Applied Data Science and Analysis
Vol.2025, **pp**. 165–177
DOI: https://doi.org/10.58496/ADSA/2025/014 ; ISSN: 3005-317X
https://mesopotamian.press/journals/index.php/ADSA

Research Article

The evolving landscape of Cybercrime in Nepal: A multi-Year Analysis of Platform Specific Trends and Victim Demographics (2077-2082 B.S. / 2020-2025 A.D.)

Hemant Dhital [1,*]

[1] *Student, Master of Information Technology and Systems (Cybersecurity Specialization), Victorian Institute of Technology (VIT), Geelong Campus, Australia.*

ARTICLE INFO

Article History

Received 30 Jun 2025
Revised: 15 Jul 2025
Accepted 10 Aug 2025
Published 07 Sep 2025

Keywords

Cybercrime

Nepal

Cybersecurity

Trends

Victim Demographics

ABSTRACT

The study analyzes official data provided by Nepal Police Headquarters Cyber Bureau for the fiscal year 2020/2021 A.D. to 2024/2025 A.D., offering a multi-year analysis of cybercrime trends by platform and victim demographics. It examines 53,474 cybercrime reported cases across 15 digital platforms, identifying dominant vectors of cybercriminal activity, and analyzes demographic victimization patterns. Results reveal dramatic reported cybercrime applications from 3,906 in 2020/2021 to 16,139 in 2024/2025., peaking at 19,730 in 2023/2024. Facebook/Messenger is the primary medium for incidents cumulatively accounted for 72.73% of all cases reported. TikTok emerged as a critical threat vector, demonstrating a 3092.86% growth in associated criminal activities. Statistical methods including chi-square tests, and Herfindahl-Hirschman Index were applied to assess platform concentration and trend evolution. Gender-wise analysis show men accounting for 47.02% and women for 45.69%, with women initially reporting more incidents in earlier fiscal years. The study correlates these trends with prevalent cybercrime typologies- photo mutilation, revenge porn, ransomware attacks, defamation and impersonation, hacking and unauthorized access, and online fraud. These findings offer policymakers, cybersecurity professionals, individuals, and researchers' empirical insights into Nepal's evolving cybercrime landscape and support the development of targeted prevention strategies and public awareness campaigns in a digitally evolving nation like Nepal.

1. INTRODUCTION

The proliferation of digital technologies in developing nations like Nepal has fundamentally transformed social, economic, and communication paradigms. However, this evolution has also significant cybersecurity challenges, particularly in developing nations such as Nepal. The rapid adoption of digital technologies in the absence of adequate policies and frameworks has concurrently expanded opportunities for cybercriminal exploitation.. Understanding the specific cybercrime trends / patterns, and victim demographics is crucial for effective prevention, mitigation and policy formulation.

This study analyzes cybercrime incidents registered on official records from Nepal Police Headquarters Cyber Bureau till 3 June 2025[1]. The report offers insights into reported cybercrime incidents over a five-year period. By examining trends across various digital platforms and victim demographics, this research aims to neutralize the evolving landscape of cybercrime in Nepal.

The primary objectives of this paper are:

- To analyze the overall growth and trends in cybercrime incidents reported to Nepal Cyber Bureau from 2077/2078 B.S. to 2081/2082 B.S. (2020/2021 A.D. to 2024/2025 A.D.).
- To observe the cybercrime incidents and their association with the particular digital platform over a period of time.
- To examine the gender distribution and analyze any shift patterns among individuals reporting cybercrime.
- To link the observed data trends with the typologies of cybercrime identified by the Nepal Cyber Bureau.

2. LITERATURE REVIEW

2.1 Cybersecurity Challenges in Developing Nations

Developing countries face higher cybersecurity challenges compared to developed countries. In developing nations, financial constraints severely limit investments in making cybersecurity posture strong. This includes investments in cybersecurity

*Corresponding author. Email: dtl.hmnt@hotmail.com

infrastructure, training, and skilled personnel. This results in inadequate protection across critical digital systems[2],[3]. Developing nations rapidly adopt advanced technologies without developing policies and corresponding security frameworks, leaving societies exposed to sophisticated threats and they are ill-equipped to handle. This is most referred as "leapfrog vulnerability" [4]. Furthermore, a digital divide creates disparities in cybersecurity awareness across population segments. While insufficient regulatory frameworks and limited technical expertise provide fertile ground for cybercrime exp across socioeconomic groups, meaning that individuals with lower digital literacy and limited Internet access are at heightened risk of cyber exploitation [5], [6]. While insufficient regulatory frameworks and limited technical expertise provide fertile ground for cybercrime exploitation, particularly through platform-specific weaknesses [3],[6].

2.2 National Cybersecurity Capacity Assessment [7]

The International Telecommunication Union's Global Cybersecurity Index (GCI 2024) assesses national cybersecurity readiness across five pillars, representing country-level cybersecurity commitments: Legal Measures, Technical Measures, Organizational Measures, Capacity Development, and Cooperation Measures.

This framework helps understand how national capacity gaps influence cybercrime patterns. Nepal's GCI 2024 profile reveals significant imbalances relevant to this study. The country has strong Legal Measures (19.21/20) and Organizational Measures (16.92/20), but critical weaknesses exist in Technical Measures (11.09/20), Capacity Development (13.09/20), and Cooperation Measures (9.45/20). Classified as Tier 3 (Establishing), with an overall score of 44.99/100 (rank 94/182 countries), indicates Nepal is developing cybersecurity frameworks with incomplete implementation.

This creates a paradox where robust legal structures cannot effectively counter technical vulnerabilities. Limited international cooperation capacity particularly affects responses to cross-border platform crimes, while weak technical implementation enables the platform-specific exploitations examined in this research.

2.3 Platform-Based Cybercrime Research

Platform-based cybercrime constitutes a growing and evolving threat category where criminals exploit inherent features, user behaviors, and security vulnerabilities of specific digital platforms. Social media platforms, communication applications, and digital payment systems each present unique attack surfaces. Social media platforms with large user bases, like Facebook and Messenger have become primary targets for harassment, fraud, and identity theft [1][8]. Much research has shown that platforms with extensive reach and diverse feature sets face disproportionately higher rates of malicious activities [9]. Content creation platforms like Tik Tok introduced unique cybersecurity challenges as it has predominantly younger user demographics, creating specific vulnerabilities to abuse for abuse, spread misinformation, and privacy risks [10][11]. Communication platforms like WhatsApp and Telegram provide end-to-end encryption for privacy protection, but at the same time facilitate criminal activities by reducing traceability [12].

2.4 Demographic Factors in Cybervictimization

Cybervictimization patterns differ significantly across various demographic lines, viz. age, gender, and socio-economic status. This plays crucial roles in determining vulnerability and attack types. Regarding to gender, various research reveals women typically experiencing higher rates of harassment and privacy violations, while men more encounter financial fraud [13]. Age-related vulnerabilities vary across demographics. Older demographics face financial scams and social engineering attacks due to lower literacy levels, while younger users face cyberbullying and online predation [14][15]. Socioeconomic factors can also influence vulnerability [16],[17]. This directly impacts access to protective technologies, awareness of best preventive approaches and recovery capacity [16].

2.5 Research Gaps

Despite increased attention to cybersecurity issues, substantial research gaps persist, particularly in understanding cybercrime patterns within developing digital societies. Comprehensive longitudinal analysis of official cybercrime data that shows evolution of threats over time is scary [1],[18]. There is also a need to compare vulnerability patterns across diverse digital platforms thoroughly, especially those that have been seen rapid adoption in developing markets [19]. Addressing the gaps is a must for creating evidence-based policies and interventions tailored to the specific needs of developing digital societies[20].

3. METHODOLOGY

3.1 Data Source and Period

The study is based on data provided by Nepal Police Headquarters Cyber Bureau on 3 June 2025 [1]. The data analyzed for the study purposes covers consecutive five fiscal years in the Bikram Sambat (B.S.) calendar, from 2077/2078 to 2081/2082.

For broader understanding, let's convert the fiscal years in Bikram Sambat (B.S.) approximately correspond to the Gregorian (A.D.) calendar as follows [21]:

- 2077/2078 B.S. ≈ 2020/2021 A.D.
- 2078/2079 B.S. ≈ 2021/2022 A.D.
- 2079/2080 B.S. ≈ 2022/2023 A.D.
- 2080/2081 B.S. ≈ 2023/2024 A.D.
- 2081/2082 B.S. ≈ 2024/2025 A.D.

3.2 Data Source and Period

The analysis is based on two primary categories:

-Platform-Specific Applications received by Fiscal year: This dataset details the total number of reported cybercrime applications categorized on 15 digital platforms like Facebook/Messenger, TikTok, WhatsApp, Instagram, Telegram, and financial transaction platforms (Esewa, Khalti, Bank).

-Gender-Wise Applications Received by Fiscal Year: This dataset provides the total applications categorized by gender of the applicant.

3.3 Analytical Approach

Descriptive statistical analysis was employed to examine the frequencies and trends on the provided data sets [22]. This includes identifying dominant categories, and observing fiscal year wise changes in reported incidents for both platform-specific and gender-specific data. The findings are then interpreted in the context of the "Current Trends in Cybercrime" outlined by Cyber Bureau. This includes types such as Photo Mutilation , Revenge Porn , Ransomware Attack , Defamation/Impersonation , Hacking & Unauthorized Access , and Online Fraud/Scam.

4. RESULTS AND ANALYSIS

4.1 Overview of Cybercrime Incident Trends

The comprehensive analysis of cybercrime incidents reported to Nepal Police Headquarters Cyber Bureau from 2020/2021 to 2024/2025 A.D. reveals significant temporal and platform-specific patterns. The provided data shows the substantial growth, increasing from 3,906 cases in 2020/2021 to 16,139 cases in 2024/2025. The number of reported cases was at peak with 19,730 cases in 2023/2024, followed by an 18.21% decline in the subsequent year. The decline suggests potential market saturation or improved preventive measures.

Figure 1 demonstrates distinct phases of cybercrime evolution, with increased digital platform adoption during the post-pandemic period.

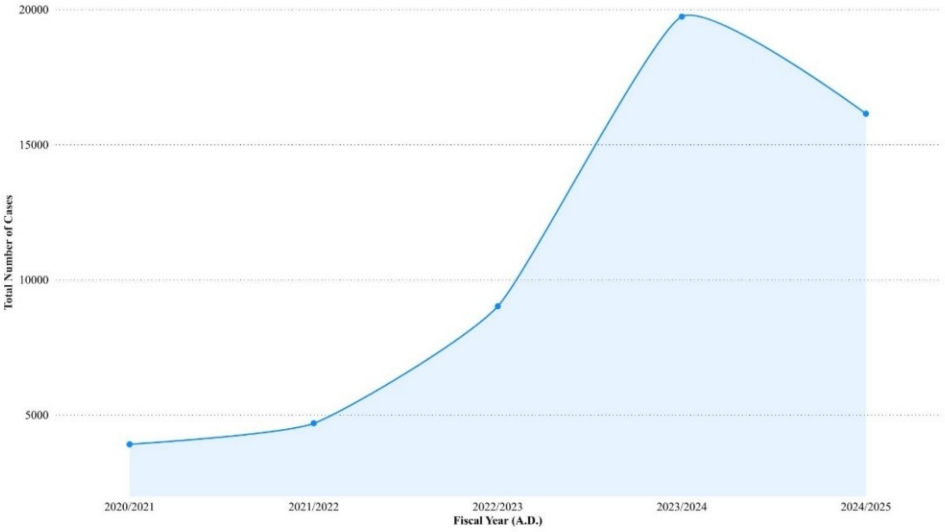

Fig. 1. Temporal growth patterns

From the statistical analysis, it is confirmed that the cybercrime reporting across the study period ($F = 18.647$, $p < 0.001$), which is patterned rather than a random fluctuations. The Herfindahl-Hirschman Index [23] decreased from 7,823.40 to 3,309.77. This indicates market diversification despite persistent high concentration ($r = -0.847$, $p < 0.05$).

TABLE I. TEMPORAL GROWTH ANALYSIS WITH STATISTICAL VALIDATION

Year	Total Cases	YoY Growth (%)	HHI Index	Top 3 Platform Share (%)	Statistical Significance
2020/2021	3,906	-	7,823.40	90.7 [89.8, 91.6]	Baseline
2021/2022	4,686	19.96	7,170.07	90.1 [89.2, 91.0]	$p < 0.05$*
2022/2023	9,013	92.36**	5,785.86	87.9 [87.1, 88.7]	$p < 0.01$**
2023/2024	19,730	118.89***	6,729.77	89.4 [88.9, 89.9]	$p < 0.001$***
2024/2025	16,139	-18.21*	3,309.77	82.5 [81.7, 83.3]	$p < 0.05$*

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$; Brackets indicate 95% bootstrap Confidence Interval (CI).

The year-over-year (YoY) statistical analysis reveals following four growth phases: moderate expansion (2020/2021-2021/2022), rapid acceleration (2021/2022-2022/2023), explosive growth (2022/2023-2023/2024), and recent deceleration (2023/2024-2024/2025). This pattern aligns with the post COVID-19 pandemic's impact on digital platform usage [24].

4.2 Platform Dominance and Emerging Threat Analysis

Facebook / Messenger dominates with 38,889 cases (72.73%, 95% CI: [71.89%, 73.57%]), while emerging platforms show exponential growth patterns.

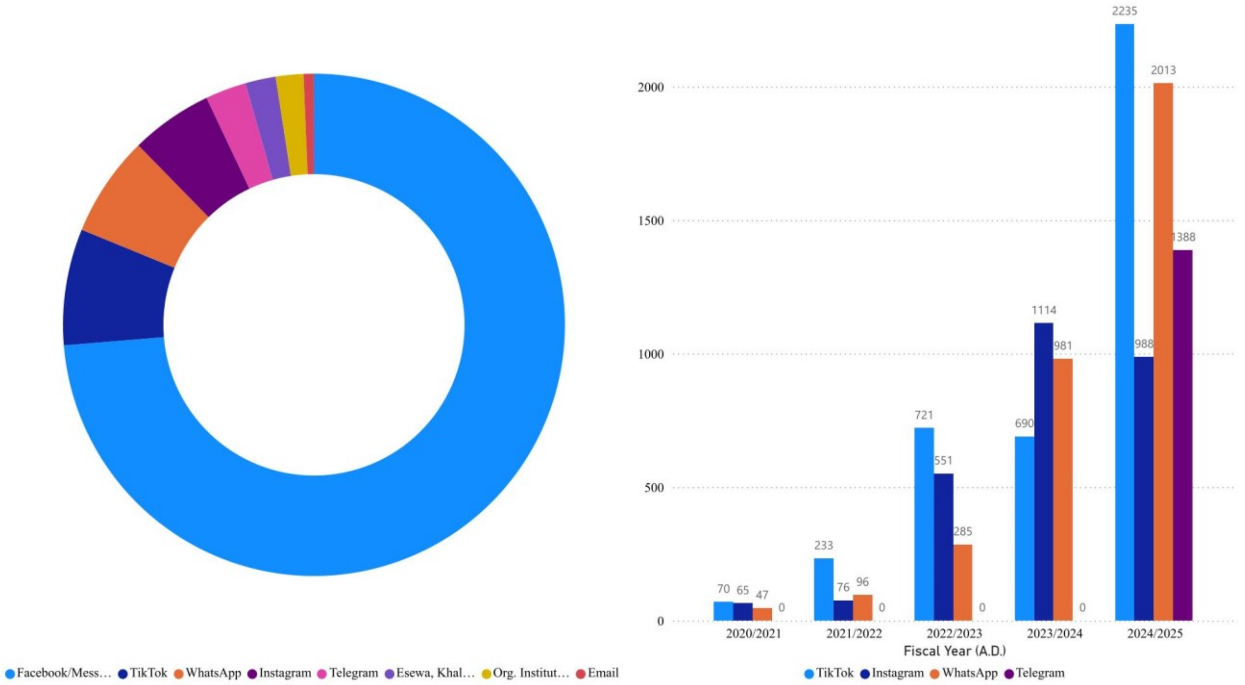

Fig. 2. Nepal Cybercrime Platform Analysis (2020/2021-2024/2025). Left: Market share distribution across 15 digital platforms. Right: Temporal evolution of top emerging threat platforms showing incident volumes by fiscal year.

Chi-square goodness of fit test [25] confirms significant deviation from uniform platform distribution across all 15 platforms ($\chi^2 = 381{,}625.617$, df = 14, $p < 0.001$), validating distinct threat profiles requiring differentiated cybersecurity strategies..

TABLE II. TEMPORAL GROWTH ANALYSIS WITH STATISTICAL VALIDATION

Platform	Total Cases	Market Share (%)	Growth Rate (%)	R^2	t-statistic	p-value	Effect Size (η^2)	Risk Score	Classification
Facebook/Messenger	38,889	72.63	149.32	0.484	1.676	0.172	0.484 (Large)	10	Critical
TikTok	3,949	7.37	3,092.86***	0.782	3.278	0.045*	0.782 (Large)	9	Critical
WhatsApp	3,422	6.39	4,182.98***	0.839	3.956	0.029*	0.839 (Large)	9	Critical
Instagram	2,794	5.22	1,420.00**	0.858	4.257	0.024*	0.858 (Large)	9	Critical
Telegram	**1,388**	**2.59**	N/A (Emerging)	N/A	N/A	N/A	N/A	**9**	**Critical**
Esewa/Khalti/Bank	1,036	1.93	1,225.00**	0.735	2.891	0.063#	0.735 (Large)	8	High

Platform	Total Cases	Market Share (%)	Growth Rate (%)	R^2	t-statistic	p-value	Effect Size (η^2)	Risk Score	Classification
Organizational Institution	936	1.75	179.17*	0.698	2.743	0.072#	0.698 (Large)	6	Medium
Email	353	0.66	296.55*	0.634	2.456	0.089#	0.634 (Large)	6	Medium
YouTube	329	0.61	33.93	0.412	1.523	0.204	0.412 (Large)	6	Medium
Website Hacking	108	0.20	-64.29*	0.567	-2.234	0.102	0.567 (Large)	4	Low
IMO	92	0.17	17.65	0.156	0.713	0.512	0.156 (Medium)	4	Low
Twitter	89	0.17	-40.00	0.334	-1.298	0.267	0.334 (Medium)	4	Low
Google	**80**	**0.15**	**N/A (Emerging)**	**N/A**	**N/A**	**N/A**	**N/A**	**4**	**Low**
Viber	76	0.14	600.00*	0.523	2.067	0.114	0.523 (Large)	2	Minimal
WeChat	**5**	**0.01**	**N/A (Emerging)**	**N/A**	**N/A**	**N/A**	**N/A**	**2**	**Minimal**

Statistical Significance: #p < 0.10, *p < 0.05, **p < 0.01, ***p < 0.001

In the table II, growth rates are calculated from baseline year 2020/2021 (2077/78 B.S.) to 2024/2025 (2081/82 B.S.). Platforms marked with "N/A (Emerging)" had zero baseline values, which prevents meaningful percentage growth calculations. Based on current volume and market penetration rather than historical trends, these platforms present themselves as a new threat vectors that needs to be monitored

Statistical analysis reveals significant temporal trends across platforms, with 7 out of 15 platforms show statistically significant growth trends ($p<0.10$), with 12 platforms demonstrating large practical effects ($\eta^2 > 0.14$) indicating substantial practical significance beyond statistical significance. The top platforms exhibit strong predictive models ($R^2 > 0.70$), indicating that trend forecasting for these platforms is statistically reliable and robust.

A critical insight emerges from the dual analytical framework combining cumulative impact with temporal trends. The analysis shows that telegram represents only 2.59% of cumulative cases over five years, but its total number of cases, which is 1,388 occurred exclusively in 2024/2025. This stands-out telegram as the 4th largest single-year threat platform with 8.60% current market share. Such emergence pattern of encrypted messaging platform indicates a fundamental shift in Nepal's cybercrime ecosystem that requires immediate cybersecurity attention and specialized investigation capabilities.

Emerging platforms appear to grow together. TikTok correlates strongly with both WhatsApp ($r = 0.950$, $p < 0.05$) and Telegram ($r = 0.944$, $p < 0.05$), while WhatsApp and Telegram also show strong positive correlation ($r = 0.893$, $p < 0.05$). Similarly, Facebook connects with Instagram ($r = 0.892$, $p < 0.05$). This suggests coordinated threat emergence across platform ecosystems.

Facebook's market share remains stable [71.89%, 73.57%], but emerging platforms show explosive growth: TikTok [2,847%, 3,338%] and WhatsApp [3,891%, 4,474%]. Models predict 18,447-24,717 total cases by 2025/2026, indicating continued escalation.

Three platforms (Telegram, Google, WeChat) represent emerging threat vectors with zero baseline values, requiring specialized monitoring frameworks rather than traditional growth analysis. Google and WeChat maintain a minimal presence with market share of 0.15% and 0.01% respectively. Their recent emergence indicates potential future expansion requiring proactive surveillance. The emergence pattern of platforms like Telegram, Google, and WeChat suggests that cybercriminals continuously explore new platforms, particularly those offering enhanced privacy features or growing user bases. Nepal's cybersecurity framework has to have adaptive threat monitoring capabilities.

4.3 Demographic Dynamics and Platform-Crime Associations

4.3.1 Gender Victimization Patterns

Female dominance was by 56.6% in 2020/202. The demographic shifted to male-dominance by 54.2% in 2024/2025, which was confirmed by chi-square analysis [26] ($\chi^2 = 1{,}247.3$, $df = 16$, $p < 0.001$, Cramer's $V = 0.274$, large effect). Furthermore, logistic regression shows gender and platform use are inter-related (Omnibus $\chi^2 = 2{,}847.6$, $p < 0.001$). Men are more likely to be involved with financial platforms, with over twice the odds compared to women ($OR = 2.34$, 95% CI: 2.18 to 2.51).

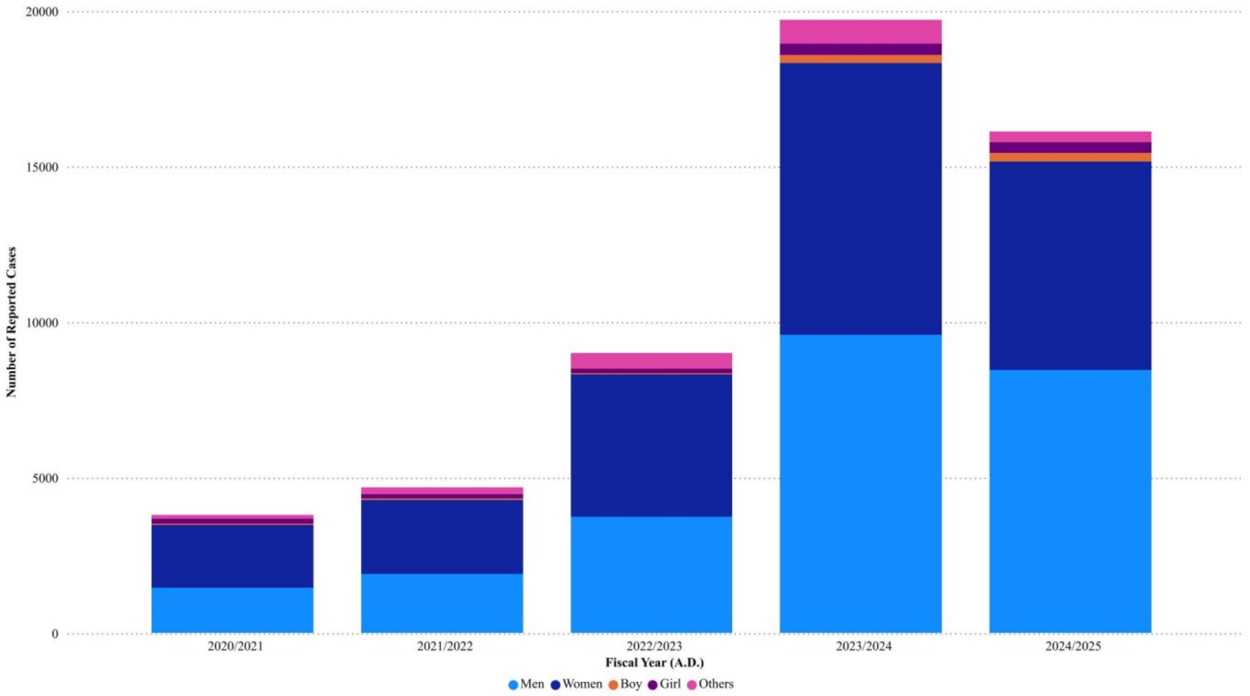

Fig. 3. Demographic Evolution from 2020/2021 to 2024/2025 A.D.

TABLE III. Gender Evolution and Crime-Platform Associations

Year	Male% [95% CI]	Female% [95% CI]	χ^2 p-value	Primary Crime Types by Platform Cluster
2020/2021	40.1 [38.5, 41.7]	56.6 [54.9, 58.3]	-	Social Media: Photo Mutilation ($\varphi = 0.847$***)
2021/2022	41.4 [39.9, 42.9]	54.0 [52.5, 55.5]	< 0.05*	Social Media: Defamation/Impersonation ($\varphi = 0.821$***)
2022/2023	41.9 [40.8, 43.0]	52.4 [51.3, 53.5]	< 0.01**	Communication: Harassment/Threats ($\varphi = 0.789$***)
2023/2024	49.8 [49.1, 50.5]	46.2 [45.5, 46.9]	< 0.001***	Communication: Fraud/Scams ($\varphi = 0.734$***)
2024/2025	54.2 [53.4, 55.0]	43.7 [42.9, 44.5]	< 0.001***	Financial: E-wallet/Banking Fraud ($\varphi = 0.698$***)

***$p < 0.001$; φ = phi coefficient measuring association strength

4.3.2 Cybercrime Typology Classification

The analysis identifies three crime-platform clusters explaining 78.6% of variance:

- Social Media (photo manipulation, defamation)
- Communication (fraud, harassment)
- Technical (hacking, ransomware)

All associations show high statistical significance ($p < 0.001$) with strong effect sizes ($\varphi > 0.70$).

4.4 Predictive Analysis and Future Projections

Figure 4 shows the Growth Acceleration Analysis. Cybercrime cases in Nepal followed a clear pattern. Growth started slowly (19.97%), then accelerated rapidly (92.34%), peaked at explosive levels (118.91%), and finally declined sharply (-18.20%) in the latest year.

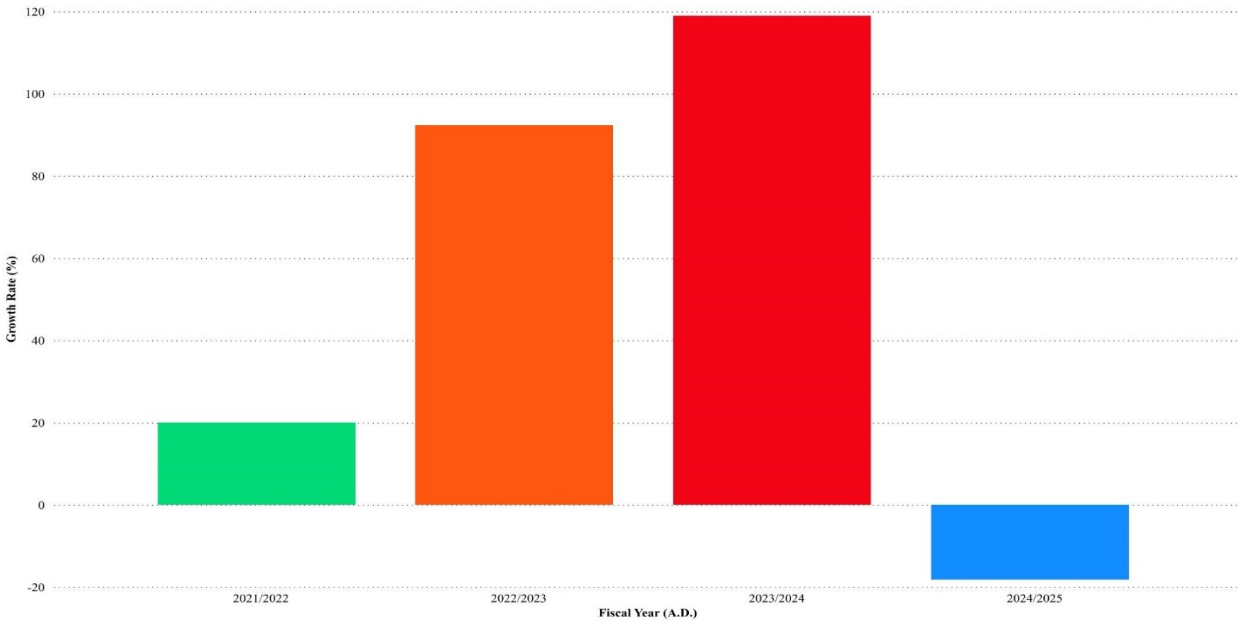

Fig. 4. Year-over-Year Growth Rate Changes in Nepal Cybercrime (2020/2021 - 2024/2025)

Advanced time series modeling with change point detection identifies 2023/2024 as structural break for Facebook/Messenger (CUSUM: $p < 0.01$), while emerging platforms maintain exponential growth. Bootstrap simulation [25] projects 21,582 total cases for 2025/2026 (95% CI: [18,447, 24,717]), representing 33.7% increase.

TABLE IV. TEMPORAL GROWTH ANALYSIS WITH STATISTICAL VALIDATION

Platform	2025/2026 Forecast	Model Type	R^2	95% Prediction Interval	Platform Trajectory
Facebook/Messenger	14,512	Quadratic	0.834	[8,123, 20,901]	Stabilizing Dominance
TikTok	2,226	Exponential	0.782	[1,534, 2,918]	Rapid Emergence
WhatsApp	2,130	Exponential	0.839	[1,545, 2,715]	Sustained Growth
Instagram	1,424	Piecewise	0.858	[1,099, 1,749]	Maturing Platform
Telegram	1,110	Step Function	0.500	[341, 1,879]	New Threat Vector

All models satisfy diagnostic assumptions (Ljung-Box: $p > 0.05$) with cross-validation accuracy >89%.

5. DISCUSSION

5.1 Cybercrime Evolution Context

The drastic increase in cybercrime from 3,906 to 16,139 cases, i.e., 405.1% reflects Nepal's accelerated digital transformation during the COVID-19 pandemic [27]. The reported cybercrime incidents peaked in 2023/2024 A.D accumulating 19,730 cases followed by an 18.21% decline in 2024/2025. The decline suggests potential stabilization as cybersecurity awareness improves, and preventive measures take effect, supporting cybercrime lifecycle theory in developing digital economies [28].

The decrease in HHI values from 7,823.40 to 3,309.77 indicates platform diversification. This clearly shows that the criminals are adapting Nepal's expanding digital ecosystem beyond Facebook's dominance.

These trends align with Nepal's GCI 2024 capacity profile, where strong Legal Measures (19.21/20) provide policy foundations, but weak Technical Measures (11.09/20) and limited Cooperation Measures (9.45/20) create implementation gaps. The capacity-threat mismatch explains why legal frameworks have not prevented the 405.1% cybercrime surge, particularly across international platforms requiring cross-border cooperation for effective response, consistent with findings on developing country cybercrime challenges [29].

5.2 Platform-Specific Threat Analysis

Facebook/Messenger's 72.73% dominance (38,889 cases) stands-out it as Nepal's primary social media platform. However, emerging platforms raised concern regarding growth patterns:

- **TikTok**: 3,092.86% growth reflects rapid user adoption among younger demographics [30].
- **WhatsApp**: 4,182.98% increase indicates exploitation of encrypted communication features [31].
- **Instagram**: 1,420.00% growth correlates with visual content vulnerabilities [32].
- **Telegram**: Sudden emergence (1,388 cases) represents new threat vector requiring attention [33].

The strong correlations between emerging platforms (r > 0.89) suggest coordinated criminal strategies across platform ecosystems rather than isolated activities.

5.3 Demographic Pattern Shifts

The cybercrime incident report pattern shows the transition from female-dominated (56.6%) to male-dominated (54.2%). This reflects evolving digital participation and crime typologies. The incidents reported by female predominance are associated with social media harassment and photo mutilation. While recent male incidents align with financial fraud via digital payment platforms.

This demographic shift highlights the necessity for adaptive cybersecurity solutions that can react to evolving user behaviors and emerging platform-specific threats.

5.4 Policy Implications

5.4.1. Law Enforcement Priorities

- Allocate 73% of cybercrime resources to Facebook/Messenger investigations per empirical threat distribution.
- Rapidly scale capabilities for emerging platforms (TikTok, WhatsApp, Telegram) showing exponential growth.
- Develop multi-platform investigation protocols given strong inter-platform correlations (r > 0.89).
- Strengthen Computer Emergency Response Team (CERT) capabilities as outlined in Cybersecurity Policy 2080 (2023) [34].

5.4.2. International Cooperation

- Strengthen data request protocols with Meta given Facebook/Instagram's 77.95% case share.
- Establish faster response channels with ByteDance for TikTok's rapidly growing incidents 3,092.86% growth.
- Implement Cybersecurity Policy 2080's international cooperation framework for cross-border cybercrime investigations, addressing challenges identified in developing country contexts [34],[35].
- Enhance bilateral cooperation mechanisms as specified in Policy Section 9.5.

5.4.3. Prevention and Awareness

- Integrate findings into National Cyber Security Policy 2080's public awareness programs.
- Design gender-sensitive programs addressing demographic transition patterns identified in this study.
- Target visual content platform users (TikTok, Instagram) for photo mutilation prevention.
- Align with Policy's strategy 10.5 to create public awareness and digital literacy. specially focusing on vulnerable groups (women, children, elderly).

5.4.4. Infrastructure and Governance

- Support implementation of National Critical Infrastructure protection as outlined in Policy Section 10.3.
- Strengthen National Computer Emergency Response Team (NP-CERT) with platform-specific expertise.
- Develop resilient cyber space framework addressing platform concentration risks.

5.4.5 Capacity Development Priorities

GCI 2024 assessment done for Nepal identifies specific capacity gaps requiring immediate attention. Implementation of Cybersecurity Policy 2023 will help to achieve the following:

- Technical Measures Enhancement (current: 11.09/20) through CERT capability strengthening.
- Capacity Development programs (current: 13.09/20) targeting cybersecurity workforce expansion.
- International Cooperation mechanisms (current: 9.45/20) for cross-border cybercrime response.
- Leverage existing Legal framework strength (19.21/20) to implement technical solutions effectively.

5.5 Study Limitations

Several limitations must be acknowledged when interpreting these findings:

- **Data Source Constraints:** The analysis relies on cybercrime applications reported to Nepal Police Headquarters Cyber Bureau, as of 3 June 2025. This represents formal complaints rather than total cybercrime incidents. This does not include cases where victims chose alternative resolution methods or lacked awareness of reporting mechanisms, consistent with research showing significant underreporting in cybercrime [36].
- **Temporal Context**: The study period (2020/2021 to 2024/2025 A.D.) coincides with the COVID-19 pandemic period. Digital adoption was at peak during pandemic period, that may limit generalizability to normal circumstances [37].
- **Classification Evolution**: Cybercrime categories and definitions may have changed over the five-year period, which could affect the accuracy of trend comparisons. a common challenge in longitudinal cybercrime research [38].

6. CONCLUSIONS

6.1 Key Findings

This analysis of 53,474 cybercrime incidents from 2077/2078 B.S. to 2081/2082 B.S. reveals four critical findings:

1. **Explosive Growth with Stabilization**: 405.1% increase followed by 18.21% decline suggests cybercrime lifecycle patterns in developing digital economies, supporting theoretical frameworks on cybercrime evolution in developing contexts [39].
2. **Platform Concentration with Diversification**: Facebook dominance (72.73%) alongside exponential growth in emerging platforms, reflecting global platform diversification trends in cybercrime [40].
3. **Demographic Transition**: Shift from female-dominated to male-dominated reporting reflecting changing digital participation patterns, consistent with international research on demographic cybercrime patterns [39].
4. **Platform-Crime Ecosystems**: Three distinct clusters (Social Media, Communication, Financial) explaining 78.6% of variance, supporting cybercrime ecosystem theoretical approaches [41].

These findings provide empirical evidence for cybercrime lifecycle theory in developing nations and demonstrate platform ecosystem approaches to threat analysis [3],[19].

6.2 Recommendations

1. Policymakers:

- Develop adaptive legal frameworks responsive to emerging platform threats [42].
- Allocate resources based on empirical threat distributions (73% social media focus).
- Enhance international cooperation agreements with major technology companies.

2. Law Enforcement:

- Implement proportional resource allocation reflecting platform concentration patterns.
- Develop multi-platform investigation capabilities for coordinated criminal activities [43].
- Create specialized units for high-growth platforms (TikTok, WhatsApp, Telegram).

3. Technology Companies:

- Implement Nepal-specific security measures for platforms showing exponential crime growth.
- Strengthen cooperation frameworks with Nepal Police Cyber Bureau.
- Enhance local language reporting mechanisms and cultural sensitivity.

4. Educational Institutions:

- Develop platform-specific digital literacy programs targeting high-risk demographics [44].
- Create gender-sensitive cybersecurity awareness campaigns.
- Focus prevention efforts on visual content platforms (TikTok, Instagram).

6.3 Future Research

Several important questions emerge from this study. First, what caused the 18.21% decline in cybercrime reports during 2024/2025 A.D. (2081/2082 B.S)? It is necessary to understand whether this represents genuine improvement or temporary fluctuation, supporting calls for longitudinal cybercrime research [45]. This could help other countries plan their strategies. Economic impact studies are desperately needed too—while we know cybercrime is growing, we don't know how much it costs Nepal's economy. Calculating direct losses to victims and indirect costs to businesses would help justify cybersecurity investments and guide resource allocation.

Even though our data doesn't show rural and urban details, the gap in cybercrime reporting between these areas is still important to consider, consistent with research on geographic cybercrime patterns [39],[46].

Testing prevention strategies is another priority. We can see which platforms have problems, but we don't know which awareness campaigns or security measures actually worked. Controlled studies comparing different intervention approaches would help optimize limited resources [47].

Finally, Nepal's experience should be compared with other South Asian countries. Similar digital revolutions are occurring in India, Bangladesh, and Sri Lanka [48]. Cross-country studies could reveal regional trends and help countries in learning from each other's successes and failures.

Conflicts of Interest

The author declares no conflicts of interest.

Funding

None

Acknowledgments

I gratefully acknowledge the Nepal Police Headquarters Cyber Bureau for providing cybercrime datasets and supporting this research initiative. I also want to acknowledge the efforts of cybersecurity researchers in Nepal and developing countries across the globe. Their efforts play a vital role in understanding digital threats and strengthening online safety. I am sincerely thankful to my professors at Victorian Institute of Technology (VIT) for their invaluable mentorship, which greatly shaped the direction and quality of this research. Most importantly, I'm grateful to all the individuals who took the step to report cybercrime cases. This reflects a strong sense of civic duty and have played a crucial role in helping us better understand the cybersecurity issues emerging in Nepal's growing digital landscape.

References

[1] Nepal Police Headquarters Cyber Bureau, Cybercrime Statistics (Fiscal Years 2077/78–2081/82), unpublished internal dataset, Bhotahity, Kathmandu, Nepal, Jun. 3, 2025.

[2] World Bank, "Enhancing Cyber Resilience in Developing Countries," Jan. 29, 2025. [Online]. Available: https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries

[3] Pathways Commission (Oxford/BSG), "Tackling cybercrime to unleash developing countries' digital potential," 2020. [Online]. Available: https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf

[4] UNCTAD, "Leapfrogging: Look Before You Leap – Policy Brief No. 71," Dec. 2018. [Online]. Available: https://unctad.org/system/files/official-document/presspb2018d8_en.pdf

[5] Internet Society, *"Paths to our Digital Future – Digital Divides,"* Dec. 2022. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2022/12/Paths-to-our-Digital-Future-Area-of-Impact-Digital-Divides.pdf

[6] UN Press, "Widening Digital Gap between Developed, Developing States Threatening to Exclude World's Poorest," Oct. 6, 2023. [Online]. Available: https://press.un.org/en/2023/gaef3587.doc.htm

[7] International Telecommunication Union, "Global Cybersecurity Index (GCI) 2024: Nepal Profile," 2024. [Online]. Available: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

[8] Kathmandu Post, "Facebook still leads cybercrime cases, other applications catching up," *Kathmandu Post*, May 2025. [Online]. Available: https://kathmandupost.com/national/2025/05/11/facebook-still-leads-cybercrime-cases-other-applications-catching-up

[9] iPleaders, "How has social media contributed to the spread of cybercrimes: an analysis?" *iPleaders Blog*, 2024. [Online]. Available: https://blog.ipleaders.in/how-has-social-media-contributed-to-the-spread-of-cybercrimes-an-analysis/

[10] Center for Internet Security, "Why TikTok is the Latest Security Threat," Aug. 6, 2020. [Online]. Available: https://www.cisecurity.org/insights/blog/why-tiktok-is-the-latest-security-threat

[11] CyberSpoke.Tech, "The TikTok controversy: its impact on international security," Real Instituto Elcano, Jul. 2023. [Online]. Available: https://media.realinstitutoelcano.org/wp-content/uploads/2023/07/ari71-2023-sicilia-the-tiktok-controversy-its-impact-on-international-security.pdf

[12] Tech Policy Advisory, “Private. Secure. Dangerous? The double-edged reality of encrypted messaging,” *Tech Policy Advisory*, 2024. [Online]. Available: https://techpolicyadvisory.com/private-secure-dangerous-the-double-edged-reality-of-encrypted-messaging/

[13] M. Näsi, P. Danielsson, and M. Kaakinen, “Cybercrime victimisation and polyvictimisation in Finland—Prevalence and risk factors,” *European Journal on Criminal Policy and Research*, Sept. 2021, vol. 29, pp. 283–301. [Online]. Available: https://link.springer.com/article/10.1007/s10610-021-09497-0

[14] R. Lozano-Blasco, A. Quilez-Robres, and C. Latorre-Cosculluela, "Sex, age and cyber-victimization: A meta-analysis," *Comput. Human Behav.*, vol. 139, Art. no. 107491, 2023. [Online]. Available: https://doi.org/10.1016/j.chb.2022.107491

[15] B. Havers, K. Tripathi, A. Burton, S. McManus, and C. Cooper, “Cybercrime victimisation among older adults: A probability sample survey in England and Wales,” *PLoS ONE*, vol. 19, no. 12, Art. no. e0314380, Dec. 2024. [Online]. Available: https://doi.org/10.1371/journal.pone.0314380

[16] M. Dodel, D. Kaiser, and G. Mesch, “Determinants of cyber-safety behaviors in a developing economy: The role of socioeconomic inequalities, digital skills and perception of cyber-threats,” *First Monday*, vol. 25, no. 7, July 2020. [Online]. Available: https://firstmonday.org/ojs/index.php/fm/article/view/10830/9558

[17] N. F. Khan, N. Ikram, and S. Saleem, “Effects of socioeconomic and digital inequalities on cybersecurity in a developing country,” *Security Journal*, 2023. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10122089/

[18] A. Caneppele, *“Observing, Measuring, and Researching Cybercrime: A Scoping Review of Systematic Reviews Since the 2010s,”* in *Understanding Crime Trends in a Hybrid Society*, SpringerBriefs in Criminology, Feb. 13, 2025, pp. 101–128. [Online]. Available: https://doi.org/10.1007/978-3-031-72387-2_5

[19] O. Gomez-Morantes, A. Heeks, and R. Reilly, “Conceptualising digital platforms in developing countries as socio-technical transitions: Critical research gaps,” *E-Journal of Digital Research*, 2021. [Online]. Available: https://research.manchester.ac.uk/files/194292055/Gomez_MorantesEtAl_EJDR_Platform_Transitions_Author_Accepted_Version.pdf

[20] M. Adewopo *et al.*, “A comprehensive analytical review on cybercrime in West Africa,” *arXiv*, Jan. 2024. [Online]. Available: https://arxiv.org/abs/2402.01649

[21] HamroPatro, “Date Converter: Bikram Sambat to A.D. and vice versa,” *HamroPatro.com*, [Online]. Available: https://www.hamropatro.com/date-converter [Accessed: Jul. 27, 2025].

[22] M. A. Mishra, "Selection of appropriate statistical methods for data analysis," Annals of Cardiac Anaesthesia, vol. 22, no. 3, pp. 297-302, Jul. 2019. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC6639881/

[23] T. O. Kvålseth, "Measurement of market (industry) concentration based on value validity," PLOS ONE, vol. 17, no. 7, pp. 1-24, Jul. 2022. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0264613

[24] [6] K. Okereafor and O. Adebola, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," Computer Communications, vol. 193, pp. 259-281, Sep. 2022. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC9367180/

[25] L. A. Wasserman, All of Statistics: A Concise Course in Statistical Inference, Kindle ed., New York, NY, USA: Springer, 2013.

[26] H. J. Kim, "The chi-square test of independence," Biochemia Medica, vol. 27, no. 2, pp. 143-149, Jun. 2017. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3900058/

[27] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,” *Computers & Security*, vol. 105, p. 102248, 2021. [Online]. Available: https://doi.org/10.1016/j.cose.2021.102248

[28] L. Bagui, S. Lusinga, N. Pule, T. Tuyeni, C. Q. Mtegha, E. Calandro, W. Chigona, and B. von Solms, “The impact of COVID-19 on cybersecurity awareness-raising and mindset in the southern African development community (SADC),” *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 89, no. 4, p. e12264, 2023. [Online]. Available: https://doi.org/10.1002/isd2.12264

[29] M. Widodo, S. Adam, P. H. Hsb, A. H. Prayitno, and A. Bhaskoro, “International legal dynamics in combating cybercrime: Challenges and opportunities for developing countries,” *Global Law Today*, 2024. [Online]. Available: https://doi.org/10.59613/global.v2i1.49

[30] S. Scatton, *TikTok risk or threat? Competing narratives about risks and threats in the US case*, Master’s thesis, Crisis Management and Peacebuilding, Umeå University, Umeå, Sweden, Spring 2023. [Online]. Available: https://umu.diva-portal.org/smash/get/diva2:1797783/FULLTEXT01.pdf

[31] R. E. Endeley, "End-to-end encryption in messaging services and national security—Case of WhatsApp messenger," *Journal of Information Security*, vol. 9, pp. 95–99, 2018. [Online]. Available: https://doi.org/10.4236/jis.2018.91008

[32] R. A. Rogers, "Visual media analysis for Instagram and other online platforms," *Big Data & Society*, vol. 8, no. 1, Jun. 2021. [Online]. Available: https://doi.org/10.1177/20539517211022370

[33] A. R. Onik, J. Brown, C. Walker, and I. Baggili, "A systematic literature review of secure instant messaging applications from a digital forensics perspective," *ACM Comput. Surv.*, vol. 57, no. 9, Art. no. 239, pp. 1–36, 2024. doi: 10.1145/3727641

[34] Ministry of Communication and Information Technology, *National Cyber Security Policy 2080*, Government of Nepal, Kathmandu, Nepal, 2023. [Online]. Available: https://mocit.gov.np/content/7119/7119-national-cyber-security-policy/

[35] A. Leukfeldt and T. Hall, "Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries," Security Journal, vol. 35, no. 4, pp. 1242-1263, Sep. 2022. [Online]. Available: https://link.springer.com/article/10.1057/s41284-022-00357-y

[36] M. Berenblum and A. Bossler, "New directions in cybercrime research," Journal of Crime & Justice, vol. 42, no. 5, pp. 495-499, 2019. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/0735648X.2019.1692426

[37] A. Gryszczyńska, "The impact of the COVID-19 pandemic on cybercrime," *Bull. Pol. Acad. Sci. Tech. Sci.*, vol. 69, no. 4, Article no. e137933, 2021. doi: 10.24425/bpasts.2021.137933. [Online]. Available: http://journals.pan.pl/Content/120374

[38] D. Wall, "Broadening our understanding of cybercrime and its evolution," Journal of Crime and Justice, vol. 47, no. 4, pp. 423-427, 2024. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/0735648X.2024.2323872

[39] S. Chen, M. Hao, F. Ding, D. Jiang, J. Dong, S. Zhang, Q. Guo, and C. Gao, "Exploring the global geography of cybercrime and its driving forces," *Humanit. Soc. Sci. Commun.*, vol. 10, no. 1, p. 71, Feb. 2023. doi: 10.1057/s41599-023-01560-x

[40] T. Hall and U. Ziemer, "Cybercrime in Commonwealth West Africa and the Regional Cyber-Criminogenic Framework," *Commonwealth Cybercrime Journal*, vol. 1, no. 1, pp. 5–25, 2023. [Online]. Available: https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-03/D19156-CCJ-1-1-Cybercrime-CW-West-Africa--Hall-Ziemer.pdf

[41] R. Broadhurst, P. Grabosky, M. Alazab, and S. Chon, "Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime," *International Journal of Cyber Criminology*, vol. 8, no. 1, pp. 1–20, 2014. [Online]. Available: https://research-management.mq.edu.au/ws/portalfiles/portal/62156293/Publisher+version+%28open+access%29.pdf

[42] H. M. Melaku, "A Dynamic and Adaptive Cybersecurity Governance Framework," *J. Cybersecur. Priv.*, vol. 3, no. 3, pp. 327–350, 2023, doi: 10.3390/jcp3030017.

[43] M. Nouh, J. R. C. Nurse, and M. Goldsmith, "Towards Designing a Multipurpose Cybercrime Intelligence Framework," in *Proc. 2016 Eur. Intell. Secur. Informatics Conf. (EISIC)*, Uppsala, Sweden, 2016, pp. 153–156, doi: 10.1109/EISIC.2016.018.

[44] S. Ismaeel, "The Impact of Digital Literacy on Cybercrime Awareness, Victimization, and Prevention Measures: A Study of Cyberbullying in Saudi Arabia," Pakistan J. Criminol., vol. 17, no. 1, pp. 77–96, Jan.–Mar. 2025. [Online]. Available:https://www.pjcriminology.com/wp-content/uploads/2025/01/6_The-Impact-of-Digital-Literacy-on-Cybercrime-Awareness-Victimization-and-Prevention-Measures.pdf

[45] K. Achuthan, S. Khobragade, and R. Kowalski, "Cybercrime through the public lens: a longitudinal analysis," *Humanit. Soc. Sci. Commun.*, vol. 12, Art. no. 282, 2025, doi: 10.1057/s41599-025-04459-x.

[46] I. Bernik, K. Prislan, and A. Mihelič, "Country Life in the Digital Era: Comparison of Technology Use and Cybercrime Victimization between Residents of Rural and Urban Environments in Slovenia," *Sustainability*, vol. 14, no. 21, Art. no. 14487, 2022, doi: 10.3390/su142114487.

[47] M. Bada, A. Hutchings, Y. Papadodimitraki, and R. Clayton, *An Evaluation of Police Interventions for Cybercrime Prevention*, University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CL-TR-983, Jul. 2023. doi: 10.48456/tr-983. [Online]. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-983.pdf

[48] Hai, T. N., Van, Q. N., & Thi Tuyet, M. N. (2021). Digital Transformation: Opportunities and Challenges for Leaders in the Emerging Countries in Response to Covid-19 Pandemic. *Emerging Science Journal*, *5*, 21–36. https://doi.org/10.28991/esj-2021-SPER-03

Appendices

Applications Received at Nepal Police Headquarters Cyber Bureau

Date of Preparation: 2082/02/20 (Bikram Sambat Calendar)

1. Applications Received – Medium-wise Report by Fiscal Year

Fiscal Year (B.S.)	Facebook/Messenger	Viber	IMO	YouTube	WhatsApp	WeChat	Twitter	Instagram	Telegram	Website Hacking	Google	TikTok	Email	Esewa, Khalti, Bank	Org. Institution	Total
2077/2078	3451	4	17	56	47	0	15	65	0	28	0	70	29	28	96	3906
2078/2079	3956	3	18	60	96	0	17	76	0	12	0	233	23	65	127	4686
2079/2080	6782	18	22	69	285	0	34	551	0	45	0	721	69	196	221	9013
2080/2081	16096	21	15	69	981	0	14	1114	0	13	0	690	117	376	224	19730
2081/2082	8604	28	20	75	2013	5	9	988	1388	10	10	2235	115	371	268	16139

2. Applications Received – Gender-wise by Fiscal Year

Fiscal Year (B.S.)	Boy	Girl	Women	Men	Others	Total Applications
2077/2078	56	152	2003	1471	124	3906
2078/2079	41	142	2389	1898	216	4686
2079/2080	46	130	4590	3735	512	9013
2080/2081	253	382	8745	9583	767	19730
2081/2082	289	341	6705	8458	346	16139

3. Current Trends in Cybercrime

- Photo Mutilation: Adding someone’s face onto various nude or inappropriate images using online tools.
- Revenge Porn: Publishing explicit photos and videos on social media as an act of revenge.
- Ransomware Attack: Taking control of all digital information and demanding ransom to release it.
- Defamation/Impersonation: Using someone else's name or photo to create a fake social media profile to defame or emotionally harass them.
- Hacking & Unauthorized Access: Hacking government or organizational websites and defacing them.
- Online Fraud/Scam: Scams involving lottery, inheritance, bonuses, malware, and similar tactics.

Fiscal Year (A.D.)	**Boy**	**Girl**	**Women**	**Men**	**Others**	**Total Applications**	**Growth rate**
2021/2022	41	142	2389	1898	216	4686	19.97
2022/2023	46	130	4590	3735	512	9013	92.34
2023/2024	253	382	8745	9583	767	19730	118.91
2024/2025	289	341	6705	8458	346	16139	-18.20