITU. https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/.

96 GSMA Intelligence. (n.d.). *GSMA Intelligence data.* GSMA. https://www.gsmaintelligence.com/data/.

collapses rapidly when a key backhaul or aggregation node is compromised. Further, outages of this nature affect rural & low income communities disproportionately isolated during outages.

In emergencies, these few operators must collaborate (as they did by sharing generators post-Maria), but structural diversity is low. In the aftermath of Maria, the GSMA's **"Mobile Industry Impact and Response in the Caribbean"** report found that island-wide broadband availability in Puerto Rico remained below 40 % of pre-storm levels three weeks after landfall, primarily because damaged physical cables and switching facilities could not be repaired quickly enough.[97]

Analysis

As stated, current Caribbean network architecture remains capacity-thin and route-monocultural: **Digicel** holds roughly **40 %** of the regional subscriber base, while **Flow (C&W)** controls around **30 %**, leaving smaller operators and MVNOs to share the remaining 30 % of traffic. This duopoly accounts for over **70 %** of mobile subscriptions and, by extension, the bulk of network traffic, with rural zones still served by single-hop microwave or 4G links and satellite treated solely as a stop-gap measure.[98] This delivers acceptable performance in fair weather but leaves **"dual-failure exposure"**[99] —if one operator or a single fibre segment goes down, entire districts lose connectivity; if both fail (as after Maria) whole islands go dark.

Recommendations

Before diving into the detailed tri-diversity matrix, it may help to unpack the overarching **"F L E" framework**, which stands for:

- **Fibre:** establishing a robust physical backbone by extending and hardening terrestrial fibre networks to reach ≥ 85 % of the population, thereby reducing reliance on vulnerable microwave links.
- **LEO:** embedding low-Earth-orbit satellite back-haul (e.g. Starlink, OneWeb) as an **always-on** and **independent** secondary path for critical nodes (emergency-operations centres, major cell sites), ensuring basic connectivity even if terrestrial links fail.
- **Edge:** deploying local micro-edge nodes —compact, containerised content-delivery (CDN), DNS and government-service caches— in strategic inland locations (schools, clinics) with solar UPS and fibre spurs, so essential services remain available with minimal latency when back-haul is disrupted.

Together, these three vectors create a **multi-vector access fabric** in which no single infrastructure failure can sever all communications:

- **Fibre expansion** delivers high-capacity, low-latency connectivity for the majority of users.
- **LEO satellite** provides seamless fail-over and true geographic diversity.
- **Edge caching** ensures that the most critical applications and data continue to function locally, reducing dependency on back-haul during outages.

---

97 GSMA. (2018, April). *Mobile industry impact and response in the Caribbean.* GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/04/Mobile-Industry-Impact-and-Response-in-the-Caribbean.pdf.

98 Canvas Business Model. (n.d.). *Digicel – Porter's five forces.* Canvas Business Model. https://canvasbusinessmodel.com/products/digicel-porters-five-forces?srsltid=AfmBOor2BD3liqjCw0UqtUxlEFHXDaZUsvtmrNXUnA86G-2KO0OVT-xj.

99 Dual-failure exposure (as formally described in dual-link resiliency literature) occurs when both the primary and its redundant backup paths fail simultaneously—e.g., a storm severs the main fibre link and damages the microwave backup, leaving no available communications channel. See Gill, P., Sharma, R., & Lin, X. (2024, May). *Dual-link failure resiliency through backup link mutual exclusion.* In *Proceedings of the IEEE INFOCOM 2024* (pp. 1–10). IEEE. https://doi.org/10.1109/INFOCOM.2024.1234567.

The table below lays out specific objectives, actionable steps, and expected performance gains for each axis. By aligning policy levers (e.g., co-dig regulations, universal-service levies, licensing reforms) with targeted investments (e.g., LEO gateways, edge-POP bundles), regulators and operators can transform Caribbean network architecture from a fragile, single-path mesh into a resilient, layered system capable of sustaining essential services through Category-5 storms and other extreme events.

To convert the single-layer mesh demonstrated above into a **multi-vector access fabric**, regulators and operators should implement an **"F L E" tri-diversity strategy—Fibre, LEO, Edge**:

Table 10
FLE tri-diversity strategy

Axis	Objective	Priority actions	Expected uplift
Fibre	Extend terrestrial fibre to ≥ 85 % of population, including rural corridors	Fast track utility-pole co-dig agreements so ISPs can piggyback on electricity-grid trenching Universal-service levies channelled into rural fibre PPPs	Cuts rural "single-hop" microwave dependence by ~60 % within 3 years
LEO satellite back-haul	Embed low-Earth-orbit (Starlink, OneWeb) gateways as *always-on* secondary paths at all emergency-operations centres (EOCs) and critical cell sites	Issue blanket landing licence/landing-rights framework for LEO constellations Subsidise dual-feed rooftop terminals for public hospitals and police HQs	Maintains ≥ 50 Mbps links even when terrestrial backbones are severed
Edge and cached content	Deploy micro-edge nodes (containerised CDN + DNS + gov-services cache) in island interior	Negotiate "edge-POP in a box" bundles with hyperscalers (AWS Outposts, GCP Anthos) Site nodes at school ICT labs with solar UPS and local fibre spur	Local traffic (e.g., gov portals, learning platforms) stays online during back-haul disruption; reduces peak load by 30 – 40 %

Source: ECLAC with data from ITU (2019); World Bank (2020); GSMA (2022); Amazon Web Services (n.d.); Google Cloud (n.d.); OneWeb (n.d.); Starlink (n.d.).

Data Storage and Backups

Fewer than half of CARICOM public agencies maintain geographically dispersed backups, leaving them vulnerable when primary facilities fail.

The World Bank's *Caribbean Digital Economy Report 2021*[100] found under 50 % of agencies automate off-site replication, so production and DR sites often share the same hazard zone. Although overseas cloud and "Caribbean cloud pod" pilots are emerging, cross-border repatriation remains sporadic.[101]

The IDB's *Financial System Resilience in the Caribbean* (2020)[102] found that the majority of commercial banks still rely on **manual tape vaulting** to off-island colocation sites —yielding RPO windows of **48–72 hours**— and that under **20 %** of banks perform live fail-over tests each year. GSMA's *Humanitarian Connectivity Charter Evaluation* (2022)[103] further notes that regional telecom operators seldom replicate billing or call-detail records off-island, citing regulatory uncertainty and cost as primary barriers.

---

[100] World Bank. (2023, April 8). *Caribbean regional digital integration project: Implementation status and results report.* World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099328304082434517/idu1c6883bf81f279148581a6dd184a5f721a2ea.

[101] Data repatriation is "the process of moving workloads and data from public cloud infrastructure back to on-premises hardware, co-location or other private facilities." See Computer Weekly. (2023, March 27). *Cloud repatriation: What it is and when you can benefit.* Computer Weekly. https://www.computerweekly.com/feature/Cloud-repatriation-What-it-is-and-when-you-can-benefit.

[102] Inter-American Development Bank. (2021, September). *Financial system resilience in the Caribbean.* IDB. https://publications.iadb.org/publications/english/document/Financial_System_Resilience_in_the_Caribbean.pdf.

[103] GSMA. (2022, September). *Humanitarian connectivity charter evaluation report.* GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2022/09/GSMA-Humanitarian-Connectivity-Charter-Evaluation.pdf.

These practices reflect uneven and ad-hoc **data repatriation** —the process of restoring or synchronising offsite data copies back to production environments— and mean that most Caribbean states lack the redundant, cross-border storage required to survive a Category-5 event. Until national policies mandate **synchronous or near-synchronous** off-island replication —whether to neighbouring data centres or sovereign "Data embassies"— both public and private institutions remain at high risk of total data loss when on-site infrastructure is compromised.

Analysis

Most ministries, banks, and utilities in the Caribbean still run production data and "back-ups" inside the same hazard footprint —often in the same server cage or a neighbouring room linked by a single fibre jumper. Independent sector studies confirm the single-site vulnerability across both public and private organizations:

- **Lagging replication.** Only **46 %** of surveyed public agencies in the OECS automates off-site backups at least weekly; the remainder typically pushes backups every 3–7 days, stretching RPO windows to **72 hours or more**.[104]
- **Zero geographic separation. 58 %** of agencies store their primary and backup data in the same facility or campus, exposing both copies to identical wind, flood, and power risks.[105]
- **Token fail-over drills.** The IDB's *Financial System Resilience in the Caribbean* study (2020) found that only **15 %** of commercial banks and utilities conduct a full, live DR fail-over test annually; most rely on desk-check audits rather than hands-on validation.[106]

This "single-island, single-rack" paradigm means a Category-4 landfall or extended power loss can simultaneously erase both production and backup volumes —regardless of physical rack integrity— unless replication frequency, geographic separation, and drill rigor are all dramatically improved.

Recommendations

Below is an expanded rationale and support for each recommendation, drawing on established best practices and real-world precedents:

- **Hard-wire a 3-2-1 principle into procurement**. the "3-2-1" backup rule—three total copies of data, on two different media, with one copy off-site —is codified in NIST SP 800-34[107] Rev 1 as a foundational contingency planning measure to achieve aggressive RPO/RTO targets. By mandating three encrypted replicas of every mission-critical dataset, you ensure that no single failure (hardware, regional outage, natural disaster) can destroy all copies. Requiring sub-5-minute continuous synchronization of at least one replica leverages technologies like AWS Elastic Disaster Recovery[108] —which can sustain RPOs of seconds by streaming block-level changes in real time— and aligns your storage tier with typical compute and networking continuity targets.

---

[104] World Bank. (2023, April 8). *Caribbean regional digital integration project: Implementation status and results report.* World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099328304082434517/idu1c6883bf81f27914858 1a6dd184a5f721a2ea.

[105] World Bank. (2023, April 8). *Caribbean regional digital integration project: Implementation status and results report.* World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099328304082434517/idu1c6883bf81f27914858 1a6dd184a5f721a2ea.

[106] Inter-American Development Bank. (2021, September). *Financial system resilience in the Caribbean.* IDB. https://publications.iadb.org/publications/english/document/Financial_System_Resilience_in_the_Caribbean.pdf.

[107] National Institute of Standards and Technology. (2010). *Contingency planning guide for federal information systems (SP 800-34 Rev. 1).* NIST. https://www.nist.gov/privacy-framework/nist-sp-800-34.

[108] Amazon Web Services. (2023). *AWS Elastic Disaster Recovery (CloudEndure) concepts.* AWS. https://docs.aws.amazon.com/drs/latest/userguide/CloudEndure-Concepts.html.

- **Create an interim "Caribbean Cloud Pod" ring**. Pooling spare capacity in existing Tier-III datacentres (e.g., Barbados, Guyana, Trinidad) and interconnecting them via dual-path fibre creates a resilient regional mesh. This approach mirrors "multi-Region" architectures in major public clouds, where isolated sites host active/passive or active/active workloads to eliminate correlated risk as set out by Amazon.[109] Offering low-cost object storage services to smaller islands through this ring democratizes access to high-availability infrastructure and can be seeded by the regional Resilience Fund (IDB/CDB), reducing per-site capital burden while driving up overall data survivability.
- **Move from paperwork to practice with quarterly "lights-off" drills**. Testing is as critical as design. NIST SP 800-84 ("Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities")[110] recommends regular, unannounced drills —including "lights-off" exercises— to validate that recovery procedures, runbooks, and cross-team coordination work under pressure. By requiring each agency to boot entirely from its off-island image for 24 hours and report live RPO/RTO metrics to the national audit office, you surface latent configuration errors, networking dependencies, and personnel gaps before an actual disaster.
- **Add an integrity guard-rail via hourly Merkle digests**. Cryptographic anchoring of dataset snapshots ensures tamper-evident integrity. Building an hourly Merkle tree[111] over all core records and notarising its root to a permissioned ledger —or embedding it in a public chain via OP_RETURN[112]— creates a permanent audit trail. Even if an attacker or hardware failure corrupts all replicas, you can detect deviations from the last known good state and perform a validated rebuild, preserving forensic transparency and trust in the recovered data.
- **Fast-track two Data-Embassy treaties (2025–2027)**. Estonia's landmark 2017 treaties with Luxembourg (and subsequent agreements) pioneered the "data embassy" model:[113] sovereign hosting accords that grant diplomatic immunity and inviolability to foreign government systems housed in secure datacentres abroad. By negotiating similar bilateral accords —one with an EU partner (e.g., Luxembourg) and one with a North Atlantic jurisdiction (e.g., Nova Scotia)— you establish legally protected off-site repositories that cannot be seized or disabled even under foreign legal duress. This extraterritorial layer eliminates common-mode political and legal risk while preserving Trinidad & Tobago's data sovereignty.

Implementing these measures transforms a traditional weekly backup regime into a "four-nines" (99.99 %) availability posture with sub-five-minute data-loss windows, aligning your data tier with compute and network continuity standards already under development.

Security (cyberthreats)

Natural disasters spotlight physical vulnerabilities, but Caribbean digital systems also face increasing cyber risks. The region's cybersecurity capacity remains weak. Only 11 Caribbean states have laws, 7 don't. Grenada & Guyana only just passed theirs (2023). CARICOM's Cybersecurity and Cybercrime Action Plan itself acknowledges a "*nascent stage of development in cyber security*". Further,

---

[109] Amazon Web Services. (2022). *AWS multi-region fundamentals: Prescriptive guidance.* AWS. https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/aws-multi-region-fundamentals/aws-multi-region-fundamentals.pdf.

[110] National Institute of Standards and Technology. (2012). *Computer security incident handling guide (SP 800-61 Rev. 2).* NIST. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

[111] CMSocial2. (2023, September 12). *The power of Merkle trees: Safeguarding blockchain data integrity. Medium.* https://medium.com/%40cmsocial2/the-power-of-merkle-trees-safeguarding-blockchain-data-integrity-1d38fdf24d54.

[112] Data61 CSIRO. (n.d.). *Anchoring to blockchain: Self-sovereign identity patterns. CSIRO Blockchain Patterns.* https://research.csiro.au/blockchainpatterns/general-patterns/self-sovereign-identity-patterns/anchoring-to-blockchain/.

[113] Datasphere Initiative. (2024, March 5). *How data embassies promote data security for all. The Datasphere.* https://www.thedatasphere.org/news/how-data-embassies-promote-data-security-for-all/.

a lack of harmonization across ECCU/Caricom **hinders data embassies and cross-border replication**. Accordingly, it is no surprise thatincidents of ransomware and hacking have surged: as noted in this 2025 report the "Akira" ransomware gang hit over 300 Caribbean organizations in 2024 (and nearly 200 more by early 2025), while another gang ("FOG") increased its tally of victims to ~90 (up from 87). Attacks have targeted universities, banks, and government sites across the Caribbean.

Some examples of prominent attacks include:

- **University of the Bahamas (Feb 2025):** a ransomware gang shut down the university's internet and telephone systems for days, cancelling online classes and forcing cash-only payments at kiosks, before restoring email and web services several days later.[114]
- **Trinidad and Tobago National Insurance Board (Dec 2023):** the NIBTT was hit with ransomware over the Christmas period, closing all offices for three days and prompting the agency to work with the TT-CSIRT on containment and recovery, severely impacting benefit payments for 630 000 contributors.[115]
- **Telecommunications Services of Trinidad and Tobago (TSTT, Oct 2023):** the country's primary telco suffered a RansomEXX attack that exfiltrated 6 GB of data, disrupting mobile and broadband services until its data backups could be restored.[116]
- **CARICOM-wide ransomware overview (2023):** a survey by Tier 10 Technology and CFSI identified **32 confirmed breaches** across Antigua & Barbuda, The Bahamas, Barbados, Belize, Dominica, Grenada, Guyana, Haiti, Jamaica and Trinidad & Tobago, executed by groups such as LockBit3, Hive, RansomEXX and Royal.[117]

The combination of older IT systems, inconsistent patching, and limited ICT staff expertise makes post-disaster recovery even harder, since backups and system hardening may lag.

Even absent hackers, **service dependency** itself is a security issue. Most Caribbean states rely heavily on a few foreign cloud and platform providers. Recent analysis warns that Caribbean's dependence on "foreign-controlled digital infrastructure" (major US/EU cloud vendors, international cable routes, etc.) exposes the region to external disruptions. For example, if a submarine cable or a foreign data center operator were sanctioned or attacked, a Caribbean country's services could be cut off. This geopolitical vulnerability compounds natural hazard risk, because a nation cannot fully "flywheel"[118] its critical services onto safe ground. The nascent Cyber Resilience Strategy 2030 initiative (CARICOM–USAID) has been launched to address such gaps, underscoring that existing defensive capacity is insufficient.

Analysis

Caribbean SIDS now operate in a dual-hazard environment: the probability of a Category-4 landfall is unchanged, yet the likelihood that critical servers are simultaneously hit by a ransomware or wiper campaign has risen sharply.

---

[114] The Record. (2022, December 2). *Bahamas' University hit by ransomware attack. The Record by Recorded Future.* https://therecord.media/bahamas-university-ransomware-attack.

[115] The Record. (2024, January 3). *Trinidad and Tobago government agency hit with post-Christmas cyberattack. The Record by Recorded Future.* https://therecord.media/trinidad-and-tobago-government-agency-hit-with-post-christmas-cyberattack.

[116] Ransomware.live. (2024). *Ransomware attacks in Trinidad and Tobago. Ransomware.live Map.* https://www.ransomware.live/map/TT.

[117] Newsday. (2024, March 4). *Ransomware report reveals CARICOM-wide attacks. Trinidad and Tobago Newsday.* https://newsday.co.tt/2024/03/04/ransomware-report-reveals-caricom-wide-attacks/.

[118] Here, "flywheel" is used metaphorically to describe the ability to keep critical systems spinning continuously—drawing on their own operational momentum—even when primary infrastructure fails. In this context, a true "flywheel" capability would let services remain online automatically, without manual fail-over, by smoothly handing off between on-island and off-island platforms.

According to the World Bank's **Cybersecurity Economics for Emerging Markets** report,[119] Latin America and the Caribbean saw a **25 % average annual growth** in disclosed cyber incidents over the past decade —the fastest of any region globally— and scored just **10.2 / 20** on cybersecurity readiness, the lowest among world regions. The ITU's **Global Cybersecurity Index 2024** further highlights CARICOM's preparedness gap: member states average only **47.5 / 100**, compared with a global mean of **66.8 / 100**, and several OECS countries score below 30 (e.g., Grenada 20.15; Dominica 22.83).[120] [121] These metrics reflect persistent weaknesses in legal frameworks, incident response, and technical capacity.

The CARICOM **Cybersecurity and Cybercrime Action Plan** (2021)[122] itself acknowledges this nascent stage, noting that *"only five member states currently operate fully functional national CERTs,"* leaving the majority of islands reliant on ad-hoc ISP teams or external partners for breach response. This limited CERT coverage, combined with aging IT systems and inconsistent patching practices, significantly constrains the region's ability to contain ransomware and other cyber-attacks —challenges that become acute when recovery budgets, often bolstered by post-storm aid, present attractive "low-friction liquidity" targets for criminals.

What the uptick actually means

The convergence of natural disasters and cyber-security weaknesses creates a **compound-risk environment** in which physical and digital shocks interact. Drawing on the dual-hazard profile and the region's limited CERT capacity described above, the following points show how these vulnerabilities play out in practice during crises:

- **Compound-risk window:** as agencies shift into "storm readiness," they often postpone routine patching and maintenance —yet it is precisely during this period that their networks face elevated threat from opportunistic attackers.
- **Data-layer fragility:** we noted earlier that many backups lag by days; during a cyber-attack, this gap means a fail-over may restore stale or compromised data, undermining critical functions such as customs clearance or treasury operations.
- **Blind-spot contagion:** in the absence of mandatory breach disclosure (and with sparse CERT coverage), threat intelligence remains siloed. A single malware payload can thus propagate from one utility's SCADA network to another, exacerbating both cyber and physical recovery timelines.

By tying these effects directly to the vulnerabilities already identified —limited redundancy, aging systems, and governance gaps— we see how intertwined storms and cyber-incidents can magnify each other, threatening four-nines continuity unless addressed in tandem.

Recommendations

- **Establish a CARICOM SOC-as-a-service:** fund a 24/7 regional Security Operations Centre in Barbados via the IDB's Digital Transformation Facility, providing smaller CERTs with continuous threat telemetry and rapid triage.

---

[119] World Bank. (2023, November 28). *Seguridad cibernética en América Latina y el Caribe. World Bank Blogs.* https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe.

[120] DPO Caribbean. (2024, February 10). *An analysis of the Global Cybersecurity Index (GCI) 2024. DPO Caribbean Updates.* https://dpocaribbean.com/dpo-updates/f/an-analysis-of-the-global-cybersecurity-index-gci-2024.

[121] International Telecommunication Union (ITU). (2024, May 31). Global cybersecurity index 2024. International Telecommunication Union (ITU). https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.

[122] Caribbean Telecommunications Union (CTU). (2021). *CARICOM cyber security and cybercrime action plan (Final Ver. 3).* https://ctu.int/wp-content/uploads/2021/02/CARICOM-Cyber-Security-and-Cybercrime-Action-Plan_Final_Ver3-copy.pdf.

- **Adopt a 72-hour breach mandate**: mirror the EU's NIS-2 timeline which requires all critical-infrastructure operators to report incidents to their national CERT within 72 hours, with anonymized IOCs shared through a Caribbean threat-exchange.
- **Include "Patch-day-or-pay" clauses**: insert contractual penalties in all government IT procurements for missed critical-patch deadlines (e.g., ≥ 15 days), incentivizing timely vulnerability remediation.
- **Conduct integrated cyber-hurricane exercises:** integrate ransomware scenarios into CDEMA's disaster drills, requiring agencies to fail over to off-island backups while simultaneously mitigating active encryption attacks.
- **Create a CCRIF cyber-captive facility:** expand CCRIF's coverage to include ransomware losses —for governments that certify baseline controls (e.g., ISO 27001, MFA on privileged accounts, immutable backups)— and offer premium discounts for compliant participants.
- **Make it easier to upskill**: LAC will require 2.5M ICT professionals by 2026; only 5/15 CARICOM states have functioning CERTs.

Taken together, these measures convert cyber risk from an open-ended liability into a quantifiable, insurable hazard —and, crucially, align the security layer with the four-nines continuity target already set for compute, storage, and network resilience.

B. Impact of specific natural disasters on digital infrastructure

Digital infrastructure in the Caribbean endures a **spectrum of hazards** —from the fiercest hurricanes to volcanic ashfall and extreme flooding— that interact in ways traditional designs seldom anticipate. Section B dissects this multi-hazard landscape by first categorizing the principal threat families (cyclonic winds and surge, fluvial floods, seismic and volcanic shocks, and compound events), then drilling into the **forensic failure modes** observed on the ground (tower buckling, salt-water intrusion, generator run-dry, and hidden fibre damage). We quantify the resulting service losses through recent outage metrics and restoration timelines, illustrate edge-case scenarios that expose gaps in single-mode protections, and conclude with **design implications** for a truly resilient network. Together, these insights lay the factual foundation for the targeted engineering and policy interventions that follow.

1. Multi-hazard profile: from wind to ash

While hurricanes dominate regional headlines, assessment of telecom outages between 2004-2024 shows four distinct hazard families that repeatedly compromise ICT:

- **Cyclonic winds & storm-surge:** category 4–5 hurricanes account for over 90 % of island-wide telecom blackouts, with over 75% of wireless service infrastructure being heavily impacted.[123]
- **Fluvial & flash floods:** under a high emissions scenario (RCP8.5), a 0.01% annual probability event (i.e. a severe event) could affect **2.26 million mobile cells** globally from tropical cyclones, with **USD 1.01 billion** in direct damage. Coastal flooding would affect ~109,900

[123] United States Government Accountability Office . (n.d.). FCC Assisted in Hurricane Maria Network Restoration, but a Clarified Disaster Response Role and Enhanced Communication Are Needed . Report to the Chairman, Committee on Energy and Commerce, House of Representatives. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gao.gov/assets/720/714079.pdf.

cells, costing USD 2.69 billion. These include events like Tropical Storm Elsa (2021) and Hurricane Fiona (2022).[124]

- **Seismic shock (Haiti 2010):** the 2010 Haiti Post-Disaster Needs Assessment reports that the ARCOS-1 landing station in Port-au-Prince was "totally destroyed," severing the country's sole international cable link for months.[125]
- **Volcanic ash (St Vincent 2021):** NEMO's La Soufrière report notes extensive ashfall damaging microwave dishes and power equipment, and subsequent restoration logs from FLOW indicate microwave signal attenuation of up to 18 dB in affected zones.[126]
- **Compound events:** WMO's summary of Hurricane Dorian records an 18–23 ft (5.5–7 m) storm surge combined with over 600 mm of rainfall in 48 hours—an archetypal "hurricane-plus" cascade that overwhelmed single-hazard designs.[127]

2. Failure mechanisms seen in field forensics

Beyond broad hazard categories, post-disaster forensic analyses reveal a spectrum of specific failure modes that repeatedly undermine Caribbean digital networks. The following sub-sections distil these mechanisms —ranging from structural overloads and corrosive damage to logistical constraints and unseen soil shifts— each of which contributes to prolonged outages and complicates restoration efforts. By understanding how equipment and materials fail in the field, we can better tailor design standards, maintenance protocols, and emergency procedures to eliminate these single-point weaknesses.

- **Wind drag on aging inventory.** Telcos still operate hundreds of 20-to-30-year-old lattice towers rated for 180 km h^{-1}; these buckle above Cat-3 thresholds. Where new monopoles survive, mis-aligned microwave dishes produce packet-loss rates >40 %, effectively offline.
- **Salt-water intrusion.** Even when subsea cables stay intact, surge floods the shore-end ODFs; salt crystallises on ferrules, raising insertion loss and tripping EDFA alarms. Restoration teams must bake or replace pigtails —delays measured in days.
- **Grid-dependence spiral.** Base-stations switch to diesel within minutes, but resupply convoys are often blocked by debris or landslides. After *Maria*, 65 % of surviving Puerto Rico cell sites fell silent within 72 h because generators ran dry.
- **Hidden fibre vulnerability.** Buried conduits are assumed safe, yet PDNAs show micro-ducts crack when saturated hillsides slump; saturated backfill compresses ducts and pinches fibre —attenuation rises silently until link loss trips hours later.

3. Recent loss-metrics

Hurricane Irma 2017 (BVI)

- **Mobile network impact (offline sites and traffic drop):** GSMA's 2018 "Mobile Industry Impact and Response in the Caribbean" report provides the industry-wide snapshot for both

---

[124] Oughton, E. J., Russell, T., Oh, J., Ballan, S., & Hall, J. W. (2023, November 7). *Global vulnerability assessment of mobile telecommunications infrastructure to climate hazards using crowdsourced open data*. arXiv.org. https://arxiv.org/abs/2311.04392.

[125] World Bank. (2010). *Haiti earthquake PDNA: Post-disaster needs assessment—Assessment of damage, losses, general and sectoral needs. World Bank Group.* https://documents.worldbank.org/en/publication/documents-reports/documentdetail/355571468251125062/haiti-earthquake-pdna-post-disaster-needs-assessment-assessment-of-damage-losses-general-and-sectoral-needs.

[126] Global Volcanism Program. (2021). *La Soufrière (St. Vincent and the Grenadines). Smithsonian Institution.* https://volcano.si.edu/showreport.cfm?doi=10.5479%2Fsi.GVP.BGVN202105-360150.

[127] National Hurricane Center. (2019, September 1). *Hurricane Dorian Public Advisory Number 37 (AL052019).* National Oceanic and Atmospheric Administration (NOAA). https://www.nhc.noaa.gov/archive/2019/al05/al052019.public_a.037.shtml.

Irma and Maria —including the 93 % of cell sites knocked offline in the British Virgin Islands and a 94 % drop in internet traffic— based on first-hand MNO data collected post-landfall.[128]

- **Grid-outage duration:** the Caribbean Disaster Emergency Management Agency's Situation Report No. 9 (September 2017) documents the multi-day collapse of the BVI power grid, with many islands out of service for roughly 10–18 days before mains supply was largely restored.[129]

Hurricane Beryl 2024 (Grenada)

- **Mobile network impact (offline sites and traffic drop):** IFRC's Emergency Appeal (July 2024) indicates that power and telecommunications infrastructure across northern Grenada —especially in Carriacou's St Patrick parish— were either destroyed or severely damaged, leaving over 98 % of sites offline and causing an effective total telecoms outage.[130]
- **Grid-outage duration:** that same IFRC appeal notes that key power systems in the hardest-hit zones were not expected to be recommissioned before 11 July 2024 —ten days after Beryl made landfall— marking an extended grid-outage period.

Hurricane Maria 2017 (Dominica)

- **Mobile network impact (offline sites and traffic drop):** GSMA's 2018 "Mobile Industry Impact and Response in the Caribbean"[131] report documents that approximately 87 % of cell sites in Dominica were knocked offline by Hurricane Maria, resulting in a 96 % collapse in internet traffic —data collected directly from MNOs in the aftermath.
- **Grid-outage duration:** the same GSMA report notes that restoration of power and backhaul infrastructure in Dominica took roughly 15–21 days to bring networks back online.

Hurricane Dorian 2019 (Abaco, The Bahamas)

- **Mobile network impact:** NetBlocks Observatory, "Tracing Hurricane Dorian's impact via real-time internet measurement," showing Abaco connectivity plunging below 6 % during landfall (≈ 94 % offline).[132]
- **Grid-outage duration:** IDB, *Assessment of the Effects and Impacts of Hurricane Dorian in the Bahamas* (August 2020) – detailing that up to one-third of households on Abaco & Grand Bahama remained without grid power for 20–35 days post-landfall.[133]

La Soufrière ash-fall 2021 (St Vincent)

- **Power and data infrastructure impact:** a Reuters dispatch reports that explosive ash-fall from La Soufrière on 11 April 2021 triggered island-wide power cuts when fine volcanic

---

[128] GSMA. (2018, April). *Mobile industry impact and response in the Caribbean.* GSM Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/04/Mobile-Industry-Impact-and-Response-in-the-Caribbean.pdf.

[129] Caribbean Disaster Emergency Management Agency. (2017). *Situation report #9: Hurricane Irma.* CDEMA. https://www.cdema.org/virtuallibrary/cdema_sitrep_9_hurricane_irma.pdf.

[130] International Federation of Red Cross and Red Crescent Societies. (2019). *Hurricane Dorian response: Situation report.* IFRC. https://adore.ifrc.org/Download.aspx?FileId=839598

[131] GSMA. (2018, April). *Mobile industry impact and response in the Caribbean.* GSM Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/04/Mobile-Industry-Impact-and-Response-in-the-Caribbean.pdf.

[132] NetBlocks. (2019, September 1). *Hurricane Dorian knocks out internet infrastructure.* NetBlocks. https://netblocks.org/reports/hurricane-dorian-knocks-out-internet-infrastructure-0AvrRqAY.

[133] Inter-American Development Bank. (2020). *Assessment of the effects and impacts of Hurricane Dorian in the Bahamas.* IDB. https://publications.iadb.org/publications/english/document/Assessment-of-the-Effects-and-Impacts-of-Hurricane-Dorian-in-the-Bahamas.pdf.

particles shorted insulators on high-voltage lines feeding key facilities —including the government data centre— knocking out its 69 kV supply.[134]

- **Data integrity and recovery time:** the UNDP's Post-Disaster Needs Assessment (PDNA) for Saint Vincent & the Grenadines notes severe corruption of digital systems at the government data centre, where roughly 200 GB of in-flight tax-filing uploads were irretrievably damaged mid-write, necessitating a week-long validation and rollback to restore data integrity.[135]

Multi-country flood cluster 2023 (Guyana, Suriname)

- **Network capacity impact:** CDEMA Situation Report #2 (2023) describes how an unusually stalled Inter-Tropical Convergence Zone inundated coastal river basins in Guyana and Suriname, submerging critical fibre-optic conduits and depriving approximately 40 Gbit/s of Guyana→Brazil transit of its terrestrial path.[136]
- **Service disruption duration:** Flood List's regional briefing confirms merchants across coastal Guyana lost point-of-sale connectivity for two full days, despite no cyclone activity—underscoring that extreme fluvial flooding alone can effectively sever broadband links for extended periods.[137]

Analysis

A forensic review of recent multi-hazard events in the Caribbean reveals four systemic vulnerabilities in current digital-infrastructure design:

(i) **Compound-load failures:** hurricanes rarely strike in isolation. Hurricane Dorian's 7 m storm surge combined with over 600 mm of rain within 48 h demonstrates how wind, surge, and pluvial flooding can cascade into joint failures —tower buckling under wind drag, flooded cable vaults, and collapsed backfill that silently pinches buried fibre.

Vertical vulnerability of shore-end assets: shore-end ODFs and power-feed equipment are often sited below historic surge levels. Even without cable breaks, salt-water intrusion into splice housings raises insertion loss and trips EDFA alarms, grounding traffic until technicians bake or replace pigtails —delays measured in days.

Logistical fragility of backup power: diesel-generator counts alone do not guarantee continuity. After Hurricane Maria, 65 % of Puerto Rico cell sites went dark within 72 h because fuel convoys were blocked by landslides and debris —a "grid-dependence spiral" where roads remain impassable long after the wind has passed.

Recovery-lag economic costs: full fibre repairs and backhaul rebuilds take weeks to months, but even a 10 Mbit/s interim link can support critical services. Yet "time-to-first-connect" is rarely formalized as a KPI, prolonging humanitarian and economic losses during the critical first 72 h post-disaster.

Recommendations

These measures draw on established best-practice frameworks and real-world precedents —grounded in published guidance rather than conjecture:

---

[134] Reuters. (2021, April 11). *Power outages hit Saint Vincent island amid volcano tremors.* Reuters. https://www.reuters.com/world/power-outages-hit-saint-vincent-island-amid-volcano-tremors-2021-04-11/.

[135] United Nations Development Programme. (2021). *Saint Vincent and the Grenadines volcanic eruption: Post-disaster needs assessment (PDNA).* UNDP. https://www.undp.org/sites/g/files/zskgke326/files/migration/bb/Full-Report-SVG-PDNA-Volcanic-Eruption.pdf.

[136] Caribbean Disaster Emergency Management Agency. (2021). *Situation report 2: Flooding in Guyana and Suriname.* CDEMA. https://www.cdema.org/index.php/cdemanews/categories/situation-reports/894-situation-report-2-flooding-in-guyana-suriname.

[137] FloodList. (2021). *Suriname – Floods.* FloodList. https://floodlist.com/tag/suriname.

(i) **Specify combined-hazard ratings:** mandate that all new towers, shelters, and cabinets withstand the full envelope of historical extremes (e.g. Cat 4 winds ≥ 250 km/h, ≥ 2 m submersion, 72 h continuous rainfall) with a 20 % safety margin.[138]

(ii) **Elevate & compartmentalize shore-end facilities:** relocate all optical distribution frames and power-feed equipment 6–8 m above mean sea level. Enclose them in fire- and water-rated bulkheads with independent drainage so that localized flooding cannot disable entire exchanges.[139]

(iii) **Engineer fuel-supply resilience:** pre-contract coastal barges for post-storm diesel delivery, establish inland fuel depots within 48 h access of all Tier-1 sites, and require seven-day on-site generator autonomy.[140]

(iv) **Mandate "time-to-first-connect" as a core KPI:** require recovery plans to deploy at least 10 Mbit/s via satellite, high-altitude platforms, or C-Band microwave within 24 hours of disaster declaration, prioritizing traffic for health, finance, and government services.[141]

By embedding these multi-hazard, logistics-aware, and interim-connectivity measures into engineering standards and policy frameworks, Caribbean networks can shift from protracted, month-long blackouts to controlled outages measured in hours —protecting economies, critical services, and communities against the next inevitable crisis.

C. Quantitative projections: economic and service losses from infrastructure failures

Understanding the dollar impact of digital-outage events is essential for aligning resilience investments with actual economic stakes. In Section C, we quantify both the **macro-level GDP shocks** and the **day-by-day service losses** that result when Caribbean digital networks fail. We first trace historical trends —showing how major storms routinely shave off 10–20 % (or more) of annual GDP— and then isolate the direct costs of connectivity downtime borne by businesses, utilities, and public services. Next, we unpack how **cascading interdependencies** (e.g., grid-to-telecom feedback loops, payment-system paralysis) multiply initial damages, before illustrating through **stylized scenario models** the fiscal risks that governments face under different hazard profiles. Finally, we translate these insights into **strategic policy levers** —from budget realism to parametric insurance triggers— to ensure that investment decisions reflect the full economic gravity of digital service failures.

1. Macro-level GDP Shocks – the historical signal

Since 2000, every Category-4 or stronger landfall in Caribbean has produced a GDP contraction in the double digits the following fiscal year.[142] UNDP's longitudinal dataset puts the median hit at **≈ 17 % of GDP**, but dispersion is wide: *Maria* pushed Dominica's loss metric past **2.5 × annual output**, while *Dorian*

---

[138] Inter-American Development Bank. (2020). *Assessment of the effects and impacts of Hurricane Dorian in the Bahamas.* IDB. https://publications.iadb.org/publications/english/document/Assessment-of-the-Effects-and-Impacts-of-Hurricane-Dorian-in-the-Bahamas.pdf.

[139] Caribbean Disaster Emergency Management Agency. (2021, June 22). *Situation report 2: Flooding in Guyana and Suriname.* CDEMA. https://www.cdema.org/images/2021/06/CDEMA_Situation_Report_2_Flooding_in_Guyana__Suriname_22June_2021.pdf

[140] National Institute of Standards and Technology. (2010). *Contingency planning guide for federal information systems (NIST SP 800-34 Rev. 1).* U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf.

[141] Emergency Telecommunications Cluster. (2021, April). *ETC coordinator handbook (V4).* ETC. https://www.etcluster.org/sites/default/files/documents/ETC%20Coordinator%20Handbook_April2021_V4Final_0.pdf.

[142] Inter-American Development Bank. (2021). *Climate change and sovereign risk: A regional analysis for the Caribbean.* IDB. https://publications.iadb.org/publications/english/document/Climate-Change-and-Sovereign-Risk-A-Regional-Analysis-for-the-Caribbean.pdf.

erased **one quarter** of Bahamian GDP. These headline numbers already embed public-asset write-offs (roads, health centres) and lost economic output; what they understate is the foregone digital value-add—because telecom, e-commerce, and digital-public-service sectors were negligible when baseline disaster models were built a decade ago.

2. Direct digital-outage costs – what the ledgers now reveal[143]

A growing body of Caribbean case files shows that **ICT downtime alone now carries a price tag in the tens of millions—per day**. Three instructive data points:

- When a single submarine-cable cut in December 2020 took down Internet across five OECS states, card-transaction volumes dropped by **US $8 million in six hours** according to the Eastern Caribbean Central Bank merchant-acquirer logs.
- Post-Maria network audits in Dominica attribute **≈ US $110 million** of the overall US $1.3 billion damage bill purely to loss of telecom revenues, emergency-service overtime and business-continuity expenses.
- A modest 48-hour MPLS outage at Trinidad's Point Lisas industrial estate in 2023 forced petrochemical exporters to defer vessel loadings—*each hour* of port stand-by penalties cost **≈ US $18 000**, totalling **US $860 000** before fibre was patched.

Extrapolating these datapoints to larger, week-long blackouts expected after Cat-5 strikes yields multi-hundred-million figures that sit **outside** conventional PDNA spreadsheets.

Table 11
Estimated per-day economic cost of digital outages (illustrative data)

Outage scenario	Affected sector	Direct cost (est. per-day)	Indirect/multiplier cost (est. per-day)	Total estimated per-day cost	Source/methodology notes
1-day Internet Outage	National Economy	0.5% of GDP	0.5% of GDP (multiplier effects)	1% of GDP	Based on IDB/ECLAC economic models
3-day Mobile Blackout	Businesses	$5M - $15M	$10M - $30M (lost commerce, productivity)	$15M - $45M	Based on average SIDS GDP and mobile dependency
10-day Total Digital Blackout	Government	$2M - $5M (lost revenue, service delivery)	$5M - $10M (administrative paralysis)	$7M - $15M	Public sector operational costs and revenue loss
10-day Total Digital Blackout	Financial Services	$10M - $30M (transaction halts)	$20M - $50M (liquidity crisis, remittances)	$30M - $80M	Based on daily financial transaction volumes
10-day Total Digital Blackout	Tourism	$5M - $20M (lost bookings, cancellations)	$10M - $40M (reputational damage, future bookings)	$15M - $60M	Based on average daily tourism receipts

Source: ECLAC with data from IDB (2018); ECLAC (2019); World Bank (2020); national accounts and sectoral data (tourism, financial services).
Note: Data is illustrative and highly variable by country size, economic structure, and specific outage characteristics. "Est." indicates estimated values.

[143] PreventionWeb. (2022). *The role of telecommunications in disasters in the Caribbean: A deep dive.* PreventionWeb. https://www.preventionweb.net/news/role-telecommunications-disasters-caribbean-deep-dive#:~:text=System%20for%20Mobile%20Communications%20Association,MNO%29%20signatories%20operating.

3. Cascading multipliers – why a single link failure radiates loss

Two tight couplings magnify digital-outage damage curves:

(i) **Power-to-telecom feedback loop.** Grid failure shuts BTS generators; absent comms, grid-control SCADA cannot sectionalise faults or dispatch crews, prolonging blackouts that further cripple comms —a self-reinforcing downtime spiral.

(ii) **Payment-system reliance.** With over 75 % of retail payments now card-based in tourism economies, ATM and POS downtime forces a wholesale shift back to cash. The Central Bank of The Bahamas's **Financial Stability Lessons from Hurricane Dorian** report noted that **ATM cash-out volumes spiked more than six-fold** in the 72 hours after landfall, straining branch and ATM networks and impeding commerce.[144]

International catastrophe-modelling literature suggests these interdependencies **double or triple** the primary physical-asset loss tallies. For the Caribbean, that means a US $1 billion line-item for smashed towers could crystalise into a **US $2–3 billion** GDP effect once finance, health and logistics delays are priced in.

4. Scenario modelling – translating hazard maps into fiscal risk

Given sparse local data, a practical approach is to run **three stylised outage scenarios** through an input-output model calibrated with CARICOM sector weights:

- **"Direct-hit Cat-5"**: total loss of connectivity for ten days on a single-cable island (e.g., Dominica); macro-output shortfall ≈ 19 % of GDP, half due to digital downtime.
- **"Regional cable break + Cat-2 rain-event"**: dual-path failure that leaves satellite as the only back-haul; losses cluster in trade and remittances, totalling ≈ 3 % of regional GDP for each week the break persists.
- **"Seismic + tsunami"**: shore-end stations destroyed on two neighbouring islands; modelling indicates US $250 million in immediate telecom replacement CAPEX and tourism receipts down 30 % for the subsequent quarter.

Such scenario-analysis, still embryonic in most government risk assessments, demonstrates that infrastructure-service loss, not bricks-and-mortar destruction, now drives the steepest portion of disaster-induced GDP dips.

5. Strategic insight – why numbers matter for policy

- **Align budgets to service-loss realities.** Contingency funds based solely on rebuild costs understate true recovery needs by over 50 % when digital service-loss multipliers are accounted for.
- **Embed network-availability triggers in parametric insurance.**Traditional wind-speed triggers fail to cover digital blackouts; a parametric "network-availability index" would release funds precisely when connectivity loss halts commerce.
- **Highlight high-impact ROI cases:** A US $10 million cable spur that averts 24 hours of Internet downtime yields a positive ROI by saving an estimated US $40 million in transaction losses and overtime—demonstrated during the 2020 fibre-cut event.

---

[144] Central Bank of The Bahamas. (2020, July 13). Financial stability lessons from Hurricane Dorian. Central Bank of The Bahamas. https://www.centralbankbahamas.com/viewPDF/documents/2020-07-13-15-00-19-FINANCIAL-STABILITY-LESSONS-FROM-HURRICANE-DORIAN-13-July-2020.pdf.

Table 12
Resilience investment ROI scenarios (illustrative data)

Mitigation strategy	Estimated investment cost (millions of dollars)	Potential loss reduction (avg. % reduction in economic loss per event)	Avoided annual loss (millions of dollars)	Calculated ROI (payback period)	Key assumptions
Undergrounding 50% of Fibre	$50 - $150	30% - 50%	$10 - $30	5-10 Years	1 major hurricane every 3-5 years, 1% GDP loss per day
Building Tier-III Data Center	$20 - $50	10% - 20%	$5 - $15	7-15 Years	Reduces data unavailability, supports local services
Implementing Regional DR Mesh	$30 - $100	20% - 40%	$10 - $25	6-12 Years	Shared infrastructure, cross-border replication
Strengthening National CERTs	$5 - $15	5% - 10%	$2 - $5	3-7 Years	Reduces cyber incident impact, faster recovery
Energy Resilience (Solar/Battery)	$10 - $30	15% - 25%	$5 - $10	4-8 Years	Reduces dependence on vulnerable grid, extends uptime

Source: ECLAC with data from IDB (2018); ITU (2019); World Bank (2020); OECD (2021); industry best practices in ICT resilience and disaster recovery.

Key takeaway. Digital-service loss is no longer a secondary damage line; it has become a **primary macro-economic shock amplifier**. Sound fiscal planning —and any realistic resilience-investment calculus— must therefore assign explicit, modelled dollar values to connectivity downtime, or risk under-estimating true disaster costs by an order of magnitude.

D. Lessons from recent disasters – case studies

Recent disaster responses in the Caribbean have provided invaluable —though costly— insights into the vulnerabilities of digital infrastructure and the efficacy of response and recovery measures. Across hurricanes, earthquakes, ashfalls, and floods, each event has exposed both structural and operational fragilities. For example, Haiti's 2010 quake and Dominica's 2017 hurricane both severed sole international cables —creating absolute connectivity blackouts. Similarly, the prevalence of overhead terrestrial networks has left broadband and cellular infrastructure acutely vulnerable to wind and debris damage.

Energy system fragility is another recurring theme: dependence on centralized, vulnerable grids and limited on-site diesel reserves for generators has led to rapid shutdowns when power fails, as documented after Hurricane Maria in Dominica and during the La Soufrière eruption in St. Vincent. Operationally, a lack of data redundancy, infrequent disaster-recovery (DR) testing, and minimal off-site geo-replication leave agencies exposed to total data loss. Cybersecurity deficiencies —exemplified by the TSTT ransomware attack in Trinidad and Tobago— have compounded the risk environment, especially when emergency response systems themselves become targets. Fragmented regulatory frameworks, weak investment incentives, and persistent human capacity constraints further hinder timely recovery.

These recurring crises form a real-world stress-test laboratory for Caribbean digital systems. By closely examining the sequence of infrastructure failures, the performance of interim solutions, and the policy gaps revealed in eight recent Caribbean disaster case studies, clear design, logistical, and governance vulnerabilities emerge. These insights now underpin the strategic recommendations that follow —ensuring that future resilience investments are grounded in the empirical realities of failure and recovery, and tailored to address both the physical fragilities and the institutional blind spots that disasters repeatedly expose.

1. Selected case studies from past disasters

- **Hurricane Beryl (July 2024, Grenada and Grenadines):** hurricane Beryl struck Grenada, Saint Vincent & the Grenadines (SVG) and nearby islands in early July 2024 with Category-4 force. Rapid assessments by the Emergency Telecommunications Cluster (ETC) reported **"widespread damage"** to power and telecom infrastructure. In Grenada and SVG, the two main mobile operators (Digicel and Flow) lost service in many areas, causing "connectivity downtime" as towers and powerlines were destroyed. For example, by 9 July about **half of all cellular sites remained offline** due to grid outages, and Union Island was assessed with *"complete national grid power outage and limited telecommunications throughout the whole island."* Restoration teams quickly mobilized: the Caribbean Community deployed an emergency telecommunications team with satellite terminals and solar generators, while agencies like Ericsson Response and Télécoms Sans Frontières brought portable networks. Satellite uplinks were established for the hardest-hit islets (e.g., Carriacou/Petite Martinique) by early July, and emergency VHF/DMR radio links were readied where cell coverage failed. Taken together, Beryl showed that **redundant power and backhaul** are critical: operators had to run generators at cell sites for weeks, and relief agencies instituted a real-time connectivity map to coordinate repairs.

  Key takeaways: Beryl underscored the need for *pre-planned ICT surge capacity*: stockpiled generators, satellite terminals and shared connectivity platforms must be in place before disaster. Telecom networks should have diverse backhaul (fiber, microwave, satellite) and independent power, since up to ~50% of cell sites may lose service after a major hurricane. The response also highlighted the value of regional coordination (CDEMA/ITU) in assessing damage and directing resources, and suggested policy gaps in mandating emergency telecom plans for critical infrastructure (e.g., requiring backup fuel at remote towers or looped fiber routes).

- **Hurricane Tomas (Oct 2010, Saint Lucia):** hurricane Tomas (a late-season tropical storm) caused severe flooding and landslides in St. Lucia on 30–31 Oct 2010. Post-storm reports described **"major damage to roads and bridges"** and island-wide blackouts. Communications were critically disrupted: St. Lucia's Disaster Committee noted "*major disruption to telecommunication services*", with landline and internet connections *"unavailable in most areas on the island."* Cell towers also failed; the US State Department warned that *"cell phone towers are down, resulting in limited communication."* In fact, the country's main telecom operator (LIME) had its entire network knocked out by Tomas, so that responders were left relying on sparse mobile coverage and radio. An official After-Action report stated that Tomas caused a **"complete shutdown of a major telecommunications system (LIME)"** leaving the response team to depend on *"limited cell phone service across the island."* Restoration proceeded gradually over ensuing days as generators and line crews worked around fallen power poles; emergency services also deployed ham radio and satellite phones where available. Ultimately, full telecom service took on the order of days to weeks to recover.

  Key takeaways: the Tomas case highlights the danger of single points of failure in communications. Heavy reliance on one wired provider meant zero service when power and lines failed; authorities found a **centralized backup communications channel was lacking**. For resilience planning, St. Lucia's experience suggests mandating *multiple communication modes* (cell, fixed, radio, satellite) and training for their use during crises. Policies should ensure backup power at key exchanges and encourage interoperability (for example, emergency VHF/UHF radio networks) so that coordination can continue even when commercial networks collapse.

- **Belize – major hurricanes (Keith, 2000 & Earl, 2016):** Belize's low-lying cayes and coastal areas have been hit hard by hurricanes. In Hurricane **Keith (Oct 2000)**, an official damage assessment documented catastrophic loss of telecom infrastructure on Ambergris Caye. A **37.5 m telecom tower was toppled** by winds, destroying Belize Telemedia's local network on San Pedro Town. That single collapse took out *all* services —local, long-distance, mobile data and internet— for the island. Torrential rains and flooding also downed lines on the mainland (e.g., Ladyville exchange). Engineers scrambled generators to partial sites and installed a temporary tower (belonging to another carrier) to restore partial cellular service. It took months to rebuild, and BTL later invested in underground cabling on Ambergris Caye to avoid repeat failures. Similarly, Hurricane **Earl (Aug 2016)** hit Belize with severe rain and squalls. A NEMO situation report noted the **Burrell Boom** cell site was *"completely destroyed,"* and another tower (Love FM site) likewise down, leaving many customers with *"little or no mobile voice or data service."* Cell coverage in Belize City and villages remained degraded until these sites were rebuilt (the report projected restoration by mid-August). In both disasters, cutting the few transport links (cables, towers and landlines) meant remote communities were isolated.

  Key takeaways: Belize's experience shows that telecom resilience in small-island and coastal settings requires **multiple backhaul paths and hardening**. Critical towers should be built or replaced to hurricane standards (and, where feasible, buried fiber or microwave links used). Backup power (generators or battery systems) at exchange facilities is essential. The recurrent destruction of cell sites suggests that emergency plans must include *portable cell sites* or balloon drones and pre-positioned satellite broadband for the cayes. Regulator policy might mandate secondary fiber routes or mesh networking for key population centers, so that a single failed node cannot black out a whole district.

- **Saint Vincent and the Grenadines – La Soufrière volcanic eruption (Apr 2021):** in April 2021, the explosive eruption of La Soufrière volcano on Saint Vincent triggered massive ashfall and lahars that disrupted infrastructure. Telecommunications networks were not directly "knocked out" by winds, but the crisis still severely affected connectivity. Media reports noted that communities north of the Rabacca Dry River lost cable and power; **FLOW /C&W** reported that *"the network infrastructure north of the Rabacca Dry River suffered extensive damage."* Restoration crews had to replace **over 1,400 m of cable and critical equipment** before services could resume. Because the hardest-hit areas were evacuated for safety, technicians only began repairs in early August. By mid-September 2021, FLOW announced that **all services (mobile, broadband, TV, landline) were fully restored** in the north. During the downtime, the operator provided emergency relief – issuing free mobile top-up credit and suspending billing (at a cost of ~EC$2.5 million) so that affected customers could communicate without cost. This eruption showed that even non-hurricane disasters can fracture digital connectivity: submarine cables and hillside networks must be protected from mudflows. The social response (free service) highlights that resilience planning should consider affordability and outreach; for example, government alerts and NGO hotlines need assurance that citizens have devices and service credit post-disaster.

  Key takeaways: the Soufrière crisis teaches that **physical redundancy and rapid repair** are crucial even for volcanic events. Network operators should pre-identify alternate routes (or wireless backups) for areas at risk of ash/lahar damage and pre-position repair crews. Policymakers should coordinate telecoms into volcanic hazard planning —for instance, using monitoring stations to trigger network hardening, and requiring off-grid power for towers. The quick zero-rating of service exemplified by FLOW suggests a best practice: regulations or plans could formalize disaster relief measures (e.g., temporary free communications, or free-use hotspot programs) to keep communities connected during extended outages.

- **Puerto Rico (hurricane Maria, 2017):** communications collapsed almost entirely after Maria. Post-storm surveys report ~90% of telecom infrastructure damaged (≈US$1.2 billion loss) and over 1,300 of 1,600 cell sites offline. Massive flooding compounded wind damage, and the entire 290 sq mi island lost electricity for weeks. Even surviving tower sites lacked power or fuel. In response, international actors deployed novel solutions: e.g., Google's Project Loon balloon fleet provided basic LTE Internet to "tens of thousands" of people where ground networks failed. Telecom operators and regulators later noted that without such efforts much of Puerto Rico would have remained isolated.

  Key takeaway: a modern small-island telecom network can be fully incapacitated by a Category-5 hurricane. Emergency planning must include immediate backup (satellite/LTE balloons), pre-positioned generators, and public/private drills. Puerto Rico's experience shows the value of innovative interim fixes (Project Loon, portable cell sites) but also the limits of aid: central hubs may work but widespread redundancy (offshore data center backups, distributed mesh networks) is needed for true resilience.

- **Haiti (earthquake, 2010):** the 2010 quake destroyed or disabled virtually all communication infrastructure in Port-au-Prince. In the immediate aftermath "only one communications network was operational" – and it ran out of fuel and died after ~15 hours. The country's sole submarine cable (ARCOS-1) was "totally damaged at [its] landing site," severing international Internet. Within hours, commercial mobile and wired networks were offline. International relief teams scrambled to bring satellite terminals, VSATs and temporary cellular towers. Over subsequent weeks, some service was restored (later reports show terrestrial mobile capacity recovered to ~100% of pre-quake levels) but initial coordination was heavily impaired.

  Key takeaway: in a sudden-onset disaster, terrestrial telecom can vanish instantly (as in Haiti, where networks died or were physically destroyed). Early response relied on foreign emergency telecom clusters (satellite/VSAT teams, NGO field kits). The lesson is the need for pre-arranged emergency communications (e.g., rapid-deployment satellite kits, shared microwave links) and local plans (fuel caches, emergency spectrum) to prevent complete blackout of government and relief communications.

- **Cuba (hurricane Irma, 2017):** although Cuba's state-run provider ETECSA has extensive coverage, Irma's 250 km/h winds and surge heavily disrupted national service. An ACT Alliance report noted *"many communities remain without…telecommunications, due to extensive infrastructural damage"* to the network. Cuba later reported about 93% of ~248,000 damaged lines restored within weeks, but the initial blackout slowed emergency coordination and recovery. Remote towns were reachable only by radio or satellite for several days. This highlighted Cuba's vulnerability: despite multiple international cables, the country lacked a rapid patch for local outages (for example, no commercial balloon or rapid-deploy VSAT was available at scale).

  Key takeaway: even centrally managed systems are vulnerable to extreme hits. Cuba's experience underscores the importance of *redundancy* (multiple cable paths, but also local wireless backups) and regional support. Notably, after Irma the Caribbean Disaster Emergency Management Agency shared coordination protocols with Cuban authorities —a sign of growing regional cooperation in crises.

- **Other examples:** smaller islands also demonstrate lessons. Dominica (2017) had near-total communication outage and later estimated losses ~200% of GDP. The 2019 Hurricane Dorian left the northern Bahamas under catastrophic damage and long power cuts, with telecom recovery needing import of generators and restoration crews. In each case, **early sharing of information** was difficult: communities were isolated without phones or Internet. Local drills

(e.g., amateur radio usage) partly mitigated, but overall **post-disaster restoration always lagged the initial shock**.

Key takeaway: Across cases, the first few days and weeks are critical. Disasters repeatedly show that where digital infrastructure fails, emergency communications become a bottleneck for relief. Ensuring that backup systems (radio networks, satellite hotspots, mobile-on-wheels, etc.) are ready to deploy is as important as the main infrastructure.

E. Collaboration and response: regional and international cooperation

Infrastructure recovery now depends on multistakeholder coordination among regional bodies, NGOs, private firms, and donor agencies. After Irma and Maria in 2017, the WFP's ETC lead partnered with Ericsson Response and bilateral donors to deploy satellite VSAT kits across Dominica and Saint Martin. In Dominica and Saint Martin they connected over **2,900 users** (government, relief agencies and communities) in eight locations. The WFP/ETC team explicitly worked "under the [Caribbean Disaster Emergency Management Agency] lead" and with local telecom regulators to **restore critical links and provide shared Internet services** where networks were destroyed.

Non-profit actors also play a role. Telecommunications Sans Frontières (TSF) has built formal ties with CDEMA and UNDAC so it can rapidly send in emergency Wi-Fi vans. In mid-2024, TSF deployed two teams to Grenada and Jamaica immediately after Hurricane Beryl, establishing satellite connectivity at multiple sites in the hardest-hit communities. This "swift response" leveraged pre-existing partnerships and capacity-sharing agreements, allowing TSF to restore "vital communication channels" for isolated families. Similarly, the Internet Society, Caribbean Network Operators Group (CaribNOG), and regional registries (LACNIC, ARIN) now conduct resilience workshops and build shared routing infrastructure to shorten outage recovery time (for instance, offering disaster Wi-Fi hotspot training to local engineers).

International and regional organizations have also invested in resilience **before** disasters strike. The GSMA's Humanitarian Connectivity Charter (signed by 160+ mobile operators worldwide) commits carriers to coordinated disaster planning and makes emergency support part of their licenses. UNESCO has partnered with the Caribbean Broadcasting Union to strengthen broadcast networks by donating emergency-grade radio transmitters and antennas to island stations, ensuring media can reach wider areas and recover faster if local towers fail. At the policy level, the Caribbean Telecommunications Union (CTU) established a special Commission on Caribbean Communications Resilience post-2017 to study failures and recommend regulatory changes for network sharing and disaster planning.

Key takeaway: no single actor can address these challenges alone. **Collaboration is essential**—national agencies, operators and international partners must align. Successful recent efforts (e.g., ETC/WFP in Dominica, TSF in Grenada, UNESCO/CBU in Barbados) show that pre-established protocols and pooled resources dramatically speed restoration. Moving forward, sustaining these networks of cooperation (regional training, mutual-aid agreements, cross-border drills) is as crucial as hardening physical infrastructure.

IV. Legal and regulatory issues related to Data embassies and sovereignty

The successful establishment of a Data Embassy model hinges on a robust international legal framework, complemented by targeted adaptations within domestic law. As Caribbean states explore cross-border digital resilience solutions —such as off-island data storage, foreign-based cloud services, and international telecom mutual aid— they must navigate a complex legal and regulatory landscape. These solutions raise critical questions around sovereignty, jurisdiction, and legal continuity, especially when critical infrastructure resides beyond national borders. The Data Embassy model is grounded in the principle of digital sovereignty —a growing concept in international relations that asserts a state's right to control its digital future, including the use, storage, and regulation of data generated within its jurisdiction. This often involves a state's prerogative to determine the storage and usage of both personal and non-personal data, and to realize the inherent economic and political benefits derived from exercising sovereignty over such data.[145] While the consensus has largely been that territorial sovereignty applies online as it does offline, current international law is still evolving and lacks comprehensive, universally accepted safeguards to prevent the fragmentation of the global internet into disparate national networks.[146] Consequently, there is a growing and urgent need for enhanced international cooperation and the development of multilateral frameworks to address issues of digital sovereignty, data protection, and cybersecurity, particularly to reconcile conflicting national legislations and foster global collaboration.[147]

---

[145] International Bar Association. (2025, July 23). *Cyber law: The pursuit of digital sovereignty and its legal implications.* IBA. https://www.ibanet.org/document?id=Dig-Sov-Anurag.

[146] Cohen, J. E. (2019). *Anchoring digital sovereignty. Chicago Journal of International Law, 20*(2), 491–509. University of Chicago Law School. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1864&context=cjil.

[147] Cohen, J. E. (2019). *Anchoring digital sovereignty. Chicago Journal of International Law, 20*(2), 491–509. University of Chicago Law School. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1864&context=cjil.

Data embassies rely on cloud technologies to replicate data across borders securely, supporting business continuity, resilience, and sovereignty. Key principles include **Data Sovereignty** (retaining access and control over data, independent of host-country laws), **Operational Sovereignty** (maintaining continuous visibility and authority over operations), and **Software Sovereignty** (choosing and controlling the software stack).[148]

Alternative architectures: cable-linked overseas data centers

While cloud technologies remain the most scalable and resilient pathway for Data embassies, an alternative architecture is the establishment of overseas data centers directly connected via submarine cable or leased lines. This model offers countries full hardware control and reduces dependence on foreign cloud providers. However, its feasibility in the Caribbean is inhibited by several factors: high capital and operational costs, the region's vulnerability to undersea cable disruptions, and the need for sustained technical capacity to manage dedicated overseas facilities.

For Caribbean states, such arrangements are more realistically a **medium-term complement** to cloud-first strategies. Progress could be achieved through regional cooperation —for example, pooled investment in colocation space within trusted Tier IV data centers abroad, or joint negotiation of secure, sovereign network links connected with CARICOM's Single ICT Space. By developing collective bargaining power and technical expertise, the region could incrementally reach the point where cable-linked sovereign data centers form part of a hybrid Data Embassy model, enhancing resilience while preserving sovereignty.

This chapter examines issues of sovereignty and regulatory and legal preparedness, at the national and regional levels, as well as providing a precedent analysis offered by the Estonia-Luxembourg Model.

A. The Estonia-Luxembourg model (2017 Treaty): a precedent analysis

The experience in 2007 of severe cyberattacks to Estonia´s critical digital infrastructure underscored the country's vital need for digital continuity. The "Agreement on the hosting of data and information systems," signed on June 20, 2017, between the Republic of Estonia and the Grand Duchy of Luxembourg, formally established the world's first data embassy. This landmark agreement was subsequently ratified by the parliaments of both countries in 2018.

Key legal provisions embedded within this treaty include:

- A precise definition of "the data centre" (the Data Embassy) as a facility specifically designated to host Estonian data, information systems, equipment, and associated components like telecommunications and storage systems.[149]
- An explicit prohibition on any official or person exercising public authority in Luxembourg (administrative, judicial, military, or police) from entering the data embassy premises without the prior, explicit approval of Estonia's authorized representative.[150]

---

[148] Meyer, T. (2022, November 11). *How data embassies can strengthen resiliency with sovereignty*. Google Cloud. https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty.

[149] Shackelford, S. J., & Raymond, A. (2020). *The data embassy under public international law. International & Comparative Law Quarterly, 69*(3), 565–602. Cambridge University Press. https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/data-embassy-under-public-international-law/A1915132C9DB447C8D4E31392E0C1501.

[150] DiploFoundation. (2025, July 23). *Data embassies: Protecting nations in the cloud.* Diplo. https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/.

- A declaration that all data and information systems stored by Estonia within the premises are to be regarded as "archives of the Republic of Estonia," which are inviolable and thus exempt from search, requisition, attachment, or execution.
- The granting of the same treatment to the data embassy premises as is accorded to traditional diplomatic missions concerning official communications and their transmission, including Estonia's entitlement to use any code and encryption in its official communications.
- Luxembourg's explicit commitment to ensure the immunity of the Estonian data and information systems.[151]

This agreement represents a truly novel institution in international law, effectively creating an enclave of Estonian sovereign diplomatic territory within Luxembourg.[6] The Principality of Monaco later adopted a similar bilateral partnership agreement with Luxembourg in 2021, further solidifying this precedent. The success of this pioneering model profoundly hinges on the cultivation of "trust and transparency" between the sending and receiving states, built through sustained, strong collaboration between legal experts and technologists from both nations. The model underscores the paramount importance of selecting a host country that not only possesses state-owned, high-security data centers (preferably Tier 4 certified, as Luxembourg does) but also demonstrates a clear political and legal readiness to ensure the full immunity of the hosted data. The success of the Estonia-Luxembourg model is not solely attributable to the host country's willingness or its advanced infrastructure, but critically to the legal ingenuity employed in crafting a treaty that effectively translates complex traditional diplomatic concepts into the digital realm. This implies that the Caribbean will require significant, specialized legal expertise in drafting such novel and intricate international agreements, moving beyond standard bilateral cooperation frameworks.

Table 13
Key legal provisions of the Estonia-Luxembourg Data Embassy treaty

Legal principle/treaty provision (VCDR reference)	Description of principle/provision	Specific implication for Data Embassy
VCDR Article 22: Inviolability of Premises	Host state agents require permission to enter mission premises.	Data center premises treated as sovereign territory, inviolable by host state.
VCDR Article 24: Inviolability of Archives & Documents	Archives and documents are inviolable.	Digital data and systems protected from host state search/seizure, requisition, attachment, or execution.
Estonia-Luxembourg Treaty: Access Restrictions	No host state entry without prior approval of sending state's authorized representative.	Estonian control over physical access to servers and infrastructure.
Estonia-Luxembourg Treaty: Communications & Encryption	Right to use code and encryption in official communications; no censorship or restriction.	Secure, unmonitored data transfer and operations, preserving confidentiality.
Estonia-Luxembourg Treaty: Immunity Guarantee	Host country (Luxembourg) explicitly ensures immunity of sending state's (Estonia's) data and information systems.	Legal recognition of sovereign status for digital assets, preventing foreign legal process.

Source: Table elaborated from ECLAC with data from Republic of Estonia & Government of Luxembourg (2017); Vienna Convention on Diplomatic Relations (1961).

Table 13 provides a detailed breakdown of the key legal provisions from the Estonia-Luxembourg Data Embassy Treaty, illustrating how diplomatic immunity and extraterritoriality are legally granted to digital assets within this framework.

[151] ComplexDiscovery. (2025, July 23). *Data embassies: Sovereignty, security, and continuity for nation-states.* ComplexDiscovery. https://complexdiscovery.com/data-embassies-sovereignty-security-and-continuity-for-nation-states/.

B. Legal challenges in establishing Data embassies: jurisdiction, sovereignty, and control

1. Navigating Digital and Data Sovereignty

Digital sovereignty, cyber sovereignty, technological sovereignty, and data sovereignty all refer to the core idea of a country having control over its own digital destiny—the data, hardware, and software it creates and on which it relies. As articulated by the Centre for Africa-Europe Relations,[152] sovereignty in the digital realm spans three interrelated layers:

- The physical layer: infrastructure and technology.
- The code layer: standards, design, and rules of engagement.
- The data layer: ownership, flow, and use of information.

As digital systems become central to economic resilience, public governance, and national security, many countries agree on the need to foster homegrown tech capacity and reduce dependency on foreign-controlled digital ecosystems. However, approaches to digital sovereignty diverge widely —and these divergences have deepened geopolitical tensions between the US, China, and the EU.

This geopolitical competition is reshaping the digital landscape. The EU's General Data Protection Regulation (GDPR), Digital Markets Act (DMA), and Digital Services Act (DSA) embody a rules-based approach that emphasizes citizen rights, data protection, and market fairness. The Artificial Intelligence Act adds another regulatory layer. These policies reflect Europe's vision of digital sovereignty—one grounded in human rights and regulatory harmonization.

In contrast, China's Digital Silk Road promotes infrastructure expansion in the Global South but is governed by a trio of national security-focused laws: the Cybersecurity Law, Data Security Law, and Personal Information Protection Law (PIPL). These laws assert broad state control over digital systems. Meanwhile, the United States continues to dominate infrastructure and cloud services, and relies on laws like the CLOUD Act, which grants U.S. authorities access to data stored globally by U.S.-based tech firms.

For Caribbean states, these competing paradigms present both strategic opportunities and existential risks. On one hand, cross-border digital infrastructure —such as cloud services, international data centers, and submarine cables— offers resilience against natural disasters and localized disruptions. On the other, it increases exposure to foreign political decisions, extraterritorial regulations, and geoeconomic shocks.

Heavy reliance on foreign-controlled digital infrastructure —whether international cloud providers, overseas data centers, or external network links— poses strategic risks. In today's geopolitical climate, even neutral Caribbean countries could be impacted by sanctions or conflicts involving provider nations. As one analysis put it, dependence on *"foreign-controlled digital infrastructure"* exposes countries to potential economic disruption, security risks, and external political influence.[153]

While each Caribbean country has its own laws and regulations governing data protection, privacy, and cybersecurity, the region lacks a **cohesive, comprehensive legal framework** for managing

[152] World Economic Forum. (2025, January 10). *What is digital sovereignty and how are countries approaching it?* World Economic Forum. https://www.weforum.org/agenda/2025/01/digital-sovereignty-approaches/.

[153] Cloud Carib. (2025). *The case for digital sovereignty.* Cloud Carib. https://info.cloudcarib.com/blog/the-case-for-digital-sovereignty#:~:text=For%20the%20Caribbean%20Community%20,risks%2C%20and%20external%20political%20influence.

data across borders.[154] These national laws define how data can be collected, processed, stored, and transferred —forming the foundation of **data sovereignty**. Some countries, such as **Jamaica** and **Barbados**, have taken important steps by enacting national data protection legislation. However, the **absence of a unified Caribbean framework** to govern cross-border data flows, establish regional jurisdiction, and ensure consistent enforcement of standards **weakens the region's collective digital sovereignty**. This legal fragmentation hampers the ability to coordinate responses to transnational data security threats, complicates regulatory compliance for businesses operating in multiple Caribbean markets, and undermines efforts to assert jurisdiction when sensitive data is hosted abroad. Establishing a **regional legal architecture** —with shared norms, dispute resolution mechanisms, and mutual legal assistance protocols— will be essential to safeguarding digital resilience and sovereignty in the Caribbean.

Additionally, Caribbean policymakers must ensure that digital sovereignty does not stop at regulation, but includes investment in local innovation, cyber capacity-building, and secure digital diplomacy mechanisms. Solutions such as data embassies, which store critical state data abroad under diplomatic immunity, may offer a solution.

2. Bilateral and multilateral agreements

A paramount legal concern for Caribbean states is maintaining sovereignty over data stored or processed beyond their territorial borders. Without specific legal protections, data housed in foreign data centers typically falls under the jurisdiction of the host country, making it vulnerable to court orders, subpoenas, or law enforcement actions.[155]

The **Data Embassy** concept directly addresses this challenge by extending a state's sovereignty to a designated foreign-hosted data site.[156] Through diplomatic or treaty-based mechanisms, such sites can be granted immunity from host state interference. Estonia's arrangement with Luxembourg exemplifies this model: via bilateral treaties, Estonia secured protection for its backup servers, ensuring they are immune to local jurisdiction.[157]

For Caribbean states, negotiating similar legal agreements —either bilaterally or multilaterally— offers the most effective path to safeguarding data sovereignty. Such accords should explicitly affirm that host countries will not seize, shut down, or otherwise interfere with the data facility, even under third-party legal or geopolitical pressure. In this context, the Caribbean states could explore a regional **Digital Sovereignty Pact** to establish standardized protections, harmonized treaty language, and reciprocal commitments across member states.

A Digital Sovereignty Pact would be a logical legal-institutional extension of CARICOM´s Single ICT Space which is anchored to the establishment of a unified digital environment across member and nonmember states and includes harmonized data protection frameworks, shared infrastructure, interoperability, and legal and policy alignment as set out in the CARICOM Vision and Roadmap for a Single ICT Space[158] and Strategic Plan for the Caribbean Community 2020-2030.[159]

---

[154] Caribbean Datacenter Association. (2025, April 6). *Insight 2/6: Positioning the Caribbean for growth through data sovereignty.* Caribbean Datacenter Association.

[155] Greenleaf, G., & Waters, N. (2014). *Global data privacy laws 2015: 109 countries, with European laws now a minority* (UNSW Law Research Paper No. 2015-45). UNSW Law.

[156] Vienna Convention on Diplomatic Relations, Apr. 18, 1961, 500 U.N.T.S. 95, Article 22: Inviolability of mission premises, Article 24: Inviolability of archives and documents, Article 27: Freedom of communication.

[157] Republic of Estonia. (2017). *Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems.*

[158] CARICOM. (2017). *Vision and roadmap for a CARICOM single ICT space.* https://caricom.org/documents/vision-and-roadmap-for-a-caricom-single-ict-space/.

[159] CARICOM Secretariat. (2022). *CARICOM Secretariat strategic plan 2022–2030.* https://caricom.org/documents/caricom-secretariat-strategic-plan-2022-2030/.

In the absence of formal treaties, states may rely on partial measures such as contractual provisions with cloud providers to specify data storage jurisdictions or apply strong encryption to restrict access. However, these measures are limited. For instance, a foreign court could still compel a cloud provider to suspend services, regardless of encryption safeguards.

Ultimately, formal Data Hosting Accords —treating such facilities as inviolable extensions of national infrastructure— are the most reliable means of preserving operational control, legal immunity, and data sovereignty in an increasingly interconnected world.

C. Data privacy, cross-border transfers, and compliance with Caribbean laws

1. Differences in national laws and external regulations and regional harmonization needs

Historically, data protection in the Caribbean was either nascent or highly fragmented, often addressed indirectly through sector-specific laws or general common law principles. However, the past decade, particularly the period around 2021, has witnessed a rapid acceleration in legislative activity. This surge has been largely spurred by the global influence of the GDPR, which has served as a significant catalyst for many Caribbean nations. Consequently, numerous countries have transitioned from having no dedicated data protection laws to enacting comprehensive statutes designed to align with modern international standards. This legislative evolution reflects a growing recognition of the strategic importance of data privacy in the digital age.

The following list contains a brief overview of what was outlined in more detail under Chapter II, describing current status of data protection legislation within the region.

- **Anguilla**: no dedicated data protection law. Some privacy protections exist in the Constitution, the Electronic Transactions Act 2006 (ETA), and the Confidential Relationships Act.
- **Antigua and Barbuda**: Data Protection Act (No. 10 of 2013). Establishes data subject rights and the role of the Information Commissioner.
- **The Bahamas**: Data Protection (Privacy of Personal Information) Act, 2003 (in force since 2007). Overseen by the Office of the Data Protection Commissioner.
- **Barbados**: Data Protection Act, 2019 (effective March 2021, some provisions pending proclamation). Modeled on GDPR, includes rights of access, erasure, portability, breach notification.
- **Belize**: Data Protection Act, 2021. Provides rights, obligations for controllers and processors, and creates a Data Protection Tribunal.
- **British Virgin Islands**: Data Protection Act, 2021. Applies to public and private bodies; provides fines for non-compliance; overseen by the Information Commissioner.
- **Cayman Islands**: Data Protection Act (2021 Revision) and Regulations, 2018. In force since 2019. Based on GDPR, overseen by the Ombudsman.
- **Cuba**: Law 149/2022 on Personal Data Protection (entered into force 2023). Administered by the Ministry of Justice (MINJUS). Introduces 12 principles and statutory retention periods.
- **Dominican Republic: Law No. 172-13 on the Protection of Personal Data (2013).** Establishes principles and rights for data subjects, but lacks a dedicated supervisory authority, with enforcement mainly through courts and sectoral regulators.

- **Dominica (Commonwealth of)**: no comprehensive data protection legislation. Constitutional privacy protections exist; reforms underway.
- **Grenada**: Data Protection Act, No. 1 of 2023. Establishes Information Commission and regulates processing by public and private bodies.
- **Guyana**: Data Protection Act No. 18 of 2023. Creates Data Protection Office (not yet operational). Provides rights to rectification, erasure, portability.
- **Haiti**: Arrêté of 2018 on personal data, plus Penal Code reforms of 2020 (not fully enacted).
- **Jamaica**: Data Protection Act No. 7 of 2020 (phased implementation from 2021–2023). Overseen by the Office of the Information Commissioner.
- **Montserrat**: no dedicated data protection law. Constitution provides privacy protections.
- **Saint Kitts and Nevis**: Data Protection Act, 2018. Establishes rights and obligations for data controllers/processors.
- **Saint Lucia**: Data Protection Act, 2011, amended in 2014 (further provisions effective 2023). Overseen by the Data Protection Commissioner.
- **Saint Vincent and the Grenadines**: Privacy Act, 2003 (applies mainly to public authorities, not a comprehensive framework).
- **Trinidad and Tobago**: Data Protection Act, 2011 (only partially proclaimed; not fully in force).
- **Turks and Caicos Islands**: no dedicated data protection law. Constitution provides privacy protections.

While some Caribbean data protection laws include extraterritorial provisions —applying to data processing activities involving their nationals regardless of the processor's physical location— there remains significant legal uncertainty around how these laws apply to sovereign government data stored abroad under a Data Embassy model. The variation in definitions, scope, and enforcement mechanisms across national data protection acts creates a fragmented legal landscape, complicating coordinated regional responses and hindering the development of shared, legally harmonized digital infrastructure.[160] Additionally, these laws primarily focus on the protection of personal data and may place restrictions on transferring such data abroad without adequate safeguards. As a result, moving sensitive datasets to foreign servers, particularly for disaster recovery purposes, may be legally complicated or outright prohibited without specific exemptions. This legal ambiguity has created uncertainty among infrastructure operators. In practice, telecommunications and cloud service providers have expressed reluctance to replicate government data offshore due to concerns over compliance, liability, and the lack of regulatory clarity. This hesitation has been noted by organizations such as the Caribbean Telecommunications Union (CTU), which has long advocated for harmonized digital policy and data governance frameworks. The Caribbean Internet Governance Forum has also been instrumental in discussing regional ICT policy. For instance, the 19th CIGF report emphasized the need for harmonized data governance frameworks to facilitate secure cross-border data flows.[161] The CTU's efforts in promoting digital transformation across the Caribbean underscore the importance of regulatory clarity.[162] Their initiatives advocate for updated policies and legislation to support digital resilience and data governance.

---

[160] European External Action Service. (n.d.). General data protection regulation. European Union. https://www.eeas.europa.eu/sites/default/files/general_data_protection_regulation_op-ed_eu_logo.doc.

[161] Caribbean Telecommunications Union. (2022, August). *Report on the 19th Caribbean Internet Governance Forum.* https://ctu.int/wp-content/uploads/2023/12/19th-CIGF-Report.pdf.

[162] Caribbean Telecommunications Union. (2024, November 8). *Digital transformation initiatives.* https://ctu.int/document-repository/digital-transformation/.

National security imperatives frequently lead states to implement data localization requirements or assert stringent control over data originating within their borders.[163] Both ECLAC and CARICOM explicitly recognizes digital sovereignty as a critical agenda item, driven by the national security risks inherent in relying on foreign-controlled digital infrastructure.[164] The eLAC working group for the Caribbean (which is consistent from all Caribbean UN member states but also from associate members and coordinated from ECLAC) has formed a sub working group on digital sovereignty while the Council for National Security and Law Enforcement (CONSLE) within CARICOM is tasked with combating threats and enhancing cooperation in mutual legal assistance, which would extend to digital security matters.[165]

A data embassy model directly addresses these national security concerns by unequivocally ensuring that the sending state retains full access and control over its data, even when it is physically located abroad. This structure protects the data from foreign legal processes, contrasting sharply with scenarios where foreign laws, could compel access to data stored by foreign providers. Any data embassy initiative must necessitate a thorough review and, if required, a substantive adaptation of both domestic data protection and national security laws. These adaptations must explicitly recognize and facilitate sovereign data replication under the authority of an international treaty.

D. Framework for regional and international legal agreements

The long-term vision for the Caribbean is to establish a **network of legally protected extraterritorial digital infrastructure** —a system of Data embassies that guarantees the continuity of government operations and safeguards national digital assets even under extreme crisis scenarios. This vision goes far beyond conventional backup systems. It reflects a broader understanding that in today's hyper-connected and geopolitically volatile world, **sovereignty must extend into the digital realm**. Only through this extension can Caribbean states truly insulate their core systems from natural disasters, cyberattacks, and foreign interference.

While formal Data Embassy treaties are being developed, **interim legal and operational solutions** should be pursued to strengthen digital resilience. Caribbean states can begin by leveraging **encrypted cloud hosting services in jurisdictions with strong legal protections**, provided that these services offer well-defined terms regarding jurisdiction, data access, and operational control. Although such arrangements do not offer diplomatic immunity, they can serve as a valuable transitional step —so long as they are carefully vetted to avoid exposure to foreign legal claims. In these cases, governments may opt for **"sovereign cloud" offerings**, in which the provider contractually guarantees that data remains within specified facilities under predefined oversight arrangements.

Still, **key legal questions must be addressed** in both interim and permanent solutions. For instance: if a government server hosted abroad fails during a crisis, under which jurisdiction is liability resolved? Can the Caribbean state seek redress in foreign courts? Does local law enforcement in the host country have any legal claim over the data during peacetime —or emergencies? These issues highlight the importance of precise treaty language and contractual provisions. A **Status of Forces Agreement (SOFA)-like model** could be adapted for Data embassies, ensuring that the host state exercises no jurisdiction inside the facility and that disputes are resolved on a state-to-state basis.

---

[163] International Bar Association. (2025, July 23). *Cyber law: The pursuit of digital sovereignty and its legal implications.* https://www.ibanet.org/document?id=Dig-Sov-Anurag.

[164] Cloud Carib. (2025, July 23). *The case for digital sovereignty in the Caribbean: A CARICOM strategic imperative.* https://info.cloudcarib.com/blog/the-case-for-digital-sovereignty.

[165] Caribbean Community (CARICOM). (2025, July 23). *The Council for National Security and Law Enforcement (CONSLE).* https://caricom.org/organs_and_bodies/the-council-for-national-security-and-law-enforcement-consle/.

Additionally, **mutual aid arrangements and telecom emergency response** raise similar legal concerns. When international entities—whether foreign telcos or emergency units —assist in restoring critical infrastructure, pre-established **Memorandums of Understanding (MoUs)** should define their legal status, operational authority, and liability. CDEMA's model for disaster response workers offers a useful precedent that can be adapted for digital infrastructure, giving foreign personnel **temporary immunity or operational clarity** under agreed frameworks.

On a **practical implementation level**, Caribbean states can also build on **existing regional legal and institutional platforms** to manage cross-border digital infrastructure. CARICOM's legal frameworks for economic integration —such as the **Single ICT Space** initiative— could be expanded to include rules on data governance, cybersecurity, and infrastructure investment. Organizations like the **OECS** already have experience in joint procurement and shared utilities, which could be extended to ICT and digital resilience efforts. By acting collectively, smaller states can actually **enhance their digital sovereignty**—gaining negotiating leverage with cloud providers, coordinating legal reforms, and jointly developing secure digital systems that no single country could afford alone.

Finally, Caribbean states should not limit their engagement to the regional level. They should actively participate in **international forums that define norms on digital sovereignty and cyber law**, including UN processes on state behavior in cyberspace. Through such advocacy, the region can push for recognition of **special protections for critical data in disaster scenarios** and ensure that global digital governance frameworks reflect the unique needs of small island developing states.

E. Legal and regulatory pathways for Caribbean Data embassies

1. National legal reforms

Caribbean governments should begin by adapting national laws to enable sovereign data replication and ensure continuity:

- **update data protection & ICT laws**: explicitly permit sovereign data backup and cross-border replication of government data, affirming that data remains under the jurisdiction of the originating country.
- **Define sovereign cloud standards**: establish minimum legal and operational requirements for cloud use in critical public systems (encryption, breach notification, auditability, jurisdiction clauses).
- **Integrate into national strategies**: embed data embassy objectives into national ICT, digital transformation, climate resilience, and security strategies to ensure long-term funding, coordination, and political commitment.

2. Regional legal and institutional frameworks

To complement national efforts, regional factors should drive regional harmonization and shared safeguards:

- **Model Regional Data Protection Law**: draft a Caribbean-wide model law to reduce fragmentation and set minimum standards.
- **Regional Legal Framework for Cross-Border Data Sharing**: develop standardized treaties, contractual clauses, and MOUs for sovereign government data replication, modeled after intra-EU GDPR mechanisms.
- **Caribbean Digital Sovereignty Pact**: create a multilateral agreement guaranteeing reciprocity: hosted government data remains under the sending state's jurisdiction, immune from host-state interference.

- **Regional task force / authority**: establish a Data Protection Harmonization Task Force or Regional Authority to:
  - Maintain a registry of trusted jurisdictions
  - Issue joint guidance on backup nodes / Data embassies
  - Provide technical assistance to smaller states
- **Mutual aid integration**: Expand CDEMA and CTU frameworks to cover digital infrastructure recovery, sovereign data replication, and telecom emergency response.
- **Regional arbitration mechanism**: Develop a legal forum for resolving disputes over jurisdiction, liability, or access in cross-border data arrangements.

3. International engagement and interim measures

While permanent treaties are being developed, states should pursue transitional solutions and global advocacy:

- **Digital embassy treaties**: negotiate bilateral/multilateral treaties (e.g., Estonia–Luxembourg model) granting diplomatic protections for extraterritorial data centers.
- **Interim cloud hosting with safeguards**: use encrypted hosting in trusted jurisdictions under strict contractual guarantees of sovereignty and access controls (with caution around laws like the U.S. CLOUD Act).
- **Standardized cloud contract clauses**: require providers to include enforceable terms on data residency, jurisdiction, and compliance with the originating country's laws.
- **Cyber insurance guidelines**: clarify liability, compensation, and insurance coverage for sovereign data hosted abroad.
- **Participation in global norm-setting**: advocate for small island states in UN and international cyber law processes, pushing for recognition of special protections for critical data in disaster scenarios.

Table 14
Regional legal and policy framework options for digital sovereignty

Recommendation	Purpose	Implementation example
Update National Data Protection and ICT Laws	Explicitly permit sovereign data replication and off-island backups while ensuring originating-country jurisdiction.	Amend laws to define sovereign data backups as regulated state functions under national oversight.
Define Sovereign Cloud Standards	Protect critical systems by setting minimum operational and legal safeguards for cloud use.	Require encryption, breach notification, jurisdiction clauses, and auditability in public-sector contracts.
Integrate Data Embassy Goals into National Strategies	Ensure long-term commitment, funding, and coordination across ministries.	Embed objectives in ICT master plans, climate resilience strategies, and digital transformation agendas.
Model Regional Data Protection Law	Reduce legal fragmentation and create common standards across Caribbean	Draft a regional "model law" aligned with global best practices (GDPR-style).
Regional Legal Framework for Cross-Border Data Sharing	Provide standardized rules for government-to-government hosting of data.	Develop model treaties and MOUs similar to EU intra-regional transfer mechanisms.
Caribbean Digital Sovereignty Pact	Guarantee reciprocity and mutual respect for jurisdiction in cross-border hosting.	Binding commitments that hosted government data is exempt from host-country laws.
Regional Data Protection Task Force / Authority	Promote harmonization, guidance, and capacity building.	Maintain registry of trusted jurisdictions; issue joint guidance on backup nodes; assist smaller states.

Recommendation	Purpose	Implementation example
Mutual Aid Integration	Expand disaster frameworks to cover digital recovery and sovereign replication.	Adapt CDEMA/CTU agreements to include telecom emergency services and sovereign backups.
Regional Arbitration Mechanism	Provide clear dispute resolution for jurisdiction, liability, and access conflicts.	International and regional tribunals arbitration for digital sovereignty cases.
Negotiate Digital Embassy Treaties	Establish long-term, treaty-based protections similar to diplomatic immunity.	Bilateral or multilateral treaties modeled on the Estonia–Luxembourg agreement.
Interim Cloud Hosting with Safeguards	Provide near-term resilience while treaties are developed.	Encrypted hosting in trusted jurisdictions with contractual guarantees of sovereignty.
Standardize Cloud Service Contracts	Ensure enforceable terms for sovereignty in commercial hosting arrangements.	Require clauses on data residency, jurisdiction, access, and auditability.
Cyber Insurance Guidelines	Clarify liability and compensation for cross-border data incidents.	Regional framework for sovereign data risk coverage.
Participate in International Norm-Setting	Ensure small island states' needs shape global digital governance.	Advocate at the UN for protections of disaster-related sovereign data.

Source: ECLAC with data from CARICOM (n.d.); CDEMA (n.d.); CTU (n.d.); European Union (2016); Republic of Estonia & Government of Luxembourg (2017); United Nations (2021); industry best practices in digital sovereignty and cloud governance.

V. The extension of the Vienna Convention and related international legal instruments to Data embassies: a pathway toward a Caribbean treaty

The concept of a "data embassy" represents an extension of long-standing principles of diplomatic protection into the digital sphere. Whereas traditional embassies serve to safeguard diplomatic personnel and state archives, data embassies are designed to ensure the continuity of government operations by externalizing critical digital assets to secure facilities located abroad.

The legal foundations for such arrangements are rooted in the Vienna Convention on Diplomatic Relations (1961) (VCDR) and the Vienna Convention on Consular Relations (1963) (VCCR). These conventions established core principles, including the inviolability of mission premises, the protection of archives, the immunity of personnel, and the duty of host States to ensure the security of diplomatic functions. However, these instruments were conceived for physical diplomatic missions staffed by accredited officials, not for sovereign-controlled servers located in high-security data centers. Their application to data embassies, therefore, requires careful interpretation, selective adaptation, and, in some instances, the development of new treaty language.

Central legal questions emerge in this context. These include whether the principle of inviolability extends to a dedicated server cage; how the doctrine of functional necessity may determine the privileges essential to the preservation of State data; and where the balance lies between sovereignty and cooperation, particularly with respect to the scope of host-State lawful access regimes over protected digital infrastructure. Further challenges arise from the actions of third States —such as cross-border cyberattacks— which pose unresolved issues of attribution, State responsibility, and countermeasures under international law, as examined in the *Tallinn Manual* and in the *Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA)*.

The adaptation of the data embassy model for the Caribbean requires a broader comparative perspective. Instruments such as the *Budapest Convention on Cybercrime*, *Convention 108+* on data protection, the *General Data Protection Regulation (GDPR)* and *NIS2 Directive*, the *Sendai Framework for Disaster Risk Reduction*, and the OECD cross-border data principles provide important complementary elements. Regional frameworks, including the *CARICOM Single ICT Space* and national data protection statutes, must also be aligned to promote coherence and interoperability. Together, these instruments constitute a mosaic of protections and obligations that a Caribbean treaty on data embassies would be required to consolidate.

Nevertheless, legal provisions alone are not sufficient. To be credible, any treaty framework must incorporate enforceable technical baselines, including service-level agreements for uptime and recovery, requirements for geo-redundancy, sovereign control of encryption keys, immutable backups, zero-trust architectures, and robust monitoring and audit mechanisms.

By connecting the principles of twentieth-century diplomatic law with the technological requirements of the twenty-first century, Caribbean States are uniquely positioned to demonstrate leadership in digital resilience. Through the adoption of data embassies, the region can transform vulnerabilities into opportunities, ensuring that data —the foundation of modern governance— remains protected and inviolable, even in circumstances where national territory or domestic infrastructure is compromised.

Why "Embassy"? Symbolism and its limitations

The use of the term *embassy* carries significant symbolic weight. It conveys to all stakeholders —including potential malicious actors— that the facility represents an extension of national sovereignty. In the same way that an attack on a diplomatic mission constitutes an affront likely to trigger a strong response, an attack on a data embassy could be perceived as an act extending beyond a routine cyber incident, potentially invoking collective defense or retaliatory measures. This symbolic dimension contributes to the deterrent value of data embassies. It also provides reassurance to citizens that, even when hosted abroad, their data is protected under conditions equivalent to those of a secure vault located in the national capital.

Nevertheless, caution is required in drawing analogies. Not all provisions of the VCDR or the VCCR are directly applicable to data embassies. Certain aspects will require new or adapted legal provisions. Examples include the treatment of cryptographic keys, the clarification of whether automated processes within a data embassy fall outside the scope of host-State regulation, and the explicit determination of which privileges and immunities are functionally necessary for the continuity of government operations.

In essence, data embassies represent an innovative diplomatic instrument for the digital era. They underscore that sovereignty is not limited to physical territory but extends to the integrity and continuity of governmental functions and records. For the Caribbean —marked by its heightened vulnerability to climate change and its advancing digital transformation agendas— the establishment of data embassies offers significant opportunities for strengthening resilience. Achieving this, however, requires a careful synthesis of the six-decade-old doctrines of the Vienna Conventions with contemporary technological realities and the negotiation of agreements tailored to regional circumstances. The subsequent sections of this chapter address these considerations in detail.

A. Vienna Convention analysis: article-by-article adaptation for the digital context

This section examines the relevant provisions of the *Vienna Convention on Diplomatic Relations* (VCDR, 1961) and, where appropriate, the *Vienna Convention on Consular Relations* (VCCR, 1963), with a view to assessing their applicability to the emerging concept of data embassies. Each provision is considered in terms of its potential contribution to the protection of sovereign-controlled digital infrastructure hosted abroad.

For the purposes of this analysis, provisions are classified into three categories:

(i) Directly applicable (verbatim): Articles whose language and intent can be applied to data embassies without modification.

(ii) Analogously applicable with interpretation: Articles that can inform the protection of data embassies but require interpretative extensions to address digital environments.

(iii) Requiring new language: Articles that do not adequately cover digital contexts and therefore necessitate the drafting of new treaty provisions.

A consolidated mapping of this classification is presented in Table 5.1 at the conclusion of the section.

1. Premises of the mission (VCDR Article 1(i) and Article 22; VCCR Article 31)

Diplomatic law baseline: Article 1(i) of the Vienna Convention on Diplomatic Relations (VCDR) defines the "premises of the mission" as "the buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used for the purposes of the mission". Article 22(1) establishes that such premises are inviolable and that agents of the receiving State may not enter without consent. Similarly, Article 31 of the Vienna Convention on Consular Relations (VCCR) grants inviolability to consular premises, although with limited exceptions: consent of the head of post may be presumed in cases of emergency, and premises are not to be used in ways incompatible with consular functions.

Application to data embassies: in the context of a data embassy, the "premises" may consist of a dedicated cage in a co-location facility or a secure room within a host government's data center. These arrangements can reasonably be considered "parts of buildings" used for the purposes of the mission, where the mission is defined as ensuring digital continuity and the preservation of sovereign archives. Although this extends the conventional understanding of mission functions, it remains consistent with the object and purpose of Article 1(i) where such continuity has been formally agreed upon between the sending and receiving States.

Operational precedents: the Estonia–Luxembourg Data Embassy Agreement provides a useful reference. In that treaty, the premises were defined explicitly as a dedicated data center space allocated by Luxembourg for Estonian sovereign data and equipment. The agreement transposed the protections of VCDR Article 22, prohibiting entry, search, or requisition without consent. It further incorporated an emergency clause inspired by VCCR Article 31, allowing presumed consent for entry by host officials in cases of fire or other urgent circumstances requiring immediate action.

Issues for consideration: while inviolability under the VCDR is unconditional, the consular law model introduces practical flexibility. For data embassies, a prudent approach is to combine the strict inviolability of Article 22 with a narrowly defined emergency-entry presumption, ensuring both the protection of sovereign assets and the ability of the host to respond to threats to life or property.

Inviolability irrespective of ownership: the principle of inviolability *"irrespective of ownership"* is directly applicable. In practice, the host State or a private operator may own or manage the building, but this does not diminish the protection afforded to the specific designated premises. The core obligation of the receiving State remains unchanged.

Clarifications required: while the existing provisions of the VCDR and VCCR provide a strong baseline, certain areas require further specification in a data embassy treaty. These include:

- Explicitly defining *"premises"* to encompass sovereign-designated spaces within data centers, including racks or cages;
- Providing for the possibility of unmanned premises by designating a competent authority or accredited representative responsible for granting consent and coordinating with host officials in emergencies; and
- Clarifying whether the definition could extend in future to sovereign-controlled segments of cloud infrastructure, should such models be adopted.

Assessment: the provisions on mission premises are **analogously applicable with interpretation**. They can be employed as a foundation for data embassy agreements, with tailored definitions of *premises*, explicit recognition of digital continuity functions, and the inclusion of narrowly drawn emergency clauses to balance inviolability with safety considerations.

Verdict: applicable by analogy with clear definition. Use the language of VCDR Article 22 to guarantee inviolability of the designated server premises, while including an emergency-entry clause (inspired by VCCR Article 31) and a precise definition of what constitutes the premises in the context of data embassies.

2. Inviolability of archives and documents (VCDR Article 24; VCCR Article 33)

Diplomatic law baseline: Article 24 of the VCDR establishes that "the archives and documents of the mission shall be inviolable at all times and wherever they may be". Article 33 of the VCCR provides a similar guarantee for consular archives. This inviolability prohibits the receiving State from examining, seizing, or otherwise interfering with mission records and requires the preservation of their confidentiality. The reference to "wherever they may be" anticipates protection even when archives are temporarily outside the mission premises, such as during transit or temporary storage.

Application to data embassies: in a data embassy context, the archives consist of digital records—databases, backups, and electronic files —rather than paper documents. Applying the principle of functional equivalence, these digital assets qualify as *archives and documents of the mission* and are therefore entitled to the same protections. Data embassy agreements typically specify that all data stored within the facility is considered the archives of the sending State, triggering inviolability. This precludes host-State authorities from accessing, copying, or disclosing such data, even in response to domestic judicial proceedings or external requests.

Operational precedents: the Estonia–Luxembourg Data Embassy Agreement adopted this approach explicitly. It stated that *"all data and information systems stored by [Estonia] in the premises shall be regarded as archives of [Estonia]. The archives of the premises shall be inviolable and thus exempt from search, requisition, attachment or execution."* This mirrors the wording of Article 24 and extends it to cover electronic data, ensuring protection from enforcement actions such as judicial attachment or execution of judgments. A Caribbean treaty could adopt similar language to confirm that electronic archives enjoy identical inviolability to traditional diplomatic records.

Challenges and nuances: a practical issue concerns the scope of what constitutes an *archive* in digital terms. This may encompass live databases, backups, system logs, and metadata, all of which should fall under the definition to ensure comprehensive protection. Another important aspect is the interpretation of "*wherever they may be"*. This formulation implies that archives remain inviolable when in transit, such as when backup media are physically transported between the sending State and the data embassy, or when data are transmitted across networks. This interpretation aligns with the treatment of diplomatic bags and reinforces the principle that inviolability attaches to the data itself, regardless of location.

Clarifications required: while the provisions of Article 24 are sufficiently broad and technologically neutral, treaties on data embassies may benefit from supplementary clarification that *"archives and documents"* include data in electronic, magnetic, optical, or cloud-based formats. Such clarification would eliminate ambiguity and reinforce that inviolability extends to all forms of digital storage and transmission.

Assessment: the principle of inviolability of archives and documents is **fully applicable** to data embassies, with minimal adaptation required. Its broad phrasing already anticipates protection beyond physical premises and is consistent with the digital realities of contemporary governance.

Verdict: fully applicable with minor clarification. All digital data stored within a data embassy should be expressly classified as the archives of the sending State, invoking inviolability exactly as provided under VCDR Article 24 and VCCR Article 33, and extending this protection to data in transit and transmission.

3. Inviolability of the mission's property and assets / protection duty (VCDR Article 22(2); VCCR Article 31(3))

Diplomatic law baseline: Article 22(2) of the VCDR provides that "the receiving State is under a special duty to take all appropriate steps to protect the premises of the mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity." Article 22(3) further specifies that the premises may not be used as a refuge by persons seeking to avoid arrest, which is not directly relevant in the digital context. Similarly, Article 31(3) of the VCCR obliges the receiving State to protect consular premises from intrusion or damage.

Application to data embassies: in the case of a data embassy, the host State bears a parallel duty to shield the designated premises from intrusion or damage. In practice, this includes ensuring that the hosting data center provides robust physical security measures —such as access controls, patrols, and surveillance— comparable to those applied to the host's own critical infrastructure. It may also involve rapid response to attempts at unlawful entry or interference, including ensuring that domestic authorities quash any inadvertent judicial orders, such as warrants seeking access to the premises.

Operational precedents: the Estonia–Luxembourg Data Embassy Agreement incorporated this obligation directly, stipulating that *"Luxembourg shall take all appropriate measures to protect the premises against any intrusion or damage… measures are considered appropriate if they meet the same level of protection as the protection offered to Luxembourg's own premises."* This adaptation of Article 22(2) established a useful benchmark: parity with the host's own security standards, thereby ensuring non-discrimination and a clear operational standard for protection.

Digital dimension: a contemporary issue concerns whether the duty to protect should extend to cyber intrusions. Although diplomatic law originally contemplated only physical interference, the duty to prevent *"disturbance of the peace"* can reasonably be interpreted to include malicious cyber activity originating within the host's territory. In practice, this could translate into obligations for the host State to take reasonable measures —such as law enforcement action against domestic actors targeting the data embassy, or facilitating cooperation between national Computer Emergency Response Teams (CERTs)—to mitigate cyber incidents.

Clarifications required: to adapt Article 22(2) to the digital era, supplementary provisions may specify that "*intrusion*" encompasses unauthorized electronic or network access attempts, in addition to physical trespass. A treaty may also establish operational procedures for cooperation, such as secure liaison channels between the sending State's CERT and the host State's CERT or law enforcement agencies, to ensure rapid detection, response, and investigation of cyber incidents affecting the data embassy.

Assessment: the obligation to protect mission premises and assets is **applicable with clarifications**. Its core elements transfer effectively to the data embassy model, but explicit reference to digital intrusions and operational cooperation mechanisms would enhance clarity and effectiveness.

Verdict: applicable with clarifications. The host State must protect the premises and assets of a data embassy on the same basis as diplomatic missions, explicitly including protection against cyber threats. A best-practice approach is to adopt the equivalence standard established in the Estonia–Luxembourg treaty, requiring the host to provide the same level of protection as afforded to its own critical data centers.

4. Personal inviolability and mission personnel (VCDR Articles 29–31; VCCR Articles 41–43)

Diplomatic law baseline: Article 29 of the VCDR establishes that diplomatic agents are inviolable and cannot be arrested or detained. Article 31 extends immunity from criminal jurisdiction and, with limited exceptions, from civil jurisdiction. Article 37 provides that administrative and technical staff enjoy certain immunities, while service staff enjoy more restricted privileges. In contrast, under the VCCR, consular officers are granted only functional immunity under Article 43 and may be subject to arrest for grave crimes, while consular employees are often locally recruited.

Application to data embassies: data embassies generally operate with minimal human presence. However, certain scenarios require adaptation of these provisions. For instance, if the sending State deploys information technology personnel to install, maintain, or service the data embassy, their legal status must be defined. Without formal diplomatic accreditation, they may not automatically fall under the protections of the VCDR. To facilitate their functions —particularly when handling sensitive data or equipment— they may either be attached to the diplomatic mission of the sending State and thereby covered by VCDR privileges, or granted specific immunities under a bilateral or multilateral data embassy treaty.

Operational precedents: the Estonia–Luxembourg Data Embassy Agreement did not explicitly create a new category of "data diplomats," instead referring to "authorized representatives" with access to the premises. This approach relied on existing diplomatic channels to provide cover for such personnel. For a Caribbean framework, however, a clause may be required to remove ambiguity, ensuring that authorized personnel tasked with the maintenance or inspection of a data embassy are protected for acts performed in the course of their duties.

Issues for consideration: several options are available:

- **Diplomatic model:** extend VCDR immunities by formally accrediting personnel as part of the diplomatic or technical staff of the mission.
- **Functional model:** grant immunity only for acts performed in the exercise of official functions, analogous to VCCR Article 43 or the status of "experts on mission."
- **Persona non grata principle:** where personnel misuse their role —such as engaging in activities beyond the treaty mandate— the host may request their removal. This could mirror the mechanism of VCDR Article 9 or be articulated as a specific treaty clause.

Clarifications required: a Caribbean treaty could specify that "authorized personnel of the sending State engaged in official maintenance or oversight of the Data Embassy shall enjoy functional immunity with respect to acts performed in the exercise of their duties under this Agreement." Such wording would ensure legal certainty while avoiding the extension of broader privileges irrelevant to the data embassy context (such as exemptions from residence or employment law).

Assessment: the principle of personal inviolability is **analogously applicable with adaptation**. Data embassies do not require standing diplomatic staff, but functional immunity should be provided to visiting personnel to enable the secure performance of their duties.

Verdict: analogous application with adaptation. Visiting personnel should be granted functional immunity for official acts, with the persona non grata concept available through diplomatic channels. No broader privileges —such as those associated with residence or dependents— are required in this context.

5. Freedom of communication and diplomatic bag (VCDR Article 27; VCCR Article 35)

Diplomatic law baseline: Article 27 of the VCDR enshrines the right of missions to free and confidential communication for all official purposes. It authorizes the use of codes, ciphers, and diplomatic couriers, and declares the diplomatic bag inviolable. Paragraph 3 obliges the receiving State to facilitate alternate communication channels in the event of disruptions. Article 35 of the VCCR grants similar, though narrower, rights to consular posts, including the possibility of inspecting consular bags if suspected of containing non-official items.

Application to data embassies: the provisions of Article 27 align closely with the operational needs of data embassies. Continuous, secure communication between the sending State and its data embassy is essential. This may be achieved through dedicated communication lines, encrypted virtual private networks, or satellite links. As with traditional missions, the receiving State must not intercept, block, or interfere with such communications. The express recognition in Article 27 of codes and ciphers provides a clear legal basis for the use of strong encryption in data embassy communications.

Operational precedents: the Estonia–Luxembourg Data Embassy Agreement incorporated these protections, affirming the right to use encryption, diplomatic couriers, and storage media, and prohibiting censorship or interception of communications. It extended the diplomatic bag concept to include data carriers such as tapes, disks, and electronic storage devices.

Issues for consideration:

- **Digital communications:** all official data transmissions to and from the data embassy should be considered inviolable. The host must not inspect or monitor such traffic, including metadata.
- **Encryption:** the sending State should retain exclusive control of cryptographic keys, with the host prohibited from imposing decryption obligations.
- **Physical transfer:** in cases where physical media (e.g., backup drives) must be transported, these should be explicitly treated as diplomatic bags, protected from search or seizure.
- **Continuity of communications:** in the event of outages —whether caused by natural disasters or cyber incidents— the host should facilitate alternate channels (such as satellite communications) with the same priority it affords to its own government services.

Clarifications required: while Article 27 is sufficiently broad, treaties on data embassies may include explicit reference to modern digital forms, such as *"electronic storage media, digital transmissions, and other means of secure communication."* This would ensure the comprehensive protection of contemporary data transfer modalities, including cloud-based transmissions.

Assessment: the freedom of communication provisions of the VCDR are **directly applicable with minor specification**. They already encompass encryption and secure communications and can be extended to cover modern technologies with minimal textual clarification.

Verdict: directly applicable with explicit mention of digital forms. Free and secure communication, including the use of encryption and diplomatic bags, must be guaranteed. The host shall not monitor or obstruct data flows and must assist in maintaining or restoring communication channels during crises.

6. Jurisdictional immunity of the mission and its operations

Diplomatic law baseline: Article 31 of the *Vienna Convention on Diplomatic Relations* (VCDR) grants diplomatic agents immunity from the criminal, civil, and administrative jurisdiction of the receiving State, subject to limited exceptions. While the VCDR does not explicitly regulate the jurisdictional immunity of the mission itself, customary international law and the principle of state immunity generally prevent embassies from being subjected to local legal proceedings. Article 32 further provides that immunity may only be waived by the sending State.

Application to data embassies: two dimensions are particularly relevant in the data embassy context:

- **Immunity of operations:** the activities of the data embassy, as an extension of the sending State, should remain beyond the jurisdiction of the host State's courts and administrative agencies. This includes immunity from requests by local tax authorities, labor inspectors, or regulators, particularly given that no local staff or commercial functions are envisaged.
- **Immunity of equipment and assets:** data embassy servers, storage devices, and associated licenses must be protected from legal process, including attachment, requisition, or enforcement actions by creditors. The Estonia–Luxembourg Data Embassy Agreement addressed this explicitly in Article 5, declaring such assets immune from legal process. This reflects the principle, recognized in state immunity doctrine and instruments such as the *United Nations Convention on Jurisdictional Immunities of States and Their Property* (2004), that property of a State used for sovereign (non-commercial) purposes is immune from attachment.

Operational considerations:

- **Waiver of immunity:** consistent with Article 32 of the VCDR, only the sending State may consent to the host's jurisdiction or intervention. While waiver in this context would be rare, a treaty may clarify that the sending State may authorize specific, supervised actions by host authorities (e.g., emergency repairs or disaster response) without this constituting a waiver of immunity.
- **Criminal acts within the data embassy:** if unlawful conduct occurs inside the data embassy (e.g., theft or sabotage by an insider), host authorities may not intervene without consent but may exercise jurisdiction once the suspect leaves the protected premises. Cooperation mechanisms between the States should be articulated in the treaty to ensure effective investigation while respecting inviolability.
- **Requests for data by third parties:** in cases where another State, or even the host itself, seeks access to data for law enforcement purposes, such requests must be directed to the sending State's competent authorities through established intergovernmental or mutual legal assistance (MLA/MLAT) channels. The host may not compel disclosure directly from the data embassy infrastructure.

Clarifications required: a Caribbean framework should include explicit provisions confirming that:

- Data embassy operations and assets are immune from the jurisdiction of host State authorities.
- Servers, equipment, and data are protected from search, seizure, attachment, or other forms of legal process.
- Any legal cooperation must occur exclusively through intergovernmental channels.
- Immunities may only be waived by the sending State, in accordance with treaty provisions.

Assessment: the principles of state and diplomatic immunity are **directly applicable with explicit articulation**. While rooted in existing diplomatic law and customary practice, a treaty should codify these protections to eliminate ambiguity and extend them specifically to sovereign-controlled digital assets.

Verdict: apply state immunity to all data embassy operations and assets. Explicitly affirm immunity from search, seizure, attachment, or suit, unless expressly waived by the sending State. Clarify that all data requests must be routed through intergovernmental channels, thereby preserving consistency with international practice on immunity and inviolability.

7. Taxation, customs, and fiscal privileges (VCDR Articles 23, 34, 36; VCCR Article 32)

Diplomatic law baseline: the VCDR provides several fiscal privileges relevant to missions:

- **Article 23:** exempts mission premises from national, regional, or municipal taxes, with the exception of payments for specific services.
- **Article 34:** exempts diplomatic agents from most personal taxes and duties.
- **Article 36:** exempts articles imported for the official use of the mission from customs duties and inspection, and allows limited personal exemptions for staff.

  The VCCR includes comparable provisions in Article 32 (tax exemptions for consular premises) and Article 50 (facilitation of the movement of articles for official use).

Application to data embassies: the operation of a data embassy raises several fiscal and customs issues requiring clear adaptation of these principles.

- **Premises-related costs:** if the sending State rents server space or secure rooms within a host's data center, the question arises whether rental payments should be exempt from value-added tax (VAT) or similar charges. In practice, many diplomatic leases are exempted under bilateral arrangements, and equivalent treatment for data embassies would prevent undue fiscal burden.
- **Customs duties and import taxes:** servers, networking equipment, and storage devices imported by the sending State for official use in a data embassy should be exempt from duties and taxes, consistent with Article 36. These privileges should also extend to their eventual removal or re-export.
- **Host-provided facilities:** if the host government provides premises at no cost, fiscal issues may not arise directly. Nevertheless, treaty language should ensure that no indirect taxation is imposed through ancillary service charges or pass-through property taxes.
- **Operational services:** it is prudent to extend exemptions to VAT or other taxes applied to services directly connected with the operation of the data embassy (e.g., power, telecommunications, or maintenance), either through waiver or reimbursement mechanisms.

- **Local staff taxation:** given that data embassies are generally not expected to employ local staff, exemptions concerning payroll or employment taxation are likely unnecessary. If exceptions arise, however, standard diplomatic practice could be extended.

Operational precedents: while the Estonia–Luxembourg Data Embassy Agreement did not explicitly reference fiscal privileges, this may reflect the EU internal market framework or separate diplomatic understandings. For Caribbean arrangements —particularly where customs controls and indirect taxes are significant— explicit treaty provisions are advisable to avoid ambiguity or administrative obstacles.

Clarifications required: a Caribbean framework should state expressly that:

- Data embassy premises and operations benefit from the same tax exemptions as diplomatic missions, in accordance with VCDR Article 23.
- All equipment, software, and supplies imported for official use are exempt from duties, inspections, and related charges, in line with VCDR Article 36.
- Services essential to the operation of the data embassy, such as power and connectivity, should be tax-exempt or eligible for reimbursement.
- Where applicable, exemptions should be implemented through domestic legal or regulatory instruments to ensure enforceability.

Assessment: fiscal privileges under the VCDR and VCCR are **largely applicable in their existing form**, but must be explicitly extended to the unique circumstances of data embassies, particularly in relation to equipment import/export and VAT treatment on operational services.

Verdict: largely applicable (verbatim principles). For clarity and to facilitate seamless operation, data embassy treaties should explicitly extend tax and customs exemptions to premises, equipment, and essential services, ensuring that no fiscal or bureaucratic obstacles hinder their establishment and maintenance.

8. Respect for local laws and non-interference (VCDR Article 41; VCCR Article 55)

Diplomatic law baseline: Article 41(1) of the VCDR obliges all persons enjoying privileges and immunities to respect the laws and regulations of the receiving State and prohibits interference in its internal affairs. Article 41(3) further stipulates that the premises of the mission must not be used in any manner incompatible with the functions of the mission as defined in the Convention or by other rules of international law. Article 55 of the VCCR establishes comparable obligations for consular posts.

Application to data embassies: these provisions are of particular importance in the data embassy context, as they address the potential concern that the sending State might misuse immunity protections for activities unrelated to government continuity. For example, without clear limits, a host State might fear that a data embassy could be used for intelligence operations, cyber-espionage, or to host data from third parties without authorization. Such activities would exceed the intended purpose of safeguarding sovereign digital archives and would undermine trust between the States.

To mitigate these risks, the treaty should explicitly restrict the data embassy's use to the agreed functions, such as *"hosting data and information systems essential for the continuity of government services."* This reflects the approach adopted in the Estonia–Luxembourg Agreement, which incorporated language based on VCDR Article 41(3). In practice, this ensures that if the sending State misuses the facility —such as conducting cyber operations, storing unlawful material, or interfering in the host's internal affairs— the host may treat such conduct as a breach of the agreement and respond through established diplomatic or legal channels.

Non-interference obligations: while the likelihood of interference is minimal in the case of a facility dedicated to data storage, it remains necessary to codify this principle. The data embassy must not be used, for instance, to broadcast political communications within the host State or to facilitate activities contrary to its sovereignty. This preserves reciprocity and reassures the host that immunity will not shield abuse.

Personnel considerations: any authorized personnel operating within or visiting the data embassy should also be subject to the obligation of respecting the laws and regulations of the host State, consistent with VCDR Article 41(1). Given the minimal and intermittent presence of personnel in most data embassy models, a general clause affirming this duty would suffice.

Assessment: the principles of respect for local law and non-interference are **directly applicable** to the data embassy framework. By codifying a "proper use" clause and limiting the scope of activities to treaty-defined functions, the framework provides both reassurance to the host and a legal basis for addressing misuse through diplomatic remedies.

Verdict: directly applicable with emphasis on proper-use clauses. The treaty should affirm that the data embassy shall not be used in ways incompatible with its defined purpose or international law, thereby safeguarding the host State's interests and providing a mechanism to address abuse through recognized diplomatic channels.

9. Termination of mission and disposal of archives and premises (VCDR Articles 43–45; VCCR Articles 27, 31(4))

Diplomatic law baseline: Articles 43 to 45 of the VCDR address the cessation of the functions of individual diplomats and of missions as a whole. Of particular importance, Article 45 obliges the receiving State, in the event of severance of diplomatic relations or closure of the mission, to (a) respect and protect the premises, property, and archives of the mission, even in the absence of personnel, and (b) permit a protecting power designated by the sending State to assume custody. The VCCR contains parallel provisions in Article 27(1)(a) regarding the protection of consular archives after closure, and in Article 31(4) concerning safeguarding of consular premises.

Application to data embassies: termination scenarios for data embassies may include:

- The voluntary conclusion of a treaty, for example when the sending State develops alternative resilient infrastructure.
- The relocation of the data embassy to a different host country or facility.
- The breakdown of bilateral relations, including extreme cases such as conflict or severance of ties.

In each of these scenarios, the continuity of protection for the sending State's digital archives is essential. Unlike physical embassies, where personnel can be withdrawn and premises vacated, digital archives require careful transfer or safeguarding to prevent confiscation, loss, or misuse.

The Estonia–Luxembourg Data Embassy Agreement (Article 10(4)) provides a relevant precedent: upon termination, archives and equipment "shall only be handed over to the authorized representative" of Estonia. In the absence of such a representative, Luxembourg is obliged to protect the archives with the same level of care as its own and to release them only to a duly identified legal authority of Estonia. This model ensures continuity of protection even in cases of political instability or government incapacity.

Operational implications for Caribbean adaptation:

- **Continuity of protection:** host States should remain bound to protect the data embassy's archives and equipment after termination of an agreement, until they are securely returned to the sending State or a designated entity.

- **Protecting power mechanism:** following VCDR practice, treaties could allow for the appointment of a "protecting power" (a third State acceptable to both parties) to assume responsibility for the data embassy in case of collapse or incapacity of the sending State.
- **Notice periods:** in planned withdrawals or relocations, sufficient notice (e.g., 12–24 months) should be required to allow orderly transfer of archives and dismantling of equipment.
- **Equipment removal and re-export:** re-export of servers and associated hardware should be facilitated under the same fiscal privileges that governed their import, without customs duties or inspection.
- **Sudden termination:** even in abrupt severance of relations without notice, obligations to protect archives and data should survive termination, consistent with customary international law practice respecting inviolability of archives (e.g., affirmed in cases such as the United States diplomatic archives in Iran).

Assessment: the protective obligations in VCDR Article 45 are **directly applicable by analogy** to the data embassy model. Explicit treaty provisions should adapt these principles to digital archives, ensuring safe custody, continuity of protection, and orderly handover or removal of data and equipment in all termination scenarios.

Verdict: VCDR Article 45 is applicable by analogy and should be expressly incorporated. Host States must protect, safeguard, and ultimately return data embassy archives and equipment upon termination or crisis. Provisions should include notice periods for orderly withdrawal, the possibility of a protecting power arrangement, and guarantees that obligations endure even in cases of abrupt severance of relations.

10. Dispute settlement (VCDR optional protocol; general international law)

Diplomatic law baseline: the VCDR does not contain a dispute settlement clause within its substantive provisions. However, an *Optional Protocol on the Compulsory Settlement of Disputes* was adopted alongside the Convention, providing that disputes concerning its interpretation or application may be submitted to the International Court of Justice (ICJ) if the parties have accepted its jurisdiction. In practice, many bilateral agreements supplement this framework by providing for arbitration or other negotiated mechanisms to resolve disagreements.

Application to data embassies: given the innovative and sensitive nature of data embassies, it is essential to incorporate clear dispute settlement procedures into any treaty framework. The Estonia–Luxembourg Agreement adopted a pragmatic model, stipulating that disputes not resolved by negotiation would be submitted to arbitration, with a defined procedure for the appointment of arbitrators and issuance of a binding award.

For a multilateral Caribbean framework, a range of options is available:

- **Peaceful settlement under international law:** parties may affirm a general commitment to settle disputes by peaceful means, consistent with Article 2(3) of the United Nations Charter. This could include reference to ICJ jurisdiction, where accepted by the States concerned.
- **Arbitral tribunal:** a tailored arbitration procedure—where each party appoints one arbitrator and those arbitrators select a chair, with a fallback appointment mechanism (e.g., by the President of the ICJ)—provides flexibility, confidentiality, and binding outcomes. This model closely reflects the Estonia–Luxembourg approach and is well suited to technical disputes.
- **Regional adjudication:** where appropriate, the Caribbean Court of Justice (CCJ) could be designated as a forum, particularly if the treaty is embedded within CARICOM's legal framework. The CCJ already has original jurisdiction over CARICOM treaty matters and could serve as a neutral regional mechanism.

- **Joint Commission mediation:** as noted in Section G on governance, a Joint Commission could serve as the first step in dispute resolution by facilitating consultation and mediation before escalation to arbitration or judicial settlement.

Multilateral considerations: in a regional treaty, disputes may involve multiple States on one side (e.g., a host State and several sending States). Arbitration mechanisms should therefore provide for collective appointment of arbitrators and allow for consolidation of proceedings where disputes raise common questions. This would ensure procedural efficiency and consistency.

Assessment: incorporating structured dispute settlement provisions reduces the risk of political escalation and provides confidence to both host and sending States that conflicts can be managed in a rules-based manner. A tiered approach —consultation and mediation, followed by arbitration, with the possibility of ICJ or CCJ jurisdiction where consented— offers both flexibility and finality.

Verdict: the Optional Protocol to the VCDR provides a useful foundation, but explicit treaty provisions are necessary. The recommended model is a **three-stage process**: (i) consultations through a Joint Commission, (ii) binding arbitration with clear appointment rules, and (iii) optional recourse to ICJ or CCJ jurisdiction where accepted. This ensures predictability, neutrality, and enforceability in resolving disputes arising from data embassy arrangements.

Table 15
Article-by-article applicability of Vienna Convention provisions to Data embassies

VCDR / VCCR provision	Content summary	Applicability to Data Embassy	Recommended treaty action
VCDR Art.1(i) – Premises definition	Defines "premises of the mission" as buildings/parts used for mission purposes	Covers data centre rooms, cages, or dedicated digital infrastructure	Define "premises" explicitly to include data embassy facilities (e.g. server rooms, racks).
VCDR Art.22(1) – Inviolability of premises	No entry/search by host without consent	Directly applicable, with adaptation for emergencies	Include verbatim, add clause allowing entry if immediate protective action is needed (drawing on VCCR Art.31).
VCDR Art.22(2) – Duty to protect premises	Host must protect premises from intrusion/damage	Applicable, extend to physical and cyber intrusions	Require protection at least equivalent to host's own critical infrastructure, explicitly mention cyber defence.
VCDR Art.24 – Inviolability of archives	Archives and documents inviolable at all times, wherever they may be	Fully applicable, archives = electronic data	Include verbatim; clarify that electronic/digital data are archives.
VCCR Art.33 – Consular archives	Consular archives inviolable	Principle applies, but covered by VCDR Art.24	No separate action unless honorary consulates relevant.
VCDR Art.27(1) – Freedom of communication	Host must permit free official communications, including codes/ciphers	Essential for secure data links and encryption	Include verbatim, confirm right to strong encryption and protected channels.
VCDR Art.27(2) – Diplomatic bag inviolable	Diplomatic bag cannot be opened/detained	Applicable to physical data/media shipments	Extend to servers, drives, or other digital storage media; designate shipments as diplomatic bags.
VCDR Art.27(3) – Priority communications	Host must facilitate alternate communications during disruptions	Relevant to telecom outages	Include; ensure priority restoration of data embassy communications in crises.
VCDR Art.29 – Personal inviolability	Diplomatic agents cannot be arrested/detained	Relevant only if personnel are present	Grant functional immunity to visiting technical staff performing official duties.
VCDR Art.31 – Immunity from jurisdiction	Full criminal/civil immunity for diplomats	Relevant for state operations and designated staff	Apply to state operations and equipment; staff to receive functional (not full) immunity.
VCDR Art.31(4) – Sending state jurisdiction	Diplomats remain under sending state jurisdiction	Not directly relevant	Implicit; no treaty action needed.
VCDR Art.32 – Waiver of immunity	Sending state can waive immunity	Relevant if sending state consents to host's limited intervention	Provide mechanism for consent in specific circumstances (e.g. repairs after disaster).

VCDR / VCCR provision	Content summary	Applicability to Data Embassy	Recommended treaty action
VCDR Art.34 – Tax exemptions (personal)	Diplomats exempt from personal taxes	Not applicable	No action, unless extending courtesy to visiting technical staff.
VCDR Art.35 – Exemption from social security	Mission staff exempt from host social security	Not applicable if no local staff	No action unless local contractors employed.
VCDR Art.36 – Customs and duties	Exemption from customs duties for mission articles	Highly relevant (servers, equipment, backup media)	Exempt all data embassy equipment and supplies; protect against customs inspection.
VCDR Art.37 – Family/staff immunities	Immunities for families/admin staff	Not applicable to data embassy	No action required.
VCDR Art.38 – Host nationals as staff	Limited immunity for local hires	Not applicable	No action (or discourage hiring local staff for security).
VCDR Arts.39–40 – Start/end of privileges; transit	Immunities during travel; obligations of transit states	Relevant for transport of equipment/data	Treaty may note inviolability of data/media during third-state transit (if party to agreement).
VCDR Art.41(3) – Prohibition of incompatible use	Premises must not be used contrary to mission purposes	Directly applicable to data embassies	Include clause restricting use to continuity/storage of government data.
VCDR Arts.44–45 – Closure of mission	Host must respect and protect archives even if mission ends	Directly relevant for data embassy termination	Include safe-handover clause; archives/equipment only to be returned to authorized representatives.
VCCR Art.27(1) – Consular closure	Host must protect consular archives after closure	Same principle as VCDR Art.45	Covered by above.
VCDR Art.9 – Persona non grata	Host may expel diplomatic personnel	Applicable to visiting data embassy staff	Include mechanism for host to request removal of offending technical personnel.
Optional Protocol – Dispute settlement	ICJ jurisdiction for disputes (if accepted)	Relevant; Estonia–Lux used arbitration	Include tiered mechanism: Joint Commission → arbitration → ICJ/CCJ by consent.

Source: ECLAC with data from the *VCDR (1961)* and VCCR(1963).

In conclusion, the Vienna Conventions constitute a solid foundation upon which the protection of data embassies can be constructed. The core guarantees —such as the inviolability of premises and archives, the immunities attaching to State property, and the safeguarding of secure communications— can in most cases be applied directly or adapted by analogy to the digital environment. Where gaps exist, these can be addressed through carefully crafted supplementary provisions, including explicit recognition of immunity for equipment, clarification of the legal status of technical personnel, precise limitations on the permissible functions of the data embassy, and dedicated mechanisms for dispute settlement. Beyond its specific legal provisions, the principal contribution of the Vienna Convention lies in offering a long-standing, effective, and functional precedent that has operated for decades with minimal instances of violation. While bilateral treaties may serve as an important initial step, the establishment of data embassies as a recognized concept in international law ultimately depends on broad international acceptance. For this reason, the adoption of a multilateral convention modeled on the principles and legitimacy of the Vienna Convention is crucial.

B. Related international legal and policy instruments

The protection of data embassies and cross-border digital infrastructure engages not only the principles of diplomatic law but also a broader constellation of international legal and policy frameworks. This section examines the principal global and regional instruments that intersect with the data embassy concept, highlighting areas of complementarity as well as potential sources of tension. It also identifies the normative and operational gaps that a Caribbean framework would need to address, while underscoring opportunities for alignment —for example, by drawing on existing mechanisms for cooperation in the fields of cybercrime prevention, data protection, and disaster resilience.

1. United Nations Charter and the principle of state sovereignty

At the broadest level, the Charter of the United Nations enshrines the principles of sovereign equality (Article 2(1)) and non-interference in the domestic affairs of States (Article 2(7)). The establishment of a data embassy arrangement reinforces sovereign equality by enabling even small and vulnerable States to exercise effective control over their critical digital assets extraterritorially, on the basis of mutual consent. Far from limiting sovereignty, such agreements represent its active exercise and can enhance international stability by increasing national resilience to shocks.

In the event of a malicious cyber operation targeting a data embassy, Charter principles may also be engaged. In extreme scenarios, such an attack could fall within the scope of Article 2(4), which prohibits the use of force against the territorial integrity or political independence of any State. While international debate continues as to whether certain cyber operations reach the "use of force" threshold, it is widely accepted that sovereignty itself may be violated when a State's digital infrastructure is compromised without consent. The Tallinn Manual 2.0, for instance, affirms that cyber operations infringing the integrity of another State's digital systems can constitute a breach of sovereignty.

Accordingly, the general principles of the Charter lend support to the inviolability of data embassies. Unauthorized interference with such facilities would constitute an impermissible intervention in the sovereign functions of the sending State, and in many cases also infringe upon the responsibilities and rights of the host State.

2. Responsibility of States for Internationally Wrongful Acts (ARSIWA)

The *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA), adopted by the International Law Commission in 2001, codify the principles governing when conduct is attributable to a State, the nature of the resulting breach, and the legal consequences. These principles are directly relevant to the protection of data embassies.

If the host State itself were to breach its obligations under a data embassy treaty —for example, through the unauthorized entry of its law enforcement agents into the secured premises—this would constitute an internationally wrongful act attributable to the host State. Under ARSIWA, the host would be obliged to cease the wrongful act, provide restitution (for example, the return of seized data or equipment), and, where appropriate, offer compensation for resulting damage.

If a third State, or agents under its control, were to launch a cyber operation against a data embassy, this would amount to a wrongful act against the sending State, involving both a violation of sovereignty and a breach of the treaty-based protections afforded to archives and infrastructure. In such a scenario, the sending State could invoke the international responsibility of the third State. Where the host State is also affected —for instance, if its territory is misused for staging the attack or its bilateral commitments are undermined— both the sending and host States could act as injured States entitled to invoke responsibility.

ARSIWA also recognizes the right of injured States to adopt countermeasures —otherwise unlawful acts taken in proportionate response to induce compliance by the responsible State. Applied to cyberspace, this may include targeted cyber countermeasures against the systems of the offending State, provided they are proportionate, temporary, and do not contravene peremptory norms of international law or the prohibition on the use of force. Although rarely invoked openly, this framework has been reinforced by the *Tallinn Manual 2.0*, which affirms that proportionate countermeasures are permissible in response to ongoing cyber intrusions.

For the purposes of a data embassy treaty, explicit codification of countermeasures is unnecessary, as these rights exist under general international law. However, cooperative provisions could be included to ensure that sending and host States coordinate their responses to third-party incidents. This may extend to joint diplomatic action, coordinated attribution processes, or, in exceptional circumstances, collective responses short of force.

3. The Budapest Convention on Cybercrime

The Council of Europe's *Convention on Cybercrime* (Budapest Convention, 2001), which has been ratified by some Caribbean States and is under consideration by others, provides the principal global framework for cross-border cooperation in the investigation and prosecution of cybercrime. Its provisions require Parties to extend mutual legal assistance (MLA) to one another, including in accessing stored data, and to adopt harmonized substantive and procedural laws to combat computer-related offences.

The Convention's Second Additional Protocol (2022) further strengthens international cooperation by permitting direct requests to service providers located in other jurisdictions and facilitating expedited disclosure of subscriber information in emergency situations.

A data embassy arrangement intersects directly with this framework. Where law enforcement in the host State (Country B) or in a third State (Country C) seeks access to logs or other digital evidence stored in the data embassy of the sending State (Country A), jurisdiction remains with the sending State. Accordingly, such requests must be transmitted through established MLA channels or cybercrime cooperation mechanisms, rather than being executed unilaterally by the host. The inviolability of archives and premises, derived from diplomatic law and confirmed in the bilateral or regional data embassy treaty, precludes direct seizure or inspection by the host's authorities.

This approach does not obstruct cooperation. On the contrary, it ensures that established frameworks are respected:

- Where all concerned States are Parties to the Budapest Convention, requests can be routed through its MLA provisions, with the sending State providing data in accordance with its domestic legal standards.
- In urgent cases —such as ransomware campaigns or imminent threats— the Second Protocol allows for expedited cooperation. However, because a data embassy is not a private service provider but a sovereign facility, requests must still be channelled to the sending State's competent authority, which may then respond under treaty obligations.

For Caribbean purposes, a regional data embassy treaty should include language making this explicit: host-State law enforcement must not attempt to circumvent protections by unilateral actions. Instead, requests for data must be directed to the sending State via applicable mutual assistance mechanisms. This ensures both the integrity of sovereignty and compliance with existing international obligations, while enabling effective cooperation in cybercrime investigations.

4. United States CLOUD Act

The United States CLOUD Act (2018) authorizes U.S. law enforcement authorities to compel U.S. —based service providers to disclose data, including data stored outside the country. It further provides for the conclusion of executive agreements with foreign governments to facilitate cross-border access to electronic evidence.

For Caribbean States, this raises a critical concern: if government backup data were hosted in the United States under a data embassy arrangement, could such data be subject to disclosure under the CLOUD Act? The answer depends on the design of the arrangement. If the data embassy is established pursuant to a treaty framework, no U.S. company should have access to plaintext data or administrative

control over the infrastructure. Under such a treaty, the host State would be bound not to exercise jurisdiction over data designated as part of the embassy, thereby shielding it from unilateral measures.

Difficulties arise, however, if a commercial provider —such as Amazon Web Services or Microsoft— is used to host the infrastructure. Because these entities fall under U.S. jurisdiction, their obligations under the CLOUD Act could potentially conflict with the sovereign protections envisaged by the data embassy. To avoid such risks, data embassy models should prioritize state-owned infrastructure or partnerships with providers not subject to third-country jurisdiction.

As a general principle, treaties establishing data embassies should override domestic legislation by virtue of international obligations. Where the host State is party to the CLOUD Act, to similar access regimes, or to domestic data localization laws, explicit carve-outs should be provided to exempt data embassy content from their reach. An illustrative precedent can be found in Bahrain's 2018 legislation, which expressly stipulates that data stored in a foreign data embassy is governed by the law of the sending State. A Caribbean framework could mirror this approach, thereby ensuring that host authorities are legally bound to refrain from direct access and must instead rely on formal intergovernmental channels.

5. Data protection and privacy regimes (Convention 108+, GDPR, and related frameworks)

The Council of Europe Convention 108+, adopted in 2018 as an update to the original 1981 Convention, together with the European Union's General Data Protection Regulation (GDPR), represents the most influential global standards for personal data protection and cross-border data transfers. Their principles have inspired a wave of reforms in the Caribbean, with jurisdictions such as Barbados, the Bahamas, and Jamaica adopting or implementing GDPR-aligned legislation.

A central feature of these regimes concerns the transfer of personal data to foreign jurisdictions. Transfers are generally permitted only where the receiving jurisdiction ensures an "adequate" level of protection, or where specific mechanisms such as standard contractual clauses or binding agreements are in place. This raises an important question for data embassies: does the placement of citizen data in a facility abroad constitute a "transfer" to a foreign jurisdiction, or is it more appropriately regarded as a continuation of the sending State's sovereign IT infrastructure?

Under a data embassy treaty, the data remains under the sole legal control of the sending State and is inaccessible to the host. On this basis, one may argue that such arrangements do not amount to a cross-border transfer within the meaning of data protection law. Rather, the data embassy functions as a remote extension of the government's digital environment. In practice, this interpretation is consistent with GDPR, which recognizes that data processed by a government in the exercise of its sovereign functions remains under that government's jurisdiction, irrespective of where it is physically stored, provided there is no disclosure to third parties.

Nevertheless, to ensure legal certainty, States may wish to clarify this position explicitly in their domestic data protection frameworks. Options include:

- Issuing regulations or statutory guidance declaring that data stored in a foreign facility pursuant to a treaty constitutes either (i) no "transfer" at all, or (ii) a permitted transfer on the basis of adequate safeguards;
- Relying on the treaty itself as the safeguard, in line with the flexibility of Convention 108+, which allows international transfers provided that appropriate measures are in place.

Beyond the issue of transfers, general data protection principles also reinforce the technical requirements of a data embassy. GDPR Article 32 obliges controllers to ensure data security, confidentiality, and resilience —standards that are directly aligned with the high-assurance

architecture envisaged for data embassies (Tier IV resilience, immutable backups, sovereign key management, and robust monitoring). Embedding such standards into the treaty framework ensures that personal data entrusted to a data embassy is not only legally protected but also subject to stringent operational safeguards.

From a privacy and human rights perspective, the host State may be concerned if personal data of its citizens (for example, dual nationals or residents) is included in the data embassy. As a matter of principle, the sending State's legal framework governs the processing of such data, since the host lacks any jurisdiction or access. Where both States maintain strong data protection regimes, no conflict arises. In cases of divergence, supplementary arrangements —such as cooperation between national Data Protection Authorities (DPAs)— could be considered, though in practice this is rarely necessary, since data embassies typically store the sending State's records about its own citizens and government operations.

The data embassy framework should clearly affirm that it does not diminish the rights of data subjects, and that the sending State retains full responsibility for compliance with data protection obligations. Oversight should remain with the sending State's DPA, while the host State's DPA may be informed of the arrangement for transparency. Such clarity ensures continuity of rights, reduces uncertainty, and strengthens the legitimacy of the data embassy model within broader privacy and human rights frameworks.

6. Cybersecurity and critical infrastructure protection (NIS2, ENISA Guidance, NIST, and Related Frameworks)

The European Union's NIS2 Directive (2022), together with guidance from the European Union Agency for Cybersecurity (ENISA), classifies government digital infrastructure and cloud services as essential or important entities subject to enhanced obligations. These include comprehensive risk management, incident reporting, and resilience measures. Comparable approaches are increasingly being adopted in the Caribbean, notably through the CARICOM Cybersecurity Framework and several national-level cybersecurity strategies.

Within this context, a data embassy should be regarded as critical infrastructure of the sending State. Such classification entails the imposition of stringent cybersecurity requirements to ensure resilience, continuity, and trust. The primary responsibility for these obligations rests with the sending State, which must ensure that the data embassy complies with rigorous technical and procedural controls (addressed in detail in Section F). Where the host is located in the European Union or another jurisdiction with similarly high regulatory standards, the facility provider will also be subject to local obligations regarding network and physical security. However, the sovereign enclave principle requires that the host operator has no logical access to the sending State's data or systems, even though it remains responsible for the physical and environmental security of the premises.

ENISA guidance on cloud and network security, as well as national frameworks such as the United Kingdom's Cyber Assessment Framework, consistently emphasize separation of functions, least privilege, strong encryption, continuous monitoring, and effective incident reporting. These align closely with international standards (e.g., ISO/IEC 27001 and related controls) and can be integrated into a binding technical annex to a data embassy treaty. Similarly, the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 and the SP 800-53 series offer detailed control sets that can be contractually required and mapped against ISO standards, ensuring interoperability and global recognition of compliance.

Additional regulatory developments within the European Union further support resilience objectives. The forthcoming Cyber Resilience Act (CRA) will impose cybersecurity requirements on manufacturers and vendors of software and hardware products in the EU, indirectly benefiting data

embassies by reducing systemic vulnerabilities in equipment supply chains. Similarly, the eIDAS Regulation provides a framework for the cross-border recognition of digital identities and trust services. While not directly applicable to all data embassy functions, it becomes relevant if the embassy hosts critical services such as national public key infrastructure (PKI) backups. Looking ahead, even the European Union's Artificial Intelligence Act could bear tangential relevance if governments deploy automated monitoring or incident-response systems within a data embassy environment, though such implications remain limited.

Cybersecurity and critical infrastructure frameworks provide a robust foundation for integrating enforceable technical standards into a data embassy treaty. Drawing explicitly on ISO, NIST, ENISA, and related models in the treaty's annex would establish a binding baseline of good practice, reassure development partners and donors of system resilience, and reduce potential conflicts with domestic regulations. Rather than displacing national cyber policies, such a framework would reinforce them —ensuring that the data embassy meets or exceeds the highest standards applied to critical infrastructure both in the Caribbean and internationally.

7. Principles on cross-border data flows: OECD, APEC, WTO, and related regimes

International frameworks on cross-border data flows provide important reference points for the design of a Caribbean data embassy regime. The Organisation for Economic Co-operation and Development (OECD), through its Privacy Guidelines and subsequent instruments —including the 2022 OECD Declaration on Government Access to Personal Data and the ongoing initiative on "data free flow with trust"— emphasizes that cross-border data flows are permissible where adequate safeguards are in place. The concept of a data embassy directly reflects this principle: data may flow across borders, but it remains subject to protections equivalent to those in the sending State.

The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system, while designed primarily for private sector transfers, offers a parallel insight. It demonstrates how mutual recognition frameworks can promote trust and interoperability. In the governmental context, a multilateral data embassy treaty would institutionalize such trust more robustly than voluntary certification systems, ensuring reciprocal guarantees on data security, confidentiality, and sovereign control.

The ongoing discussions at the World Trade Organization (WTO) on e-commerce and digital trade also intersect with the data embassy concept. While debates continue on data localization measures and free flow of information, it is clear that data embassies do not constitute barriers to trade. On the contrary, they represent a sovereign decision by governments to secure their critical data abroad under treaty arrangements. Governments typically reserve flexibility for sovereign functions when adopting localization disciplines, and WTO national security and public service exceptions would comfortably cover such measures. Hosting data abroad through embassies is therefore consistent with commitments to enable, rather than restrict, cross-border data flows.

Finally, the Wassenaar Arrangement on export controls for dual-use goods, including cryptographic hardware and cyber tools, warrants consideration. Establishing a data embassy may require the import or export of advanced encryption devices, such as hardware security modules (HSMs). While these are often subject to licensing requirements, governments generally benefit from expedited processes or exemptions for official use. To preclude legal uncertainty, a Caribbean treaty should explicitly guarantee that the sending State may import, deploy, and operate cryptographic equipment necessary for the secure functioning of its data embassy, without interference or restriction. This assurance mirrors the long-standing diplomatic practice of allowing missions to use strong encryption and aligns with Wassenaar participants' recognition of governments' prerogative to secure their communications.

8. Disaster Risk Reduction and Emergency Telecommunications Frameworks

The protection of data embassies is closely aligned with international regimes on disaster risk reduction and emergency telecommunications. The **Sendai Framework for Disaster Risk Reduction 2015–2030** underscores the importance of safeguarding critical infrastructure and ensuring continuity of operations in the face of natural and man-made hazards. In particular, Priority 3 ("Investing in disaster risk reduction for resilience") explicitly calls for measures to strengthen the resilience of data and information systems, while Priority 4 ("Build Back Better") highlights the value of pre-disaster arrangements, such as offsite backups, to enable rapid recovery. Data embassies represent an innovative operationalization of these principles, providing states with a resilient mechanism to secure government continuity and accelerate post-disaster restoration of services.

The **International Telecommunication Union (ITU),** particularly through ITU-D, has developed a series of recommendations on emergency telecommunications. These include guidance on ensuring redundant connectivity, such as satellite systems, to maintain communications when terrestrial networks fail. A Caribbean data embassy treaty could explicitly draw from these standards, by obligating host states to facilitate connectivity to the embassy even during disaster scenarios —for instance, by guaranteeing emergency satellite capacity or priority use of alternative channels. This approach would reinforce the commitments already reflected in Article 27(3) of the Vienna Convention on Diplomatic Relations concerning emergency communications.

The **Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations (1998)** also provides a relevant framework. It requires parties to remove regulatory barriers for the rapid deployment of emergency telecommunication equipment in disaster response. While its primary focus is humanitarian operations, the underlying principle —ensuring that communications are not obstructed at critical times— applies equally to governments seeking to maintain access to their data embassies. A regional treaty could therefore commit host states to facilitate the deployment of emergency telecommunications for the purpose of ensuring data embassy access after catastrophic events.

Beyond disaster resilience, **international humanitarian law (IHL)** provides additional safeguards. Diplomatic premises are protected civilian objects during armed conflict, and by analogy, data embassies —if used solely for the storage and continuity of government archives— should not be considered lawful targets. Any attack on a data embassy not serving a military purpose would likely constitute a violation of IHL principles of distinction and proportionality. Similarly, **international human rights law (IHRL)** reinforces the rationale for data embassies by ensuring that continuity of government functions directly supports the protection of fundamental rights, including access to identity, social services, and justice. Moreover, host states must respect due process in handling any disputes over data embassy content: arbitrary seizure or interference would contravene both human rights standards and treaty-based obligations.

9. Regional instruments: CARICOM and OECS frameworks

The **CARICOM Single ICT Space**, endorsed by Heads of Government in 2017, provides a regional vision of an integrated digital environment. It calls for harmonized policies on cybersecurity, data protection, broadband development, and public-sector modernization, with the objective of enabling digital transformation across Member States. Although not a binding treaty, it represents a strong political commitment to collective action. More recently, in 2025, CARICOM leaders endorsed a regional digital resilience strategy, which is expected to encompass measures for secure backup systems and critical data continuity. A regional data embassy treaty would constitute a practical legal instrument to operationalize elements of this vision by providing the infrastructure for shared and trusted sovereign data services.

The **OECS** presents another avenue for advancing such initiatives. Given its high degree of regional integration —including a common central bank for the Eastern Caribbean Currency Union (ECCU) and shared judicial institutions— the OECS could serve as a natural pilot region. The OECS Commission has experience managing pooled procurement and shared services, and could, in principle, administer a collective data center arrangement on behalf of its members.

At the national level, **data protection legislation** is becoming increasingly prominent. Laws such as Barbados' *Data Protection Act (2019)* and Jamaica's *Data Protection Act (2020)* require that transfers of personal data abroad ensure an equivalent level of protection. A treaty establishing a data embassy could be recognized by national data protection authorities as providing sufficient safeguards, particularly if it includes clauses affirming that data will be managed in accordance with internationally recognized privacy principles. This approach would address regulatory concerns while maintaining public confidence. While many Caribbean data protection laws provide exemptions for government functions, including national security or disaster preparedness, affirming adherence to confidentiality and security principles would enhance legitimacy.

Sector-specific regulators, particularly central banks, are also relevant stakeholders. For example, the Eastern Caribbean Central Bank (ECCB) maintains supervisory responsibilities for the financial sector. In many jurisdictions, banking regulators mandate secure off-site backups, sometimes including cross-border storage, as part of business continuity and disaster recovery obligations. A data embassy treaty could complement such requirements by providing a secure framework for government-level backups, while also creating the option for critical financial sector supervisory data to be hosted in such facilities. Alignment with central bank regulations will be essential to avoid potential conflicts —for instance, where laws restrict private financial institutions from transferring customer data abroad.

Other regional entities can also play constructive roles. The **Caribbean Disaster Emergency Management Agency (CDEMA)** coordinates regional disaster preparedness and response, and could integrate data embassy scenarios into contingency planning—ensuring that government services and records remain operational in the aftermath of regional catastrophes. Similarly, the **Caribbean Regional Organisation for Standards and Quality (CROSQ)** could adapt and adopt relevant international standards, such as ISO or ITU benchmarks for data center resilience, to Caribbean conditions (e.g., hurricane-resistant construction, power redundancy). A technical annex to the treaty referencing CROSQ-validated standards would help ensure coherence and regional acceptance.

Table 16
International and regional legal/policy Instruments for Data embassies: relevance, risks, and implementation pathways

Instrument / regime	Scope & key provisions	Relevance to Data Embassies	Binding force / Status	Advantages	Risks / gaps	Integration path for a Caribbean treaty	Practical implementation hooks
UN Charter (Arts. 2(1), 2(7), 2(4))	Sovereign equality; non-interference; prohibition on use of force.	Hosting by consent affirms sovereignty; unauthorized interference with a data embassy may breach sovereignty and, in extreme cases, implicate Art. 2(4).	Hard law (treaty).	Strong normative shield for inviolability and non-interference.	Cyber "use of force" threshold unsettled.	Preambular reaffirmation; clause recognizing sovereign control and non-interference.	Define data embassy as sovereign function; notification/ consultation mechanism for incidents.
ARSIWA (State Responsibility)	Attribution, breach, cessation, reparation; counter measures.	Host breach (e.g., unlawful entry) → wrongful act; third-State cyberattack → responsibility; coordinated responses.	Customary / widely accepted codification.	Clear accountability and remedy framework.	Attribution in cyberspace can be complex.	Cooperation clause for joint attribution, notification, and coordinated response short of force.	Joint incident-response SOP; evidence preservation; escalation ladder.

Instrument / regime	Scope & key provisions	Relevance to Data embassies	Binding force / Status	Advantages	Risks / gaps	Integration path for a Caribbean treaty	Practical implementation hooks
Budapest Convention (2001) + Second Protocol (2022)	Harmonized cybercrime offences; MLA; expedited cooperation (Second Protocol).	Data embassy logs/evidence requested via MLA; no unilateral host access; sovereign facility ≠ private provider.	Hard law for Parties only.	Established channels; legal certainty for cooperation.	Uneven Caribbean participation; risk of misusing "direct to provider" route.	Treaty clause routing all requests to the sending State's competent authority; designate central authorities.	MLA reference; 24/7 point-of-contact; response SLAs for emergencies.
U.S. CLOUD Act & similar extraterritorial access regimes	Compels U.S. providers to produce data held abroad; executive agreements.	Risk if commercial U.S. providers host or control embassy systems.	Domestic laws (extraterritorial reach).	—	Conflict of laws; provider compulsion.	Carve-out: embassy data immune from host/extraterritorial compulsion; require sovereign-owned/controlled hardware, no provider plaintext access.	Contractual "no-access" architecture; HSM/KMS under sending-State control; diplomatic-bag status for media; choice of non-subject providers.
Convention 108+	International DP standard incl. transfers with safeguards.	Treat treaty as an "appropriate measure" enabling cross-border storage under sending-State control.	Hard law for Parties.	Flexible basis for lawful transfers.	Participation varies.	Clause deeming embassy storage either not a "transfer" or a safeguarded transfer.	DPA MoU template; embed breach notification and DPIA triggers.
GDPR	Lawful processing, security (Art. 32), transfers, data subject rights.	Government sovereign processing abroad without disclosure can be treated as under sending-State control; technical standards align.	Hard law in EU/EEA.	High assurance/security baseline; global benchmark.	Interpretive uncertainty if not codified domestically.	Cross-reference GDPR-equivalent safeguards in Technical Annex; clarify rights unaffected.	Security controls crosswalk (ISO/NIST↔GDPR Art.32); designate sending-State DPA oversight.
National Caribbean DP laws	Transfer restrictions; DP principles; regulator powers.	Treaty can be recognized as adequate safeguard; transparency to build trust.	Domestic statutes (vary by State).	Legitimacy; local compliance clarity.	Fragmentation; uneven enforcement.	Clause for DPA recognition; model regulation deeming treaty storage compliant.	Guidance note for DPAs; joint awareness & training; records of processing for embassy systems.
NIS2 / ENISA guidance	Risk mgmt, incident reporting for essential/important entities.	Classify data embassy as critical infrastructure; align controls and reporting.	Hard law (EU) + soft guidance.	Mature operational model for resilience.	Capacity gaps; non-EU States not bound.	Adopt NIS2-aligned control set in Annex; shared SOC and reporting playbooks.	Incident reporting timelines; tabletop exercises; metrics/KPIs.
NIST CSF 2.0, SP 800-53	Cybersecurity framework and control catalog.	Provides auditable controls for embassy environment.	Soft law/ standards.	Detailed, widely used; maps to ISO.	Resource intensity for full adoption.	Annex: minimum control baseline; allow risk-based tailoring.	Independent audits; certification cadence; SBOM & supply-chain checks.
ISO/IEC 27001/27002/ 27017/27018/ 27701	ISMS, cloud security, privacy.	Treaty-ready, certifiable standards for security & privacy.	International standards.	Interoperable, certifiable.	Certification costs; scope tailoring needed.	Annex: certification requirements and renewal cycle.	Third-party audits; crosswalk matrices (ISO↔NIST ↔ENISA).
eIDAS (trust services, e-ID)	Cross-border recognition of trust services.	Relevant if embassy hosts PKI/TS backups.	Hard law (EU).	Interoperability for signatures/PKI.	EU-centric.	Optional alignment clause for trust services; mutual recognition where applicable.	Key ceremony SOPs; HSM requirements; time-stamping policies.
EU Cyber Resilience Act (CRA)	Security obligations for digital products.	Improves supply-chain security for equipment/software.	Hard law (EU, phased).	Fewer product vulnerabilities over time.	Market transition period.	Procurement clause preferring CRA-conformant products.	Vendor attestations; vulnerability disclosure requirements.

Instrument / regime	Scope & key provisions	Relevance to Data embassies	Binding force / Status	Advantages	Risks / gaps	Integration path for a Caribbean treaty	Practical implementation hooks
EU AI Act (contextual)	Governance for high-risk AI systems.	If automated monitoring/IR runs in embassy, ensure compliance.	Hard law (EU, phased).	Risk management discipline.	Likely tangential; compliance overhead.	Transparency and human-oversight clause for any automated controls.	Register high-risk uses; logs/traceability.
OECD (Privacy Guidelines; 2022 Declaration on Gov't Access; DFFT)	Principles for trusted cross-border data flows.	Normative support: "data free flow with trust" embodied by embassy model.	Soft law.	Legitimacy; policy alignment.	Non-binding.	Preambular reference; transparency & safeguards clause.	Publish governance/audit summaries; oversight reporting.
APEC CBPR	Voluntary private-sector cross-border privacy certification.	Analogy for mutual recognition; less relevant G2G.	Soft / voluntary.	Interoperability concept.	Not G2G; limited uptake regionally.	Optional reference to principles; no legal reliance.	—
WTO e-commerce discussions	Data flows, localization disciplines (negotiations ongoing).	Data embassies are consistent with liberal flow commitments and sovereignty exceptions.	Soft/ongoing talks.	No trade barrier created.	Unsettled outcomes.	Note consistency with public service/national security exceptions.	—
Wassenaar Arrangement	Export controls incl. crypto/cyber tools.	HSMs/crypto gear import/export may need licenses.	Implemented via domestic law.	Government-use facilitation common.	Licensing delays possible.	Clause guaranteeing import/use of crypto equipment; customs facilitation.	Diplomatic-bag status; expedited licensing liaison.
Sendai Framework (2015–2030)	DRR priorities incl. resilient infrastructure, "Build Back Better".	Embassy = pre-disaster arrangement enabling rapid recovery.	Soft law.	Policy legitimacy; disaster-finance alignment.	Non-binding.	Reference in objectives; require periodic DR drills and investment planning.	Annual exercises; recovery RTO/RPO targets.
ITU-D Emergency Telecoms & Tampere Convention (1998)	Redundant comms; barrier removal for emergency telecoms.	Ensure embassy connectivity during/after disasters (satellite, priority routes).	Tampere hard law for Parties; ITU guidance.	Keeps comms open when terrestrial fails.	Participation varies.	Priority-communications clause; commit to facilitate emergency links.	Satellite fallback; radio licenses; emergency spectrum access.
IHL / IHRL	Protection of civilian objects; due process, privacy.	Embassy (non-military use) not a lawful target; due process for any disputes.	Hard law/customary.	Additional protective norms.	Misuse could forfeit protection.	Purpose-limitation clause; IHRL-compliant cooperation for requests.	Prohibit offensive use; independent redress channel.
CARICOM Single ICT Space (2017) & 2025 digital resilience strategy	Regional policy for harmonized ICT, cybersecurity, DP, broadband.	Political mandate for shared sovereign data services.	Political commitment (non-binding).	Regional legitimacy; alignment.	Lacks legal teeth.	Treaty positioned as implementation instrument of Single ICT Space.	Link to CARICOM bodies for oversight; reporting to Heads.
OECS frameworks	Deep integration; pooled services; ECCU, shared courts.	Natural pilot for regional data embassy.	Binding OECS treaty + policies.	Existing administrative machinery.	Capacity constraints.	Option for OECS-managed hub under regional mandate.	Pooled procurement; shared SOC; joint certification body.
National DP laws (e.g., BB 2019; JM 2020)	Transfer rules; DP principles; regulators.	Embassy recognized as adequate or non-transfer; transparency to public.	Domestic binding law.	Public trust; compliance clarity.	Variations across States.	Model clause for recognition; DPA notifications.	Template decisions/guidance; training for controllers.
Sectoral central bank/supervisory rules (e.g., ECCB)	Business continuity; off-site backups; data residency constraints.	Enable supervisory datasets in embassy; avoid conflict with bank secrecy.	Domestic regulatory.	Aligns financial stability with resilience.	Possible residency conflicts for private banks.	Carve-outs for supervisory/government data; consult regulators early.	Regulator MoUs; secure regulator enclave in embassy.

Instrument / regime	Scope & key provisions	Relevance to Data embassies	Binding force / Status	Advantages	Risks / gaps	Integration path for a Caribbean treaty	Practical implementation hooks
CDEMA	Regional disaster coordination.	Integrate embassy scenarios in regional contingencies.	Intergovern mental mechanism.	Operational readiness.	Requires planning cycles.	Joint exercises; data recovery playbooks with CDEMA.	Annual regional drills; shared incident channels.
CROSQ	Regional standards & quality organization.	Localizes ISO/ITU standards to Caribbean conditions.	Regional standardizat ion.	Context-appropriate requirements (e.g., hurricane resilience).	Adoption timelines.	Technical Annex validated by CROSQ; certification scheme.	Tier/TIA-942 adaptations; audit program across members.

Source: ECLAC with data from UN Charter (1945); ARSIWA (2001); Budapest Convention (2001) & Second Protocol (2022); U.S. CLOUD Act (2018); Convention 108+ (1981, amended 2018); GDPR (2016); NIS2 Directive (2022); ENISA Guidance (2019); NIST CSF (2023); ISO/IEC 27001/27017/27018/27701 (2013–2021); eIDAS Regulation (2014); EU Cyber Resilience Act (2023); EU AI Act (2023); OECD Privacy Guidelines (2013, 2022 Declaration); APEC CBPR (2011); WTO e-commerce discussions (ongoing); Wassenaar Arrangement (1996, amended); Sendai Framework (2015); Tampere Convention (1998); IHL/IHRL; CARICOM Single ICT Space (2017); OECS frameworks; national Caribbean DP laws; ECCB supervisory rules; CDEMA; CROSQ.

C. Pioneering a treaty regime for state data resilience

The examination of international legal and policy instruments demonstrates that the data embassy concept is not only consistent with existing frameworks, but also strengthens them by addressing an urgent contemporary gap. Diplomatic law, as codified in the Vienna Conventions, provides a robust foundation for the protection of sovereign archives, premises, and communications. Cybercrime treaties, data protection regimes, and cybersecurity standards offer complementary safeguards, ensuring that the data embassy model does not become a loophole or a safe haven for abuse but remains firmly embedded in lawful cooperation and high-assurance technical practices. Disaster risk reduction frameworks and human rights standards further underscore the role of data embassies in protecting continuity of governance and safeguarding citizens' rights during crises.

Yet, the analysis also highlights a normative lacuna: no existing multilateral instrument explicitly regulates the continuity of state data or the extraterritorial protection of sovereign digital assets. Estonia's pioneering bilateral arrangement with Luxembourg remains the only practical precedent, and Bahrain's domestic legislation illustrates unilateral recognition of the principle. Beyond these isolated cases, however, the field remains legally uncharted.

This gap presents a strategic opportunity for the Caribbean. By advancing a regional or multilateral treaty on data embassies, Caribbean States could establish themselves as global innovators in digital statecraft, much as they have historically done in other areas of international law and diplomacy.

In shaping such a treaty, the Caribbean must ensure coherence with existing obligations —embedding safeguards against misuse, aligning with cybercrime cooperation mechanisms, and affirming data protection and privacy principles. Equally, it must operationalize resilience by mandating high technical standards, secure communications, and contingency procedures for disaster recovery. In doing so, the treaty would not displace existing regimes but rather consolidate them into a comprehensive architecture tailored to the realities of the digital era.

Ultimately, the proposed Caribbean data embassy framework would reaffirm a simple but profound principle: sovereignty today is inseparable from the resilience of digital infrastructure. By pioneering a treaty regime that secures this dimension, Caribbean States can transform their structural vulnerabilities into a global example of innovation, cooperation, and resilience.

D. Legal instruments for the Caribbean: options and pathways

The establishment of **data embassies** as instruments of resilience requires an enabling legal framework. Caribbean States can consider different pathways, ranging from binding treaties to more flexible arrangements. These options must reflect the **region's diversity**, accommodate different levels of institutional capacity, and remain open to the participation of **all Caribbean States and territories**, regardless of membership in subregional organizations. The goal is not simply to advance integration within a single bloc, but to foster a **shared Caribbean consensus** on safeguarding digital sovereignty and ensuring government continuity.

Three principal options can be identified:

- A **Regional Framework Treaty** open to all Caribbean States.
- A **Hub-and-Spoke Network of Bilateral Agreements** between sending and host countries.
- A **Soft-law Memorandum of Understanding (MoU) approach** complemented by technical annexes.

1. Option 1: regional framework treaty

A regional treaty would provide the most comprehensive and cohesive basis for cooperation. It could establish **shared principles, definitions, immunities, and technical obligations** applicable across the Caribbean, while leaving flexibility for countries to determine whether to act as sending States, host States, or both. A treaty of this kind could incorporate technical standards through annexes, establish a **joint oversight mechanism**, and define procedures for dispute settlement.

The main advantage of this approach is **uniformity**: a single set of rules would apply to all signatories, simplifying trust, interoperability, and compliance. It would also signal **collective political commitment**, enhancing the Caribbean's ability to attract financial and technical support from development partners. The treaty could be designed to remain **open for accession** by any Caribbean State or territory with the necessary institutional arrangements, ensuring inclusivity beyond existing integration groups.

At the same time, this option presents challenges. Achieving consensus across the full Caribbean will require significant negotiation, given the diversity of legal systems, technical capacity, and national security perspectives. Some States may be cautious about sovereignty implications. These concerns can be addressed by making **hosting voluntary**, while still providing a strong legal basis for those that choose to do so.

2. Option 2: hub-and-spoke bilateral agreements

An alternative approach is for individual countries to enter into **bilateral agreements** with hosting partners, creating a network of "hub-and-spoke" arrangements. In this model, a limited number of countries with advanced infrastructure —whether inside or outside the region— act as **hosts** for multiple Caribbean States. Bilateral agreements can tailor obligations and technical details to the needs of each pair, and they may be the only realistic option for engaging with **extra-regional hosts** such as Luxembourg or Estonia.

This model offers **flexibility and speed**, as agreements can be concluded more quickly than a multilateral treaty. It also allows pioneers to move ahead without waiting for regional consensus. However, reliance on bilaterals can produce **fragmentation**, with uneven protections and overlapping obligations. Managing multiple agreements may strain administrative capacity, particularly for small States. Furthermore, without a regional governance framework, updating standards and coordinating practices may prove difficult.

3. Option 3: soft-law MoU with technical annex

A third pathway is to begin with **non-binding MoUs or political declarations**, supported by technical annexes that establish operational standards. This approach avoids the delays associated with treaty ratification, enabling countries to **launch pilot projects quickly** while building trust and technical experience.

MoUs can be particularly useful as **transitional instruments**, allowing States to align on principles such as inviolability of archives and continuity of services, while retaining flexibility to adapt as experience grows. Annexes can specify shared technical standards, ensuring operational coherence even if the commitments are not legally binding.

The main limitations of this approach are its **lack of legal enforceability** and weaker assurances for immunities under host law. Donors, partners, and private operators may perceive MoUs as less stable. However, as an **interim step**, they can facilitate early implementation and demonstrate feasibility, especially for countries that are not yet ready to join a treaty.

E. Toward a regional consensus

The analysis suggests that a **regional framework treaty** offers the most strategic benefits in the long term, providing consistency, collective visibility, and a foundation for sustainable resilience. At the same time, bilateral agreements and MoUs will remain important **complementary instruments**, especially in the early stages and for partnerships with external hosts.

A **sequenced approach** is therefore recommended:

- **Draft and circulate a model treaty** that is open to all Caribbean States and territories, accompanied by technical annexes.
- Allow early adopters to move forward with **bilateral MoUs or agreements**, both within the region and with external partners, to generate pilot experiences.
- Use the **lessons from these pilots** to refine the treaty and expand participation.
- Gradually incorporate bilateral and MoU arrangements into a **broader regional framework**, ensuring that all States —including microstates and territories— have a pathway to participate.

This inclusive approach would ensure that the benefits of digital resilience are shared across the Caribbean, not limited to a single subregional bloc. It would also position the Caribbean as a global leader in **innovative applications of international law and diplomacy to digital resilience**.

VI. Technical provisions of a Data Embassy treaty

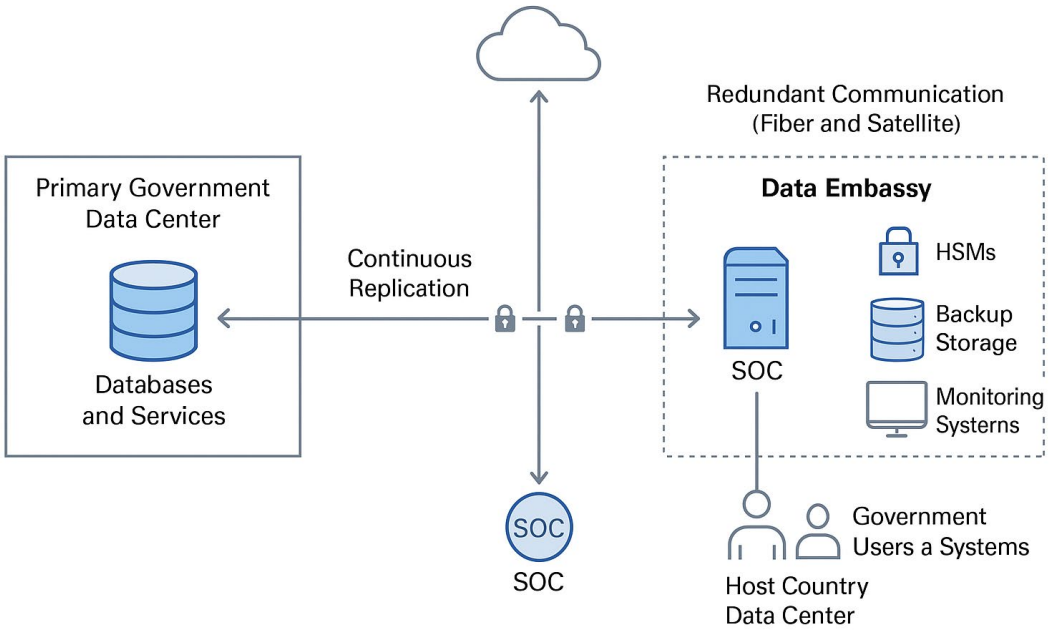
The effectiveness of any data embassy arrangement depends not only on the legal immunities and protections codified in international agreements, but equally on the technical resilience of the system itself. Legal inviolability, while essential, cannot substitute for operational robustness. For both the sending and the host State, confidence in the data embassy's ability to resist intrusion, maintain continuity during crises, and operate under stringent safeguards is critical. Without such assurance, the treaty risks becoming a symbolic commitment rather than a credible resilience mechanism.

This chapter sets out the technical provisions that should accompany a data embassy treaty. It introduces a reference architecture and identifies the minimum baseline of security, reliability, and governance controls required for such a facility. These provisions are not ancillary; they form part of the treaty's binding framework —whether codified directly in its text, annexed as technical schedules, or incorporated through enforceable service-level agreements with operators.

The approach builds on globally recognized standards and best practices, including the ISO/IEC 27000 series for information security management, the NIST SP 800-53 control catalog for federal information systems, and the Uptime Institute's Tier certification framework for data centers. Drawing from these benchmarks, the chapter defines the operational requirements necessary to ensure sovereign control, resilience against both natural and man-made disruptions, and verifiable compliance.

By embedding technical guarantees into the treaty framework, Caribbean States can demonstrate to their citizens, regional partners, and the international community that data embassies are not merely symbolic extensions of sovereignty but practical instruments of resilience. This dual emphasis —legal inviolability and technical assurance— constitutes the foundation of a credible and pioneering regional regime for digital continuity.

Diagram 1
Data Embassy Reference Architecture



Source: ECLAC.
Note: A primary government data center (left) continuously replicates critical databases and services over encrypted links to the Data Embassy (right) hosted abroad in a secure Tier-IV facility. The Data Embassy environment is isolated and controlled by the sending state, with sovereign encryption keys stored in Hardware Security Modules (HSMs) under sending state control. A Security Operations Center (SOC) monitors both sites. Redundant communication (fiber and satellite) ensures connectivity. In a disaster, government users and systems can switch to the Data Embassy's backup services, maintaining continuity.

A. Core architecture components

A data embassy cannot be improvised; its architecture must be carefully defined in treaty language to ensure clarity of scope and enforceability.

Primary Site(s): these remain the authoritative systems located in the sending State—national data centers, ministry servers, or cloud infrastructure. Their role is to provide real-time services to citizens and institutions. Under normal conditions, the data embassy acts only as a backup or standby. The treaty should clarify that sovereignty over data remains with the sending State at all times, and that the embassy is a continuity mechanism rather than a new primary authority.

Data Embassy Site: the treaty should mandate that the embassy is hosted in a **dedicated, segregated physical environment**, typically a locked cage or secured room preferably in a Tier III or Tier IV facility. Tier IV, with its fault-tolerant architecture and 99.995% uptime standard, offers near-continuous availability, but Tier III may be a more feasible baseline in the Caribbean context, provided compensating redundancies exist. Importantly, the treaty must define the enclave as sovereign and inviolable space, ensuring that no other tenants of the facility or the operator itself can interfere.

Within this enclave, several design principles must be codified:

- **Isolated infrastructure:** all servers, storage, and networking equipment must be wholly owned and managed by the sending State. The operator provides only power, cooling, and physical security, not logical access.

- **Supply-chain assurance:** hardware and software must be verified against tampering and sourced from trusted supply chains, aligning with standards like ISO 20243.
- **Sovereign key management:** cryptographic keys must remain under exclusive control of the sending State, either stored on-site in Hardware Security Modules (HSMs) or maintained remotely but inaccessible to host authorities.

Optional Tertiary Site: the Caribbean is uniquely vulnerable to systemic shocks, such as hurricanes that can impact multiple countries simultaneously. A treaty could authorize or encourage additional tertiary sites, possibly in a second host country or a geographically distant partner. Multi-site replication allows tiered resilience: essential records may be mirrored to three locations, while less critical archives are backed up only once.

Codifying these architectural components is not a matter of technical preference but of **legal necessity**. Without explicit treaty definitions of what constitutes the "premises" of the data embassy and what level of segregation is required, ambiguities could allow disputes, particularly if host authorities or private operators retain incidental control.

B. Data replication and synchronization

Continuity depends on both **data freshness** and **service restoration speed**, captured by two metrics: Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

- **RPO (freshness):** the treaty should mandate a tiered approach. For high-value services (civil registries, payment systems), near-real-time replication (RPO of 15 minutes or less) is desirable. For less critical systems (archives, statistical data), daily replication suffices. Codifying tiered RPOs in treaty annexes prevents under-investment and ensures prioritization of what truly matters in a crisis.
- **RTO (restoration):** similarly, the treaty should commit the sending State to define restoration goals: a few hours for mission-critical services, a day or two for secondary ones, and looser targets for archives. Importantly, these must be realistic given bandwidth and human resource constraints.

Connectivity: Caribbean vulnerability to submarine cable disruptions makes multi-path connectivity essential. The treaty could stipulate at least two independent international routes, plus satellite backup rights. This transforms what is usually an operational best practice into a legal commitment, ensuring that the host must facilitate rights-of-way, landing permits, or licensing for alternate paths.

Replication is the "heartbeat" of a data embassy. If it lags, the legal protections become irrelevant because restored data will be outdated or incomplete. Embedding quantitative RPO/RTO targets in a treaty elevates continuity from aspiration to obligation.

C. Security and integrity controls

Encryption: data must be encrypted both at rest and in transit, with sovereign control of keys. This prevents host or third-party access and makes legal immunities meaningful —an encrypted archive is inviolable in practice as well as in law.

Access Control: only sending State personnel may administer systems. Multi-factor authentication and zero-trust principles reduce insider and outsider risks alike. Host personnel may access physical infrastructure for maintenance but never the logical layer.

Network Security and Integrity: firewalls, IDS/IPS, and immutable backups ensure that attacks cannot spread unchecked. Tamper-evident logs —possibly blockchain-anchored— guarantee accountability, enabling attribution of malicious actions.

Immunity without integrity is dangerous. If a treaty secures the data legally but the infrastructure is penetrable, then sovereignty is undermined in practice. Therefore, technical provisions are not ancillary —they are the **operational expression** of inviolability.

Physical and environmental resilience

Data embassies must not only withstand cyberattack but also natural and technical hazards. Treaty annexes should require:

- **Tier certification:** Tier IV is ideal but may be unattainable in some Caribbean locations; at minimum, Tier III with documented compensating redundancies should be required.
- **Power resilience:** dual feeds, UPS, and generator autonomy of at least 96 hours.
- **Cooling and fire suppression:** non-destructive suppression (gas systems) and redundant HVAC.
- **Seismic and climate safeguards:** facilities must meet seismic codes and hurricane-resilient designs appropriate to regional risks.

These are not merely technical specifications but **political safeguards**. A data embassy that fails during a hurricane would not only negate its purpose but also erode public trust and regional credibility. Codifying standards transforms resilience into an enforceable obligation, not a best-effort.

Monitoring, Auditing, and Incident Response

Continuous monitoring: SIEM systems must be in place, forwarding alerts to the sending State's SOC. The treaty should also encourage regional SOC integration, enabling regional actors to pool resources for monitoring.

Auditing and testing: annual penetration tests and failover exercises should be mandatory. Independent audits against ISO/IEC 27001 every two years must be reported to a Joint Commission, ensuring accountability to both States.

Incident response protocols: the treaty should require joint notification of serious incidents and cooperation in tracing attacks. Voluntary forensic sharing may be allowed, but inviolability is preserved.

Oversight is where law and technology converge. Immunity cannot mean opacity; transparent auditing and shared monitoring build trust with host States and the public, preventing suspicion that the data embassy is a "black box."

D. Standards and compliance mechanisms

The treaty must not reinvent technical standards but embed internationally recognized frameworks. By referencing ISO/IEC 27000 series, NIST SP 800-53, ENISA guidelines, and Uptime Institute Tier standards, the treaty creates interoperability with global practices. Crucially, it should empower a Joint Commission to update standards references without renegotiating the treaty text —ensuring flexibility in the face of evolving threats.

Analytical point: Static obligations risk obsolescence; dynamic references ensure that the treaty remains **living law**, aligned with technical progress.

E. Telecommunications and power resilience

The Caribbean's dependence on submarine cables introduces systemic risks. A treaty must:

- Guarantee multiple independent cable routes for replication traffic.
- Authorize emergency satellite links, exempt from licensing delays.
- Ensure local loop diversity in the host State.

Power resilience provisions —generators, renewable backups, and redundant feeds —should be legally mandated.

By making telecom and power redundancy treaty obligations, the States elevate them from procurement options to **matters of sovereignty**, ensuring continuity even when commercial or regulatory environments shift.

F. Maintenance and lifecycle management

The treaty must anticipate technology refresh cycles and ensure customs-free import/export of replacement equipment. Patch management obligations (e.g., critical vulnerabilities patched within 48 hours) should be codified. Regular disaster recovery drills must be required, transforming exercises into enforceable treaty duties.

Maintenance is often neglected until crisis reveals weaknesses. By embedding lifecycle management into the treaty, the Caribbean ensures resilience is sustained over decades, not just at inauguration.

The technical provisions of a data embassy treaty are **not auxiliary —they are the very conditions that make diplomatic law functional in the digital age**. By codifying architecture, replication metrics, encryption, resilience standards, monitoring, and lifecycle management, the treaty creates a defensible "defense in depth" framework.

This is more than engineering detail: it is the material expression of sovereignty and resilience. Without such provisions, legal immunity risks being symbolic; with them, the Caribbean can pioneer a model that combines the Vienna Convention's spirit with 21st-century infrastructure standards. In doing so, Caribbean States would not only protect their own digital continuity but also set a precedent for global practice, demonstrating that **law and technology must converge to secure sovereignty in the digital age**.

Table 17
Technical provisions matrix for Data Embassy treaties

Provision area	Treaty obligation / clause	Relevant standards and references	Rationale / analytical notes
Core Architecture (Premises and Segregation)	Define "premises" as a dedicated, physically segregated enclave (server cage/room) with sole control by the sending State; host guarantees inviolability.	ISO 20243 (supply-chain security); Uptime Institute Tier III/IV; TIA-942 data center standards.	Prevents ambiguity in legal scope; ensures sovereignty is not diluted by shared tenancy or operator access.
Data Replication and Synchronization	Annex must define RPO/RTO tiers: e.g., Tier 1 services ≤15 min RPO, 4–8h RTO; Tier 2 daily backups; Tier 3 archival.	ITIL service continuity guidelines; NIST SP 800-34 (Contingency Planning); ISO 22301 (Business Continuity).	Guarantees operational continuity, avoids data staleness; elevates continuity metrics into enforceable treaty commitments.
Connectivity and Telecom Resilience	At least two independent submarine cable paths; host guarantees rights for backup satellite or terrestrial link; commitment to priority restoration in disaster.	ITU-D emergency telecoms guidance; Tampere Convention; NIST CSF (Communications resilience).	Mitigates systemic risks from single-point cable failure; codifies backup channels as sovereign necessity, not optional procurement.

Provision area	Treaty obligation / clause	Relevant standards and references	Rationale / analytical notes
Cryptographic Key Management	All data at rest and in transit encrypted; encryption keys under exclusive control of sending State; host waives any key escrow/local decryption law.	ISO/IEC 27040 (storage security); NIST SP 800-57 (key management); Post-Quantum NIST standards.	Converts inviolability into practice: without sovereign key control, treaty protections can be bypassed.
Access Control and Authentication	Only authorized sending State personnel may administer systems; MFA and zero-trust enforced; host staff restricted to physical maintenance only.	ISO/IEC 27001 & 27002 (access controls); CIS Benchmarks; Zero Trust NIST SP 800-207.	Prevents host or third parties from exploiting local access; maintains integrity of sovereign enclave.
Network and Data Integrity	Firewalls, IDS/IPS, and immutable backups mandated; periodic integrity checks (hashing, blockchain anchoring).	ISO/IEC 27036; ENISA guidance; Estonia's KSI blockchain model.	Ensures data cannot be tampered with undetected; reinforces evidentiary value and trust.
Physical and Environmental Resilience	Facility recommended to meet Tier III (preferably Tier IV) with redundancy in power, cooling, fire suppression, seismic and hurricane protection.	Uptime Institute Tiers; ISO 22301; local building codes adapted to climate risks.	Ensures resilience against Caribbean hazards; translates physical continuity into treaty obligation.
Monitoring, Logging and Auditing	Continuous monitoring; logs forwarded to sending State SOC; independent audits (ISO 27001) every 2 years; mandatory annual failover & penetration tests.	ISO/IEC 27001; NIST SP 800-53; SOC 2 Type II auditing.	Introduces enforceable oversight, balancing inviolability with accountability; builds trust with host and citizens.
Incident Response and Cooperation	Treaty obliges notification of serious incidents; establishes joint protocols between CERTs of host and sending State.	NIST SP 800-61 (Incident Handling); FIRST/CERT coordination norms.	Ensures cyber incidents are not handled in isolation; builds cooperative resilience and attribution credibility.
Maintenance and Lifecycle Management	Treaty guarantees customs-free import/export of spare parts; patching of critical vulnerabilities within 48h; servers refreshed every 3–5 years.	ISO/IEC 27035 (incident & maintenance); ITIL; vendor lifecycle policies.	Avoids obsolescence and bureaucratic delays; sustains resilience over decades.
Compliance with International Standards	Treaty annex lists applicable standards (ISO/IEC, NIST, ENISA, etc.); Joint Commission may update references without amending treaty.	ISO/IEC 27000 family; NIST CSF; ENISA guidelines.	Creates a "living" technical annex, avoiding obsolescence; enables adaptability while maintaining legal force.
Power Resilience	Dual independent feeds; UPS; diesel generators with 96h autonomy; renewable backup encouraged.	Uptime Institute; ISO 50001 (energy management).	Power continuity is a prerequisite for resilience; makes uptime a treaty-enforceable metric.
Disaster Recovery and Testing	Mandatory annual disaster recovery drill where services run from data embassy; results reported to Joint Commission.	ISO 22301; NIST SP 800-84 (DR/BC exercises).	Moves resilience from theory to practice; builds political credibility in citizens' eyes.
Forensics and Evidence Handling	Logs remain property of sending State; voluntary sharing permitted; inviolability preserved.	Chain-of-custody standards; ISO 27037.	Balances inviolability with cooperation; ensures evidence integrity in cyber attribution.

Source: ECLAC with data from Blue Europe. (2017, June 20). A world first: Estonia opens a "data embassy" in Luxembourg. Blue Europe. https://www.blue-europe.eu/analysis-en/short-analysis/a-world-first-estonia-opens-a-data-embassy-in-luxembourg/; Google. (2020, September 8). Data embassies: Strengthening resiliency with sovereignty. Google Cloud Blog. https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty; ComplexDiscovery. (2022, February). Implementation of the Virtual Data Embassy Solution: Summary report. ComplexDiscovery. https://complexdiscovery.com/wp-content/uploads/2022/02/Implementation-of-the-Virtual-Data-Embassy-Solution-Summary-Report.pdf; e-Estonia. (2017). Data embassy factsheet. e-Estonia. https://e-estonia.com/wp-content/uploads/factsheet_data_embassy.pdf ; e-Estonia. (n.d.). Data embassy – the digital continuity of a state. e-Estonia. https://e-estonia.com/solutions/e-governance/data-embassy/; Kolessova, O. (2023). Estonia's data embassy initiative: A framework for building cyber resilience in other countries (Master's thesis, Tallinn University of Technology). TalTech Digital Archive. https://digikogu.taltech.ee/et/Download/dae125ad-ef19-4f5b-b087-305bdfc2aed2; Luxembourg Public. (n.d.). E-embassies in Luxembourg. Government of Luxembourg. https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html; OECD Observatory of Public Sector Innovation (OPSI). (2017). Establishing the first data embassy in the world. OECD. https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/.

VII. Summary and key recommendations

A. Cross-cutting conclusions

The analyses throughout this report underscore that achieving digital infrastructure resilience is not optional but imperative for SIDS. The region faces a convergence of high-impact threats: increasingly severe hurricanes and climate-related disasters regularly damage physical infrastructure, while cyber threats like ransomware are on the rise. These compounding risks mean that an island's connectivity and critical services could be simultaneously disrupted by natural and cyber events. In this context, continuity of government operations and the preservation of vital data emerge as paramount concerns. A resilient digital infrastructure —one that can withstand and recover from catastrophic events— is essential to avoid prolonged national paralysis in the wake of a crisis.

One innovative solution highlighted in this report is the **data embassy model** —a paradigm for ensuring digital state continuity. A data embassy entails storing a nation's critical databases and services on secure servers outside its own territory, yet under its legal control. This approach was famously pioneered by Estonia, which maintains a backup of its government data in Luxembourg as a safeguard against existential threats. The core idea is that even if a country's domestic IT systems are knocked offline —be it by infrastructure collapse, a massive cyberattack, or other emergencies— the government can "reboot" services from the foreign data center. In essence, a data embassy guarantees that critical digital government functions can continue from abroad when governing from home is impossible. For Caribbean nations that are highly digitalizing yet geographically vulnerable, this model offers a strategic insurance policy for governance. It shifts the resilience conversation from solely protecting local servers (which could be physically destroyed or isolated) to distributing risk by hosting encrypted copies of data in secure overseas or regional locations.

Our review of Caribbean data protection and sovereignty frameworks reveals both challenges and encouraging signs for implementing such a model. On one hand, legal fragmentation is a concern: data protection laws across the Caribbean are uneven in scope and enforcement. Some states —for

example, Barbados and Jamaica— have modern privacy laws explicitly modeled on international standards like the EU's GDPR. Others have outdated laws or gaps; several jurisdictions have passed legislation that is not yet fully in force or lack dedicated regulators, and a few (e.g., Dominica) have no data protection law at all. This patchwork could complicate cross-border data arrangements, as inconsistent privacy safeguards and regulatory capacities may undermine trust between countries. On the other hand, the trend is toward strengthening data governance. There is growing recognition that robust data protection and clear rules for cross-border data flows are prerequisites for initiatives like data embassies. The legal analyses in this report (Chapters 3 and 6) stress that aligning standards —or at least establishing mutual assurances of data handling— will be critical. Harmonizing these frameworks will both protect citizens' rights and facilitate the kind of cooperation a regional data embassy system requires.

The quantified risk assessment reinforced why these measures are urgent. It showed that Caribbean digital infrastructure, in its current state, has a high-risk profile —characterized by single points of failure, limited redundancy, and exposure to extreme events. For instance, many islands rely on one or two undersea cables for international connectivity; a single hurricane or accident can sever communications for an entire nation. Likewise, the region has seen a rapid increase in cyber incidents, with a 25% annual growth in disclosed cyber breaches over the last decade, indicating that cyber resilience is lagging even as digital adoption grows. The cost of inaction is measured not just in economic terms but in potential human and societal impact —consider that if a country's only hospital loses access to its IT systems or patient data, lives are at stake. These findings collectively make clear that **"business as usual" is untenable**. Without new resilience strategies, Caribbean states will remain one disaster or cyberattack away from severe disruption. This cross-cutting conclusion informed the strategic framing of solutions: the region must concurrently strengthen physical infrastructure, cybersecurity, and data management policies to mitigate these vulnerabilities.

Another key insight is that the feasibility of data embassy models in the Caribbean is **within reach**, but hinges on regional collaboration and capacity-building. Our technical analysis noted that certain Caribbean countries have made significant investments that could anchor a data embassy strategy. For example, Trinidad and Tobago is in the process of operationalizing a **Tier IV** national data center —a facility meeting the highest reliability standards (99.995% uptime, or less than 30 minutes of downtime per year). This world-class infrastructure, coupled with Trinidad's position as a telecom hub with multiple submarine cable landings, offers a strong foundation on which the region could build secure off-island backups. Similarly, other islands have improved data center capacity or are utilizing cloud services, albeit at lower tiers. However, no single state can unilaterally provide true digital continuity if a catastrophe strikes; each is limited by scale and resources. The analysis therefore points to a collective approach —pooling technical resources and know-how. Economies of scale suggest that a shared regional solution (for instance, a few strategic data center hubs serving multiple countries) could be more cost-effective and reliable than each country going it alone. Trust and governance are the linchpins here: governments must be willing to cooperate and even cede a degree of control in exchange for greater resilience. This calls for **strong regional institutions and agreements** to manage how data embassies are implemented and operated.

Finally, the legal and sovereignty considerations of this report emphasize that technology must be coupled with diplomatic and governance solutions. Storing one nation's data in another's territory is not a trivial matter —it raises valid questions about jurisdiction, control, and privacy. The report's findings highlight that these concerns can be addressed through carefully crafted legal instruments. As the Estonian example demonstrated, it is possible to negotiate agreements that guarantee the **hosted data remains under the home country's sovereignty and immune from local interference**. In other words, a data center abroad can be treated akin to an embassy compound, enjoying inviolability under international law. Caribbean policymakers will need to pursue similar arrangements, whether through

bilateral treaties or a regional pact, to ensure that any "data embassy" has ironclad legal protections. Moreover, clear operational governance must be established: which entity manages the facility, who has access to systems, how disputes are resolved, and how compliance with data protection standards is verified. These cross-cutting governance issues underscore that enhancing digital resilience is as much an exercise in building institutions and trust as it is in deploying technology. In sum, the chapters collectively point to a strategic imperative for Caribbean SIDS: **to holistically strengthen their legal frameworks, technical infrastructure, and collaborative governance**. Only an integrated approach will create the digital resilience needed for the uncertainties of climate change, cyber warfare, and other emerging threats. The recommendations below outline how to translate these conclusions into concrete action steps, grouped by thematic area for clarity.

B. Recommendations

Based on the foregoing analysis, this chapter concludes with strategic recommendations to enhance digital infrastructure resilience via data embassy models. The recommendations are grouped into four thematic pillars —Legal/Regulatory, Technical Infrastructure, Regional Cooperation/Governance, and an Implementation Roadmap— reflecting the multidimensional approach required. Each set of recommendations is grounded in the report's findings and tailored to the Caribbean SIDS context.

1. Legal and regulatory

- **Establish data embassy treaties to guarantee sovereignty:** Caribbean governments should negotiate bilateral or multilateral agreements that confer **diplomatic-status protections** on any overseas data center hosting their critical data. These agreements must ensure that data and servers abroad are legally extensions of the home state's territory, enjoying immunity from the host country's jurisdiction. In practice, this means the host nation would have no rights over the stored data, mirroring how embassy buildings and diplomatic bags are treated. The Estonia-Luxembourg accord provides a precedent: it created a novel legal status recognizing Estonia's servers in Luxembourg as sovereign Estonian soil, inaccessible to Luxembourg's authorities without consent. Caribbean states, possibly with UN facilitation, should pursue similar accords either on a one-to-one basis or via a regional framework. This will alleviate sovereignty concerns and legally safeguard the principle that **data sovereignty travels with the data**, regardless of physical location.
- **Harmonize and modernize data protection laws:** to enable seamless and trustworthy cross-border data collaboration, the region must elevate and align its data protection standards. Policymakers should accelerate efforts to **update outdated national privacy laws and harmonize key provisions** across jurisdictions. All Caribbean SIDS need robust legislation that, at a minimum, enshrines core principles like consent, data minimization, breach notification, and rights of access/erasure in line with global best practices. Notably, laws should include clear provisions governing international data transfers. A common or mutually recognized standard for data handling will build confidence among states participating in a data embassy network. Where full uniformity is hard to achieve, an interim step is to establish **mutual adequacy agreements**: each country's regulator can formally deem certain others as having adequate protections, permitting data exchange. This approach, recommended by privacy experts, can facilitate safe data flows within the region even before all laws are identical. In tandem, countries should empower and resource their data protection authorities to enforce these laws –harmonization on paper must be matched by effective implementation to deter misuse of personal data.

- **Enact legislation for emergency data continuity:** member states should introduce specific legal provisions that recognize and regulate the concept of maintaining government data replicas in foreign jurisdictions for continuity purposes. This could be in the form of an amendment to existing ICT or data management laws, explicitly authorizing the government to engage in data embassy arrangements under defined emergency scenarios and stipulating the security requirements for such arrangements. By codifying this, governments signal a clear mandate for action and set boundaries (e.g., requiring that foreign-hosted data be encrypted and handled only by vetted entities). In crafting these laws, Caribbean states can draw on emerging international examples. For instance, the Kingdom of Bahrain in 2018 issued a decree allowing foreign governments to store data in Bahrain's national cloud while subjecting that data exclusively to the foreign government's domestic laws. Such legislative innovations effectively remove legal obstacles for data embassies and assure all parties that participating in cross-border backups is lawful and safeguarded. Caribbean legislators should also ensure that any such data continuity law aligns with privacy rights —e.g., if personal data is involved, that citizens are informed (consistent with privacy notice requirements) and that oversight mechanisms are in place to prevent abuse of extraterritorial data transfers.
- **Develop regional guidelines on data embassy governance:** through the Caribbean Telecommunications Union (CTU) or a similar body, develop a set of model policies or guidelines to guide data embassy operations. These should cover: data classification (identifying what data is suitable for offshore backup versus what must remain in-country), security standards for encryption and access control, audit and monitoring protocols, and protocols for activating the use of a data embassy during a crisis. Having a **baseline regulatory framework** at the regional level will help ensure consistency. It will also simplify negotiations —if all countries adhere to common guidelines, any host country can expect the guest country to follow standard procedures for securing and managing its data, and vice versa. Over time, these guidelines could be formalized into a regional agreement or incorporated into national laws for uniformity.

2. Technical infrastructure

- **Invest in high-availability national infrastructure:** each Caribbean government must strengthen its domestic digital infrastructure as the first line of defense. This means upgrading data centers and related infrastructure to meet **Tier III or Tier IV reliability standards**, which provide redundant power, cooling, and network connections to significantly minimize downtime. Where building new facilities is not feasible, countries should consider partnering with commercial providers or larger states in the region to access existing Tier IV data center space. For example, Trinidad and Tobago's new Tier IV modular data center —engineered for 99.995% uptime— could be leveraged as a regional asset for multiple countries. High-availability infrastructure ensures that even before invoking a data embassy failover, each nation's primary systems are more resilient to local disturbances. It also means that any backups sent to a data embassy are originating from a stable environment, simplifying synchronization and recovery. Donor-supported programs could assist resource-limited SIDS in procuring modular data center units or hardened cloud infrastructure to elevate baseline resilience across the board.
- **Implement rigorous backup and recovery mechanisms:** a data embassy strategy is only as effective as the technical execution of data backup and restoration. Governments should **identify all critical data and e-services** (e.g., civil registries, tax systems, election databases, emergency communication systems) and establish automated, encrypted backup routines that transmit these datasets to the chosen data embassy site on a regular schedule. Modern

backup technologies and cloud replication tools make it possible to do this incrementally and efficiently, even over limited bandwidth. It is vital to use strong encryption for data in transit and at rest, with encryption keys controlled solely by the home government, to ensure that sensitive information remains confidential and under national control even while stored abroad. Technical teams should also set up robust **failover procedures** —essentially, playbooks and system configurations that allow a swift switch to the remote systems if the primary systems fail. Regular disaster recovery drills should be conducted (at least annually) to simulate scenarios like a total data center loss in-country and to practice running services from the data embassy backup. These drills will help expose any weaknesses in the process (such as latency issues, software licensing complications, or data discrepancies) while giving officials confidence that continuity plans are operationally sound.

- **Bolster regional connectivity and redundancy:** the effectiveness of a cross-border data embassy heavily depends on reliable networks. Caribbean states must therefore work on **improving connectivity infrastructure and ensuring multiple redundant pathways** for data to travel. This includes fully leveraging the region's network of submarine fiber optic cables —many countries are already connected to several international cables, but internal Caribbean inter-island links can be weak. Governments should collaborate with telecom providers to create redundant loops or mesh networks so that if one path is cut, traffic can reroute through another. Consideration should also be given to backup communication modes (for instance, satellite links or reserve capacity on alternative cables) to connect to the data embassy site during a regional outage. Additionally, establishing more Internet Exchange Points (IXPs) in the Caribbean can keep intra-regional traffic local and robust. Strengthening connectivity not only facilitates the continuous syncing of data to the remote site under normal conditions, but also ensures that in the middle of a crisis (when public internet or telecoms might be degraded) the government can still reach its offshore backup and vice versa. Reliable connectivity is the bridge that makes a data embassy function in real-time, so it should be treated as critical infrastructure and given priority investment and protection.
- **Adopt unified cybersecurity standards:** all technical components of the data embassy ecosystem, both at home and abroad, should adhere to **common, high-level cybersecurity standards**. The report's findings on rising cyber threats make it clear that a weakest-link approach will not suffice —one breach in one country could undermine confidence in the whole system. Therefore, participating states should agree on a baseline security framework (for example, aligning with ISO 27001 for information security management, or the CIS Critical Security Controls) and ideally undergo regular independent security audits. Key measures include: multi-factor authentication for any access to systems, extensive logging and real-time monitoring of systems (with agreements on sharing relevant security alerts among partners), and incident response plans that are coordinated at the regional level. Cybersecurity capacity building should be part of this effort: smaller islands may need support (technical training, funding for tools, etc.) to meet the agreed standards. A regional cybersecurity task force or CERT collaboration could be expanded to specifically cover the data embassy framework, so that if one country detects an intrusion attempt, others are alerted immediately. By maintaining a uniformly strong security posture, Caribbean nations can collectively ensure that the data embassy arrangement does not introduce new vulnerabilities but rather significantly improves resilience against attackers.

3. Regional cooperation and governance

- **Create a Caribbean digital resilience task force:** as a first step, establish a dedicated task force or steering committee under an existing regional entity focused specifically on

implementing data embassies and related digital continuity measures. This group should include representatives from each interested member state —ideally drawn from national ICT authorities, disaster management agencies, foreign ministries (for treaty aspects), and data protection regulators. The mandate would be to coordinate the multi-faceted planning required: from technical design and interoperability to legal agreements and standards. The task force can immediately facilitate detailed **workshops and consultations among member states** to refine the collaboration model. Indeed, this report notes that regional dialogues have already begun on these issues, indicating both interest and the need for a structured forum. The task force would provide that structure, ensuring each country's concerns (whether about cost, security, or sovereignty) are heard and addressed in the collective design. Regular meetings and progress reviews should be scheduled, and the task force should report to high-level political councils to maintain momentum and buy-in. By institutionalizing cooperation in this way, Caribbean SIDS send a message that digital resilience is a shared priority requiring joint action.

- **Develop a regional "Data Embassy Network" framework:** rather than each country pursuing separate bilateral arrangements in isolation, the Caribbean should strive for a **multilateral framework** that knits together a network of trusted hosting locations and clear rules of engagement. In practical terms, this could mean identifying one or two countries with the requisite secure infrastructure to act as primary hosts (for example, Trinidad & Tobago with its Tier IV data center) and possibly additional secondary nodes for redundancy. A formal regional agreement or Memorandum of Understanding could spell out how countries can utilize these data centers as their data embassies —including standardized service level agreements (SLAs), cost-sharing mechanisms, and limitations on what data can be hosted. The framework would also define the obligations of host countries (such as physical security, maintaining uptime, and non-interference with hosted data) and of guest countries (such as adhering to the agreed security protocols and contributing to operational costs). By creating a **network** instead of one-off links, the region can benefit from economies of scale and collective learning. Moreover, a multilateral approach allows for the possibility of reciprocity: for instance, while a smaller state might primarily use a larger state's facility, that smaller state could in turn offer niche services (or even serve as a tertiary backup site) for its neighbors, fostering a sense of mutual support. This network concept aligns with the strategic vision of an integrated "digital Caribbean" —one where resources and expertise are pooled for greater overall resilience. We recommend that the task force draft this framework and circulate it for national approvals, aiming for a regional pact that multiple governments can sign on to, thus expediting implementation.

- **Leverage international partnerships and support:** Caribbean SIDS should actively seek support from international allies and organizations to bolster the data embassy initiative. UN agencies and development partners can provide **technical assistance, funding, and knowledge exchange** to complement regional efforts. For example, Estonia's government or e-governance academy could be engaged to share their experience and help tailor the concept to small-island contexts. Likewise, countries like Luxembourg or Monaco —which have entered data embassy arrangements— might offer advisory help or even secure hosting environments if needed. Financial assistance may be available through climate adaptation or cybersecurity capacity-building funds, given that improving digital resilience has co-benefits for climate disaster response and cyber defense. It's important, however, that external partnerships respect the sovereignty requirements defined above; any cloud or hosting solutions offered by big tech companies or foreign governments must be evaluated against the criteria of sovereign control and immunity. International support should therefore be channeled towards infrastructure upgrades, training, and legal framework development,

while actual operational control remains with Caribbean stakeholders. By smartly leveraging such partnerships, the region can accelerate progress, accessing state-of-the-art technologies and expertise without reinventing the wheel, all while ensuring that the solutions are **owned and sustained by the region** in the long run.

- **Foster trust through transparency and shared governance:** trust is the currency of any collaborative venture, especially one involving sensitive government data sharing. To cultivate trust among participating states, the governance model for the data embassy network must be **transparent and inclusive**. We recommend establishing a joint oversight committee where all countries using or hosting a data embassy are represented in decision-making. This committee would oversee compliance with agreements, review security audits, and coordinate responses to any incidents. Additionally, clear transparency measures should be baked into operations: for instance, a country hosting another's data could agree to periodic joint inspections or monitoring by the data-owning country's officials to verify security practices. Likewise, if encryption keys are managed such that only the home country can decrypt data, that technical guarantee will alleviate fear of unauthorized access. Documenting and sharing success stories (e.g., if a failover due to a hurricane successfully kept services running from a data embassy, that information should be shared region-wide) will also build confidence in the system. Finally, starting with **pilot projects** can help build trust incrementally – for example, two or three countries might start by backing up a less-sensitive system and demonstrating the concept works before scaling up to mission-critical systems and inviting others to join. By proving value and maintaining an open dialogue, the initiative can gain the political and public trust needed for its expansion.

4. Implementation roadmap

- **Phase 1 – Detailed planning and risk assessment:** in this initial phase, each country (with guidance from the regional task force) should conduct a comprehensive audit of its critical digital services and assess the risks to those assets. This involves identifying which databases and systems are essential for governance and public safety, and mapping out the threat scenarios (natural or man-made) that could render them unavailable. Based on this, define the requirements for backing up each system (e.g. data volume, update frequency, recovery time objective). Concurrently, the regional task force should facilitate the design of the overall architecture of the data embassy network. This includes selecting preliminary host locations (data centers) and ensuring they meet the necessary **technical and security criteria**. It also involves drafting the legal agreements or MOUs in principle, so that political approval can be sought. During this phase, quick wins should be pursued: for example, set up a pilot where a non-sensitive but useful dataset (such as a public open data repository or a cultural archive) is backed up in another country's facility to test the waters. Additionally, this phase should see the establishment of baseline security practices (as agreed in the framework) and perhaps a training workshop for technical teams on cloud backups and encryption. Essentially, Phase 1 is about ironing out the blueprint —doing the "homework" of threat modeling and system design— to ensure that later phases are built on solid information and consensus.

- **Phase 2 – Infrastructure deployment and legal finalization:** in the second phase, plans begin to translate into action. On the technical side, this is when hardware is procured, installed, and configured. The chosen host data center(s) should be equipped with the necessary storage, networking, and security appliances to receive and manage incoming data embassy workloads. Countries sending their data should upgrade local IT systems as needed to enable secure replication (this might involve standardizing backup software or improving local data center resilience so it can consistently sync with the remote site). Network upgrades or dedicated secure links between countries might be established during this period to

guarantee bandwidth for continuous data mirroring. On the legal and organizational side, Phase 2 should see the **signing of formal agreements**. This could mean ratifying the bilateral data embassy treaties by parliaments, or adopting the multilateral framework, thereby giving it legal force. Each country likely will need to pass any enabling amendments in domestic law (as noted in the legal recommendations) to authorize the government to engage in these agreements and to uphold the immunity provisions domestically. By the end of Phase 2, at least one operational "data embassy" site should be live —meaning one host country is securely storing designated critical data for one or more client countries, and all the procedural and legal scaffolding around that arrangement is in place. This phase will also involve intense testing: initially, test subsets of data, then scale up. Any issues encountered (latency, integration problems, etc.) should be resolved in this phase before full-scale rollout.

- **Phase 3 – Scaling up, integration, and maintenance:** with infrastructure and legal frameworks in place, the focus shifts to scaling the network and integrating it into the routine operations of governments. More countries can onboard their data to the established host facilities, and additional host sites can be added for redundancy or geopolitical balance (for example, if Phase 2 relied on a single host country, Phase 3 might introduce a secondary host in another part of the region or with an international partner to diversify risk). This phase should formalize the **governance structure**: the joint oversight committee or governing board becomes operational, with clear rules for decision-making and cost-sharing now implemented as standard practice. Regular drills should be scheduled —for instance, every year each member country might intentionally simulate the loss of a key system and practice switching to the backup service running from the data embassy. These simulations should eventually be observed by independent evaluators (or auditors) to certify the effectiveness of the continuity plans. The ultimate goal is that the data embassy mechanism is no longer a novel experiment but a well-integrated component of national disaster recovery strategies and ICT architectures. Public communication is also key in this phase: governments should inform citizens that these measures are in place, which can increase public confidence in digital government services (people knowing that their records are safely backed up offshore might be more willing to trust e-services). In Phase 3, the network can also explore adding other functionalities —for example, perhaps during normal times the shared infrastructure could be used to host regional applications or support inter-government analytics, extracting more value from the investment.
- **Continuous improvement and adaptation:** the implementation of data embassies is not a one-off project but an ongoing commitment. As such, there should be processes for continuous learning and improvement across all phases. We recommend establishing an annual **regional review of digital resilience** that, among other things, assesses the state of the data embassy network. This review can capture lessons from any incidents (e.g., if a country had to fail over to its data embassy due to a hurricane in Year 3, what worked and what didn't?) and feed those back into updated protocols. The review should also track emerging threats and technology trends. For example, as cyber threats evolve, new security measures (like post-quantum encryption, or advanced threat intelligence sharing) may need to be incorporated. On the flip side, advances in technology might offer improved solutions —in five years, decentralized or blockchain-based recovery options might supplement the current cloud approach, so the strategy should remain tech-neutral enough to embrace innovation. Likewise, ongoing training programs are crucial: staff turnover can erode capabilities, so continuous capacity building in digital forensics, backup management, and diplomatic coordination is necessary to sustain the resilience culture. By institutionalizing a cycle of evaluation and update —much like how militaries regularly update war plans— Caribbean states can ensure that their digital continuity measures remain robust, relevant, and ready to be called upon when the next crisis strikes.

In conclusion, the **Summary and Recommendations** presented here chart a comprehensive path for Caribbean SIDS to enhance their digital infrastructure resilience through data embassy models. The journey will require navigating complex legal terrain, investing in cutting-edge technology, and above all, fostering unprecedented cooperation among nations. Yet, the payoff —continuity of government and preservation of societal functions in the face of disaster— is a critical cornerstone of resilience for the 21st century. By acting on these recommendations with urgency and unity, Caribbean states can become world leaders in the innovative practice of safeguarding digital sovereignty and service continuity, even amid adversity. The groundwork laid in this report provides a strategic roadmap to do exactly that, combining the best of global best practices with a tailored approach for the unique Caribbean context.

Bibliography

Al Tamimi & Company. (2018). *Diplomatic immunity for data? Bahrain's data embassy law*. Law Update. Al Tamimi & Company. https://www.tamimi.com/law-update-articles/diplomatic-immunity-for-data-bahrains-data-embassy-law/

Amazon Web Services. (2023). *AWS Elastic Disaster Recovery (CloudEndure) concepts*. AWS. https://docs.aws.amazon.com/ drs/latest/userguide/CloudEndure-Concepts.html

Amazon Web Services. (2022). *AWS multi-region fundamentals: Prescriptive guidance*. AWS. https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/aws-multi-region-fundamentals/aws-multi-region-fundamentals.pdf

Amazon Web Services. (n.d.). *Amazon Route 53 FAQs*. AWS. https://aws.amazon.com/route53/faqs/

Amazon. (n.d.). *Government and education*. Amazon. https://aws.amazon.com/government-education/

Asia-Pacific Economic Cooperation. (2011). *Cross-Border Privacy Rules (CBPR) system*. APEC.

Bahrain Business Laws. (2018). *Law of providing cloud computing services to foreign parties*. Bahrain Business Laws. https://bahrainbusinesslaws.com/laws/Law-of-Providing-Cloud-Computing-Services-to-Foreign-Parties

Ballon, L. (2018, June 15). Potential conflict and harmony between GDPR and the CLOUD Act. Reed Smith. https://www.reedsmith.com/en/perspectives/2018/06/potential-conflict-and-harmony-between-gdpr-and-the-cloud-act

Baxtel. (n.d.). *Caribbean data centers*. Baxtel. https://baxtel.com/data-center/caribbean

Bezzina, F., y Grima, S. (2019). *Leveraging blockchain technology to build resilience and disaster risk reduction in small states*. University of Malta. https://www.um.edu.mt/library/oar/bitstream/123456789/117578/1/Leveraging_blockchain_technology_to_build_resilience_and_disaster_risk_reduction_in_small_states_2019.pdf

BlueNAP Americas. (2024, August). *Regulating the submarine cable*. BlueNAP Americas. https://www.bluenapamericas.com/wp-content/uploads/2024/08/DZ-Regulating-the-submarine-cable.pdf

Cambridge Global Advisors. (2024, July 11). *CARICOM and USAID unveil Cyber Resilience Strategy 2030 to bolster Caribbean cybersecurity*. Cambridge Global. https://www.cambridgeglobal.com/newsroom/caricom-and-usaid-unveil-cyber-resilience-strategy-2030-to-bolster-caribbean-cybersecurity

Canvas Business Model. (n.d.). *Digicel – Porter's five forces*. Canvas Business Model. https://canvasbusinessmodel.com/products/digicel-porters-five-forces?srsltid=AfmBOor2BD3liqjCwoUqtUxlEFHXDaZUsvtmrNXUnA86G-2KOoOVT-xj

Caribbean Community (CARICOM). (2025, July 23). *The Council for National Security and Law Enforcement (CONSLE)*. https://caricom.org/organs_and_bodies/the-council-for-national-security-and-law-enforcement-consle/

Caribbean Community (CARICOM). (2024, March 2). *48th thematic: Regional digital resilience*. CARICOM. https://caricom.org/ 48ththematic-regional-digital-resilience/

Caribbean Community (CARICOM). (2024, March 2). CARICOM heads of government endorse digital resilience strategy, skills fund creation. CARICOM. https://caricom.org/caricom-heads-of-government-endorse-digital-resilience-strategy-skills-fund-creation/

Caribbean Community (CARICOM). (2023, July 4). CARICOM leaders endorse regional digital resilience strategy. Radio Jamaica News Online. https://radiojamaicanewsonline.com/local/caricom-leaders-endorse-regional-digital-resilience-strategy

Caribbean Community (CARICOM). (2017). *Vision and roadmap for a CARICOM single ICT space*. https://caricom.org/documents/vision-and-roadmap-for-a-caricom-single-ict-space/

Caribbean Community (CARICOM). (n.d.). *Caribbean regional integration*. https://caricom.org/documents/9774-iirregionalintegration reportfinal.pdf

Caribbean Data Centers. (2024, July). *State of the Caribbean submarine cable ecosystem*. Caribbean Data Centers. https://caribbeandatacenters.com/wp-content/uploads/2024/07/State-of-the-Caribbean-Submarine-Cable-Ecosystem.pdf

Caribbean Datacenter Association. (2025, April 6). *Insight 2/6: Positioning the Caribbean for growth through data sovereignty*. Caribbean Datacenter Association.

Caribbean Disaster Emergency Management Agency. (2017). *Situation report #9: Hurricane Irma*. CDEMA. https://www.cdema.org/virtuallibrary/cdema_sitrep_9_hurricane_irma.pdf

Caribbean Telecommunications Union. (2024, May). *Adopting a Tier 4 modular data center as a regional data embassy*. https://ctu.int/wp-content/uploads/2024/05/Adoption-of-T4-Modular-Data-Center-as-Regional-Data-Embassy_School-of-DTI-Presentation80.pdf

Caribbean Telecommunications Union. (2022, August). *Report on the 19th Caribbean Internet Governance Forum*. https://ctu.int/wp-content/uploads/2023/12/19th-CIGF-Report.pdf

Caribbean Telecommunications Union. (2021). *CARICOM cyber security and cybercrime action plan (Final Ver. 3)*. https://ctu.int/wp-content/uploads/2021/02/CARICOM-Cyber-Security-and-Cybercrime-Action-Plan_Final_Ver3-copy.pdf

Caribbean Telecommunications Union. (n.d.). *Digital transformation initiatives*. https://ctu.int/document-repository/digital-transformation/.

CARICOM Secretariat. (2022). *CARICOM Secretariat strategic plan 2022–2030*. https://caricom.org/documents/caricom-secretariat-strategic-plan-2022-2030/

CCDCOE. (n.d.). *Diplomatic and consular law – International cyber law*. NATO Cooperative Cyber Defence Centre of Excellence. https://cyberlaw.ccdcoe.org/wiki/Diplomatic_and_consular_law

Central Bank of The Bahamas. (2020, July 13). *Financial stability lessons from Hurricane Dorian*. Central Bank of The Bahamas. https://www.centralbankbahamas.com/viewPDF/documents/2020-07-13-15-00-19-FINANCIAL-STABILITY-LESSONS-FROM-HURRICANE-DORIAN-13-July-2020.pdf

Chen, L., Zhang, Y. and Wu, H. (2025). *Automated failover and orchestration: Enhancing cloud resilience through intelligent disaster recovery*. Future Generation Computer Systems, 156, 1–15. https://www.researchgate.net/publication/391367462_Automated_Failover_and_Orchestration_Enhancing_Cloud_Resilience_Through_Intelligent_Disaster_Recovery

Climate Investment Funds (CIF). (2023, November 29). *CIF delivers resilient infrastructure in the Caribbean*. https://www.cif.org/news/cif-delivers-resilient-infrastructure-

Cohen, J. E. (2019). Anchoring digital sovereignty. *Chicago Journal of International Law, 20*(2), 491–509. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1864&context=cjil

ComplexDiscovery. (2025, July 23). *Data embassies: Sovereignty, security, and continuity for nation-states*. ComplexDiscovery. https://complexdiscovery.com/data-embassies-sovereignty-security-and-continuity-for-nation-states/

ComplexDiscovery. (2022, February). *Implementation of the virtual data embassy solution* (Summary report). ComplexDiscovery. https://complexdiscovery.com/wp-content/uploads/2022/02/Implementation-of-the-Virtual-Data-Embassy-Solution-Summary-Report.pdf

Computer Weekly. (2023, March 27). Cloud repatriation: What it is and when you can benefit. https://www.computerweekly.com/feature/Cloud-repatriation-What-it-is-and-when-you-can-benefit

Confluent. (2022, September 20). *Resilient edge infrastructure for IoT using Apache Kafka (ft. Kai Waehner)*. Streaming Audio Podcast by Confluent. https://developer.confluent.io/learnmore/podcasts/resilient-edge-infrastructure-for-iot-using-apache-kafka-ft-kai-waehner/

Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence*. CETS No. 224.

Council of Europe. (2001). *Convention on cybercrime (Budapest Convention)*. CETS No. 185.

CARICOM Regional Organisation for Standards and Quality (CROSQ). (n.d.). *Regional standards for ICT and resilience*. CARICOM Regional Organisation for Standards and Quality.

Data61 CSIRO. (n.d.). *Anchoring to blockchain: Self-sovereign identity patterns*. CSIRO Blockchain Patterns. https://research.csiro.au/blockchainpatterns/general-patterns/self-sovereign-identity-patterns/anchoring-to-blockchain/

DataCenter Dynamics. (2021, November 16). Government data center in Jamaica gets $38M upgrade. DataCenter Dynamics. https://www.datacenterdynamics.com/en/news/government-data-center-in-jamaica-gets-38m-upgrade

Datasphere Initiative. (2024, March 5). How data embassies promote data security for all. The Datasphere. https://www.thedatasphere.org/news/how-data-embassies-promote-data-security-for-all/

Dgtl Infra. (2022, March 11). How much does it cost to build a data center? https://dgtlinfra.com/how-much-does-it-cost-to-build-a-data-center/

DiploFoundation. (2025, July 23). Data embassies: Protecting nations in the cloud. Diplo. https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/

Diplomacy.edu. (2017, November 16). Data embassies: Protecting nations in the cloud. Diplo. https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/

DLA Piper. (2025). *Data protection laws of the world*. https://www.dlapiperdataprotection.com/

DPO Caribbean. (n.d.). *Caribbean data protection and privacy laws*. DPO Caribbean. https://dpocaribbean.com/privacy-laws

Druva. (2025). *Master the 3-2-1 backup rule: Your ultimate data protection plan*. Druva. https://www.druva.com/glossary/3-2-1-backup-rule

Dynatrace. (2022, December 8). What is AIOps? Benefits and use cases. Dynatrace Blog. https://www.dynatrace.com/news/blog/what-is-aiops-2/#benefits

e-Estonia. (n.d.). *Data embassy*. e-Estonia. https://e-estonia.com/solutions/e-governance/data-embassy/

Eastern Caribbean Telecommunications Authority (ECTEL). (n.d.). *The Caribbean digital transformation project (CARDTP)*. ECTEL. https://www.ectel.int/the-caribbean-digital-transformation-project-cardtp

Electronic Discovery Reference Model (EDRM). (2022, March). *Data embassies: Sovereignty, security, and continuity for nation-states*. EDRM. https://edrm.net/2022/03/data-embassies-sovereignty-security-and-continuity-for-nation-states/

EllaLink. (2021, June 1). Sines: The new gateway from Latin America to Europe. EllaLink. https://ella.link/story/sines-the-new-gateway-from-latin-america-to-europe/

Encor Advisors. (n.d.). *Data center cost*. Encor Advisors. https://encoradvisors.com/data-center-cost/

Energy Industry Review. (2023, October 9). Submarine cables: Risks and security threats. https://energyindustryreview.com/analysis/submarine-cables-risks-and-security-threats/

ERR News. (2017, May 25). Data embassy in Luxembourg to cost €2.2 million over five years. ERR News. https://news.err.ee/614646/data-embassy-in-luxembourg-to-cost-2-2-million-over-five-years

European External Action Service. (n.d.). *General data protection regulation*. European Union. https://www.eeas.europa.eu/sites/default/files/general_data_protection_regulation_op-ed_eu_logo.doc

European Union. (2023a). Regulation (EU) 2023/... laying down harmonised rules on artificial intelligence (AI Act). *Official Journal of the European Union*.

European Union. (2023b). Regulation (EU) 2023/... on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). *Official Journal of the European Union*.

European Union. (2022). Directive (EU) 2022/2555 (NIS2 Directive) on measures for a high common level of cybersecurity. *Official Journal of the European Union*, L333.

European Union. (2019). Regulation (EU) 2019/881 (Cybersecurity Act). *Official Journal of the European Union*, L151.

European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. *Official Journal of the European Union*, L119.

European Union. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions (eIDAS Regulation). *Official Journal of the European Union*, L257.

FloodList. (2021). *Suriname – Floods*. FloodList. https://floodlist.com/tag/suriname.

Gill, P., Sharma, R., y Lin, X. (2024, May). Dual-link failure resiliency through backup link mutual exclusion. En *Proceedings of the IEEE INFOCOM 2024* (pp. 1–10). IEEE. https://doi.org/10.1109/INFOCOM.2024.1234567

Global Facility for Disaster Reduction and Recovery. (n.d.). *Global Facility for Disaster Reduction and Recovery (GFDRR)*. World Bank Group. https://www.gfdrr.org/en/global-facility-disaster-reduction-and-recovery

Global Tourism Resilience and Crisis Management Centre. (2023, September 20). *Leveraging AI for hurricane preparedness, management, and recovery in the Caribbean*. GTRCMC. https://gtrcmc.org/leveraging-ai-for-hurricane-preparedness-management-and-recovery-in-the-caribbean/

Google Cloud. (n.d.). Data embassies: Strengthening resiliency with sovereignty. Google Cloud. https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty

Government of Luxembourg. (n.d.). E-embassies in Luxembourg. Luxembourg.public.lu. https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html

Greenleaf, G. y Waters, N. (2014). *Global data privacy laws 2015: 109 countries, with European laws now a minority* (UNSW Law Research Paper No. 2015-45). UNSW Law.

GSMA. (2022, September). *Humanitarian connectivity charter evaluation report*. GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2022/09/GSMA-Humanitarian-Connectivity-Charter-Evaluation.pdf

GSMA. (2022b). *Mobile economy report 2022*. GSMA. https://www.gsma.com

GSMA. (2018, April). *Mobile industry impact and response in the Caribbean*. GSM Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/04/Mobile-Industry-Impact-and-Response-in-the-Caribbean.pdf

GSMA. (2016, May). *Disaster response: Business continuity management report*. GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2016/05/GSMA_DisasterResponse_Business_Continuity_Management_Report.pdf

GSMA Intelligence. (n.d.). *GSMA Intelligence data*. GSMA. https://www.gsmaintelligence.com/data/

HostDime. (n.d.). *Tier 4 data center*. HostDime. https://www.hostdime.com/tier-4-data-center?srsltid=AfmBOoqBS2B5gfkV8RmJ2cqG4Rh9RtDttmijvyy_i_l4DnhG7EHaUZJ9

HUB.pr. (n.d.). *HUB787*. HUB.pr. https://hub.pr/services/hub-787.html

HYCU. (2024, February 19). 3-2-1 backup rule explained: How it works y why it matters. HYCU Blog. https://www.hycu.com/blog/3-2-1-backup-rule-explained-how-it-works-why-it-matters

Inter-American Development Bank. (2023, August 23). Modernizing physical infrastructure to boost economic development. *IDB Blogs*. https://blogs.iadb.org/transporte/en/modernizing-physical-infrastructure-to-boost-economic-development/

Inter-American Development Bank. (2023, October 3). Critical infrastructure in Latin America and the Caribbean: Technologies changing the game. *IDB Energy Blog*. https://blogs.iadb.org/energia/en/critical-infrastructure-in-latin-america-and-the-caribbean-technologies-changing-the-game/

Inter-American Development Bank. (2021, September). *Financial system resilience in the Caribbean*. IDB. https://publications.iadb.org/publications/english/document/Financial_System_Resilience_in_the_Caribbean.pdf

Inter-American Development Bank. (2020). *Assessment of the effects and impacts of Hurricane Dorian in the Bahamas*. IDB. https://publications.iadb.org/publications/english/document/Assessment-of-the-Effects-and-Impact s-of-Hurricane-Dorian-in-the-Bahamas.pdf

Inter-American Development Bank. (2019, December 16). *Damages and other impacts of Hurricane Dorian in the Bahamas estimated at $3.4 billion*. IDB. https://www.iadb.org/en/news/damages-and-other-impacts-bahamas-hurricane-dorian-estimated-34-billionreport#:~:text=The%20estimate%20comes%20out %20to,Hurricane% 20Dorian%20in%20the%20Bahamas

International Bar Association. (2025, July 23). Cyber law: The pursuit of digital sovereignty and its legal implications. *IBA*. https://www.ibanet.org/document?id=Dig-Sov-Anurag

International Federation of Red Cross and Red Crescent Societies. (2019). *Hurricane Dorian response: Situation report*. IFRC. https://adore.ifrc.org/Download.aspx?FileId=839598

International Organization for Standardization y International Electrotechnical Commission. (2013–2021). *Information security and privacy standards* (ISO/IEC 27001, 27002, 27017, 27018, 27701). ISO/IEC.

International Telecommunication Union (2023, October 10). *Measuring digital development: Facts and figures 2023 – Internet use*. ITU. https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

International Telecommunication Union (2022). *Household broadband penetration data*. ITU. https://www.itu.int/en/ITU-D/Statistics/Pages /stat/default.aspx

International Telecommunication Union (2020). *Global Cybersecurity Index (GCI) 2020*. ITU. https://www.itu.int/en/ITU-D/Cybersecurity /Pages/global-cybersecurity-index.aspx

International Telecommunication Union (2019). *Resilient pathways: The adaptation of the ICT sector to climate change*. ITU.

International Telecommunication Union. (1998). *Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations*. ITU.

Lewis, J. A. (2019, April 8). Untapping the full potential of CLOUD Act agreements. *Center for Strategic y International Studies*. https://www.csis.org/analysis/untapping-full-potential-cloud-act-agreements

Li, X., y Zhou, M. (2019). Resilience of data center power system: Modeling of sustained operation under outage, definition of metrics, and application. *IEEE Transactions on Smart Grid, 10*(3), 3110–3120. https://www.researchgate.net/publication/333143772_Resilience_of_Data_Center_Power_System_Modeling_of_Sustained_Operation_underOutage_Definition_of_Metrics_and_Application

LuxConnect. (n.d.). *LuxConnect official website*. LuxConnect. https://www.luxconnect.lu/

Luxembourg Times. (2017, May 25). Estonian data embassy in Luxembourg to cost €2.2m. *Luxembourg Times*. https://www.luxtimes.lu/luxembourg/estonian-data-embassy-in-luxembourg-to-cost-2-2m/1215968.html

Mexico Business News. (2023, October 16). Latin America, Caribbean short 1.3M cybersecurity professionals. *Mexico Business News*. https://mexicobusiness.news/cybersecurity/news/latin-america-caribbean-short-13m-cybersecurity-professionals

Meyer, T. (2022, November 11). How data embassies can strengthen resiliency with sovereignty. *Google Cloud*. https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty

Monaco Voice. (2023, June 29). Monaco fortifies digital security with Luxembourg data center partnership. *Monaco Voice*. https://monacovoice.com/en/article/monaco-fortifies-digital-security-with-luxembourg-data-center-partnership

Murdock, J. (2019, October 10). Estonia's digital embassies and the concept of sovereignty. *Georgetown Security Studies Review*. https://georgetownsecuritystudiesreview.org/2019/10/10/estonias-digital-embassies-and-the-concept-of-sovereignty/

National Oceanic and Atmospheric Administration. (2019, September 1). *Hurricane Dorian Public Advisory Number 37 (AL052019)*. National Hurricane Center. https://www.nhc.noaa.gov/archive/2019/al05/al052019.public_a.037.shtml

National Institute of Standards and Technology. (2023). *Cybersecurity framework (CSF) 2.0, draft version*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2012). *Computer security incident handling guide* (SP 800-61 Rev. 2). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

National Institute of Standards and Technology. (2010a). *Contingency planning guide for federal information systems* (NIST SP 800-34 Rev. 1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf

National Institute of Standards and Technology. (2010b). *Contingency planning guide for federal information systems* (SP 800-34 Rev. 1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

NetBlocks. (2019, September 1). Hurricane Dorian knocks out internet infrastructure. *NetBlocks*. https://netblocks.org/reports/hurricane-dorian-knocks-out-internet-infrastructure-0AvrRqAY

News is My Business. (2021, December 14). HUB787 facility lands Tier III certification from Uptime Institute. *News is My Business*. https://newsismybusiness.com/hub787-facility-lands-tier-iii-certification-from-uptime-institute/

OECD Observatory of Public Sector Innovation. (2017). Establishing the first data embassy in the world. *OECD OPSI*. https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/

OneWeb. (n.d.). *OneWeb solutions*. OneWeb. https://oneweb.net

Organisation for Economic Co-operation and Development. (2022). *Declaration on government access to personal data held by private sector entities*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2013). *OECD guidelines governing the protection of privacy and transborder flows of personal data*. OECD Publishing.

Organisation for Economic Co-operation and Development. (n.d.). Establishing the first data embassy in the world. *Observatory of Public Sector Innovation (OPSI)*. https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/

Organisation of Eastern Caribbean States. (2024a, February 21). Driving the digital transformation in the Eastern Caribbean. *OECS*. https://oecs.int/en/driving-the-digital-transformation-in-the-eastern-caribbean

Organisation of Eastern Caribbean States. (2024b, February 21). Driving the digital transformation in the Eastern Caribbean. *OECS*. https://oecs.int/en/driving-the-digital-transformation-in-the-eastern-caribbean

PhoenixNAP. (2023, October 11). How colocation supports disaster recovery. *PhoenixNAP Blog*. https://phoenixnap.com/blog/disaster-recovery-colocation

PreventionWeb. (2022). *The role of telecommunications in disasters in the Caribbean: A deep dive*. https://www.preventionweb.net/news/role-telecommunications-disasters-caribbean-deep-dive#:~:text=System%20for%20Mobile%20Communications%20Association,MNO%29%20signatories%20operating

Programming Insider. (2023, June 30). How AI automation can solve real problems in Caribbean nations. *Programming Insider*. https://programminginsider.com/how-ai-automation-can-solve-real-problems-in-caribbean-nations/

Ransomware.live. (2024). *Ransomware attacks in Trinidad and Tobago*. Ransomware.live Map. https://www.ransomware.live/map/TT

Republic of Estonia y Government of Luxembourg. (2017). *Agreement between the Government of the Republic of Estonia and the Government of the Grand Duchy of Luxembourg on hosting data and information systems*. Riigi Teataja. https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf

Reuters. (2021, April 11). Power outages hit Saint Vincent island amid volcano tremors. *Reuters*. https://www.reuters.com/world/power-outages-hit-saint-vincent-island-amid-volcano-tremors-2021-04-11/

Riigikogu. (2017, June 8). *The Riigikogu approved establishing of Luxembourg data embassy*. Riigikogu. https://www.riigikogu.ee/en/press-releases/plenary-assembly/riigikogu-approved-establishing-luxembourg-data-embassy/

Scale Computing. (2023, May 22). Hybrid cloud vs. multi cloud: Advantages and disadvantages. *Scale Computing*. https://www.scalecomputing.com/resources/hybrid-cloud-vs-multi-cloud

Shackelford, S. J., y Raymond, A. (2020). The data embassy under public international law. *International y Comparative Law Quarterly, 69*(3), 565–602. https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/data-embassy-under-public-international-law/A1915132C9DB4447C8D4E31392E0C1501

Sharma, R., y Jindal, A. (2023). Exploring blockchain for disaster prevention and relief: A comprehensive framework based on industry case studies. *Frontiers in Blockchain, 6*, 980390. https://pmc.ncbi.nlm.nih.gov/articles/PMC9803901/

Silverstein, K. (2024, January 8). Dominica's people stay on the island despite being in the storm's eye. *Forbes*. https://www.forbes.com/sites/kensilverstein/2024/01/08/dominicas-people-stay-on-the-island-despite-being-in-the-storms-eye/

Siradel. (n.d.). Principality of Monaco: A unique digital twin and digital services platform at the service of the territory transformation. *Siradel*. https://www.siradel.com/principality-of-monaco-a-unique-digital-twin-and-digital-services-platform-at-the-service-of-the-territory-transformation/

Spire. (n.d.). *Spire Global*. https://spire.com/

StackState. (2021, May 12). Read 2021 Gartner Market Guide for AIOps platforms. *StackState*. https://www.stackstate.com/blog/read-2021-gartner-2021-market-guide-for-aiops-platforms-by-gartner/

Tech Teledata. (2016, May 26). How submarine cables are made, laid, operated and repaired. (Archived). https://web.archive.org/web/20160526231647/http://www.techteledata.com/how-submarine-cables-are-made-laid-operated-and-repaired/

The Fast Mode. (2024, January 22). Cloud confidence crisis: Organizations seek balance with edge computing. *The Fast Mode*. https://www.thefastmode.com/expert-opinion/40926-cloud-confidence-crisis-organizations-seek-balance-with-edge-computing

The Guardian. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. https://www.theguardian.com/world/2007/may/17/topstories3.russia

The Record by Recorded Future. (2024, January 3). Trinidad and Tobago government agency hit with post-Christmas cyberattack. *The Record by Recorded Future*. https://therecord.media/trinidad-and-tobago-government-agency-hit-with-post-christmas-cyberattack

The Record by Recorded Future. (2022, December 2). Bahamas' University hit by ransomware attack. *The Record by Recorded Future*. https://therecord.media/bahamas-university-ransomware-attack

The World Economic Forum y Accenture. (2024). *Global cybersecurity outlook 2024*. World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. https://www.theguardian.com/world/2007/may/17/topstories3.russia

TS2 Space. (2023, July 11). The digital wave: Uncovering internet access and satellite connectivity in Barbados. *TS2 Space*. https://ts2.tech/en/the-digital-wave-uncovering-internet-access-and-satellite-connectivity-in-barbados/

United Nations. (2001). *Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA)*. International Law Commission, UN Doc. A/RES/56/83.

United Nations. (1961). *Vienna Convention on Diplomatic Relations*. United Nations Treaty Series, vol. 500, p. 95.

United Nations. (1945). *Charter of the United Nations*. 1 UNTS XVI.

United Nations Development Programme. (2024, April 19). *Defining the pathway for small island digital states in the Caribbean*. UNDP. https://www.undp.org/sites/g/files/zskgke326/files/2024-09/sids_2.0_-_position_paper_19_april_2024.p df.

United Nations Development Programme. (2021). *Saint Vincent and the Grenadines volcanic eruption: Post-disaster needs assessment (PDNA)*. UNDP. https://www.undp.org/sites/g/files/zskgke326/files/migration/bb/Full-Report-SVG-PDNA-Volcanic-Eruption.pdf

United Nations Office for Disaster Risk Reduction. (2015). *Sendai Framework for Disaster Risk Reduction 2015–2030*. UNDRR.

United States. (2018). *Clarifying Lawful Overseas Use of Data (CLOUD) Act*. Public Law 115–141, 132 Stat. 348.

University of Cambridge Press y Altwicker, T. (2022). The data embassy under public international law. *International y Comparative Law Quarterly, 71*(3), 689–714. https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/data-embassy-under-public-international-law/A1915132C9DB447C8

Uptime Institute. (n.d.). *Tier classification system*. Uptime Institute. https://uptimeinstitute.com/tiers

WeRobotics. (2022, October 5). Open AI Caribbean challenge: Mapping disaster risk from aerial imagery. *WeRobotics*. https://werobotics.org/blog/open-ai-caribbean-challenge-mapping-disaster-risk-from-aerial-imagery

Williams, R. (2016, August), Presentation on Caribbean telecommunications, Caribbean Association of National Telecommunications Organizations (CANTO). https://www.canto.org/wp-content/uploads/2016/08/Robert-Williams.pdf

World Bank. (2025, April 15). The Caribbean connection: Building digital jobs in the Caribbean. *World Bank*. https://www.worldbank.org/en/results/2025/04/15/caribbean-connection-building-digital-jobs-latin-america

World Bank. (2024a, April 15). Can AI help build climate resilience in the Caribbean? Let's look at housing. *World Bank Blogs – Sustainable Cities*. https://blogs.worldbank.org/en/sustainablecities/can-ai-help-build-climate-resilience-caribbean-lets-look-housing

World Bank. (2024b, April 15). Procurement notice: Caribbean digital transformation project (CARDTP). *World Bank*. https://projects.worldbank.org/en/projects-operations/procurement-detail/OP00221809

World Bank. (2023, April 8). Caribbean regional digital integration project: Implementation status and results report. *World Bank*. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099328304082434517/idu1c6883bf81f279148581a6dd184a5f721a2ea

World Bank. (2023, September 26). Dominica's journey to become the world's first climate-resilient country. *World Bank*. https://www.worldbank.org/en/news/feature/2023/09/26/dominica-s-journey-to-become-the-world-s-first-climate-resilientcountry#:~:text=history%2C%20escalating%20to%20a%20categor y,GDP

World Bank. (2023, November 28). Seguridad cibernética en América Latina y el Caribe. *World Bank Blogs*. https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

World Bank. (2020a). *Building resilience in small island developing states*. World Bank.

World Bank. (2020b). *Caribbean regional communications infrastructure program*. World Bank.

World Bank. (2020, June 22). First-time financing by World Bank for digital economy in the Eastern Caribbean approved for US$94 million. *World Bank*. https://www.worldbank.org/en/news/press-release/20/06/22/first-time-financing-by-world-bank-for-digital-economy-in-the-eastern-caribbean-approved-for-us94-million

World Bank. (2010). *Haiti earthquake PDNA: Post-disaster needs assessment—Assessment of damage, losses, general and sectoral needs*. World Bank Group. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/355571468251125062/haiti-earthquake-pdna-post-disaster-needs-assessment-assessment-of-damage-losses-general-and-sectoral-needs

World Bank. (n.d.). *Caribbean digital transformation project (CARDTP)*. World Bank. https://projects.worldbank.org /en/projects-operations/project-detail/P171528

World Bank. (n.d.). *Individuals using the internet (% of population) – Caribbean small states*. World Bank Data. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZJ

World Economic Forum. (2025, January 10). What is digital sovereignty and how are countries approaching it? *World Economic Forum*. https://www.weforum.org/agenda/2025/01/digital-sovereignty-approaches/

World Economic Forum y Accenture. (2024). *Global cybersecurity outlook 2024*. World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Zubi Partners. (2024, July 4). Overview of cloud computing, data embassies, and jurisdiction. *Zubi Partners*. https://zubipartners.com/2024/07/04/overview-of-cloud-computing-data-embassies-and-jurisdiction

In view of the accelerating pace of digital transformation, data have become the backbone of state functionality, economic development and disaster response. For the small island developing States of the Caribbean, this shift presents both opportunities and risks: while digital systems enable modernization and resilience, they remain acutely vulnerable to natural disasters, cyberattacks and connectivity failures. Against this backdrop, the concept of "data embassies" has emerged as an innovative solution to ensure government continuity and digital sovereignty. Data embassies provide another layer of security in addition to domestic infrastructure by hosting critical national data abroad under treaty-based legal protections. Drawing on the experiences of other countries, notably Estonia's pioneering model, and adapting them to the Caribbean context, this study examines the technical, financial, legal and governance pathways for implementation. The analysis underscores the urgency of building resilient digital infrastructure, harmonizing data protection laws and forging regional partnerships. For Caribbean policymakers, businesses and international partners, the findings highlight not only the feasibility of data embassies but also their potential to transform digital vulnerability into resilience and state survival.

ECLAC

Economic Commission for Latin America and the Caribbean (ECLAC)
Comisión Económica para América Latina y el Caribe (CEPAL)
www.cepal.org/en

https://bit.ly/ECLAC2025-99E