Central Asia Cybersecurity Baseline Study: Executive Summary

Team Europe Initiative on Digital Connectivity in Central Asia: Cybersecurity Component

June 2025

Authors: Kadri Kaska, Merle Maigre, eGA (lead editors)
Design: Dada OÜ

This synthesis report is based on the national Cybersecurity Baseline Studies authored by:
Siim Alatalu, Mari Tomingas-Sibul, Hanna Urva (Kazakhstan Cybersecurity Baseline Study)
Markko Künnapu, Klaid Mägi, Elsa Neeme (Kyrgyzstan Cybersecurity Baseline Study)
Andro Gotsiridze, Merle Maigre, Mari Tomingas-Sibul (Tajikistan Cybersecurity Baseline Study)
Piret Hirv, Mari Tomingas-Sibul (Uzbekistan Cybersecurity Baseline Study)

This publication has been produced with the assistance of the European Union within the project „ Team Europe Initiative on Digital Connectivity in Central Asia: Cybersecurity Component" (Contract number: Multipartner Contribution Agreement 700002428). The contents of this publication are the sole responsibility of its authors and can in no way be taken to reflect the views of the European Union.

Find out more about the project ega.ee/project/cybersecurity-central-asia/

The e-Governance Academy (eGA) is an Estonian centre of excellence to increase the prosperity and openness of societies through digital transformation. In more than 20 years, we have cooperated with more than 300 organisations from 145 countries, supporting a more efficient use of information and communication technologies in governance and democratic processes. The core of our team consists of the architects and founders of the Estonian and Ukrainian digital state.

Find out more about eGA at ega.ee

Follow us on social media:

Contents

About the project

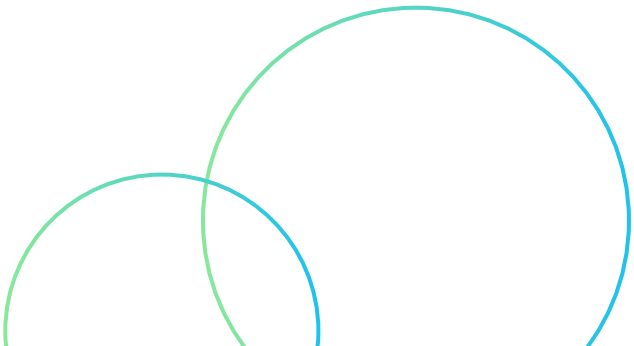
This report summarises the findings of the cybersecurity component of the "Team Europe Initiative on Digital Connectivity in Central Asia" project. The project aims to promote digitally driven socio-economic inclusion in Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan by enabling safe and inclusive access to satellite connectivity across the region.

This report synthesises the results of the assessment conducted in each of the four countries and offers actionable, non-binding recommendations to support strategic planning, guide donor engagement, and provide a roadmap for strengthening national cyber resilience.

The project comprises four components:

1. Policies and regulations to foster the development and use of ICT connectivity, implemented by CPVA (lead), HAUS, Expertise France (EF).
2. Improved public and private connectivity services, with a focus on rural areas, gender equality and marginalised groups, implemented by CFLA (lead), CPVA, HAUS.
3. The use of satellite-based technologies to foster local digital innovation and tackle local challenges, implemented by EF (lead), CFLA.
4. Cybersecurity frameworks, implemented by EF and eGA.

Component Four of the project, focused on **Cybersecurity Frameworks**, is jointly implemented by Expertise France (EF) and the e-Governance Academy (eGA). This component supports participating countries in strengthening their cybersecurity capacities and enhancing their responsiveness to cyber threats through establishing resilient cybersecurity governance mechanisms and improving national cybersecurity capabilities.



eGA experts meeting with stakeholders in Tajikistan

Specifically, the work includes:

- Assessing national cybersecurity capacities and gaps, and proposing appropriate frameworks.
- Providing legal, regulatory, policy, and procedural advisory services for cybersecurity frameworks, aligned with international best practices.
- Delivering comprehensive capacity-building for public authorities, CSIRTs, and other key national stakeholders, with a focus on technical training and incident response.
- Raising public awareness on cybersecurity issues.
- Fostering regional and international cooperation on cybersecurity.

Within this objective, eGA conducted a detailed Cybersecurity Baseline Study in each of the four participating countries, covering four key focus areas of cybersecurity:

1. Governance, institutional and legal frameworks,
2. Critical information infrastructure protection and risk management,
3. CERT/CSIRT capacities, and
4. Public awareness of digital security.

The study was built on a three-step mixed-methods approach:

1. **Desk research (Feb–Mar 2025)**, conducted by eGA experts using publicly available sources and eGA's in-house expertise. The data was validated via widely recognised validation methods for information quality assurance consistent with those applied in the management of the eGA National Cyber Security Index (NCSI). This phase provided initial insights into national cybersecurity ecosystems.
2. **Survey and field interviews (Apr–May 2025)**: Semi-structured interviews held with key national and international stakeholders, including public authorities responsible for or involved in designing, implementing, and evaluating national cybersecurity capabilities and related regulation or legislation, private sector actors, academia and the education sector, and representatives of European Union delegations and international organisations based in each country.[1] Interviews were guided by a survey developed by eGA, consistent with the NCSI and ENISA's CSIRT Maturity Assessment Model and exploring the four core areas of cybersecurity noted above.
3. **Field visits (Apr–May 2025)**: Site visits were made to key national cybersecurity institutions and stakeholder organizations in each country. The findings from these engagements enhanced the study's understanding of institutional maturity and real-world challenges.

1 A list of interviews and interviewees is provided in the relevant annex of each country report.

The study was designed to provide a nuanced, comprehensive and up-to-date picture of each country's cybersecurity capacities and institutional ecosystem, thereby allowing to build a strategic understanding of the needs and resources that determine their cybersecurity development journey. In particular, this awareness allows to recognise key challenges, understand how each country can improve their cybersecurity capacities and frameworks, and to propose recommendations to guide the development of greater national cyber resilience, based on locally validated information and insights.

The findings of the study are captured in an individual Cybersecurity Baseline Study for Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. Recommendations are grounded in international norms and practices but tailored to the local context, with an emphasis on regional cooperation, institutional reform, and long-term capacity building. This report synthesises the results of the assessment conducted in each of the four countries and offers actionable, non-binding recommendations to support strategic planning, guide donor engagement, and provide a roadmap for strengthening national cyber resilience.

Geopolitical Context and Recent Developments

EU-Central Asia relations have grown in importance in the past years, developing a strong, multi-faceted, and forward-looking partnership. Recent EU policy developments and initiatives are a strong asset allowing to offer European know-how, experience, and models to Central Asian partners under this project. The EU's engagement in Central Asia is based on and guided by the EU Strategy for Connecting Europe and Asia (Connecting Europe & Asia: The EU Strategy | EEAS) and the Digital Decade Policy Programme (Digital Decade Policy Programme 2030 | Shaping Europe's digital future), which emphasise commitment to a secure, safe, and sustainable digital transformation that puts people at the centre, in line with core EU values and fundamental rights.

Astana – the capital of Kazakhstan

Digital transformation and cybersecurity posture in the region

Over the course of the past decade, Central Asian countries have embraced economic reform and digitalisation to varying degrees, linking these efforts to broader goals of modernisation, governance reform, and geopolitical positioning. However, the scale, focus, and implementation of their digitalisation efforts varies, as does the maturity of their cybersecurity frameworks and capacities.

Kazakhstan (KZ) is geographically the largest and most resource-rich country in the region, with a population of 20 million. Situated in a strategic location between China, Russia, and the Central Asian republics, Kazakhstan has been transitioning towards a knowledge-based economy, where digitalisation is seen as both an economic enabler and a geopolitical asset. KZ has pursued rapid digitalisation and improved cybersecurity through infrastructure expansion and IT upskilling initiatives. A new high-ranking priority appears to be AI, with a dedicated strategy adopted in 2024.

In 2014, KZ adopted the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) as a metric for measuring its progress in cybersecurity and invested in developing a legal, technical and organisational framework for cybersecurity. It has made strong advances, with steady progress across global digital development and cybersecurity indices. Still, while digitalisation is perceived as a political priority, cybersecurity investment trails behind, reflecting a familiar usability-security trade-off.

Kyrgyzstan (KG), a lower-middle-income parliamentary republic with a population of 7.28 million, has a competitive telecom sector, especially in mobile broadband, where penetration rates have been high over half a decade and 5G services began pilot testing in 2024. Overall technology adoption, though, lacks the pace of significant progress, and international indices report substantial gaps in ICT regulatory environment and regulatory quality. Cybersecurity has gained policy visibility in response to rising threat levels, but the country is still early-stage in cybersecurity maturity, signifying a basic cybersecurity commitment but with some capacity and cooperation gaps.

Tajikistan (TJ), with its population of approximately 10 million, remains at the early stages of digital transformation and experiences underinvestment in digital governance and cybersecurity. Its digital infrastructure is underdeveloped, and, while recognising the importance of digitalisation, the country lacks a coherent national strategy or institutional framework to support it. Recent international indices

highlight the urgent need for legal and policy reform, with low scores across strategic, organizational, and technical capacities. There have been signs of progress in basic legal provisions (cybercrime).

Uzbekistan (UZ), with a population of 35 million, is a lower-middle-income economy and bordered by all other Central Asian republics. With abundant natural resources and traditional industrial production, it has in recent years been implementing extensive economic and social reforms and is actively working to attract foreign investment. Government-led programmes have modernised and expanded the digital infrastructure. The country is also improving in internet speed and ICT service volume. The mobile broadband market is in a rapid growth stage, driven by the young population's high demand for digital services. With market demand for digital services and service volumes rapidly growing, and cybercrime becoming a rising problem, cybersecurity is increasingly prioritized by the government. In 2024, the ITU classified Uzbekistan under the *Tier 2 – Advancing* category, which denotes significant progress in cybersecurity development. Its areas of relative strength are cooperation, legal and capacity development measures, while technical and organisational maturity is still developing.

		KZ	KG	TJ	UZ
Digitalisation	ICT Development Index 2024	90.1	88.3	N/A	81.7
	Network Readiness Index 2024	50.52 (61st)	44.16 (86th)	N/A	44.87 (81st)
	UN E-Government Development Index 2024	0.9009 (24th)	0.7316 (78th)	0.5606 (123rd)	0.7999 (63rd)
Cyber-security	National Cybersecurity Index (NCSI)	70.83 (32nd)	60.00 (40th)	15.83 (84th)	55.00 (50th)
	ITU Global Cybersecurity Index (2024)	Tier 2 – Advancing (94.4)	Tier 3 – Establishing (65.59)	Tier 4 – Evolving (25.36)	Tier 2 – Advancing (89.2)

Cyber threat environment and trends

Cyberattacks have grown in variety and impact across all four countries in recent years, with financial institutions, government agencies, and media among the most targeted. There have also been attacks against industry and critical infrastructure, and attack campaigns have occasionally singled out journalists and political activists, mainly in Kyrgyzstan. The most common threat vectors include malware (notably ransomware), phishing and credential theft, as well as exploitation of public-facing systems, leading to data breaches and system compromises causing operational disruption. Email and social media account hijacking, doxxing, and mobile malware deployment have also been reported, particularly in Kazakhstan.

Poor cybersecurity awareness, widespread use of outdated or unlicensed software and infected external devices – all of which are common across the region – exacerbate vulnerabilities. While the private sector, particularly in finance and telecom, has strengthened cybersecurity measures, public sector infrastructure remains exposed. In Tajikistan, many government websites lack security certificates, and the widespread use of foreign servers and cloud-based email services by public institutions raises data sovereignty and jurisdictional concerns.

Notably, sophisticated threat actors are active in the region. In 2025, a group dubbed Silent Lynx targeted Kyrgyzstan and neighbouring states, using complex, multi-stage attacks aimed at government and diplomatic institutions. These leveraged social engineering and exfiltrated data via Telegram bots. Since 2020, Tajikistan has been the focus of prolonged cyber-espionage by the Russian-affiliated group Nomadic Octopus (DustSquad), which infiltrated telecom infrastructure to monitor high-ranking government officials and public systems. Although their tools were technically not sophisticated, the operations managed to compromise a wide range of networks and devices.

Poor cybersecurity awareness, widespread use of outdated or unlicensed software and infected external devices – all of which are common across the region – exacerbate vulnerabilities.

Street view in Samarkand, Uzbekistan

Findings

eGA experts meeting with stakeholders in Kazakhstan

Strategic and legal framework for cybersecurity

The four Central Asian countries trend towards integrating cybersecurity into their broader digital agendas, but approaches differ significantly in prioritization, maturity, and implementation. Effective governance and resilience across the region is undermined by persistent gaps in legal frameworks, institutional clarity, and enforcement capacity.

Kazakhstan leads with the most solid strategic framework, anchored in its CyberShield strategies (2017, 2022) and the 2023 Concept for Digital Transformation, ICT Development, and Cybersecurity. **Kyrgyzstan** and **Uzbekistan** embed cybersecurity within digitalisation strategies; however, both are still updating legal frameworks and institutional structures. **Tajikistan** is in a more embryonic stage of policy development, drafting its first national cybersecurity strategy with ITU support. Three of the countries (KZ, TJ, and UZ) have also signalled ambition towards AI through the adoption of dedicated strategies.

Cybersecurity-related strategic agendas across the region commonly target infrastructure and institutional development, incident response capacity, personal data protection, public awareness, and legal reform. Implementation challenges persist, however:

- overlapping institutional mandates,
- inconsistent application of concepts and terminology,
- limited contingency planning, and
- a shortage of skilled personnel are common.

In Uzbekistan, institutional responsibilities are not yet clearly defined, and coordination mechanisms could be further strengthened. Kyrgyzstan's new cybersecurity law awaits several implementing acts, while being part of an ongoing, broader digital governance overhaul. Tajikistan faces limitations in stakeholder engagement and has room to enhance the inclusiveness of its policy processes.

Effective governance and resilience across the region is undermined by persistent gaps in legal frameworks, institutional clarity, and enforcement capacity.

Across the region, cybersecurity is often approached through a personal data protection lens, which narrows institutional mandates and challenges alignment with broader national security, critical infrastructure resilience, and digital service continuity goals.

Legal references to cybersecurity are scattered across laws on data protection, telecommunications, e-commerce, and electronic signatures, their enforcement is often weak and regulatory accountability remains limited. Tajikistan in particular encounters challenges related to institutional overlap and gaps, with responsibilities not always clearly defined, and regulatory powers remaining largely limited in practice. Clearer mandates, coordination among state agencies, and practical enforcement mechanisms remain important areas for development across all four countries.

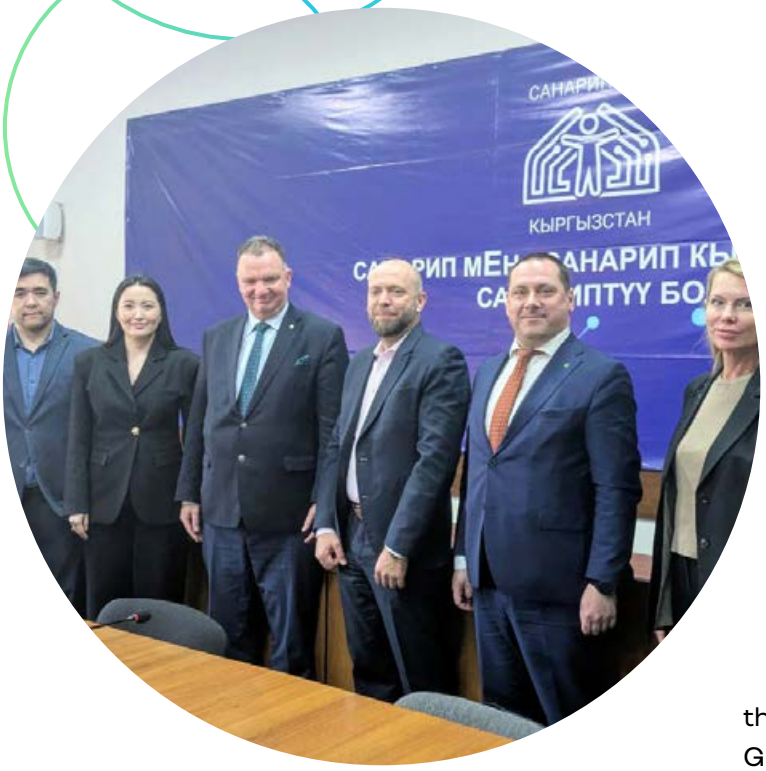
In terms of cybersecurity legislation, Kazakhstan and Kyrgyzstan both provide for CII designation and related obligations in national law; Kazakhstan also has mandated incident monitoring linked to ICT audits. Uzbekistan has formal CERT authority and certification rules, but practical enforcement is limited, and some operational CII resilience frameworks could be improved. Kyrgyzstan's response framework is still under development, and Tajikistan has yet to establish a functional CII or fully enforceable incident response structures.

All countries are increasingly aware of international frameworks, such as the EU GDPR or the Council of Europe Budapest Convention, and interested in harmonisation to some degree, but objectives differ. Kazakhstan, for instance, is interested in extracting useful elements rather than full alignment, including for the drafting of its new AI law. It is cautious about over-regulation, which has been seen as problematic in the EU due to its potential to limit or constrain innovation.

Main institutions responsible for cybersecurity

Most Central Asian countries now have designated lead ministries or national agencies tasked with developing and coordinating cybersecurity policy, typically housed under ministries for digital development or innovation. Still, common institutional challenges persist in terms of some overlapping mandates (notably in Uzbekistan and Tajikistan), lack of clear interagency coordination mechanisms, and weak enforcement capacity. All countries also report shortages of skilled personnel.

Kazakhstan has the most mature institutional framework, with a two-tiered governance structure in place (Information Security Committee under the Ministry of Digital Development, Innovation and Aerospace Industry; and State Technical Service under the National Security Committee) with defined roles in policy, regulation, and technical oversight. It also stands



eGA experts meeting with stakeholders in Kyrgyzstan

Common institutional challenges persist in terms of some overlapping mandates, lack of clear interagency coordination mechanisms, and weak enforcement capacity. All countries also report shortages of skilled personnel.

out with an established CERT and SOC infrastructure. **Kyrgyzstan's** cybersecurity governance system also demonstrates a relatively well-developed structure, as it evolves and matures further. The Ministry of Digital Development and Innovative Technologies, amongst its digitalisation-related tasks, is responsible for cybersecurity policy, while the Coordination Centre under the State Security Committee is the main government body responsible for policy implementation and operating the national CERT. Recent institutional developments (such as a new SOC) indicate further progress, but key implementing acts remain pending.

Tajikistan is in early stages of development, with a clear government-level commitment to strengthening national cybersecurity capabilities. An institutional base is being built with new bodies like the Communications Service under the Government, and the Agency for Innovation and Digital Technologies, established in 2024, tasked with both strategic and operational cybersecurity leadership, and operating as the main driver of digital transformation and relevant legislation in the country.

Uzbekistan has formalised its institutional architecture, including the Cybersecurity Centre under the State Security Service, but legislation remains fragmented and lacks clarity regarding institutional mandates. The UZ-CERT remit is focused narrowly on government systems. Agencies like Uzkomnazorat provide regulatory support, but interagency cooperation and cross-sectoral engagement are weak.

There is also an increasing recognition of the importance of public-private partnerships, particularly in Kazakhstan and Kyrgyzstan. Kazakhstan has established meaningful public-private engagement (e.g. with TSARKA, a leading private CERT, and Transtelekom, a major telecom operator with an own CERT), with the largest ICT

operator National Information Technologies JSC (NITEC) managing Kazakhstan's e-government infrastructure, operating a 24/7 SOC, and also engaging with both private and public entities internationally. Kyrgyzstan has growing, although still limited, coordination with the private sector. Tajikistan's initiatives such as the IT Park and planned Tier 3 data centre within the Smart City Dushanbe indicate national ambitions, while their success depends on sustained resources and continued skills development. The establishment of the University of Innovation and Digital Technologies points to the Tajik government's commitment to building long-term digital competence.

eGA experts meeting with stakeholders in Kazakhstan

International cooperation and capacity building

Central Asia is heading toward greater international integration in cybersecurity, with all four countries engaging in international cooperation, albeit with distinct country-specific strategies. While engagement is expanding through treaties, multilateral platforms, and bilateral partnerships, operational capacity needs to catch up with strategic ambition, and there is room to enhance institutional continuity. Cyber diplomacy generally remains a side task within broader ministries (such as trade or security) across the region. Nonetheless, there is demonstrable interest and capacity to absorb international support, particularly from the EU and other key partners.

Regional cooperation is increasing, with several cross-border cybercrime projects and joint training exercises by OSCE.

Kazakhstan leads both in diplomatic and operational engagements, aiming to position itself as a regional leader in digitalisation and cybersecurity. Its officials emphasise autonomy in navigating between Western, Russian, and Chinese models. Kazakhstan participates actively in UN (OEWG), OSCE (ICT security working group, Confidence Building Measures) and was, in 2023, invited to join the Budapest Convention. It is party to the CSTO, CIS, SCO, and OTS frameworks and has hosted regional cybersecurity events. Its national and private CERTs (KZ-CERT, TSARKA) are connected to international platforms such as OIC-CERT and CAMP. The State Technical Service (STS) has signed cybersecurity MoUs with Turkey, Azerbaijan, and Afghanistan.

Kyrgyzstan emphasises standards alignment and technical cooperation, working to harmonise its cybersecurity standards with international benchmarks such as ISO/IEC, IEEE and IETF, but also with the Russian GOST. While its institutional base is still developing, it benefits from sustained donor engagement and is investing in international capacity-building partnerships, notably with OSCE, KOICA, and the EU.

Uzbekistan maintains a non-aligned foreign policy but advocates greater connectivity within and beyond Central Asia. While remaining outside the CSTO and its engagement with the CIS and SCO frameworks is modest, it participates in ITU, OSCE, OIC, and CAMP networks. It also engages in bilateral and regional MoUs, including with Turkmenistan. Cooperation with the EU and the United States continues to grow, notably in cyber resilience and digital governance.

Tajikistan remains in an early development phase but is building competence through donor-funded programmes. Its new Agency for Innovation and Digital Technologies is a central coordination body for digital cooperation, currently involved in over €170 million worth of externally funded projects. However, it faces challenges with institutional continuity and absorption capacity.

All four countries benefit from capacity-building efforts, with different levels of depth and coordination. Kazakhstan and Kyrgyzstan participate in regional OSCE exercises; Kyrgyzstan has also engaged in EU Twinning and KOICA SOC development projects. Uzbekistan benefits from bilateral EU and US support, while Tajikistan relies heavily on donor coordination platforms such as its Digital Development Working Group.

Regional cooperation is increasing, with several cross-border cybercrime projects and joint training exercises by OSCE. However, donor-driven efforts often lack long-term sustainability, making handover strategies, domestic training budgets, and clearer institutional anchoring essential. International support can add most value where it reinforces country-led reforms and strengthens long-term institutional capacity. Where appropriate, efforts to foster regional and donor coordination could reduce duplication, align investments, and reduce strain on the existing limited capacities in target countries to improve their impact and effectiveness.

Critical information infrastructure protection and risk management

All four countries acknowledge the strategic importance of critical information infrastructure (CII) protection but are at different levels of legal and operational maturity. Legal frameworks exist, but implementation is uneven, and there remain noteworthy gaps in CII identification and risk management, institutional mandates, and technical capability.

Kazakhstan has the most advanced framework. A 2022 governmental decree formalised the status of 'critically significant objects of information and communication infrastructure' and mandated stringent cybersecurity requirements, which include SOC-style operational information security centres (OTsIB), incident monitoring, reporting, and audit obligations, as well as service location and reliability requirements. In 2023, 514 objects were classified as critical. An annual review

Common regional challenges include unclear institutional mandates, overlapping regulatory roles, and uneven technical capacity across public and private operators.

mechanism, overseen by the Ministry of Digital Development, Innovation and Aerospace Industry, keeps classifications current. Yet, security standards vary, as do organisational disparities in terms of implementation. Only 54 certified OTsIBs exist, and the rigid licensing process complicates quality control, as there is no mechanism for reassessment or revocation.

Kyrgyzstan has enacted core implementing regulations as of April 2025, defining CII sectors, CII identification criteria, and a certification system for cybersecurity tools, as well as cybersecurity audit requirements. However, the necessary CII identification methodology is still pending and the law is not yet implemented in practice. Information security requirements intended for application by public entities and CII operators are only in early drafting stages.

Tajikistan is in the earliest phase of development. Its legislation currently covers only public institutions, and there is no CII designation or registry. A national cybersecurity strategy (2025–2030) is being developed, and private sector engagement and risk management processes are just emerging. Practical implementation will require substantial capacity building and interagency coordination.

Uzbekistan, under its 2022 Cybersecurity Law, provides broad definitions for CII and risk-based classification. It mandates monitoring systems, reporting, and mitigation, but implementation remains inconsistent. Many operators are uncertain of their status or obligations, and the implementation of cybersecurity requirements faces multiple institutional and technical challenges. Uzbekistan's Central Bank CERT (CERT-CBU) in the banking sector is a rare example of sector-specific more advanced maturity.

Common regional challenges include unclear institutional mandates, overlapping regulatory roles (e.g. telecom operators also acting as regulators in TJ and UZ), and uneven technical capacity across public and private operators. Incident response mechanisms are available mostly where legislative maturity is higher (KZ, UZ), but even so, most countries are yet to establish comprehensive crisis response planning and regular testing. Sectoral

readiness is stronger in banking and energy than in healthcare, education, or general administration. The emerging need for cloud usage policies and local data centre information security standards appears to complicate work, with blanket prohibition on cloud use being a significant barrier to modernising digital services and ensuring resilience.

Kazakhstan has adopted a national cyber crisis response plan, but it needs to be tested through cybersecurity exercises. Uzbekistan has expressed strong interest in tabletop exercises and train-the-trainer formats to test joint incident response readiness and support the creation of a national cyber incident master plan.

While foundational elements are in place in varying degrees, Kyrgyzstan and Tajikistan would benefit from further support to build CII registries, risk frameworks, and functional governance systems. Across the region, there is a demand for improved coordination between public and private stakeholders, sector-specific risk assessments, and targeted training and certification to build a sustainable cybersecurity workforce.

CERT/CSIRT capacities

All countries in the study recognise the importance of CERTs/CSIRTs and aim to establish or expand incident response capabilities. Kazakhstan leads with a mature, multi-layered CERT ecosystem combining public and private CERTs (all members of FIRST) which offer advanced services such as intrusion detection, malware analysis, vulnerability assessment, etc. Over 50 technical response centres (OTsIBs) support the protection of critical infrastructure, currently covering around 10% of CII operators and with their numbers increasing due to legal requirements. Close public-private cooperation, notably between the STS and TSARKA, reinforces Kazakhstan's operational strength.

Kyrgyzstan's has a partially operational national CERT, but it remains somewhat under-resourced and has gaps in technical expertise. Uzbekistan has two active CERTs (one government-based, the other under the Central Bank), focused on public services and the financial sector, respectively. Tajikistan remains in the planning phase, with its national CERT yet to be established.

Beyond Kazakhstan, though, overlapping institutional mandates, gradually improving cross-sector coordination, and unclear private sector roles continue to pose challenges. There is a shared interest in joining global and regional cybersecurity platforms such as FIRST and OIC-CERT, and in developing sector-specific CERTs, particularly for finance. Furthermore, workforce shortages are common across the region, with scarcity of expertise in malware analysis, threat hunting, and incident response. Qualified cybersecurity professionals tend to be concentrated in capitals, with limited specialist training opportunities available to them.

While the strategic direction is clear and international alignment is a priority, further support is needed to strengthen coordination, develop specialist expertise, and extend response capacity beyond urban centres.

Kazakhstan leads with a mature, multi-layered CERT ecosystem combining public and private CERTs.

	Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan
National CERT status	Fully operational	Partially functional	Not yet established	Operates within national security
Sectoral CSIRTs	Financial + mandated SOCs	None established	Planning underway in draft strategy	Financial (Central Bank)
Private sector role	Strong participation (TSARKA etc.)	Absent	Minimal, *ad hoc* response	With the Central Bank's CERT
International cooperation	FIRST members, threat intel sharing	Member of OIC CERT, plans for FIRST	ITU and EU support for setup	Part of FIRST/ OIC CERT, finance only

Cybersecurity education

The four countries are at the opposite ends of the scale in integrating cybersecurity training into the public education system. **Kazakhstan** and Kyrgyzstan have introduced digital literacy and cybersecurity into official school curricula. Kazakhstan partners with international actors like UNICEF and offers extracurricular training through initiatives like TSARKA's Cyber School. **Kyrgyzstan** has similarly introduced basic digital safety content into education policy. In contrast, **Tajikistan** and Uzbekistan grapple with inconsistent internet connectivity outside major cities, and ICT-qualified teachers are scarce. However, both countries are taking steps to catch up: Tajikistan's education ministry is training teachers and introducing cyber hygiene topics in schools, and **Uzbekistan** has adapted ITU's Guidelines on Online Safety for national use.

Tertiary-level cybersecurity education is expanding. Dedicated undergraduate and postgraduate programmes exist in Kazakhstan, Kyrgyzstan, and Uzbekistan, with Tajikistan embedding basic cybersecurity in broader ICT programmes. Universities have begun aligning curricula with international guidance and now include topics such as network security, cryptography, and, increasingly, digital forensics and cyber law, with degree programmes in cybercrime and cyber law launched within some governmental training institutions.

Kazakhstan supports access to higher education through scholarship programmes and encourages industry partnerships and practical training components like Capture the Flag competitions, which bring practical training to traditionally theoretical higher education. Private sector-led training initiatives in Kazakhstan and Kyrgyzstan further offer practical, skills-based instruction to both government and industry professionals.

Cybersecurity research is limited but growing, with Kyrgyzstan hosting a dedicated centre focused on applied research. Cross-university collaboration remains underdeveloped, though partnerships with international and private sector actors are increasing (and the latter tend to be led by the private sector rather than academia).

Despite progress, however, gaps persist in public sector training, research infrastructure, and cross-sector coordination.

Overall, while there is no uniform model across the region, the trajectory is toward increased institutionalisation, practical engagement, and stakeholder cooperation. International support, notably from ITU and OSCE, has helped build capacity through targeted programmes, mostly focused on government (e.g. law enforcement) and technical personnel (forensics). Despite progress, however, gaps persist in public sector training, research infrastructure, and cross-sector coordination.

Public cybersecurity awareness

Overall public cybersecurity awareness remains low, especially among older adults and rural populations. While mobile usage is high, knowledge of cyber risks and personal data protection is limited, and many citizens still expect the state to protect from them cyber threats, rather than understanding individual responsibility and agency. Awareness among women and seniors is particularly low.

Kazakhstan stands out with a number of awareness campaigns conducted over the recent years, led by both governmental and civil society actors; it provides an online learning platform (a similar initiative exists in **Uzbekistan**), and annual cyber hygiene training for public officials. **Kyrgyzstan's** Personal Data Protection Agency has a dedicated training centre, and **Tajikistan** relies on smaller-scale efforts led by civil society groups, albeit both with limited reach and funding.

Efforts to raise awareness are often fragmented and project-based, with limited coherence or coordination amongst the actors driving them. While there is growing recognition of the need for digital and cybersecurity literacy, coordinated and sustainably funded national strategies need further enhancement.

Overall public cybersecurity awareness remains low, especially among older adults and rural populations.

Eight Recommendations

Based on these findings, the study recommends targeted actions organised by thematic areas and focusing on actions to be taken by national stakeholders and support that the project can offer.

Strategic cybersecurity planning

To strengthen strategic cybersecurity planning, the study recommends targeted support for drafting and refining national cybersecurity strategies and related policy documents, aligning cybersecurity strategy with digital transformation and incorporating governance, risk management, and compliance principles in the national strategic toolbox. Assistance could include comparative insights from EU member states, offering technical guidance on structuring strategic frameworks, contributions to national working groups, and expert input into policy design. Tested models should be promoted to help ensure strategies are coherent, realistic, and produce impact. Throughout these activities, attention should be given to aligning national objectives with international standards and best practices, including those reflected in the EU's cybersecurity approach.

Developing legal frameworks

To support the development of modern, coherent legal frameworks, the study recommends EU assistance in drafting and reviewing cybersecurity-related legislation, drawing on NIS2, GDPR, the AI Act, and eIDAS (electronic identification, authentication and trust services directive) as reference points. Priority areas for legislative action include public sector information security requirements, responsibilities of CII providers, and tasks related to incident prevention and response, with a focus on modernising terminology, clarifying institutional roles, and aligning implementation mechanisms. Project support should extend beyond primary legislation to encompass implementing regulations, methodologies, and procedures. Also, given that national stakeholders emphasised the need for practical guidance, tools like model templates, expert-led workshops, advisory support, and sharing EU best practices for implementation can be valuable. To reinforce stakeholder engagement and ensure consistency in interpretation and application, activities such as legal peer exchanges, targeted training, and stakeholder consultations should furthermore be considered in the scope of this work.

Strengthening institutional capacity

To reinforce institutional capacity, targeted support should focus on building the skills of legal, policy, and operational staff through structured training, technical workshops, and curriculum support aligned with international cyber norms. Participation in international conferences, study visits, and regional dialogues is encouraged to foster cross-border cooperation and knowledge exchange.

Emphasis should also be placed on clarifying interinstitutional roles and enabling more structured coordination among public sector bodies and private sector stakeholders. National role and mandate clarification should extend to sector-specific institutions to formalise their roles in the institutional architecture. Formal collaboration platforms should be created for public-private engagement, covering areas of policy development, risk planning, and incident response. Project support here could draw on EU models to ensure structured, accountable cooperation with private sector and civil society actors; where relevant, successful domestic initiatives can be identified and scaled up with targeted technical assistance and participation in regional or EU-supported networks. Additionally, formalising strategic cooperation with trusted European partners will enable sustained knowledge transfer and alignment with international best practices.

Enhancing critical information infrastructure

To enhance critical information infrastructure resilience, the study recommends targeted support for developing legal and procedural frameworks for CII designation with clear designation criteria, as well as adopting security standards, risk management frameworks, and compliance supervision mechanisms. Project assistance could include sharing EU experience in methodologies for identifying and classifying critical infrastructure, risk management methodologies, and guidance on supervisory and audit frameworks. Technical training on risk management and information security standards should be prioritised, complemented by the exchange of best practices.

The capacity of sector-specific regulators and CII operators requires particular attention: preparedness through advanced training in incident response, threat intelligence, and ICS/SCADA security should be promoted, with emphasis on job-specific learning and train-the-trainer formats. Technical and tabletop exercises, supported by national cyber ranges, should be conducted at institutional and interagency levels to test crisis response and promote regional cooperation. As noted above, public-private platforms for threat intelligence exchange and risk planning are needed to build trust and enable coordinated action. Countries should be further encouraged to institutionalise incident response plans and test them through national and regional exercises.

Support may also target cybersecurity risk assessments in emerging technologies, including biometric digital identity and AI-enabled services, and assist in drafting certification standards aligned with EU practices.

Strenghtening CERT/CSIRT capabilities

To strengthen national CERT/CSIRT capabilities, support should focus on establishing and operationalising incident response entities in line with international standards. This includes assistance in developing SOPs, certification processes, and training schemes.

Human and technical capacity gaps should be addressed via advisory support, structured training, study visits, and provision of technical equipment and knowhow, as most appropriate in the particular circumstances, given the uneven readiness of incident response entities across the countries. Priority training areas include ICS/SCADA protection, threat intelligence, malware analysis, intrusion detection, network defence, digital forensics, and legal aspects of digital evidence. Scalable, standardised training models should be co-developed with universities and private sector partners to ensure a sustainable supply of talent.

Interagency and cross-border exercises are recommended to improve joint incident response, and there is local interest for joint drills and simulations with Central Asian cybersecurity stakeholders and their EU counterparts. In addition to procedural, training, and infrastructure support, the project could facilitate technical and tabletop exercises (national, interagency, cross-border); assist in setting up cyber ranges; and foster collaboration with ENISA and global incident response communities.

Increasing public awareness

Public awareness efforts should be selective and tailored to national contexts. In Kazakhstan, where general campaigns are well established, further broad initiatives would likely offer limited value. On the other hand, Uzbekistan may benefit from nationwide campaigns addressing prevalent threats like phishing and online fraud. Regional outreach should prioritise youth, rural populations, and public servants. Partnering with youth centres and innovation hubs to deliver interactive workshops, cyber hygiene campaigns, and capture-the-flag competitions can further digital literacy and early career interest. Standardised cyber hygiene training for civil servants should be promoted; where possible, existing e-learning platforms such as Uzbekistan's AIstudy.uz should be leveraged for that purpose. Aligning outreach with international initiatives (e.g. Cybersecurity Awareness Month) can enhance both credibility and impact. Authorities should also encourage public-private partnerships and cooperation in these areas, and coordinate awareness efforts to maximise their impact without duplicating already existing campaigns. Institutional partnerships between governments, academia, and civil society should be formalised to promote continuity and reduce dependence on external grants.

Strengthening cybersecurity education

Efforts to scale up cybersecurity education should focus on improving academic capacity and modernising curricula. Introducing cybersecurity modules in school and university IT programmes and integrating challenge-based learning formats can help build foundational knowledge and practical skills. Particular attention should be given to strengthening bachelor's and master's level programmes and producing job-ready graduates for both public and private sectors. Collaboration between educational institutions and cybersecurity agencies should be formalised, particularly around (co-)developing curricula and enabling faculty exchanges.

Curriculum design and training formats would benefit from technical assistance and collaboration with EU academic and training institutions. EU study visits and faculty exchanges to exchange teaching methodologies and research practices can be a starting point for deeper curriculum alignment and academic partnerships.

Developing the workforce

To build a sustainable workforce, practical and inclusive training opportunities must be expanded and aligned with labour market needs. Programmes targeting working-age adults and upskilling IT professionals should be promoted, alongside national initiatives to attract foreign experts and reskill domestic talent. International formats, such as Estonia's Kood/Jõhvi, offer adaptable models for adult cybersecurity education. Structured collaboration with EU academic and training institutions will be key to curriculum development and training delivery. Finally, regional and international forums, including cybersecurity conferences, should be used to promote exposure to global best practices, bilateral engagement, policy dialogue, and visibility of national efforts.

By focusing on these key areas – strategic coherence, legal clarity, strengthening institutions and coordination, CII protection, incident response, targeted awareness, and workforce development – Central Asian countries could significantly strengthen their national cybersecurity. The project's support can amplify and sustain these efforts, help close capacity gaps, and align regional approaches with EU and international best practices.

e-Governance Academy
Ahtri 6, 10151 Tallinn, Estonia
+372 663 1500 | info@ega.ee | ega.ee
Facebook, LinkedIn: egovacademy