POLITICAL INSIGHTS
ESTD.2026

Sri Lanka's $2.5M Treasury Hack

Cyberattack or a Breakdown in Public Finance Governance?

A Political Analysis of the Treasury Fraud, Institutional Vulnerability and Democracy Under Strain.

Sakya Attygalla

April 2026

Executive Summary

In late January 2026, what began as a routine review of Sri Lanka's foreign currency transactions exposed a critical breach at the heart of the states financial system. A seemingly minor alteration in beneficiary account details, was enough to trigger the alarms. As officials retracted the transaction, it became evident that it was no longer an administrative error, rather USD 2.5 million that was meant as a debt obligation to Australia was diverted to an unauthorized account. The Sri Lankan government made the payment, yet the intended creditors received nothing. By every measure that matters, may it be intent, authorization or timing, these course of events represents a breakdown in the states ability to guarantee the integrity of its own financial obligations and raisers a deeper question about institutional control, governance discipline and the credibility of Sri Lankas financial architecture.

For a nation that has just clawed its way out of the worst economic crisis in its modern history, the unfolding of these events is a direct threat to the entire architecture of recovery. Sri Lanka spent 2022 in sovereign default, the first in its independent history. It took months of negotiations, the International Monetary Fund (IMF) conditionalities and international diplomatic pressures to stabilize the situation. By 2026, the country has a USD 2.9 billion restructuring program, with new bilateral agreements with key creditors that included Australia, and a carefully calibrated narrative that the country was paying its obligations and rebuilding trust of the general public. Then USD 2.5 million vanished into cyberspace, and suddenly the narrative is no longer the question of whether Sri Lanka is recovering, but whether its most crucial institution, the Treasury had the basic competence to manage the nation's finances.

What followed the discovery was worse than the breach itself: approximately four months of silence. The government knew. The Treasury knew. The Central Bank knew. Yet the Parliament,

which holds the constitutional authority over public finance, learned and knew nothing nor was the creditors immediately informed. The breach remained hidden until April 22, 2026 when a formal complaint from the "Free Lawyers" Association led by Presidents Council Maithri Gunaratne formally petitioned the Speaker of Parliament, that led to the disclosure of the events.[1] Following which the Ministry of Finance issued an official statement confirming the hack of the External Resource Department (ERD).[2] What they did not say, was the executive had decided it could manage a USD 2.5 million theft without democratic accountability.

The Anatomy of Failure: Did Cybercrime outmanoeuvre a Sovereign Treasury

The breach occurred within the External Resources Department (ERD), the Treasury unit is responsible for managing Sri Lanka's foreign funded payments and external debt servicing. It is clear that this series of events was not a random target. The ERD is where the most sensitive financial operations occur, the very place where billions in bilateral and multilateral loans flow, where debt restructuring is negotiated and where the pulse of international credit relationships is monitored. With that understanding, if one wanted to strike a developing nation's financial credibility, the Treasury's international payment department would be the perfect target.

According to the narrative of the government, the hackers were sophisticated enough to understand Sri Lanka's Treasuries organisational structure, international payment protocols and the specific mechanics of bilateral debt servicing. Along with the information of when the payment was due, which accounts were legitimate and most significantly they knew the bureaucratic rhythm of government financial transaction. According the official information released the hackers are said to have infiltrated the ERD's email systems in late 2025.

For a private individual, paying a fraudulent invoice may be justified as a scam. For the Treasury of a country its far more serious: it is a direct failure of public finance governance. The Sri

[1] Free Lawyers Organization. (April 22, 2026). 'Letter to Speaker of Parliament regarding Treasury diversion.' Parliamentary petition record.

[2] Ministry of Finance, Planning and Economic Development. (April 23, 2026). Official statement on cybersecurity incident at External Resources Department.

Lankan Treasury is no ordinary payer, it is the central financial arm of the state, therefore, the explanation issued by the government that the state simply "*made a payment*" based on email communication is fundamentally and institutionally inadequate.

According to the official reports submitted, the CID informed the Colombo Fort Magistrate's Court that the payments to *Export Finance Australia* had been processed using invoices sent through what was believed to be the official email domain, exportfinance.gov.au. However, a similar domain, exportfinanceav.com had later been created and used. Following which a warning had been issued in late October 2025 that the relevant domain name had changed. The Treasury officials are said to follow the standard procedure and acted on the emails and redirected the funds accordingly. The real revelation of what took place didn't come following a sophisticated monitoring systems that detected the attack in real time, rather it was when the Treasury officials in January 2026, was processing a separate payment to an Indian creditor that had the same pattern: unusual modifications to the account details, similar to the Australian transaction. At which point, retracting the USD 2.5 million payment which was part of a larger USD 22.9 million debt repayment to Australia was nearly impossible according to the government officials.[3]

In public finance, especially in external debt servicing, a change in creditor account details should never be accepted through email alone. Such changes should immediately trigger multi-layer verification: direct institutional confirmation, bank-to-bank validation, creditor or diplomatic confirmation, internal escalation and senior authorisations. The Treasury was not paying a supplier for office equipment; it was making a debt related payment on behalf of a sovereign state. The weight a sovereign debt repayment carries is not mere, it leads to legal, diplomatic and reputational consequences. The Australian government released an official statement, stating that money was not credited, therefore, Sri Lanka has not efficiently discharged its obligation.

Finance Ministry Secretary Dr Harshana Suriyapperuma, described the attackers as a part of an 'organised international cybercrime network',[4] politically, this shifts the matter from 'cyber

[3] News First. (April 28, 2026). 'Court Locks Case Files in Treasury Cyber Scandal; Travel Bans on Five Officials.'
[4] Suriyapperuma, H. (April 23, 2026). Press conference statement on Treasury cyber fraud. Official Ministry transcript

fraud' to a possible governance scandal. The most crucial question is no longer only "who stole the money?" but "how did the state allow the payment architecture to be manipulated?". As the Finance Ministry stated, a cybercriminal trap may have been created but a functioning treasury of a sovereign state should have had enough institutional safeguards that would prevent public money from being on the receiving end of such schemes.

The political conclusion is blunt: for a government administration that came into power with a two-thirds majority that campaigned for accountability and zero tolerance for corruption, under the banner of 'Clean Sri Lanka' this incident sheds light on a dangerous gap between reform rhetoric and administrative reality. Sri Lanka can pass laws, restructure debt and speak of digital transformation but if the Treasury can process a multimillion-dollar sovereign payment based on compromised email instructions, that evidently points to the fact that the state's financial governance remains dangerously underdeveloped.

The Institutional Catastrophe

In order to fully understand how the Treasury became so vulnerable, one must understand a vital change in restructuring that set the stage for what followed. In 2024, under the new Finance Act, Sri Lanka shifted responsibility for external debt servicing away from the Central Bank of Sri Lanka (CBSL) towards the Treasury linked institutions, in particular the External resources Department and the Public Debt Management Office. The reasoning of such a move was to centralize debt management, improve coordination and to take the initiative to reduce fragmentation across institutions. The execution of such a restructuring led to a catastrophe that we see today.

On paper, this reform seems defensible. The IMF, itself had identified a structural weakness in Sri Lanka's public debt architecture. According to the International Monetary Fund (2024) the country operated under a "fragmented public debt management legal framework," with responsibilities dispersed across multiple institutions that included the Central Bank of Sri Lanka, the Ministry of Finance and the External Resource Department that resulted in a "lack of coherent management" of public debt.[5] The report further clarifies that debt functions were

[5] IMF / World Bank, *Sri Lanka: Debt Management Reform Plan*, Technical Assistance Report No. 24/102, January 2024. (Pg7)

divided between CBSL's Public Debt Department, the External Resource Department and the Treasury Operations Department.[6] And recommended the consolidation of these functions into a single intuitional body as a reform priority.[7]

The fatal vulnerability was therefore not the existence of the reform but the manner in which the reform was executed. Sri Lanka attempted to modernize debt management without first building the operational architecture. What the IMF proposed as a sequenced institutional consolidation that would be supported by capacity building, legal clarity and operational safeguards appeared to have been implemented without the corresponding institutional maturity. This divergence between reform design and reform execution is where policy intended collapsed into institutional vulnerability.

Hon. Dr Harsha de Silva steps in and shifts the narrative to reframe the scandal away from the governments preferred language of "Cyber theft", instead to posing the visible question of state competence. According to Hon. Dr. de Silva, COPF had already urged the Treasury to recruit competent and experienced staff when sovereign debt operations shifted from CBSL to the Treasury's PDMO, since managing sovereign det in global financial markets requires specialist expertise.[8] Such concerns are not technical alone: it is constitutional and institutional. Further, Hon. Dr de Silva has now summoned the Treasury Secretary and senior Finance Ministry officials before COPF, stating that the issue at hand must be treated as a national issue rather than a partisan matter as Parliament has full control over public finance under the Article 148 of the Constitution of Sri Lanka, with limited Presidential exceptions.

The Silence: When the Executive Decided to Manage Crisis Without Democracy

The Treasury breach in January 2026 was not an isolated financial incident, rather it could also be seen as a constitutional test. The government has a clear choice that could go one of the two ways: inform Parliament and activate oversight through the Committee on Public Finance or

[6] Ibid., p.11
[7] Ibid., p.9
[8] NewsWire (April 23,2026) "What happened to $2.5 million of Sri Lankan peoples' money?"

contain the issue internally. The administrative government chose containment, for nearly four months, until the April 23rd, 2026 Parliament remained uninformed.

This silence was not received as neutral; it had institutional consequences. Parliamentary oversight is non- discretionary; it is embedded within the Sri Lanka's constitutional framework that governs public finance. The failure to notify COPF at the point of discovery led to an absence of legislative scrutiny at one of the most critical phase of the incident, being when the funds was diverted, systems were compromised and response to protocols were being defined. Due to how the events unfolded, by the time of disclosure the Parliament was no longer overseeing a live institutional failure, rather it was simply reacting to a complete failure of financial governance.

The justification offered by the Treasury Secretary Dr Suriyapperuma, stated that disclosure of events as it took place could possibly alert the perpetrators and compromise the integrity of the investigation: such a stand significantly narrows the interpretation of accountability. While noting that operational secrecy is recognised as a requirement in financial crime investigations, the reasoning given by the administrative government that has a two-thirds majority does not justify withholding information from the constitutionally mandated oversight bodies. Comparative governance practices demonstrates that parliamentary committees can be briefed *in camera,* preserving investigative integrity while maintaining democratic oversight. Note, that pathway was not utilised.

In the same light, Hon. Dr Harsha de Silva publicly stated that the Finance Ministry failed to appear before the Committee for three consecutive sittings despite repeated summons.[9] By the time the breach gained public awareness, the Executive had already controlled the investigative timeline, the evidentiary process and the initial narrative. Parliament was relegated to retrospective oversight; the issue no longer was mere delay but institutional displacement.

The Legal Vacuum

What distinguishes the Treasury breach is not the absence of judicial involvement but the absence of prosecutorial escalation. Proceedings are currently underway before the Colombo

[9] *Daily Mirror*, (April 2026), "Finance Ministry failed to appear before COPF: Harsha"

Fort Magistrate's Court where the matter was taken up on reports filed by the CID.[10] The Courts has imposed a travel ban on several officials, authorised access to financial records and permitted forensic investigations. Yet these are investigative safeguards, not a criminal prosecution.

As of April 29, 2026, no charges have been framed, no indictment has been filed and no trail has been initiated in a competent criminal court. The case remains at the B-report stage: a pre-prosecutorial phase where the judiciary supervises investigation but does not adjudicate guilt.

The Default Question: Execution Failure as Sovereign Risk

The Treasury breach is no longer looked at as an isolated cyber incident, rather its preserved as a sovereign payment failure in functional terms. Sri Lanka authorised and executed the transaction but the creditors did not receive the funds. In sovereign finance that distinction is decisive: obligations are discharged only by the receipt of payment and not intent to pay.[11]

This creates exposure to a technical default scenario. Hon. Dr Harsha de Silva expresses that this risk is not a single payment itself but the contractual consequences, being cross default and acceleration clauses that can escalate a discrete failure into systemic exposure.[12] In a post restructuring context, even an irregular payment introduces disproportionate risk. As of late April 2026, the issue is being managed as a bilateral irregularity rather than a declared default, with Australia acknowledging the issue while avoiding formal escalation. This reflects creditor discretion that is not to be mistaken as absolution. Under the IMF programme, credibility depends not just on paying but also on ensuring payments are reliably delivered.[13]

The Australian government's response, articulated by the Australian High Commissioner to Sri Lanka, Mr Matthew Duckworth, suggests conditional confidence, that can be understood in light of support contingent on competent resolution. The broader implications are structural: this is not failure of intent, but of execution. In the space of sovereign finance, execution failure is itself a form of risk, one that directly affects credibility, market access and debt sustainability.

---

[10] *NewsWire*, (29 April 2026), 'Court hears CID probe into $2.5 million Treasury theft'
[11] Lee C Buchheit and G Mitu Gulati, *The Law of Sovereign Debt* (2nd edn, OUP 2019) 45–47.
[12] *NewsWire*, (April 2026), 'Harsha warns of default risk after Treasury payment irregularity'
[13] International Monetary Fund, *Sri Lanka: First Review Under the Extended Fund Facility Arrangement* (2024).

A Global Precedent: The Lesson from The Bangladesh Bank Lesson That Sri Lanka Did Not Learn From

In February 2016, a similar breach occurred at the Bangladesh Bank. Hackers infiltrated the central bank's systems and attempted a heist of USD 1 billion via SWIFT instructions. The hackers succeeded in diverting approximately USD 81 million before detection.[14] Following which, the Bangladesh heist became a watershed moment in global cybersecurity discourse, a decade later, Sri Lanka walked straight into the same trap.

The Bangladesh heist revealed fundamental vulnerabilities that should have been obvious lessons to any developing nation handling critical financial infrastructure. The banks SWIFT terminals were connected to the internet without firewalls. Network segmentation was non-existent, which allowed the hackers to install software to disable the printer that recorded SWIFT transaction logs, with no one to notice immediately, the bank had no independent monitoring systems. The hackers were able to capture legitimate SWIFT operator credentials through keylogger software and use them to issue fraudulent transfer instructions. The heist was timed for a weekend in order to minimize detection, following the heist the governor at that point Mr Atiur Rahman stepped down from office on the 15th of March 2016, citing 'moral responsibility' for the security breach amidst heavy criticism for handling the situation and for not immediately informing the government about the theft. The incident triggered international discussions about financial system security and yet a decade later, a South Asian nations central financial institution repeated the same pattern.

The Sri Lankan breach lacked some of the Bangladesh style technical sophistication as it relied on email compromise rather than direct software-based infiltration of SWIFT systems. However, the underlying vulnerabilities were identical: payment authorisation systems dependent on email, no secondary verification procedures, no real time fraud detection, inadequate network isolation between payment systems and general IT infrastructure. In more ways than one, Sri Lanka's breach was worst because it directly reflects that after the heist in Bangladesh, even after a decade of public discussion and international attention, the nation had still built its sovereign

[14] *The Hedge Fund Journal*, 'The Bangladesh Cyberheist' (2016)

debt payment system in a way that made it vulnerable to commodity level cybercrime techniques.

The Investigation That No One Trust

When the breach was made public, the Treasury responded with a Technical Investigation Committee appointed in late March 2026. The committee was staffed by senior Treasury officials: two Deputy Secretaries to the Treasury, the Director General of the National Planning Department, the Additional Director General of the Legal Affair Department and an Assistant Director from the IT Management Department. On the face of it, this looks as a serious institutional response. In reality, it seems to be structured to guarantee that any findings would be politically managed rather than independently verified.

The co-chairs were Deputy Treasury Secretaries with operational responsibility for the very debt repayment systems that had failed. Asking them to investigate their own operational failure is asking them to find fault with their own judgement, staffing their own decisions and their own oversight mechanisms. It is a structural conflict of interest designed into the inquiry from the beginning. Civil society organisations from the Free Lawyers immediately called for an independent investigation by the National Audit Office or a dedicated parliamentary body. These calls were ignored, the Treasury maintained control over the investigation into its own institutional failure.

By late April 2026, the Committee on Public Finance was preparing to decide whether to summon Treasury Secretary Dr Suriyapperuma and other officials before Parliament.[15] This represented a critical moment for Sri Lanka's democracy. If Parliament asserted its constitutional authority and conducted a genuine independent investigation, it would send a message that even fundamental breaches of public financial security could not be managed through executive discretion ad internal inquiries. If Parliament deferred to the Treasurys internal process, it would signal that the constitutional principle of parliamentary oversight had eroded so far that the executive could handle major institutional failures without real accountability.

[15] *Ada Derana*, 'COPF reveals details on Treasury payment irregularity; investigations underway' (April 2026)

Conclusion: A Nation at the Crossroads

In the middle of 2026, Sri Lanka is confronted with a fundamental choice about its own future. The choice is no longer, at its root about cybersecurity or even about USD 2.5 million but the bigger picture of governance. It's a question of whether the nation that had survived the economic collapse could once again rebuilt itself, not just economically but also its democratic institutions. Along with an even bigger question of whether crisis could be an opportunity that could strengthen accountability and transparency or whether it would be used as a cover for consolidating executive power and avoiding oversight.

The immediate concerns at hand are clear: would the Committee on Public Finance exercise its constitutional authority and conduct an independent investigation? Would the Treasury Secretary Dr Suriyapperuma be summoned to Parliament? Would senior officials be held accountable for institutional failures? Would the internal investigation be supplemented or replaced by independent inquiry? Would formal criminal charges be filed in courts for the theft of public funds? These are not abstract constitutional questions. These are a test of whether the institutions that constrain executive power in a democracy still functioned in the nation.

But the most important question is very simple: who decides on what the public should know about how public finance is spent? If the executive could unilaterally choose to conceal a major institutional failure for approximately four months, the Parliaments constitutional authority is meaningless. If an internal investigation is conducted by officials with stakes in the outcome, is there a possibility of the democratic principle of oversight being eroded beyond recovery? All of these questions boils down to the fact that, if a government could lose USD 2.5 million of its public funds and manage that loss through secrecy rather than transparency, while avoiding formal legal prosecution through administrative referrals, then the crisis is not remotely over, it simply continues under a different disguise.

Sri Lanka had emerged from a sovereign default in 2022, but only barely. The nation entered 2026 with a restructuring program, under the manifesto of 'clean Sri Lanka' with renewed bilateral relationships and a narrative for recovery. The Treasury breach threatens to unravel that seemingly airtight narrative not because public funds were mismanaged but because the governments response exposed that the underlying governance pathologies that created the 2022

crisis in the first place are not fully addressed. The institutions that constrain executive powers have not been strengthened. The states capacity to manage critical infrastructure is seemingly deteriorating rather than improving. A cybercrime or a bank heist as they government labels it sheds light on a bigger governance crime: the crime of believing that a nation can recover from economic collapse without actually changing how it governs itself.

Sources and References

Free Lawyers Organisation, 'Letter to Speaker of Parliament regarding Treasury diversion' (22 April 2026) Parliamentary petition record.

Ministry of Finance, Planning and Economic Development, 'Official Statement on Cybersecurity Incident at External Resources Department' (23 April 2026).

NewsFirst, 'Court Locks Case Files in Treasury Cyber Scandal; Travel Bans on Five Officials' (28 April 2026

Mahinda Siriwardana Suriyapperuma, 'Press Conference Statement on Treasury Cyber Fraud' (23 April 2026) Ministry of Finance transcript.

International Monetary Fund and World Bank, *Sri Lanka: Debt Management Reform Plan* (Technical Assistance Report No 24/102, January 2024) Pg 7.

International Monetary Fund and World Bank, *Sri Lanka: Debt Management Reform Plan* (Technical Assistance Report No 24/102, January 2024) Pg 11.

International Monetary Fund and World Bank, *Sri Lanka: Debt Management Reform Plan* (Technical Assistance Report No 24/102, January 2024) Pg 9.

NewsWire, 'What happened to $2.5 million of Sri Lankan people's money?' (23 April 2026)

Daily Mirror, 'Finance Ministry failed to appear before COPF: Harsha' (April 2026)

NewsWire, 'Court hears CID probe into $2.5 million Treasury theft' (29 April 2026)

Lee C Buchheit and G Mitu Gulati, *The Law of Sovereign Debt* (2nd edn, Oxford University Press 2019) 45–47.

NewsWire, ‘Harsha warns of default risk after Treasury payment irregularity’ (April 2026)

International Monetary Fund, *Sri Lanka: First Review Under the Extended Fund Facility Arrangement* (2024).

The Hedge Fund Journal, ‘The Bangladesh Cyberheist’ (2016)

Ada Derana, ‘COPF reveals details on Treasury payment irregularity; investigations underway’ (April 2026)