State Technical Service

AI-Driven Threats

Privacy and cybersecurity as constitutional values

Kazakhstan’s legal framework increasingly treats data protection, cybersecurity and responsible AI governance as foundations of public trust.

Constitutional reforms

Stronger protection of privacy, personal data and digital rights

Law «On Informatization»

National cybersecurity mandate, critical infrastructure and KZ-CERT status

Personal data protection

Secure processing of citizens’ data in a rapidly digitalizing state

Communications & digital policy

Secure services, trusted infrastructure and responsible innovation.

Privacy
+
cybersecurity
+
AI trust

now sit in one policy frame

KZ-CERT | National CERT of Kazakhstan: monitoring, response, resilience

Established in 2009 and granted national status under the Law «On Informatization», KZ-CERT provides national-level coordination and 24/7 assistance.

National coordination

Citizens & organizations

Critical infrastructure

24/7 channels

1400 hotline, Telegram channels, email and cert.gov.kz portal

Incident coordination

Government systems, Kazakhstan Internet segment and critical infrastructure

Proactive capabilities

Penetration testing, digital forensics, malware analysis, threat hunting

Cyber defense is stronger when intelligence moves faster

KZ-CERT is a full member of 6 international cybersecurity alliances and has signed 16 MoUs with national CERTs and cybersecurity organizations

6 **international alliances**

FIRST, APWG, TF-CSIRT, OIC-CERT, CAMP, APCERT

16 **MoUs signed**

incl. Azerbaijan, Türkiye, Uzbekistan, Japan, China, UAE

2012

FIRST
APWG
TF-CSIRT

2015

OIC-CERT

2019

CAMP

2020

APCERT

The scale of attacks changed dramatically in 2025

Blocked attacks against Kazakhstan’s critical infrastructure almost doubled year-on-year

1.15B

blocked cyberattacks in 2025

Jan 1–Dec 31, 2025

552M

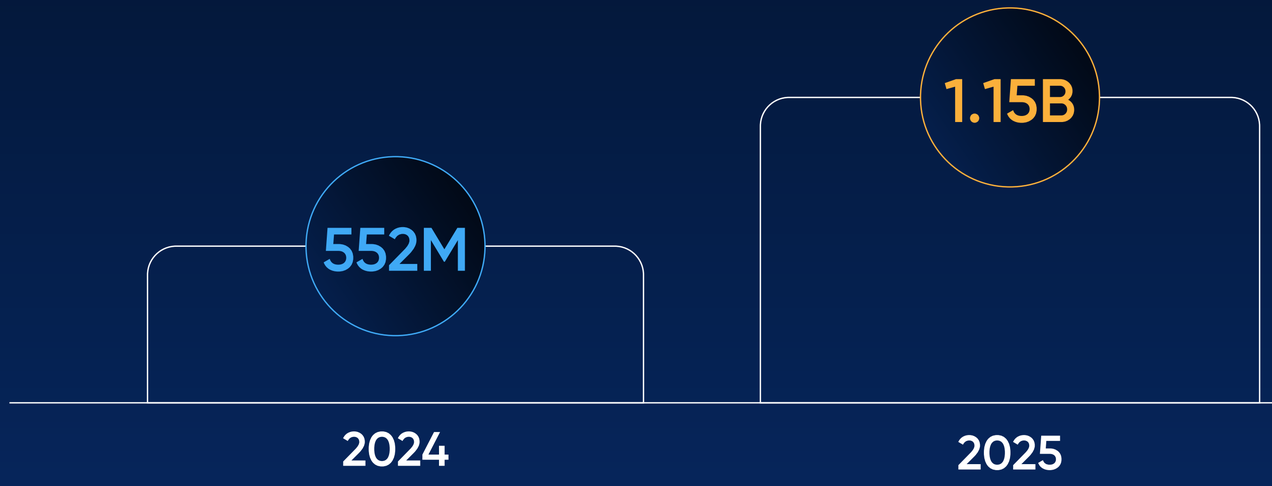
cyberattacks in 2024

baseline comparison

3.9K

attacks per day

average 2025 volume



≈2.1× increase

More than 7,900 DDoS attacks were identified and mitigated in 2025, including around 4,000 targeting government organizations

The same technology now accelerates both attack and defense

Attackers use AI to

- automate phishing and social engineering
- generate malicious content and code
- identify vulnerabilities at scale
- adapt tactics faster than manual response

Defenders use AI to

- analyze telemetry and anomalies
- automate triage and response
- predict risks before escalation
- scale SOC operations responsibly

But the rules are not the same — and that is the core asymmetry

Why defenders cannot simply «move fast and break things»

The strategic problem is not only technology. It is the unequal operating environment of malicious actors and national defenders

ATTACKER	DEFENDER
Needs to succeed once	Must protect continuously
Can scale with minimal cost	Must defend complex ecosystems
Has high risk tolerance	Must be legal, ethical and accountable
Adopts offensive AI immediately	Must validate, govern and integrate safely

From reactive protection to resilient, adaptive cyber defense

Kazakhstan’s response is focused on building a digital ecosystem that can absorb shocks, adapt to machine-speed attacks, and preserve trust.

Resilience

Critical infrastructure protection, continuity and rapid recovery

AI governance

Responsible, secure and accountable use of AI systems

Autonomous SOC

AI-assisted detection, triage, playbooks and response

Secure transformation

Digital services built with security and privacy by design

Strategic priority:

national AI resilience

Kazakhstan and Azerbaijan face shared threats — and need shared defense

To our Azerbaijani partners

Cyber threats do not respect borders, sectors or time zones. A DDoS campaign, phishing wave or AI-generated intrusion can move through regional ecosystems faster than formal processes can respond.

Cooperation gives us speed: trusted contacts, threat intelligence exchange, coordinated response and joint learning before crises escalate.

Shared threats
require shared defense

CONTACTS

Ulykbek Shambulov

First Deputy Chairman at JSC State Technical Serivce –
Head of the National Coordination Center for Information Security