CYBERSECURITY GOVERNANCE AND FOREIGN POLICY FORMATION IN NEPAL:

INSTITUTIONAL FAILURES AND THEIR DIPLOMATIC CONSEQUENCES

SABIN SHARMA

Budhiganga-01, Morang
Cybersecurity Enthusiast and BCA Student
Nihareeka College of IT and Management
Biratnagar-05, Morang, Nepal

NEPAL POLICY RESEARCH — 2026

ABSTRACT

Nepal's accelerating digital transformation has delivered tangible public benefits online tax filing, e-passport services, digital land records, and a unified citizen portal among them. Yet this expansion has consistently outpaced the security frameworks needed to protect it. By 2025, repeated high-profile breaches had exposed millions of citizens' personal records, disrupted critical government services, and demonstrated that Nepal's public digital infrastructure was being built without adequate security foundations.

This paper examines Nepal's cybersecurity governance failures not as a domestic administrative shortfall but as a structural condition that shapes how foreign policy is formed, constrained, and exploited. It argues that Nepal's cybersecurity deficit is not primarily a technical problem but a foreign policy formation failure one rooted in weak enforcement, dispersed institutional responsibility, chronically inadequate resourcing, and a cultural undervaluation of security as a sovereign function. Particular attention is given to the first phase of foreign policy formation intelligence gathering and situational assessment where adversarial actors exploit insecure government infrastructure to compromise the information environment on which diplomatic decision-making depends. The paper concludes with a tiered set of policy recommendations positioning cybersecurity reform as an instrument of Nepal's foreign policy capacity, not merely a component of its domestic IT governance.

TABLE OF CONTENT

1. INTRODUCTION

1.1 Digital Insecurity as a Foreign Policy Condition

When Nepal's Government Integrated Data Centre at Singha Durbar went dark in January 2023 under a distributed denial of service attack, approximately 1,500 government websites became inaccessible simultaneously [10]. Immigration verification systems at Tribhuvan International Airport failed. Officers reverted to manual passport checks. Flights were delayed by over an hour.

This was not merely an IT incident. It was a demonstration, visible to every diplomatic counterpart, investor, and regional power watching, that Nepal's state apparatus could be destabilised by a relatively unsophisticated attack. For a small landlocked state whose foreign policy depends on projecting institutional credibility to bilateral partners, multilateral donors, and regional powers, that demonstration carries consequences that extend far beyond server downtime. This paper argues that Nepal's cybersecurity deficit must be understood through the lens of foreign policy formation because the same infrastructure failures that expose citizens' data are the failures that expose Nepal's diplomatic communications, negotiating positions, and institutional decision-making processes to adversarial collection.

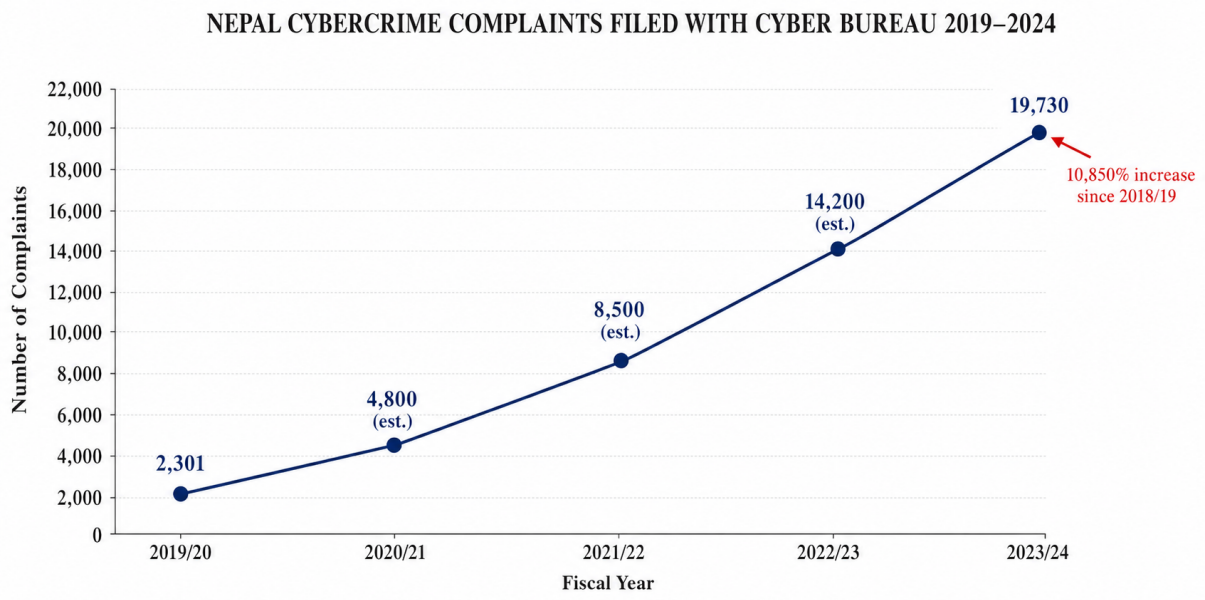


Figure 1: Nepal Cybercrime Complaint Growth 2019–2024

Source: Nepal Police Cyber Bureau, 2024

1.2 Statement of the Problem

Nepal's e-governance rollout has been ambitious and, by measures of service delivery scope, genuinely impressive. The Digital Nepal Framework launched in 2018–19 envisioned a paperless government spanning finance, land records, health, education, and identity management [5]. Internet penetration reached 90 percent of the population by 2024, with over 30 million users a figure that stood at just 35,000 in 2000. Yet digital service expansion and security investment have not moved together. Development was outsourced to vendors without security expertise, systems were launched without audits, patches were not applied, and the bodies responsible for cybersecurity were given neither the authority nor the resources to act leaving the information environment that feeds foreign policy formation open to adversarial collection in one of Asia's most geopolitically contested neighbourhoods.

This paper addresses the following specific research question: **to what extent do Nepal's cybersecurity governance failures compromise the intelligence environment on which its foreign policy formation depends, and what institutional reforms are necessary and sufficient to address this as a matter of foreign policy capacity?** Existing treatments of Nepal's cybersecurity including the ITU's GCI country assessments and the government's own National Cyber Security Policy 2023 frame the deficit as a technical capacity and legal compliance problem, measuring commitment through legislative existence rather than enforcement outcome. No prior work has systematically mapped specific vulnerability classes and governance failures onto the phases of foreign policy formation, nor connected Nepal's bilateral relationships with India and China to the intelligence collection risks its insecure infrastructure creates. Existing treatments including the ITU's GCI country assessments, which measure commitment through legislative existence rather than enforcement outcome, and Nepal's own National Cyber Security Policy 2023, which frames the deficit as a technical capacity problem treat cybersecurity governance as a domestic IT administration challenge. This paper departs from that framing by treating governance failures as conditions that directly shape foreign policy formation capacity. That reframing is the paper's original contribution.

1.3 Methodology

The methodology employed is structured comparative institutional analysis, combining three analytical layers. First, policy document review of Nepal's primary legal and governance instruments the Electronic Transactions Act 2006, the Privacy Act 2018, the National Cyber Security Policy 2023, and the draft IT and Cybersecurity Bill 2082 [1][2][3][4] assessed against the enforcement architecture each instrument does or does not create. Second, incident documentation analysis drawing on verified breach reports, Nepal Police Cyber Bureau statistics, and ITU Global Cybersecurity Index data to establish an evidence base for the vulnerability landscape [6][7]. Third, structured comparison with three peer cases Rwanda, Bangladesh, and Estonia selected because each represents a distinct trajectory: Rwanda as a successful small-state sequencing model, Bangladesh as a cautionary peer with similar institutional characteristics, and Estonia as the benchmark for crisis response doctrine. The comparisons are structured against identical criteria: the legal basis of the cybersecurity authority, its enforcement power over line ministries, its staffing and resource allocation, and its incident response record. This approach is consistent with comparative institutionalist frameworks applied to cybersecurity governance in developing states.

1.4 Significance of the Study

Cybercrime complaints filed with Nepal Police's Cyber Bureau grew from 2,301 in 2019/20 to 19,730 in 2023/24 [7]. Two million citizenship records were placed for sale on dark web marketplaces in April 2025. The Hello Sarkar portal was breached and its data circulated on Telegram. The National Medical Council and Election Commission were similarly compromised. These documented events erode the institutional credibility, sovereign information security, and diplomatic standing on which Nepal's foreign policy capacity depends.

2. THE FOREIGN POLICY FORMATION AND CYBERSECURITY

2.1 Framework and Where Cybersecurity Enters

Foreign policy formation proceeds through several interrelated phases: intelligence gathering and situational assessment; agenda-setting and problem definition; option generation; decision-making by authorised actors; and implementation with feedback loops. Each phase depends on the quality, integrity, and confidentiality of information available to decision-makers. Nepal's cybersecurity failures are most consequential at Phase One, the phase where the information environment that drives all subsequent foreign policy action is either protected or compromised.

2.2 Phase One: Intelligence Gathering and Situational Assessment

The first phase of foreign policy formation is the most structurally exposed to adversarial exploitation. Before a foreign ministry can define a problem, frame options, or authorise a response, it must know what is happening what counterpart governments are doing, what their negotiating positions are, and what threats are emerging. This intelligence function is the foundation on which all foreign policy action rests, and what adversarial actors most actively seek to compromise.

2.3 How Adversarial Actors Exploit Phase One: Documented Entry Methods

Spear Phishing and Credential Harvesting. The most common entry vector for targeted foreign policy espionage is not a sophisticated technical exploit it is deception. Spear phishing communications impersonating trusted contacts extract login credentials for government email accounts, VPN systems, and document management platforms. Nepal's documented absence of multi-factor authentication despite a 102-point NCSC advisory in January 2025 mandating it [11] means stolen credentials provide uncontested access to the information environment foreign policy depends on. For MoFA specifically, compromised email credentials expose bilateral negotiating positions, counterpart assessments, and diplomatic appointment records precisely the Phase One intelligence a foreign actor needs to anticipate Nepal's positions before negotiations begin.

SQL Injection Against Government Portals. The variant most commonly observed in Nepal is Boolean-based injection, requiring minimal sophistication but yielding access to entire databases when target systems lack input validation [8]. A foreign intelligence service needs only a basic automated tool and an unpatched portal

Nepal has provided both conditions consistently. Access to civil service personnel files enables adversarial profiling of diplomatic staff identifying pressure points, financial vulnerabilities, and

posting histories that inform targeted recruitment or coercion operations against Nepal's foreign policy apparatus.

Server-Side Request Forgery. Growing in relevance as Nepal integrates external APIs under the Digital Nepal Framework, SSRF exploits trusted server relationships to access internal systems not directly exposed to the internet moving an adversary laterally from a visible government portal into backend infrastructure connecting ministries, payment gateways, and identity systems. Lateral movement into inter-ministry communication systems during an active negotiation over BRI financing terms or MCC implementation gives an adversary real-time access to Nepal's deliberative process before positions are finalised.

Persistence Through Misconfigured Infrastructure. The concentration of government hosting within the Government Integrated Data Centre creates systemic single-point-of-failure conditions. The January 2023 attack that took down 1,500 websites simultaneously, and the March 2025 DDoS assault that downed over 400, exploited architectural misconfigurations at the hosting layer [10]. Beyond service disruption, persistent access through misconfigured infrastructure enables long-term passive collection an adversary maintaining undetected presence during a sensitive diplomatic period extracts situational intelligence continuously, not episodically.

The international dimension is not theoretical. Reports from 2025 suggested the group responsible for breaching the Hello Sarkar portal claimed association with Russia's APT28 threat actor group, illustrating the threat landscape within which Nepal's insecure infrastructure operates.

PHASE ONE FOREIGN POLICY VULNERABILITIES — INTELLIGENCE GATHERING AND CYBER EXPLOITATION IN NEPAL

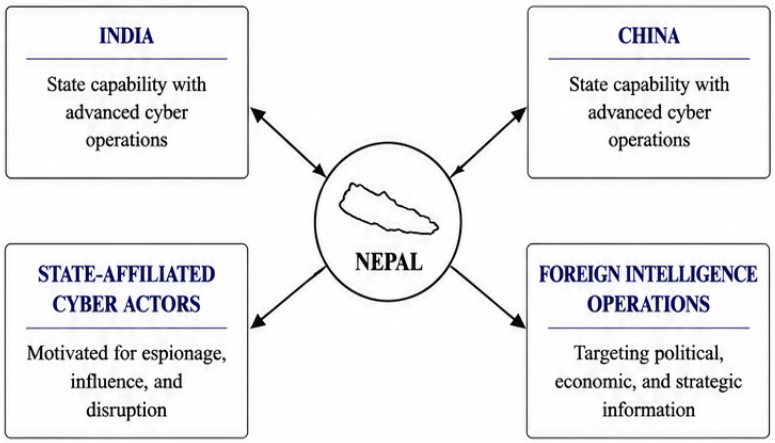
1. INTELLIGENCE GATHERING AS THE FOUNDATION OF FOREIGN POLICY

Compromise at the intelligence-gathering stage allows adversarial actors to influence or monitor policy formation before state responses are authorised.

2. DOCUMENTED CYBER ENTRY VECTORS IN NEPAL

ENTRY VECTOR	DESCRIPTION	SEVERITY LEVEL
1. SPEAR PHISHING & CREDENTIAL HARVESTING	• Diplomatic impersonation attacks • Credential theft from email and VPN systems • Absence of enforced MFA across agencies • NCSC 102-point advisory (January 2025) ignored	SEVERITY VERY HIGH ■■■■■
2. SQL INJECTION	• Over 85% of documented cybercrime cases involved SQL injection where technical evidence existed • Boolean-based injection dominant in Nepal • Weak input validation across government portals • Risk to land records, citizenship databases, civil service systems	SEVERITY HIGH ■■■■□
3. SERVER-SIDE REQUEST FORGERY (SSRF)	• Increased exposure under Digital Nepal Framework • Exploits trusted server relationships • Enables lateral movement into ministry backend systems • Threat to identity and payment infrastructure	SEVERITY MODERATE ■■■□□
4. MISCONFIGURED CENTRALISED INFRASTRUCTURE	• Government Integrated Data Centre creates systemic single-point-of-failure risk • January 2023 cyberattack disrupted 1,500 government websites • March 2025 DDoS attack disrupted over 400 websites • Weak segmentation and monitoring amplified impact	SEVERITY MODERATE ■■■□□

3. REGIONAL AND INTERNATIONAL CYBER THREAT LANDSCAPE



2025 reports linked the Hello Sarkar portal breach claims to actors associated with Russia's APT28 threat ecosystem.

Nepal's geographic position between India and China increases exposure to regional cyber espionage and influence operations.

4. POLICY INTERVENTIONS TO PROTECT FOREIGN POLICY INTELLIGENCE

1. MANDATORY MFA ENFORCEMENT

- Legal enforcement authority required
- Advisory-only frameworks ineffective

2. MANDATORY BREACH NOTIFICATION

- Update Electronic Transactions Act
- Transparency as remediation mechanism

3. RESPONSIBLE DISCLOSURE SAFE HARBOUR

- Protect ethical security researchers
- Formal vulnerability disclosure system

4. SECURITY-BY-DESIGN PROCUREMENT

- Third-party security audits before deployment
- No unsupported systems in production

Rwanda's National Cyber Security Authority possesses direct enforcement authority over ministries.

Nepal's NCSC operated in 2025 with only three engineers and no enabling legislation.

5. FOREIGN POLICY CONSEQUENCES OF CYBER GOVERNANCE FAILURE

1. WEAK GOVERNANCE
Lack of enforcement, resources, and accountability mechanisms

2. INTELLIGENCE EXPOSURE
Sensitive diplomatic and strategic information compromised

3. DIPLOMATIC VULNERABILITY
Negotiating positions and communications exposed or manipulated

4. FOREIGN INFLUENCE RISKS
Adversaries gain leverage through information access and influence operations

5. REDUCED POLICY AUTONOMY
State decisions influenced or constrained by external actors

6. NATIONAL SECURITY INSTABILITY
Long-term erosion of sovereignty, stability, and national interests

Sources: National Cyber Security Policy 2023, NCSC Advisory January 2025, Electronic Transactions Act, Proposed IT & Cybersecurity Bill 2082, documented incidents involving Hello Sarkar portal, Koshi Province systems, Government Integrated Data Centre attacks (2023–2025), and publicly reported cyber incident analyses.

3. NEPAL'S VULNERABILITY LANDSCAPE: THE EVIDENCE

Nepal's government digital infrastructure suffers not from sophisticated nation-state intrusions but from well-documented, preventable weaknesses that persist because of governance failure and governance failures have direct foreign policy consequences. These are not technical facts. They are governance facts.

SQL injection remains the dominant attack vector, documented in over 85 percent of cases where technical evidence was available [8][7]. Boolean-based techniques exploit legacy content management systems and absent input validation to yield access to citizenship databases and civil service personnel files. For foreign policy formation, this is a specific mechanism: access to civil service personnel files enables adversarial profiling of diplomatic staff identifying posting histories and financial vulnerabilities that inform targeted recruitment or coercion operations against Nepal's foreign policy apparatus before negotiations begin.

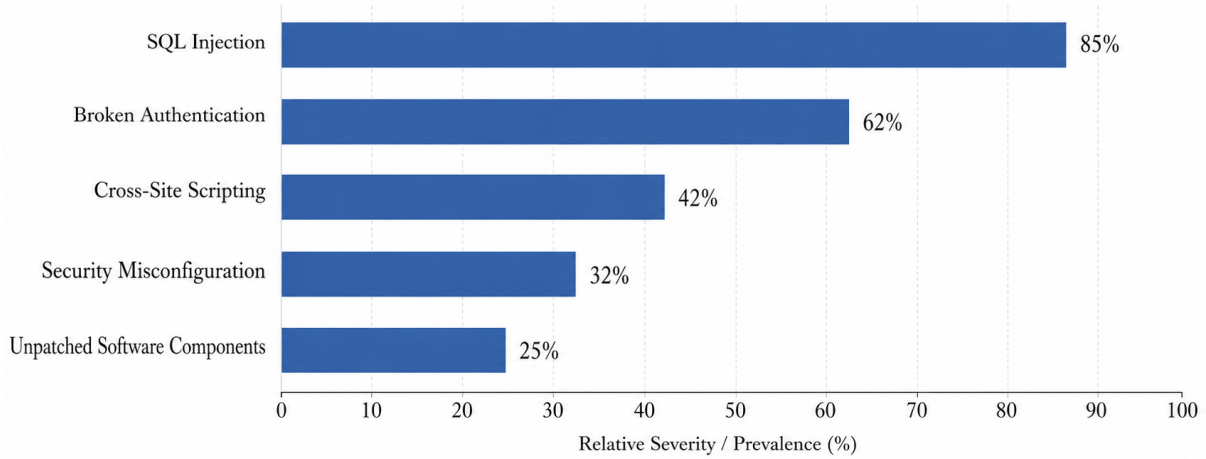
Broken authentication has enabled repeated unauthorised access at scale. The April 2025 Nepal Police Headquarters compromise placed two million citizenship records on dark web marketplaces by exploiting unpatched API vulnerabilities in an environment without enforced multi-factor authentication. The foreign policy consequence is direct: national-scale adversarial profiling of Nepali officials creates leverage over the individuals who staff Nepal's diplomatic missions.

Cross-site scripting enabled coordinated defacement of 21 Koshi Province subdomains simultaneously in February 2025. Each public compromise signals to diplomatic counterparts that Nepal's state apparatus cannot protect its own infrastructure eroding the institutional credibility on which foreign policy engagement depends.

Unpatched software remains the most persistently exploited category. Nepal scored 44.99 out of 100 on the 2020 Global Cybersecurity Index, ranking 94th of 182 nations [6]. The Hello Sarkar portal was breached while running an obsolete framework; the Prime Minister's Office was informed only when a developer noted the weakness during routine updates. The NCSC was operating with three engineers. For Phase One intelligence integrity, unpatched systems in active government use mean adversaries can maintain persistent, undetected presence during sensitive diplomatic periods extracting situational intelligence continuously, not episodically.

PRIMARY CYBER ATTACK VECTORS TARGETING NEPAL GOVERNMENT WEB INFRASTRUCTURE

Based on documented incident data, Nepal Police Cyber Bureau and OnlineKhabar Analysis 2024



Source: OnlineKhabar Security Analysis 2024; Nepal Police Cyber Bureau 2024; B360 Nepal 2025

4. NATIONAL SECURITY AND FOREIGN POLICY IMPLICATIONS

Nepal's geopolitical position makes its cybersecurity deficit specifically and bilaterally consequential. Large-scale breaches of citizenship records names, addresses, IDs, biometric data enable foreign actors to cross-reference digitised government databases for long-term intelligence collection. India's CERT-In has established cooperative frameworks with regional states, but Nepal has not formalised a bilateral cybersecurity arrangement, meaning threat intelligence sharing depends on informal channels rather than institutional agreement.

Service disruption carries direct foreign policy consequences: failed immigration systems damage Nepal's reputation as a functional transit state, and compromised electoral or law enforcement databases invite foreign commentary that erodes the diplomatic standing MoFA depends on.

4.1 The Ministry of Foreign Affairs as an Institutional Target

Nepal's Ministry of Foreign Affairs manages a communications and information environment specifically valuable to adversarial collection. It holds records of bilateral negotiation positions, internal assessments of counterpart governments, personnel files of diplomatic staff posted abroad, and coordination records with multilateral institutions including the United Nations, the World Bank, and regional bodies. None of these categories are inherently more secure than the citizenship databases, electoral systems, and land records already documented as compromised. MoFA operates on the same .gov.np domain infrastructure that has been repeatedly breached, uses the same government email systems that lack enforced multi-factor authentication, and is subject to the same absence of mandatory security audit requirements that left the Hello Sarkar portal running an unsupported framework for years before its compromise was noticed.

There is no public evidence that MoFA's systems have been specifically audited or treated as a priority category within Nepal's cybersecurity governance framework. The NCSC's January 2025 advisory was addressed to government agencies generically it did not differentiate between a rural municipality portal and the foreign ministry of a state navigating relationships with two nuclear powers. A functioning cybersecurity governance architecture would identify MoFA, the Office of the Prime Minister, the National Intelligence Department, and the Ministry of Finance as a tier requiring priority protection. Nepal's current architecture makes no such distinction, meaning the institutions most valuable to foreign adversaries are no more defended than those of least intelligence interest.

5. INSTITUTIONAL AND GOVERNANCE GAPS

Nepal's cybersecurity vulnerabilities are a governance problem, not a technical one. The laws exist. The policies exist. What does not exist is the institutional capacity, enforcement authority, and resource allocation to translate them into practice.

The Electronic Transactions Act 2006, the Privacy Act 2018, and the National Cyber Security Policy 2023 collectively establish a framework that should underpin digital security across government [1][2][3]. The proposed IT and Cybersecurity Bill 2082 goes further, mandating annual security audits for critical infrastructure [4]. Yet the NCSC was operating in 2025 with three engineers, no dedicated office space, and no enabling legislation giving it enforcement authority over line ministries.

The consequences are documented and specific. The Koshi Province IT department denied any investigation five months after a February 2025 defacement. The Prime Minister's Office learned of the Hello Sarkar compromise from a developer, not a security monitor. Responsibility for cybersecurity is dispersed across dozens of independently managed agencies. No unified technical standards exist. No mandatory audit requirements exist. No penalties for negligence exist. This is not a failure of individual agencies it is a structural failure of governance design with direct consequences for Nepal's foreign policy environment.

Nepal's governance failure is not unique in the developing world, but its geopolitical context makes it unusually consequential. States that cannot secure their own institutional data cannot credibly negotiate data-sharing arrangements, participate meaningfully in regional cybersecurity frameworks, or protect the confidentiality of diplomatic communications. The question is no longer whether Nepal has a cybersecurity problem. The question is whether Nepal has the institutional will to treat it as the foreign policy liability it already is.

NEPAL CYBERSECURITY GOVERNANCE FAILURE — STRUCTURAL VULNERABILITIES 2024–2025

1. LEGAL FRAMEWORK EXISTS

Electronic Transactions Act 2006	Privacy Act 2018	National Cyber Security Policy 2023	Proposed IT & Cybersecurity Bill 2082

Legal and policy frameworks formally exist but remain weakly enforced.

2. INSTITUTIONAL CAPACITY CRISIS

National Cyber Security Centre (NCSC)

3	!	!	!	!
Only 3 engineers operating nationally in 2025	No dedicated office space	No enabling enforcement legislation	No authority over line ministries	No budgetary autonomy or resources

3. DOCUMENTED GOVERNANCE FAILURES

February 2025

Koshi Province Government Website Defacement

No formal investigation confirmed five months after breach.

2024–2025

Hello Sarkar Portal Compromise

Prime Minister's Office informed only after developer identified weakness during update.

4. STRUCTURAL CONSEQUENCES

Fragmented agency management → No unified cybersecurity standards → No mandatory audits → No penalties for negligence → Weak institutional accountability → Direct foreign policy and national security implications

Sources: National Cyber Security Policy 2023, Proposed IT & Cybersecurity Bill 2082, Publicly documented incidents involving Koshi Province government systems and Hello Sarkar portal (2024–2025).

6. COMPARATIVE ANALYSIS: LESSONS FROM DEVELOPING NATIONS

Nepal's situation mirrors patterns documented across peer countries, offering both cautionary lessons and transferable models. In Bangladesh, a security lapse in July 2023 exposed personal data of over 50 million citizens when the national Birth and Death Registration website leaked sensitive records acknowledged by Bangladesh's state minister for ICT as the product of security weaknesses. Bangladesh has a Digital Security Act, a national CIRT, and a 2021–25 cyber strategy. None of it prevented the breach. Bangladesh's case demonstrates that legal frameworks without enforcement architecture cannot protect the information environment foreign policy formation depends on a lesson Nepal's own gap between the Electronic Transactions Act and the NCSC's operational reality reproduces exactly.

In Sri Lanka in 2026, hackers stole approximately 2.5 million US dollars by breaching the Finance Ministry payment system, with authorities suspecting state-sponsored actors manipulated inter-bank communications to divert funds. Sri Lanka's breach illustrates that compromised financial infrastructure is not merely a domestic failure, it is a foreign policy event that damages bilateral credibility and signals institutional vulnerability to every counterpart watching. For Nepal, this is a Phase One warning: financial infrastructure compromised by state-suspected actors signals to every bilateral partner that Nepal's institutional systems cannot be trusted as a foundation for sensitive cooperation.

Rwanda presents the most instructive model for Nepal. Both are small, landlocked developing nations that pursued aggressive digital government expansion before security frameworks were ready. Rwanda's National Cybersecurity Strategy 2024–2029 established a dedicated agency with real governance authority from the outset legal mandate, defined reporting lines, and enforcement authority over other agencies before broader strategy was built around it [9]. Assessed against the four criteria applied in this paper legal basis, enforcement power, staffing, and incident response Rwanda meets all four. Nepal meets none. Rwanda's sequencing model matters for Phase One intelligence integrity specifically: a foreign ministry operating within a governance architecture where the cybersecurity authority has real enforcement power can assume baseline protection of its communications infrastructure; Nepal's cannot.

Estonia's experience reinforces the crisis response dimension: structured planning, coordinated communications, and embedded innovation are prerequisites, not reactions. Nepal's institutional response to the 2023 DDoS, the 2025 Hello Sarkar breach, and the Nepal Police records exposure demonstrated the opposite, each inadequate response visible to the diplomatic community Estonia's doctrine is designed to reassure. Rapid digital expansion without commensurate security investment creates national liability that shapes the foreign policy environment.

CYBERSECURITY GOVERNANCE CAPACITY COMPARISON: NEPAL AND REGIONAL PEERS

Country	GCI Score /100	National CERT Established	Dedicated Cyber Law	Mandatory Audit Requirement	Enforcement Authority
Nepal	44.99	Partial	Pending (Bill 2082)	No	No
Rwanda	68.4	Yes	Yes (Law 60/2018)	Yes	Yes
Bangladesh	53.2	Yes	Yes (DSA 2018)	Partial	Partial
Sri Lanka	51.0	Yes	Partial	No	Partial

Sources: ITU GCI 2020; Rwanda NCSA 2024; Digital Policy Alert 2025

7. POLICY RECOMMENDATIONS: A TIERED FRAMEWORK

Nepal does not lack cybersecurity policies. It lacks the institutional architecture to make them mean anything. The recommendations below are calibrated to what Nepal can realistically achieve given its governance capacity, budget, and technical workforce but sequencing is as important as substance. Legal authority must precede enforcement. Enforcement must precede compliance. Workforce capacity must precede policy obligation. Out of sequence, these recommendations produce exactly what Nepal has produced for a decade: frameworks that exist on paper and fail in practice.

Immediate Priority: 0 to 6 Months (Stop The Bleed)

Nepal's National Cyber Security Centre currently operates with three engineers, no dedicated office space, and no legal authority over the agencies it is supposed to protect. The single most urgent action is giving the NCSC the legal mandate, staffing, and budget it requires following Rwanda's model of legal empowerment first, strategy second, deployment third.

Simultaneously, every active government portal must undergo mandatory security audit. Identity systems, financial platforms, electoral infrastructure, and border management cannot remain operational on unsupported frameworks. Any system found running obsolete software must be taken offline until upgraded there is no diplomatic justification for leaving documented vulnerabilities unpatched. Web application firewalls, HTTPS enforcement across all .gov.np domains, and multi-factor authentication are not aspirational targets. They are the floor. The NCSC must enforce them with penalties attached, not issue advisories into institutional silence.

Institutional Reform: 6 to 18 Months(Build the Response Capacity)

When Nepal's next major breach occurs and it will the international community will be watching how Nepal responds. Currently, that response is improvised, opaque, and slow. A functioning Government Computer Emergency Response Team, with defined authority and resources to serve agencies lacking in-house capacity, is not optional infrastructure. It is the institutional face Nepal presents to every bilateral partner after a crisis. Regular simulated incident drills, following Rwanda's National CyberDrill model with ITU support, must build the procedural muscle memory that effective crisis response requires before the crisis arrives.

The human layer is equally critical. The NCSC's 102-point advisory of January 2025 was not ignored because it was unclear. It was ignored because the people it was directed at lacked the

training and institutional culture to act on it. Mandatory cybersecurity awareness training for all government IT personnel structured, assessed, annually repeated, with consequences for non-completion is the only way to close that gap. Responsible disclosure frameworks with legal safe harbour provisions, and breach notification obligations with defined timeframes, must follow.

Strategic Framework: 18 Months and Beyond (Institutionalise the Gains)

Legislative progress without enforcement architecture is not progress. The IT and Cybersecurity Bill 2082 must be passed with financial penalties for institutional negligence, mandatory annual audits for critical infrastructure, and enforceable data protection obligations [4]. Rwanda's cybercrime law succeeded because it placed specific, verifiable obligations on critical infrastructure operators. Without that architecture, Nepal's Bill joins the Electronic Transactions Act of 2006 as a well-intentioned document institutions have no structural incentive to follow. Critically, the Bill must designate MoFA, the Office of the Prime Minister, and the National Intelligence Department as a priority protection tier institutions whose compromise carries foreign policy consequences that routine portals do not.

Nepal's most consequential near-term foreign policy move in this domain is formalising a bilateral cybersecurity cooperation agreement with India's CERT-In. The absence of a formal arrangement with Nepal's most significant neighbour is simultaneously a security gap and a missed diplomatic opportunity. A formalised partnership provides regional threat intelligence, incident response support, and technical capacity building while signalling to every other bilateral partner that Nepal is moving toward the governance standards credible digital cooperation requires. Concurrent engagement with ITU Asia-Pacific programmes and INTERPOL's cybercrime mechanisms builds the multilateral visibility small states cannot generate independently.

The workforce that sustains all of this does not yet exist at scale. Rwanda's national cybersecurity strategy addresses this from primary school to university level, recognising that the pipeline cannot be built through recruitment alone [9]. Nepal's IT programmes and polytechnic institutions must be formally engaged to develop a cybersecurity curriculum producing graduates capable of contributing to government security functions. The Ministries of Education and Communication must coordinate on this currently they do not, and that misalignment is itself a governance failure. A foreign ministry that depends on security-conscious staff cannot wait for the labour market to produce them by accident.

Cybersecurity reform pursued in this sequence is not a cost Nepal's foreign policy bears. It is a capacity Nepal's foreign policy requires.

NEPAL'S CYBERSECURITY REFORM ROADMAP

A TIERED POLICY FRAMEWORK FOR STRENGTHENING FOREIGN POLICY CAPACITY

Purpose: Secure Nepal's information environment to protect intelligence integrity, institutional credibility, and foreign policy autonomy.

TIER 1 IMMEDIATE PRIORITY 0 – 6 MONTHS

BUILD THE FOUNDATION. CLOSE THE MOST CRITICAL GAPS.

LEGAL EMPOWERMENT OF NCSC
- Grant NCSC legal authority, adequate staffing and budget.
- Empower to enforce standards across all agencies.

MANDATORY SECURITY AUDITS
- Audit all active government web portals.
- Prioritise identity, finance, election, immigration and border systems.
- Take unsupported systems offline until upgraded.

ENFORCE BASELINE PROTECTIONS
- Deploy Web Application Firewalls.
- Enforce HTTPS on all .gov.np domains.
- Mandate Multi-Factor Authentication.
- NCSC to enforce with penalties.

RISK-BASED PRIORITISATION
- Protect systems whose compromise has foreign policy and national security implications first.

TIER 2 INSTITUTIONAL REFORM 6 – 18 MONTHS

BUILD INSTITUTIONS, CAPACITY, AND ACCOUNTABILITY.

ESTABLISH GOVERNMENT CERT
- Create a national CERT with mandate, resources and authority.
- Provide centralised services to agencies lacking capacity.

MANDATORY CYBER AWARENESS TRAINING
- Annual training for all government IT personnel.
- Structured, assessed and documented.
- Completion tied to performance and compliance.

SIMULATE. PREPARE. RESPOND.
- Conduct regular simulated incident drills.
- Adopt Rwanda CyberDrill model with ITU support.
- Build procedural muscle memory for crisis response.

GOVERNANCE & TRANSPARENCY
- Establish responsible disclosure with legal safe harbour.
- Mandate breach notification within defined timeframes.
- Build transparency and international trust.

TIER 3 STRATEGIC FRAMEWORK 18 MONTHS AND BEYOND

INSTITUTIONALISE REFORM. BUILD RESILIENCE. STRENGTHEN FOREIGN POLICY.

ENACT & ENFORCE CYBERSECURITY LAW (BILL 2082)
- Pass IT & Cybersecurity Bill 2082 with strong enforcement.
- Impose financial penalties for negligence.
- Mandate annual security audits for critical infrastructure.

DESIGNATE PRIORITY PROTECTION TIER
- Designate MFA, Office of the PM, National Intelligence Dept. as priority protection tier.
- Apply higher security standards for systems with foreign policy impact.

REGIONAL & INTERNATIONAL COOPERATION
- Formalise bilateral cybersecurity cooperation with India's CERT-In.
- Engage ITU Asia-Pacific programmes.
- Collaborate with INTERPOL on cybercrime cooperation and intelligence sharing.

BUILD THE NATIONAL CYBER TALENT PIPELINE
- Partner with universities, polytechnics, and IT institutes.
- Develop cybersecurity curriculum at all levels.
- Align Ministry of Education and MoCIT for workforce development.

CYBERSECURITY AS FOREIGN POLICY CAPABILITY
- Treat cybersecurity reform as an instrument of foreign policy capacity.
- Strengthen credibility, trust, and diplomatic autonomy.

THE SEQUENCE MATTERS

LEGAL & INSTITUTIONAL AUTHORITY — Establish mandate and accountability → POLICY & STANDARDS — Define requirements and frameworks → CAPACITY & TOOLS — Build skills, deploy technology → ENFORCEMENT & OVERSIGHT — Monitor, audit, and apply consequences → RESILIENCE & TRUST — Secure systems, strengthen nation.

> *A secure information environment is the foundation of credible diplomacy.*
> *A secure Nepal strengthens regional stability and global trust.*

CROSS-CUTTING PRINCIPLES

- LEGAL AUTHORITY BEFORE ACTION
- ENFORCEMENT BEFORE COMPLIANCE
- CAPACITY BEFORE OBLIGATION
- TRANSPARENCY BEFORE TRUST
- SECURITY BEFORE DIGITAL EXPANSION

OUR MODEL: LEARN. ADAPT. IMPLEMENT.

RWANDA
Authority first, Strategy second, Implementation third.

ESTONIA
Plan before crisis, Communicate clearly, Innovate continuously.

NEPAL
Secure to lead.
Secure to negotiate.
Secure to influence.

EXPECTED OUTCOMES

- Protect intelligence integrity
- Strengthen institutional credibility
- Enhance national security
- Build digital trust with partners
- Increase foreign policy autonomy

THE BOTTOM LINE

Cybersecurity reform pursued in the right sequence is not a cost Nepal's foreign policy bears—it is a capacity Nepal's foreign policy requires.

8. CONCLUSION

Nepal's digital government is not failing because its adversaries are sophisticated. It is failing because its foundations are insecure, its oversight is fragmented, its enforcement mechanisms are toothless, and its resource allocation has not kept pace with its ambitions. These failures compromise the intelligence environment in which foreign policy decisions are made, expose diplomatic communications and institutional processes to adversarial collection, and erode the governance credibility on which bilateral partnerships and regional diplomatic standing depend. The 1,500 government websites taken offline in January 2023, the two million citizenship records placed for sale in April 2025, the Prime Minister's Office portal breached on obsolete software while decision-makers remained unaware these are governance failures. Governance failures can be corrected. The question is not whether Nepal can afford to act. It is whether Nepal's foreign policy can afford continued inaction.

For Nepal's Ministry of Foreign Affairs specifically, the stakes of continued inaction are not abstract. Every unpatched portal, every unenforced authentication requirement, and every breach met with institutional silence is a concession made without negotiation to every foreign actor with an interest in knowing what Nepal knows, what Nepal is deciding, and what Nepal can be pressured to accept.

REFERENCES

[1] Government of Nepal, Electronic Transactions Act, 2063 (2006), Kathmandu, Nepal, 2006.

[2] Government of Nepal, Individual Privacy Act, 2075 (2018), Kathmandu, Nepal, 2018.

[3] Ministry of Communication and Information Technology, Government of Nepal, National Cyber Security Policy 2023, Kathmandu, Nepal, 2023.

[4] Government of Nepal, Information Technology and Cybersecurity Bill, 2082 (Draft), Kathmandu, Nepal, 2025.

[5] Ministry of Communication and Information Technology, Government of Nepal, Digital Nepal Framework, Kathmandu, Nepal, 2019.

[6] International Telecommunication Union (ITU), Global Cybersecurity Index 2020, Geneva, Switzerland, 2021.

[7] Nepal Police Cyber Bureau, Annual Cybercrime Statistics Report 2024, Kathmandu, Nepal, 2024.

[8] OWASP Foundation, OWASP Top 10: Web Application Security Risks, 2021.

[9] Ministry of ICT and Innovation, Republic of Rwanda, Rwanda National Cybersecurity Strategy 2024–2029, Kigali, Rwanda, 2024.

[10] Business360 Nepal, “Nepal’s Digital Collapse: The Government’s Cyber Crisis and Path toRecovery,” 2025.

[11] National Cyber Security Centre, Government of Nepal, *Cybersecurity Advisory for Government Agencies*, Kathmandu, Nepal, January 2025.