SAFEGUARDING ECONOMIC STABILITY IN THE AGE OF DIGITAL TRANSFORMATION

Ayubov Rakhmatullo Ravshanbek ugli
Leading Speacialist, Institute of Macroeconomics and Regional Studies under the Cabinet of Ministers of Uzbekistan, r.ayubov@imrs.uz, +998902222388

Annotation: Cyberattacks are increasingly affecting Uzbekistan's economic growth by causing direct financial losses, disrupting digital services, and raising operational costs for organizations. By the end of 2025, the typology of recorded cyber offences expanded from 18 to 62 categories, with growing incidents of personal data theft, AI-enabled impersonation (deepfakes), and malware distribution. In Tashkent alone, reported cases exceeded 16,000 and losses approached UZS 2 trillion, while the clearance rate remained below 8%. This paper discusses how AI-driven threats and ransomware-as-a-service may intensify economic risks in 2026 and argues that reducing national cyber losses requires faster detection and response. It proposes establishing an AI-based Analysis and Monitoring Unit within UZCERT to continuously analyze telemetry and automate early containment actions.

Introduction

Rapid digitalization has become a central driver of economic growth in Uzbekistan, enabling higher productivity, improved service delivery, and broader participation in the digital economy. The expansion of e-government platforms, online financial services, and data-driven business processes is reducing transaction costs and accelerating innovation across multiple sectors. However, this transformation also expands the national attack surface: as more critical functions, assets, and data flows move into interconnected digital environments, vulnerabilities scale alongside connectivity.

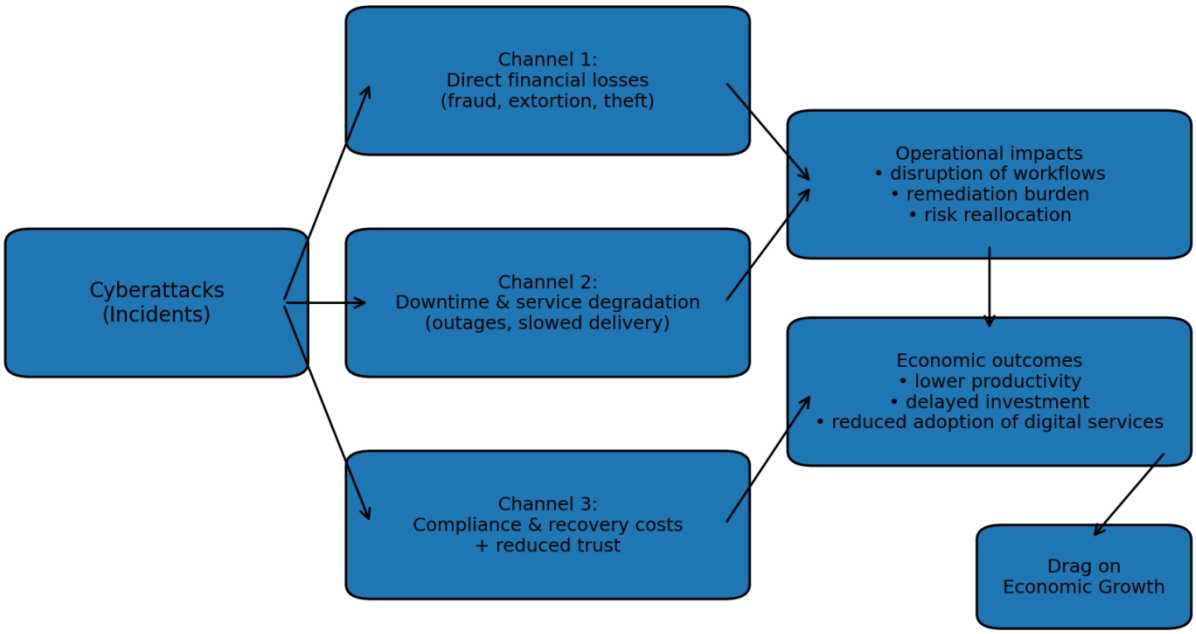
Consequently, cybersecurity can no longer be treated solely as a technical or IT operational concern. It has evolved into a macro-relevant economic factor that can influence growth through direct financial losses, disruption of essential digital services, increased compliance and recovery expenditures, and erosion of trust in digital channels. In this context, strengthening cyber resilience is not only a security priority but also a prerequisite for sustaining the long-term economic benefits of digital transformation.

Economic impact pathway

Cyberattacks affect Uzbekistan's economic growth through three primary transmission channels (***Figure 1***). **First**, they generate **direct financial losses** via fraud, extortion, theft, and the associated costs of incident response and remediation. These losses reduce firm profitability and household welfare, lowering reinvestment capacity and weakening consumption. **Second**, cyber incidents cause **downtime and service degradation**, disrupting business operations and public digital services; such interruptions create productivity losses, operational backlogs, and opportunity costs that can accumulate

across interconnected systems. **Third**, cyberattacks increase **compliance and recovery expenditures** (e.g., for forensic investigations, legal and regulatory actions, system hardening, and continuity measures) while simultaneously **eroding trust** in digital channels. Reduced trust can slow adoption of e-services and digital payments, diminishing the productivity gains expected from digital transformation. Collectively, these channels reallocate resources from growth-enhancing investment toward defensive spending and recovery, producing a measurable drag on overall economic performance.

Figure 1. Conceptual pathway linking cyber incidents to macro-relevant economic effects



Threat outlook for 2026

The 2026 threat outlook points to **faster and more scalable cyberattacks** driven by three reinforcing factors: **(i) AI-enabled automation**, which lowers attacker effort and accelerates phishing, social engineering, and post-compromise activity; **(ii) Ransomware-as-a-Service (RaaS)**, which industrializes extortion and enables less-skilled actors to launch high-impact campaigns using shared tooling and infrastructure; and **(iii) supply-chain compromise**, where attackers exploit third-party software and service dependencies to reach multiple downstream victims. These dynamics increase the probability that incidents expand beyond IT into **critical infrastructure and industrial control systems (ICS/OT)**, raising the risk of operational disruption rather than data loss alone[1].

Building on this threat outlook, the core operational and research challenge is **speed with precision**: as AI-enabled campaigns, RaaS ecosystems, and supply-chain intrusions increase both **volume** and **complexity**, defensive teams must reduce the window in which attackers can escalate, move laterally, and translate compromise into economic harm especially in environments where IT incidents can spill into **ICS/OT** and cause real-world disruption. Therefore, this study is motivated by the need to measurably reduce **Mean**

[1] https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf

Time to Detect (MTTD) and **Mean Time to Respond (MTTR)**, since faster detection and containment directly lower expected loss per incident and limit propagation across interconnected systems. In high-telemetry settings, traditional rule-based monitoring and manual triage increasingly suffer from alert overload and rapidly shifting attacker behavior, leading to delayed decisions and inconsistent response quality. **AI-enabled monitoring**, applied to telemetry such as email flows, network traffic, authentication events, and endpoint logs, offers a scalable mechanism to detect anomalies earlier and trigger standardized containment actions more quickly linking improved cyber defense performance to reduced aggregate economic damage.

Proposed solution

This thesis proposes establishing an **AI-based Analysis & Monitoring Unit** inside **UZCERT** to operationalize **continuous, intelligence-driven defense** at national scale. The unit extends UZCERT's core mandate centralized collection and analysis of cyber-threat information and rapid incident response by embedding **AI** capabilities that can process high-volume telemetry and convert detections into coordinated action[2].

The proposed contribution has three integrated pillars:

1. **Continuous telemetry analytics**: build a unified pipeline to ingest and correlate telemetry (e.g., email flow, network traffic, authentication/endpoint logs) for real-time anomaly detection, threat scoring, and situational awareness consistent with continuous monitoring principles.
2. **Containment playbooks (SOAR-style response)**: codify standardized response playbooks for common incidents (phishing, credential abuse, malware, ransomware precursors), enabling faster and more consistent containment aligned with incident handling guidance and response playbook practice.
3. **AI assurance (governance + security controls)**: introduce lifecycle controls for models used in monitoring and decision support drift monitoring, performance/FP-FN tracking, audit trails, and protections against model/data attacks to ensure trustworthy and secure operational use of AI.

Operationally, this unit also provides a structured interface for **active defense and coordination** with public/private stakeholders, drawing on international collaborative defense approaches and common threat-modeling language (for playbook mapping and reporting).

Conclusion

Cyberattacks should be treated as an economic risk factor for Uzbekistan as digitalization expands the national attack surface and increases losses through direct financial damage, service disruption, and rising recovery/compliance costs alongside declining trust in digital channels. The 2026 outlook suggests faster and more scalable attacks driven by AI-enabled automation, ransomware-as-a-service, and supply-chain compromise, increasing the likelihood of spillover into ICS/OT and higher-consequence operational disruption. To reduce this growth-dampening effect, the thesis emphasizes

[2] https://uzcert.uz/en/about/

"speed with precision" by lowering MTTD/MTTR and proposes establishing an AI-based Analysis & Monitoring Unit within UZCERT that combines continuous telemetry analytics, standardized containment playbooks, and AI assurance controls to enable earlier detection, faster containment, and measurable reduction in aggregate economic loss.

REFERENCES:

1. NIST, "SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations." https://csrc.nist.gov/pubs/sp/800/137/final
2. MITRE, "MITRE ATT&CK®." https://attack.mitre.org/
3. UK NCSC, "NCSC Annual Review 2025." https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf
4. CISA, "Federal Government Cybersecurity Incident and Vulnerability Response Playbooks." https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf