Infrastructure–Governance Asymmetry and Cybersecurity Exposure in Nepal's E-Governance: A South Asian Comparative Study

Ganesh Bhusal

Softwarica College of IT & E-Commerce, Kathmandu, Nepal

DOI: https://doi.org/10.47772/IJRISS.2026.101000605

Received: 26 October 2026; Accepted: 31 October 2026; Published: 12 November 2026

ABSTRACT

E-governance is expanding rapidly across South Asia, but building digital infrastructure does not automatically build the capacity to secure it. This study examines Nepal's record on the United Nations E-Government Development Index (EGDI) from 2003 to 2024, compares Nepal with the seven other South Asian states using a single source, and tests those trends against the International Telecommunication Union's Global Cybersecurity Index (GCI) 2024 and six reported security incidents affecting Nepal's government systems between 2020 and 2026, each graded for evidential strength. Between 2020 and 2024, Nepal's Telecommunication Infrastructure Index rose about 63 percent while its E-Participation Index fell about 41 percent, even as overall EGDI rose about 23 percent. We term this gap infrastructure–governance asymmetry; it is wider in Nepal than in the two regional peers examined. Nepal's GCI Legal Measures score (19.21 of 20) is among the region's strongest, but its Technical (11.09) and Cooperation (9.45) scores are its weakest, so the binding constraint is technical and operational capacity rather than law. Pakistan scores near the GCI maximum while ranking second-lowest on EGDI, a warning against treating commitment scores as proof of security. A state-owned enterprise has also begun building government systems with AI assistance in hours rather than weeks; no public evidence shows this has caused harm, and we do not claim it has. Nepal's October 2026 PHP2Shell response is analysed as an illustrative case of shared-platform exposure, not as confirmed exploitation.

Index Terms—AI-assisted development, cybersecurity governance, e-governance, EGDI, Global Cybersecurity Index, Nepal, South Asia

INTRODUCTION

E-government means using information and communication technology (ICT), the internet and web platforms to deliver public services, improve transparency and involve citizens. It is usually described through four interaction models: government-to-citizen (G2C), government-to-business (G2B), government-to-employee (G2E) and government-to-government (G2G) [1]. Governments across South Asia have taken up e-governance to improve services, reduce corruption and meet transparency goals under the Sustainable Development Goals. Nepal's digital history is longer than it is often given credit for. The National Computer Centre was set up in 1974. The first Information Technology Policy came in 2000, alongside an E-Government Master Plan prepared with the Korea IT Industry Promotion Agency [1]. More recently the effort has been consolidated under the Digital Nepal Framework (2019) and the Nagarik App, a single citizen-services platform run by the National Information Technology Center (NITC) that holds identity, tax, vehicle and civil-registration records. Individual agencies have also digitised their own functions separately: online PAN registration at the Inland Revenue Department, personal records at the Election Commission, a data centre at the Supreme Court, an online gate-pass system at NITC, online tendering at the Department of Roads, and computerised citizenship records under the Ministry of Home Affairs [1]. This fragmented, agency-by-agency pattern matters for the argument developed below. Nepal is a useful case for this kind of study. It is landlocked and mountainous, and has been federal since 2015, with power divided across federal, provincial and municipal tiers [1]. Its literacy rate was 76.3 percent in 2023 [1], which is low for a country pushing citizen-facing digital services. At the same time Nepal has made real gains in telecommunications. This combination of fast infrastructure growth

and slower institutional growth is what the study examines. Most of the incidents discussed later fall in the G2C category, where privacy and fraud risk lands most directly on individuals. A growing regional literature makes a similar point: in developing countries, digital services tend to expand faster than the capacity to secure them [2], [3]. This study asks whether that pattern appears in Nepal's own data, and whether documented security incidents match it. It does not claim that falling institutional or participation scores cause security failures. It shows an association, and a structural mismatch, between how fast infrastructure grows and how fast the capacity to govern it grows. The incident evidence is gathered separately and read alongside the index data, not derived from it.

The study addresses three research questions:

1. Does Nepal's EGDI sub-index data from 2003 to 2024 show infrastructure growing faster than governance and human-capital measures, and how does this compare with other South Asian states?
2. Do independently reported security incidents in Nepal's government systems fit the same pattern?
3. What governance measures follow directly from these findings?

RELATED WORK

Civil-Service and Governance-Model Studies

Abdulnabi [2] examined how developing countries implement e-governance through their civil-service models. The study found the same barriers recurring across contexts: limited digital infrastructure, weak institutional skills and cybersecurity threats. It also reported that user-credential security is often not kept to an acceptable standard, and argued that formal security policies and tested incident-response processes are preconditions for dependable e-government.

Country Studies

Nazuk et al. [3] studied e-governance in Pakistan using interviews and survey data. They found poor internet infrastructure, an underdeveloped cybersecurity framework, and language and digital-literacy gaps acting as linked constraints. Pakistan is the closest structural comparator to Nepal in the region: both face infrastructure limits alongside security weakness, and both are under-studied relative to high-income countries.

Nepal-Specific Work

Chalaune [1] reports the same EGDI, OSI, TII and HCI figures for Nepal used here, drawn from the same UN source, and identifies Nepal's main e-governance barriers as low literacy, a shortage of skilled staff, political instability, weak coordination between agencies and poor infrastructure outside the cities. It is the closest Nepal-specific peer-reviewed treatment available, and its independently compiled tables match this study's figures. Its barrier analysis, however, contains no security dimension. Literacy, human capital and coordination are treated purely as service-delivery problems, with nothing on data protection, past breaches or security governance. This study fills that gap by reading the same trajectory as a security-governance indicator.

Systematic and Bibliometric Work

Mushtaq and Shah [4] reviewed e-government cybercrime research published between January 2015 and January 2025, covering 3,790 studies from Web of Science and Scopus. Of 88 security-related studies, only 19 dealt specifically with cybersecurity in e-government services. They called for more work on management-level practice rather than purely technical fixes, a direction this study follows. Taken together, these studies leave the security side of Nepal's e-governance largely unexamined.

CONCEPTUAL FRAMEWORK

A simple comparison of infrastructure growth against one participation score captures part of the picture but oversimplifies it. Two countries can reach similar infrastructure levels and still end up in very different

security positions, depending on whether governance, skills and day-to-day detection capacity grow at the same rate [2], [4]. What matters is not income level or infrastructure score alone, but the alignment between how fast digital services expand and how fast the capacity to govern and secure them grows. This study therefore treats infrastructure–governance asymmetry as the visible sign of a broader digital expansion–capacity alignment relationship. When expansion outpaces governance and operational security capacity, exposure rises and resilience falls. Fig. 1 shows this, with the dashed path representing the capacity gap. The framework has four dimensions. Dimensions 1 and 2 are measured directly with EGDI data. Dimension 3 is partly measured using the GCI Technical and Cooperation pillars and supported by the incident evidence, because detailed operational figures such as SOC or CSIRT response times are not published for Nepal.

a. Digital expansion (TII, OSI). The scale and depth of digital-government development, measured through the Telecommunication Infrastructure Index and the Online Service Index.

b. Institutional and human governance capacity (HCI; GCI Legal, Organizational and Capacity Development pillars). Governance structures, policy, enforcement and skills, measured through HCI together with the matching GCI pillars [5], which score national strategy, legal instruments and institutional mandates directly.

c. Operational security capacity (GCI Technical and Cooperation pillars). The practical ability to prevent, detect and respond to incidents. By ITU's own account the GCI pillars measure commitment rather than performance, so this dimension is also supported by whether each incident was found internally or by an outsider.

d. Security outcome. The real balance between exposure and resilience, observed here through the incident record rather than any composite score, in line with ITU's caution that commitment scores should sit alongside outcome evidence, not replace it.

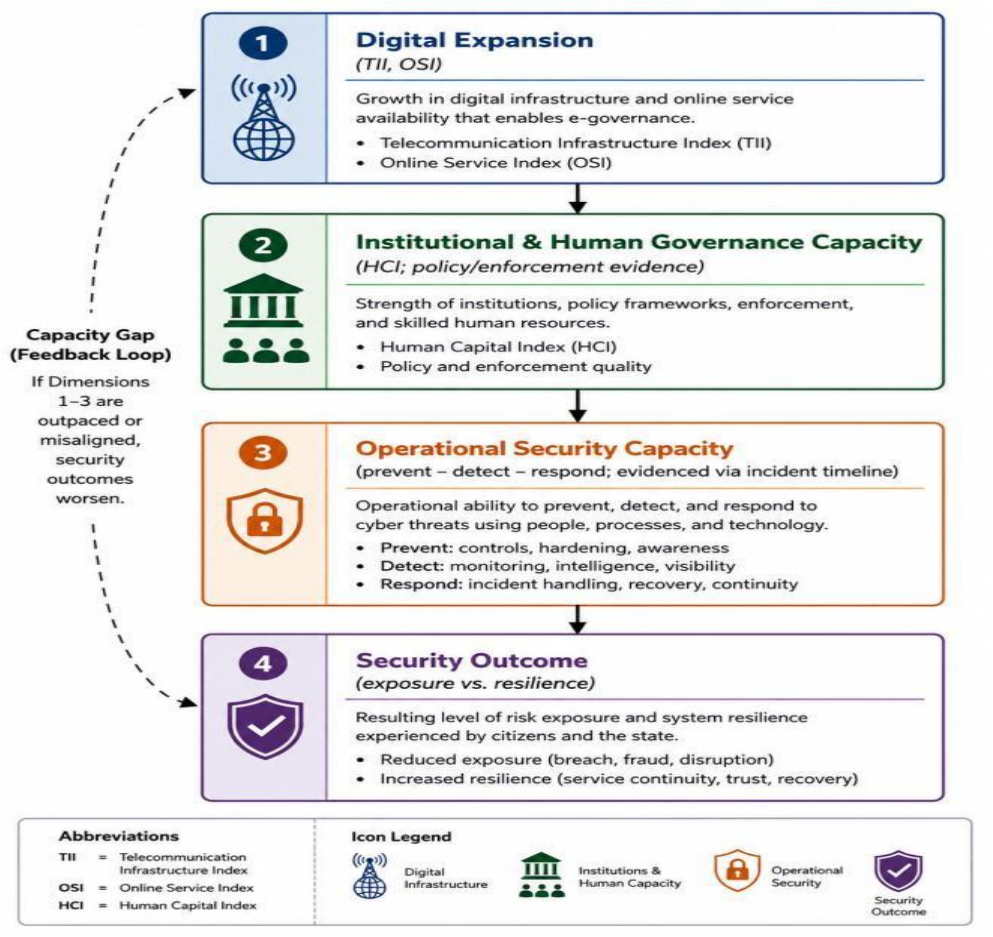

Fig. 1. Digital expansion–capacity alignment framework. Solid arrows show the main expansion-to-outcome path. The dashed arrow shows the capacity gap: when Dimension 1 grows faster than Dimensions 2 and 3, exposure rises and detection shifts from internal to external.

The mechanism at the centre is a capacity gap. When digital expansion grows faster than governance and operational capacity, exposure rises and detection moves outside the institution. This is treated as a conceptual relationship, not a quantity to be calculated. The index data (Tables I–III) and the incident record (Table VI) are used to ask whether Nepal's data is consistent with a widening gap, not to measure the gap directly.

The model is not only about Nepal. In digitally mature countries, expansion usually comes with regulatory enforcement, independent audit and a standing incident-response function, which is why similar infrastructure growth does not produce similar exposure. In many developing countries the literature describes infrastructure running ahead of the skills and enforcement needed to secure it [1], [2]. The framework does not assume that developing countries are unsafe and developed ones safe. It explains differences through alignment, which is also why India and Bhutan, both richer and higher on EGDI, show the same directional pattern rather than escaping it.

One caution concerns the E-Participation Index (EPI). EPI measures online citizen-participation mechanisms [6], not cybersecurity governance, and it is not used here as Dimension 3 evidence. Its role is limited to Dimension 2, next to HCI, and it is read beside the incident evidence rather than merged with it. A falling EPI is not read as falling security capacity; it is one input among several supporting the broader point that institutional capacity is not keeping pace with infrastructure.

METHODOLOGY

This is a desk study using secondary data, with descriptive and comparative analysis. No interviews, surveys or system testing were carried out.

Index Data

All EGDI, OSI, LOSI, TII, HCI and EPI values come from one primary source: the United Nations E-Government Survey 2024 [6], specifically its country annex table. Nepal's time-series figures were cross-checked against the UN E-Government Knowledgebase [7] and against the independently compiled tables in Chalaune [1]; all three agree to four decimal places on every value checked. Taking every country's figures from one table, rather than mixing press reports that round differently or cite different survey years, removes the rank and value inconsistencies that appear when sources are mixed.

Cybersecurity Commitment Data

To give Dimensions 2 and 3 something firmer than qualitative description, the study also uses the ITU Global Cybersecurity Index 2024 [5]. The GCI scores national cybersecurity effort across five pillars (Legal, Technical, Organizational, Capacity Development and Cooperation), each out of 20, combined into a score out of 100 and a five-level tier from T5 (Building) to T1 (Role-modelling). Pillar scores and tiers for all eight South Asian states were taken directly from the report's country-profile pages.

ITU states plainly that the GCI measures commitment, not verified results, and is meant to complement rather than replace outcome-based measures such as incident counts [5]. This study follows that instruction: the GCI is treated as commitment-side evidence, and the incident record in Table VI is treated as a separate outcome-side check. The 2024 edition is ITU's most recent at the time of writing; the sixth-edition questionnaire was under internal approval as of mid-2026.

How Incidents Were Selected

An incident was included only if it met all four of the following conditions. First, it occurred between 2020 and 2026, covering Nepal's most recent expansion phase. Second, it affected a government-run or government-mandated platform, not a purely private breach.

Third, at least one detailed public account described what happened. Fourth, it was checked against the number of independent outlets reporting it and assigned an evidence rating of High, Medium or Low. Incidents supported by only one source are rated Low or Medium and flagged; none are presented as equally certain.

Sources Considered and Left Out

Nepal Rastra Bank (NRB) and the Commission for the Investigation of Abuse of Authority (CIAA) were considered but left out of the incident evidence. NRB publishes payment-system and financial-stability data but does not disclose bank-level security incidents, and CIAA reporting covers corruption rather than security governance.

Publications of the Ministry of Communication and Information Technology and NITC were used only for policy background, since they do not publish security audits or breach reports.

Contemporary Illustrative Case

The October 2026 PHP2Shell event is analysed separately from the historical incident sample. Public reporting documents vulnerability disclosure, precautionary shutdowns, patching and restoration, but does not establish successful exploitation or a resulting government data breach in Nepal.

The event is therefore used to examine shared-platform dependency and service-continuity implications and is not counted as a confirmed security incident in Table VI.

RESULTS

Nepal's EGDI Record, 2003–2024

Table I sets out Nepal's EGDI and sub-index values across selected survey years, and Table II gives the percentage change in each component between 2020 and 2024.

TABLE I NEPAL EGDI AND SUB-INDEX VALUES, SELECTED YEARS

Year	EGDI (Rank)	OSI	TII	HCI	EPI (Rank)
2016	0.3458 (135)	0.3986	0.1675	0.4714	0.5085 (89)
2018	0.4748 (117)	0.6875	0.2413	0.4957	0.7809 (55)
2020	0.4699 (132)	0.4000	0.4691	0.5405	0.3690 (137)
2022	0.5117 (125)	0.4592	0.5123	0.5636	0.2386 (143)
2024	0.5781 (119)	0.4481	0.7653	0.5210	0.2192 (152)

Source: [6], [7]. Ranks are out of 193 states.

TABLE II PERCENTAGE CHANGE IN NEPAL'S EGDI COMPONENTS, 2020–2024

Indicator	2020	2024	Change
EGDI	0.4699	0.5781	+23.0%
Telecom. Infrastructure Index	0.4691	0.7653	+63.1%
Online Service Index	0.4000	0.4481	+12.0%
Human Capital Index	0.5405	0.5210	−3.6%
E-Participation Index	0.3690	0.2192	−40.6%

Computed from [6], [7].

Telecommunications infrastructure grew almost three times as fast, in percentage terms, as overall EGDI over the same period, while the human-capital and participation measures moved the other way. This is the quantitative core of the asymmetry examined here.

Table III compares Nepal with two regional peers over the same period.

TABLE III TII and EPI Change, 2020–2024, Three Countries

Country	TII 2020	TII 2024	TII Δ	EPI 2020	EPI 2024	EPI Δ
Nepal	0.4691	0.7653	+63.1%	0.3690	0.2192	−40.6%
India	0.3515	0.5700	+62.2%	0.8571	0.6575	−23.3%
Bhutan	0.5367	0.8170	+52.2%	0.6310	0.4932	−21.8%

Source: [6], [7]; changes computed from the tabulated values.

Two things stand out. The Telecommunication Infrastructure Index has risen in every survey round since 2016, by about 63 percent between 2020 and 2024 alone. The E-Participation Index has fallen in every survey round since its 2018 peak of 0.7809 (rank 55), down to 0.2192 (rank 152) in 2024. The pattern is not unique to Nepal: India and Bhutan move in the same direction over the same years. But Nepal's EPI decline is the steepest of the three in proportional terms.

South Asian Comparison

Table IV gives the full 2024 sub-index comparison across all eight South Asian states, taken from one source.

TABLE IV EGDI 2024, SOUTH ASIA, FULL SUB-INDEX COMPARISON

Country	EGDI	Rank	OSI	LOSI	TII	HCI	EPI	Inc.
Maldives	0.6745	94	0.6220	0.3750	0.7886	0.6130	0.4795	UMC
India	0.6678	97	0.8184	0.5625	0.5700	0.6149	0.6575	LMC
Sri Lanka	0.6667	98	0.5494	0.3021	0.7936	0.6570	0.4110	LMC
Bangladesh	0.6570	100	0.7374	0.3854	0.6501	0.5834	0.6164	LMC
Bhutan	0.6511	103	0.5886	0.5000	0.8169	0.5478	0.4932	LMC
Nepal	0.5781	119	0.4481	0.4583	0.7653	0.5210	0.2192	LMC
Pakistan	0.5096	136	0.7042	0.2500	0.4745	0.3500	0.4932	LMC
Afghanistan	0.2083	188	0.1438	0.3438	0.2167	0.2643	0.1096	LIC

Source: [6], annex table. Unweighted mean EGDI across the eight states: 0.5766. Rank is out of 193. Inc. = income group: LIC = low income; LMC = lower-middle income; UMC = upper-middle income. Nepal ranks sixth of eight, below the eight-country mean and ahead only of Pakistan and Afghanistan. Two further points emerge. First, Nepal's OSI of 0.4481 is the lowest among the region's lower-middle-income states, below both Pakistan (0.7042) and Bangladesh (0.7374), even though Nepal's overall EGDI is higher than Pakistan's. Nepal's regional standing therefore rests mostly on infrastructure, not on service quality. Second, Nepal's EPI of 0.2192 is the second lowest of the eight, above only Afghanistan's 0.1096. Afghanistan's value fits its low EGDI overall, whereas Nepal's EPI is unusually low given its EGDI and TII position.

Cybersecurity Commitment: GCI Results

Table V gives each South Asian state's ITU GCI 2024 pillar scores, total and tier.

TABLE V ITU Global Cybersecurity Index 2024, South Asia

Country	Legal	Tech.	Org.	Cap.	Coop.	Total	Tier
India	20	20	18.49	20	20	98.49	T1
Bangladesh	17.44	20	20	19.52	20	96.96	T1
Pakistan	20	18.21	20	20	18.48	96.69	T1
Sri Lanka	19.21	20	16.42	17.11	14.28	87.02	T2

Nepal	19.21	11.09	16.92	13.09	9.45	69.76	T3
Bhutan	14.18	16.43	13.14	9.71	7.15	60.61	T3
Afghanistan	5.81	3.29	6.99	2.32	0	18.41	T5
Maldives	4.52	0	4.88	3.16	2.26	14.82	T5

Source: [5], country-profile pages. Pillars: Legal; Technical (Tech.); Organizational (Org.); Capacity Development (Cap.); Cooperation (Coop.). Each pillar is scored out of 20; total out of 100. T1 = Role-modelling, T2 = Advancing, T3 = Establishing, T5 = Building.

Two findings stand out, and the second is an anomaly worth stating rather than smoothing over. First, Nepal's own profile is lopsided. Its Legal Measures score of 19.21 out of 20 sits near the regional ceiling, level with Sri Lanka and behind only India and Pakistan, and ITU lists it as an area of relative strength alongside Organizational Measures at 16.92 [5]. By contrast, Nepal's Cooperation (9.45) and Technical (11.09) scores are its two weakest pillars, and together with Capacity Development (13.09) are flagged by ITU as areas for growth [5]. This sharpens the policy–enforcement gap argued elsewhere in this paper: Nepal's formal legal commitment is comparatively strong, while its practical and cooperative capacity to act on that commitment is comparatively weak.

Second, and more importantly, the GCI ranking does not follow the EGDI ranking. Pakistan is the clearest case: it ranks 136th of 193 on EGDI and seventh of eight in the region, yet third of eight on the GCI, at 96.69 and Tier T1, above Sri Lanka, Nepal and Bhutan, all of which are well ahead of it on EGDI. Bangladesh shows a milder version of the same thing, with a GCI score of 96.96 against a mid-table EGDI rank. This is not a data error. It reflects what the two indices measure. EGDI captures realised digital-service development; the GCI captures stated cybersecurity commitment, and ITU is explicit that commitment scores complement rather than replace outcome measurement [5]. A country can score near the maximum on the GCI's Legal, Organizational and Capacity Development pillars, as Pakistan does, without that implying a mature digital-government footprint or a low rate of real incidents. This study therefore treats the GCI as evidence of stated commitment only, and relies on the incident record in Table VI for evidence of what actually happened.

Security Incidents

Table VI sets out the incident record built using the criteria described earlier. Each entry is graded for evidential strength using the criteria in the table note; entries that could not meet the minimum bar were removed rather than retained with a caveat, and the removals are reported below.

TABLE VI REPORTED SECURITY INCIDENTS AFFECTING NEPAL'S GOVERNMENT SYSTEMS, 2020–2026

Date	System	Type	Summary	Evidence
Apr 2020	Vianet Communications	Data exposure	Breach exposing roughly 160,000–170,000 customer records; confirmed by the company and investigated by Nepal Police's Cyber Bureau [8]	High
Jan 2023	Government Integrated Data Centre	Denial of service	Distributed denial-of-service attack on the government's only central data centre knocked out most ministry websites and the immigration and passport databases for about four hours. Immigration desks at the international airport went out of action and several international flights were delayed by up to three hours [9]	High
Jan 2025	Ministry of Federal Affairs and General Administration	Unauthorised access	The group FunkSec advertised super-admin access to four government portals covering budget and municipal records; the ministry spokesperson stated he was unaware of the breach [10]–[12]	Medium
Jan 2025	Government-wide	Policy response	National Cyber Security Centre issued a 102-point advisory mandating updates, multi-factor authentication and network segmentation; compliance reported as inconsistent [10]	Medium

Feb 2025	Koshi Provincial Government	Unauthorised access	A group calling itself "YNR" accessed 21 subdomains under the provincial government domain [13]	Medium
Apr 2025	Nepal Police Headquarters	Data exposure	The group "Kaju" claimed citizenship records for about two million citizens, offered online for USD 7,000 [13], [14]	High
2026	Nagarik App web portal	Impersonation	Unauthorised clone of the government portal on a third-party domain; the platform holds citizenship, passport, PAN and education records [13]	Medium

Evidence: High = detailed first-hand reporting in a mainstream national newspaper, or corroboration by two or

more independent outlets, or confirmation by the affected institution. Medium = at least two independent sources, of which at least one is a specialist security outlet or a breach-tracking database

Two exclusions are reported rather than buried. A researcher's vulnerability assessment of a government platform, published in mid-2026, could not be corroborated by any second source and was removed. Separately, several secondary sources describe a denial-of-service attack on more than 400 government websites in March 2025, in terms nearly identical to the January 2023 event reported in detail at the time [9]. Treating these as two events would double-count, so the date conflict is recorded as a data-quality problem in Nepali cyber-incident reporting, itself a finding in a literature that depends heavily on such reporting. What matters here is less the count than the discovery route. The January 2023 outage announced itself: a national outage is visible immediately and does not test internal monitoring. Setting that aside, every remaining incident came to light through an external party rather than internal monitoring: a security researcher, a breach-tracking service, a group advertising stolen data, or a newspaper. In the FunkSec case the responsible ministry's own spokesperson stated he was unaware of the breach [11]. Most recently, Nepal identified 135 compromised government email accounts, spanning the Office of the Prime Minister and the ministries of Home Affairs, Finance and Foreign Affairs, only after becoming the 47th government worldwide to join the external breach-tracking service Have I Been Pwned [15], [16]. Detection is not merely externalised case by case; the capability itself is being procured from outside.

DISCUSSION

The Asymmetry, Restated

The results show, from one consistent source, that Nepal's infrastructure growth (TII +63.1 percent, 2020–2024) clearly outpaces growth in institutional and participation measures (EPI −40.6 percent, HCI −3.6 percent), and that this is sharper in Nepal than in the two regional comparators. This matches Chalaune's independent finding that Nepal is strong on telecom infrastructure but behind regionally on service quality and human capital [1], and extends it by reading the same divergence as a security matter rather than only a service-delivery one.

Policy Without Enforcement

Nepal has had IT policy since 2000 and issued a detailed 102-point advisory in January 2025. That fits Abdulnabi's broader finding that security policy documents often exist without matching enforcement capacity [2]. The GCI data in Table V puts firmer numbers on this: a Legal Measures score near the regional ceiling sitting next to Technical and Cooperation scores that rank in the lower half of the region. The gap is not between having policy and lacking it, but between policy and the capacity to act on it. This also echoes Chalaune's point about weak coordination between agencies [1], now grounded in an independent international index rather than Nepal-specific reporting alone.

Detection From Outside

Across the incidents in Table VI, discovery came from outside rather than from internal monitoring. This is offered as case evidence consistent with the fourth dimension of the framework, not as proof, given the evidence limits already stated. It aligns with Mushtaq and Shah's observation that management-level

mitigation is under-represented in e-government research [4], and with Nepal's low GCI Technical and Cooperation scores. A state with a weak technical and cooperation footprint is less likely to catch incidents itself, and the record bears that out. The Have I Been Pwned case reported in Section V-D extends this further: detection was not merely externalised in a particular incident but procured as a capability from outside the state.

Emerging Risk: AI-Assisted Development

One development is unfolding as this paper is written and bears directly on the argument. Nepal's digital expansion is accelerating again through AI-assisted "vibe coding", where software is generated from plain-language prompts rather than built through conventional development practice. Nepal Telecom, a state-owned enterprise, has confirmed building roughly half a dozen working internal systems this way in hours to days, including procurement, workflow and meeting-management portals, with a ticketing system, customer-care portal and billing system in progress [17]. The practice is reported as spreading across government offices and private firms alike [18]. The government's own position deserves fair statement, because it is not that review is absent. An official described the workflow as using AI to produce an initial code structure which the technical team then modifies and tests against government requirements, stating: "We do not build systems blindly" [18]. This paper takes that at face value as a description of intent. What is not publicly available is any account of what that review consists of, who performs it, against what standard, or whether it is documented. That is the distinction between a review practice and review assurance, and it is a governance question rather than a technical one. Concern about the practice comes from the responsible national authority itself, not only from outside commentators. The National Cyber Security Centre reports that it has intensified vulnerability assessment and penetration testing (VAPT), auditing approximately 40 government systems in the preceding three to four months, and its director states that rapid AI adoption has introduced new security blind spots, particularly where agencies build portals without understanding the underlying encryption [15], [16]. His formulation concedes the governance problem directly: AI tools have made development fast and accessible, but those using them often do not know how secure the resulting systems are [15]. A named Nepali practitioner quoted separately makes the same trade-off explicit, observing that because the objective of these tools is task completion, less attention is paid to security when working at speed [18]. This mirrors, from domestic sources, what the international literature has reported about AI-generated code and the confidence of those deploying it [19], [20]. Table VII assembles this evidence and states, for each item, what it does and does not support.

TABLE VII EVIDENCE ON AI-ASSISTED DEVELOPMENT AND GOVERNANCE RISK IN NEPAL

Source	Observation	What It Supports
Nepal Telecom [17], [18]	Several internal systems developed with AI assistance in hours to days	Adoption is real and at production scale in a state-owned body
Government official [18]	AI produces an initial structure; technical team modifies and tests it	A review practice is claimed; its form, standard and documentation are not public
NCSC director [15], [16]	VAPT completed on approximately 40 government systems in three to four months	Assurance capacity exists and is expanding, at a measurable rate
NCSC director [15]	AI adoption creating security "blind spots"; portals built without understanding encryption	The responsible national authority itself identifies a review and skills gap
Named practitioner [18]	At speed, less attention is paid to security	Domestic expert concern, consistent with international findings
Municipal data exposure [21]	Citizen data left publicly accessible; attributed by an expert to the practice	One attributed case, single outlet; illustrative, not demonstrative
Independent assessment	No public security assessment of any named AI-developed government system exists	Causal impact is unproven and is not claimed here

Adoption is well documented, and official concern is on the record. What is missing is any public assessment linking a named AI-developed government system to a specific weakness and a measurable consequence. We therefore make no causal claim: the evidence does not show that AI-assisted development has caused a cybersecurity incident in Nepal. It shows only that AI-assisted government software production and official concern about assurance, encryption, dependency management and human oversight have emerged at the same time.

What matters for governance is whether security review is keeping pace with software production, which is the same asymmetry measured elsewhere in this paper, now at the level of software delivery. If development speed rises faster than review capacity, AI-assisted development may widen the capacity gap. The NCSC's figure of roughly 40 systems audited in four months is the only public measure of assurance throughput, and so the one benchmark against which production speed could be compared.

What the Data Does Not Show

The data do not support a statistical or causal link between index scores and incident frequency. Six incidents is too small a sample, and the evidence behind them is uneven. A strong GCI score does not show that a country has few incidents either, and Pakistan is the counter-example. Where the three bodies of evidence disagree, as they do for Pakistan, we report the disagreement rather than smooth it away.

Reading Commitment Indices Critically

The Pakistan and Bangladesh results caution against taking commitment indices at face value, Nepal's included. Both score near the GCI maximum yet rank no higher than mid-table on EGDI (Pakistan seventh, Bangladesh fourth of eight). A high GCI score shows that a country has formally committed to protecting its systems, largely through legal and organisational instruments that cost far less to pass than the capacity to operate them; it does not show that the systems are well protected. A future GCI edition could show Nepal's Legal score rising while its Technical score stays flat, which would widen the gap described here.

Regional Context

All eight South Asian states in Table IV are lower-middle-income or low-income, except the Maldives. That shared profile matters. Nepal's institutional lag is unlikely to be a uniquely Nepali failure, given that India and Bhutan show the same direction of travel. This supports reading the asymmetry as a regional structural feature tied to shared income and administrative constraints, and strengthens the case for the regional-cooperation recommendation in Table IX.

Emerging Systemic Exposure: The October 2026 PHP Vulnerability

Nepal's response to the PHP2Shell vulnerabilities in October 2026 provides a contemporary illustration of systemic exposure arising from shared digital infrastructure. On 21 October 2026, the PHP project disclosed two critical vulnerabilities, CVE-2026-109618 and CVE-2026-109619, and released fixed PHP versions. International technical advisories described the vulnerabilities as potentially enabling unauthenticated remote code execution in affected PHP installations [22], [23]. In Nepal, government agencies temporarily took websites and selected online services offline as a precaution while technical teams assessed exposure and applied updates. Reporting identified the Government Integrated Website Management Information System (GIWIMS) as a shared platform supporting thousands of government websites. The Software Development and Operation Centre reported central patching and gradual restoration; some vendor-managed sites and services remained unavailable during the restoration period [24], [25]. Other reported suspensions included Nepal Rastra Bank's website and the Vehicle Consignment Tracking System [24].

The episode illustrates how a vulnerability in a widely deployed software runtime can create correlated exposure across multiple institutions that share a platform or technology dependency. Centralisation can simplify standardisation and coordinated remediation, but it also means that a common weakness may require simultaneous risk decisions across many services. The temporary withdrawal of public-facing websites

demonstrates an availability and continuity impact even where precautionary shutdowns prevent or reduce the opportunity for exploitation. Nepali officials quoted in contemporaneous reporting stated that no unauthorised access or cyberattack linked to the PHP issue had been identified in Nepal at that time [24]. The event must therefore not be characterised as a confirmed breach (Table VIII). The restoration process also highlights operational governance questions: whether agencies maintain an accurate inventory of software versions and dependencies; whether patching responsibilities are clearly divided between central platform operators, agencies and vendors; whether legacy systems can be upgraded promptly; and whether security testing and source-code review are completed before services return online. These observations are consistent with the paper's broader argument that digital service expansion must be accompanied by operational assurance, coordinated vulnerability management and tested recovery arrangements. The case is illustrative rather than causal evidence of the EGDI–GCI relationship.

TABLE VIII OCTOBER 2026 PHP VULNERABILITY AND GOVERNMENT SERVICE DISRUPTION IN NEPAL

Dimension	**Evidence**
Disclosure period	21 October 2026; response and restoration reported during 21–26 October 2026
Vulnerability identifiers	CVE-2026-109618 and CVE-2026-109619 (PHP2Shell)
Affected technology	PHP runtime; fixed releases are specified in the PHP security advisory [22]
Shared infrastructure	Government Integrated Website Management Information System (GIWIMS) and associated government portals [24], [25]
Government response	NCSC advisory, precautionary shutdowns, technical assessment, patching and staged restoration [24], [25]
Reported service impact	Temporary unavailability of government websites and selected online services; restoration proceeded in stages [24], [25]
Confirmed exploitation in Nepal	No unauthorised access or cyberattack linked to this issue had been reported by Nepali officials at the time of the cited report [24]
Confirmed data breach	The reviewed reports do not establish a PHP2Shell-related government data breach in Nepal
Research significance	Illustrates common software dependency, correlated exposure, patch-coordination requirements and service-continuity risk

RECOMMENDATIONS

Table IX maps each recommendation to a specific finding rather than offering general security advice. To operationalise these recommendations, Fig. 2 presents a governance-led cybersecurity lifecycle that links central accountability with asset visibility, continuous assurance, secure change, and incident response and service resilience.

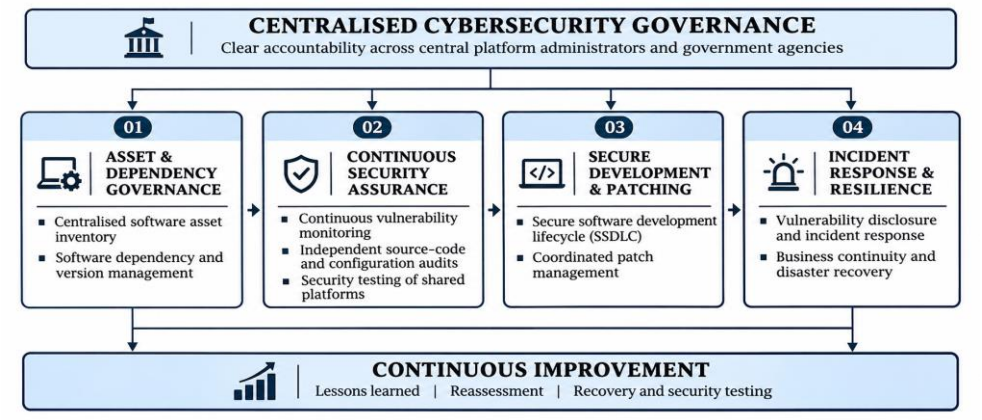

Fig. 2. Governance-led cybersecurity lifecycle framework for Nepal's government digital infrastructure.

TABLE IX FINDINGS MAPPED TO GOVERNANCE RECOMMENDATIONS

Finding	Weakness Implied	Recommendation
Incidents were found by outsiders, not internally	Weak continuous monitoring of government platforms	Require continuous, government-run security monitoring on flagship platforms, with a defined internal detection standard
EPI fell 40.6% while EGDI rose 23%	Oversight and participation not scaling with infrastructure	Tie future infrastructure budgets to published, parallel investment in oversight and participation mechanisms
HCI slipped slightly while TII rose 63%	Skills base not scaling with technical infrastructure	Fund public-sector cybersecurity workforce development specifically, not generalist ICT training
A 102-point advisory was issued but uptake is inconsistent	Policy without verification or consequence	Set up recurring independent third-party audit of flagship platforms, with remediation timelines published
Legal score near regional ceiling; Technical and Cooperation scores weakest	Law is not the binding constraint; technical and cross-border capacity is	Shift near-term spending away from further legal drafting and toward staffed monitoring, patch management and formal CERT-to-CERT information sharing
Working systems built by prompt in hours, with a review practice claimed but not documented (Table VII)	Review is asserted but not verifiable; new attack surface reaches production without evidenced sign-off	Require that any AI-assisted system handling citizen or financial data pass a documented review by a party other than the team that produced it, and publish that the review occurred
Nepal's pattern is shared with India and Bhutan	Single-country capacity building cannot match shared regional growth	Pursue regional technical-assistance cooperation on incident response rather than purely national efforts

An additional recommendation arises from the PHP2Shell case. Government platform operators should maintain a centrally governed inventory of internet-facing software assets and PHP versions; define patching responsibilities among central operators, agencies and vendors; prioritise supported software versions; conduct independent configuration and source-code reviews for legacy systems; test shared platforms before restoration; and maintain documented continuity and recovery procedures.

LIMITATIONS AND FUTURE RESEARCH

This is a desk study using secondary data; no interviews, surveys or system testing were carried out. The October 2026 PHP2Shell case is based on contemporaneous public reporting and technical advisories. The study did not independently inspect Nepali government servers, verify their PHP versions, conduct forensic analysis, or establish whether any system was exploited. Reported shutdowns and restoration are therefore treated as service-continuity evidence, while compromise and breach claims are excluded unless independently established.

The incident record in Table VI is small and unevenly sourced. Two entries rest on detailed first-hand reporting in a single mainstream newspaper, and four on a combination of specialist security outlets and breach-tracking databases. None rests on an uncorroborated blog or an unattributed claim, but the record should be read as indicative of a pattern rather than as a complete census of incidents, since Nepal has no mandatory breach-disclosure regime and unreported incidents are by definition absent from it. EGDI is a comparative index, and its weighting and method have changed across survey rounds, which affects strict year-on-year comparison, especially for the pre-2018 values in Table I. The GCI carries a similar limit that ITU itself states: it measures stated commitment, not verified outcomes, and country submissions originate with the countries being scored, even though ITU reviews them. This is a structural limitation of any self-reported

commitment index, and a reason this study leans on the incident record rather than either index for outcome evidence. The 2024 GCI is also a single time point, not a trend, unlike the multi-year EGDI series. Finally, Nepal-specific peer-reviewed work on e-governance service delivery now exists [1], but nothing comparable exists on the cybersecurity-governance side, so the framework proposed here should be read as a lens supported by this dataset and the wider regional literature, not as a theory already validated by multiple Nepal-focused security studies.

Each limitation above points to a specific direction for future work. Three are proposed, each tied to a finding or constraint already established in this manuscript.

a. Longitudinal empirical validation. The framework is currently supported only by secondary data. Interviews with NCSC officials, government IT directors and shared-platform administrators, repeated over successive survey rounds, would test whether the proposed infrastructure–governance framework holds in practice and address the absence of Nepal-focused security studies noted above.

b. AI software assurance. Building on the AI-assisted development discussion, future work should examine mandatory, documented independent security verification before deployment of high-risk government software, since review practice is claimed but not publicly evidenced (Table VII).

c. Operational cybersecurity measurement. Because the GCI measures commitment rather than performance, the EGDI/GCI analysis should be extended with outcome measures: mean time to detect (MTTD), mean time to respond or recover (MTTR), vulnerability remediation time, patch compliance, CERT activity and service downtime.

CONCLUSION

Using one consistently sourced UN dataset alongside the ITU Global Cybersecurity Index, this study shows that Nepal's digital-government infrastructure has grown far faster (TII +63.1 percent, 2020–2024) than its institutional and participation measures (EPI −40.6 percent, HCI −3.6 percent). We call this infrastructure–governance asymmetry, and it is shared in direction with, but sharper than, two regional peers. Law is not the problem: Nepal's GCI Legal score is among the region's strongest. What is missing is technical and cooperative capacity, and with it the ability to detect incidents internally. Pakistan's near-maximum GCI score alongside the region's second-lowest EGDI shows why commitment scores should not be read as outcomes, and the same applies to Nepal's own.

AI-assisted development poses the same question at the level of software delivery. Production speed has increased sharply; assurance is also expanding, on the only public measure available, but whether the two are scaling together is not currently answerable from public evidence, and that unanswerability is itself a governance finding. Future work should prioritise further-verified incident data at larger sample size, incorporate GCI data as new editions appear, and test this framework against other developing-country e-governance programmes to see whether the pattern holds beyond South Asia.

The October 2026 PHP2Shell response adds a contemporary illustration of the risks associated with shared government technology dependencies. The precautionary withdrawal and staged restoration of public websites show that resilience must include software-version inventory, coordinated patching, vendor accountability, independent testing and continuity planning. The case does not establish successful exploitation in Nepal; rather, it demonstrates how vulnerability exposure alone can require coordinated action to protect service availability across interconnected public platforms.

REFERENCES

1. T. B. Chalaune, "Status of e-government and public service delivery in Nepal," Karnali Outlook: Knowledge Across Disciplines, vol. 1, no. 1, pp. 183–192, Feb. 2026.

2. S. M. Abdulnabi, "Issues and challenges of implementing e-governance in developing countries: A comprehensive analysis of civil service models," Cogent Bus. Manage., vol. 11, no. 1, Art. no. 2340579, 2024, doi: 10.1080/23311975.2024.2340579.
3. A. Nazuk, A. U. N. Erkin, M. Noor, and R. Zahid, "Exploring the potential and challenges of e-governance in Pakistan," Sustain. Futures, Dec. 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666188825010330
4. S. Mushtaq and M. Shah, "Mitigating cybercrimes in e-government services: A systematic review and bibliometric analysis," Digital, vol. 5, no. 1, Art. no. 3, Jan. 2025, doi: 10.3390/digital5010003.
5. Global Cybersecurity Index 2024, 5th ed., Int. Telecommun. Union, Geneva, Switzerland, 2024.
6. E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development, United Nations Dept. Econ. Social Affairs, New York, NY, USA, 2024.
7. United Nations Dept. Econ. Social Affairs, Div. Public Institutions Digit. Government, "UN E-Government Knowledgebase: Country information." [Online]. Available: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/120-Nepal
8. "Vianet suffers data breach, leaking personal customer details online," The Kathmandu Post, Apr. 8, 2020. [Online]. Available: https://kathmandupost.com/national/2020/04/08/vianet-suffers-data-breach-leaking-personal-customer-details-online
9. "Open season on hacking into gov.np," Nepali Times, Jan. 29, 2023. [Online]. Available: https://nepalitimes.com/news/open-season-on-hacking-into-gov-np
10. "Sensitive government data of Nepal's Prime Minister's Office allegedly for sale," CyberPress, Mar. 26, 2025. [Online]. Available: https://cyberpress.org/data-nepals-pms-sale/
11. "Nepal's ministerial data hacked, now available on dark web," Resonant News, Jan. 5, 2025. [Online]. Available: https://resonantnews.com/2025/01/05/nepals-ministerial-data-hacked-now-available-on-dark-web-for-50/
12. "Nepal's Ministry of Federal Affairs and General Administration data breach," BreachSense, Jan. 2, 2025. [Online]. Available: https://www.breachsense.com/breaches/nepals-ministry-of-federal-affairs-and-general-administration-data-breach/
13. "Weak data protection exposes Nepal to growing cybersecurity risks," OnlineKhabar English, 2026. [Online]. Available: https://english.onlinekhabar.com/weak-data-protection-exposes-nepal-to-growing-cybersecurity-risks.html
14. "Nepalis' data are insecure; personal information is at high risk," Nepal News, Mar. 3, 2026. [Online]. Available: https://english.nepalnews.com/s/long-reads/nepalis-data-are-insecure-personal-information-is-at-high-risk/
15. "Nepal uncovers 135 compromised government email accounts after joining global breach tracker," The Kathmandu Post, Aug. 6, 2026. [Online]. Available: https://kathmandupost.com/science-technology/2026/08/06/nepal-uncovers-135-compromised-government-email-accounts-after-joining-global-breach-tracker
16. "Government emails at risk of theft, data from 135 accounts breached," Kantipur, Aug. 6, 2026. [Online]. Available: https://ekantipur.com/news/2026/08/06/en/135-government-emails-compromisedspam-of-misleading-emails-in-the-name-of-government-officials-31-19.html
17. "AI-driven vibe coding gains ground in Nepal," The Kathmandu Post, Jun. 25, 2026. [Online]. Available: https://kathmandupost.com/science-technology/2026/06/25/ai-driven-vibe-coding-gains-ground-in-nepal
18. "How 'vibe coding' is taking off in Nepal," OnlineKhabar English, Aug. 2026. [Online]. Available: https://english.onlinekhabar.com/vibe-coding-in-nepal.html
19. H. Pearce, B. Ahmad, B. Tan, B. Dolan-Gavitt, and R. Karri, "Asleep at the keyboard? Assessing the security of GitHub Copilot's code contributions," in Proc. IEEE Symp. Secur. Privacy, 2022, pp. 754–768.
20. N. Perry, M. Srivastava, D. Kumar, and D. Boneh, "Do users write more insecure code with AI assistants?" in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2023, pp. 2785–2799.
21. "AI's entry into software development: A wave of 'vibe coding' from Nepal Telecom to the private sector," Kantipur, Jun. 25, 2026. [Online]. Available: https://ekantipur.com/technology/2026/06/25/en/wave-of-vibe-coding-from-nepal-telecom-to-the-private-sector-35-02.html

22. The PHP Group, “Security advisory: Critical remote code execution vulnerabilities, update now,” Oct. 21, 2026. [Online]. Available: https://www.php.net/?p=6507
23. European Union Agency for Cybersecurity (ENISA) et al., “Joint statement on critical PHP vulnerabilities,” Oct. 21, 2026. [Online]. Available: https://www.enisa.europa.eu/news/joint-statement-on-critical-php-vulnerabilities
24. S. Baral, “PHP2Shell security flaw forces thousands of Nepali websites offline,” The Kathmandu Post, Oct. 25, 2026. [Online]. Available: https://kathmandupost.com/science-technology/2026/10/25/php2shell-security-flaw-forces-thousands-of-nepali-websites-offline
25. S. Baral, “Most Nepal government websites back online after PHP2Shell flaw,” The Kathmandu Post, Oct. 26, 2026. [Online]. Available: https://kathmandupost.com/science-technology/2026/10/26/most-nepal-government-websites-back-online-after-php2shell-flaw