TSARKA | Cybersecurity leader in Central Asia

IV NATIONAL CYBERSECURITY FORUM, BAKU (AZERBAIJAN)

Digital Sovereignty in the Era of Global Challenges

- Redefining the Rules of Engagement in Global Cyberspace
- **A Holistic Approach to National Security:** Software, Hardware, and Cloud
- Public-Private Partnership (PPP) as the Cornerstone of Genuine Cyber Defense

Olzhas Satiyev
Founder & CEO, TSARKA

BAKU 2026

International Ecosystem of Trust: TSARKA and the OTS Cybersecurity Council

TSARKA

The Leading Cybersecurity Ecosystem in Central Asia (Est. 2015)

Global Footprint

ITU · First · OIC-CERT Computer Emergency Response Team

First 24/7 Commercial SOC in Kazakhstan

Key Recognitions

STANDOFF · TechCrunch

GISEC Cyber Drill Winners (Dubai)

Strategic Vision

Initiation of a Cybersecurity Council for OTS Member States (Proposed by Kazakhstan's President Kassym-Jomart Tokayev at the 12th OTS Leaders' Summit in Gabala)

The Core Postulate: Technological Independence = Political Independence

Cyberspace as a New Theatre

of Inter-State Confrontation

Foreign IT Stacks in Critical Infrastructure

A Hidden Systemic Vulnerability

The Imminent Threat of External Paralysis

over State Governance

Core Principle: No Country or Region Can Remain Politically Independent if it is Technologically Dependent

The Engine of Cyber Defense: Legalizing Crowdsourcing & Trusted PPP

State Agencies Cannot Cover the Entire Perimeter Alone

The Need for Private Sector Agility

Establishing Safe Harbor

Moving the White-Hat Community from a Legal Vacuum to a Validated Framework

Institutionalized Interaction Rules

and Legal Vulnerability Payouts

The Scientific Shift

Practical PPP Success Driving the State to Allocate Targeted Research Grants for Sovereign Cyber R&D

The First Pillar: Tumar.One Platform & Open Source for the OTS

- **Tumar.One:** The Largest National Bug Bounty Platform in Central Asia (Covering)

ECOSYSTEM SCALE

4,000+	7,200+	3,300+
Researchers	Verified Reports	Critical Digital Assets Protected

- **Real-World Impact:** Prevented Takeovers of Capital Water Supply Infrastructure, eGov Portals, and Leaks of 7M+ Patient Medical Records

os.tumar.one — **Free Open-Source Version**

The Second Pillar: Hardware Sovereignty & Combating Hardware Backdoors

The Deep Threat: Hardware-Level Implants and Hidden Kernel Backdoors Bypassing Software Defenses

TAUTAN Secure Phone

Zero Trust Architecture

- Isolated Environments
- Bring Your Own Encryption
- FPGA Shield Against Hardware Implants

TAUTAN Security Key

Proprietary FIDO2 Hardware Token

- Protecting VPN, SSH
- Dev Pipelines (CI/CD, GitHub/GitLab)
- Against Phishing and Social Engineering

Full Sovereign Control Over the Engineering, Firmware, and Assembly Chain

būlt.ai

The Third Pillar: Global Shift Towards Sovereign Clouds

Value Migration

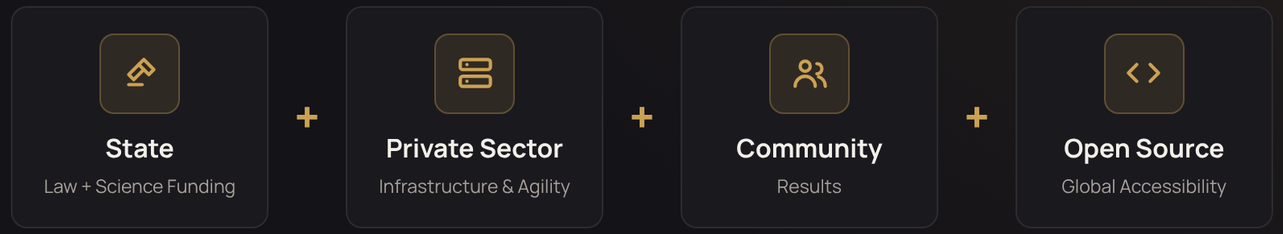
The Global Shift from Commodity Infrastructure (IaaS) to Managed Platform Services (PaaS)

Strict Regulatory Mandates for Absolute Data Localization

Within National Borders

Bult.ai (3 Years of R&D)

A Proprietary PaaS Platform Delivering 1-Click Code Deployment (Zero Config, Auto-Scaling)



= Secure OTS Space

Driving Collective Cyber Resilience Across the Region
Complete Readiness to Share Technologies, Source Code, and Practical Blueprints within the OTS