

No. 27, March 2026

# EUCAM Watch



 **EUCAM**  
WWW.EUCENTRALASIA.EU

 **CESS** Centre for  
European  
Security Studies

**Navigating cyber threats  
on a digital Silk Road**

Photo: AI

## Editorial - Navigating cyber threats on a digital Silk Road

Digitalisation and cybersecurity are central items on the agendas of Central Asian countries, both in domestic policy debates and in engagement with international partners. As states across the region expand digital infrastructure and services, questions of governance, security, and regulation have gained prominence. Accordingly, Central Asian states are making, to varying extents, progress in articulating national approaches to digitalisation that are formally reflected in policy frameworks. Meanwhile, China and Russia are extending their influence in Central Asia through strong positions in the digital domain, while the European Union (EU) has also established a presence through its Global Gateway initiative on digital connectivity.

As I write these lines, I am reminded of a conversation dating back to 2018, when I was actively encouraging greater attention to cybersecurity research in the region. During a meeting in Almaty, Kazakhstan, several colleagues responded with a mixture of scepticism and humour. As one put it bluntly, 'We don't even have stable electricity, and you want us to focus on cybersecurity?'. The remark captured a widely shared perception that cybersecurity was a distant, almost abstract concern – something to be addressed only after more basic infrastructural challenges had been resolved. Yet it also revealed how digital risks were being underestimated precisely because they were seen as secondary to material development, rather than as deeply entangled with it. Since then, reports of petty cybercrime in Central Asia have increased consistently; and while stable electricity remains an issue, the volume and nature of cyber threats have evolved disproportionately.

This issue of *EUCAM Watch* explores how Central Asian states are navigating this complex terrain. It opens with a regional overview of developments in digitalisation and cybersecurity, highlighting both convergence and divergence. Matei Ciocan shows that national strategies, laws, and institutional frameworks adopted to improve digital governance and cyber resilience have produced differentiated outcomes. Kazakhstan and Uzbekistan have positioned themselves as regional frontrunners, investing heavily in institutional capacity, e-government services, and legal frameworks. Kyrgyzstan is progressing more slowly, while Tajikistan and Turkmenistan continue to lag behind, constrained by limited infrastructure, fragmented governance, and weak institutional capacity. This uneven landscape underscores a core theme running through the issue: digitalisation does not follow a single path, nor does it automatically translate into greater security or resilience.

Several contributions in this issue show that cybersecurity challenges in Central Asia cannot be reduced to technical deficits alone. In *Kyrgyzstan*, digitalisation has been accompanied by the rise of digital vigilantism, with citizens using platforms such as *Telegram* and *Instagram* to publicly expose, shame, and punish alleged offenders. As Samir Sultanov demonstrates, these practices thrive in a context of low trust in state institutions and limited law enforcement capacity in the digital sphere.

*Tajikistan* lacks a solid legislative base for digitalisation. As Alisher Melikov argues, the country's digital transformation has advanced without the foundational elements required for cybersecurity governance, including a national strategy, an operational Computer Emergency Response Team (CERT), and data protection legislation.

Tajikistan's reliance on foreign technologies, particularly from China and Russia, combined with limited oversight and domestic expertise, raises significant concerns about digital sovereignty and long-term resilience.

The interviews with Madina Tursunova from *Uzbekistan* and Tlegen Kuandykov from *Kazakhstan* illustrate how digital leadership in the region brings its own challenges. Uzbekistan's rapid digital expansion has been accompanied by growing awareness of the need for rights-based governance, yet gaps remain in data protection, judicial oversight, and multistakeholder participation. Kazakhstan, meanwhile, has adopted ambitious strategies on digitalisation, cybersecurity, and artificial intelligence, positioning itself as a regional hub.

The case of *Turkmenistan*, explored by Jos Boonstra and Matei Ciocan (with input from EU interviews), represents perhaps the opaquest approach to digitalisation. While formal laws and programmes exist, limited transparency makes it difficult to assess their implementation or effectiveness. At the same time, the EU's engagement with Turkmenistan through the Team Europe Initiative on Digital Connectivity illustrates how external actors seek to promote digital development, cybersecurity capacity, and regulatory reform even in highly restrictive environments.

As digitalisation accelerates, the stakes are likely to grow. Cyber threats can quickly evolve from petty crime into risks to critical infrastructure. The articles and interviews in this issue make it clear that there are no easy solutions. They nevertheless point to areas where progress is possible: clearer legal definitions, stronger institutions, investment in human capacity, and greater engagement with civil society. This issue of *EUCAM Watch* provides a set of grounded analyses that reflect the region's diversity and complexity. In doing so, it invites policymakers, practitioners, and researchers to think beyond rankings and strategies and to engage more deeply with the social and political dimensions of cybersecurity on the digital Silk Road.

***Rashid Gabdulhakov, assistant professor, Centre for Media and Journalism Studies, University of Groningen; EUCAM associate researcher, the Netherlands.***

## Table of Contents

<b>2</b>	<b><i>Editorial – Navigating cyber threats on a digital Silk Road – Rashid Gabulhakov</i></b>
<b>4</b>	<b><i>Article – Central Asia's cybersecurity and digital governance – Matei Ciocan</i></b>
<b>8</b>	<b><i>Article – Digital vigilantism in Kyrgyzstan – Samir Sultanov</i></b>
<b>9</b>	<b><i>Article – Tajikistan's digital catch-up – Alisher Melikov</i></b>
<b>11</b>	<b><i>Interview on Uzbekistan – Madina Tursunova</i></b>
<b>12</b>	<b><i>Interview on Kazakhstan – Tlegen Kuandykov</i></b>
<b>14</b>	<b><i>Article – Turkmenistan can't go at it alone – Jos Boonstra and Matei Ciocan</i></b>
<b>16</b>	<b><i>EUCAM Publications</i></b>

## Article – Central Asia’s cybersecurity and digital governance

*Matei Ciocan, intern at CESS, the Netherlands*

Central Asia has taken important steps in digitalisation and cybersecurity through the adoption of national strategies, new legislation, and international cooperation initiatives over the past decade. Once considered one of Asia’s least developed and least modernised regions, it has begun to close the gap with its regional peers. Progress, however, is uneven. Kazakhstan and Uzbekistan are frontrunners in digitalisation and cyber resilience, Kyrgyzstan is advancing more slowly, while Tajikistan and Turkmenistan often top international rankings for cybercrime exposure while remaining at the bottom of those for digitalisation.

According to World Bank data, internet use in Central Asia has increased steadily over the past 30 years. Kazakhstan currently leads this trend, followed closely by Kyrgyzstan and Uzbekistan. Turkmenistan records the lowest level as a result of extensive state-imposed internet restrictions, and available assessments rely on outdated figures.

Country	Most Recent Year	Internet Users (% of population)
Kazakhstan	2024	93%
Kyrgyzstan	2023	88%
Tajikistan	2023	57%
Turkmenistan	2017	21%
Uzbekistan	2023	89%

*(Table 1 – Internet users as a percentage of the population – values extracted from the [World Bank](#))*

Regarding cybersecurity capabilities, the ITU Global Cybersecurity Index (see table below) also points to divergent performances across Central Asia. Kazakhstan and Uzbekistan are emerging as regional leaders, both categorised as Tier 2 (‘Advancing’), indicating well-developed legal, technical, organisational, cooperation, and capacity building measures. Kazakhstan scores particularly strongly in legal, technical, and cooperation measures, while Uzbekistan follows closely in legal and cooperation. Kyrgyzstan is ranked in Tier 3 (‘Establishing’), reflecting solid progress in legal and organisational measures but lagging in capacity development and cooperation. This indicates an uneven yet tangible improvement.

In contrast, Tajikistan and Turkmenistan record significantly lower scores and are placed in Tier 4 ('Evolving'). Their cybersecurity sectors face considerable challenges and require structural improvement. While they register moderate results in legal measures, their scores for technical and capacity-development measures remain low, pointing to both a lack of strategic direction and an urgent need for infrastructure development.

Country	Legal Measures	Technical Measures	Organisational Measures	Capacity Development	Cooperation Measures	Tier Performance 2024
Kazakhstan	20	19.38	18.30	16.36	20	T2 – Advancing
Uzbekistan	19.59	16.22	15.75	17.64	20	T2 – Advancing
Kyrgyzstan	16.71	14.87	16.32	5.53	12.16	T3 – Establishing
Tajikistan	13.30	0	3.62	0.35	8.09	T4 – Evolving
Turkmenistan	10.12	0	10.67	1.85	3.21	T4 – Evolving

(Table 2 – Cybersecurity response measures graded ascendingly from 0 to 20 – values extracted from the [ITU Cybersecurity Report 2024](#))

Over the past decade, Central Asian countries have developed institutions to oversee digitalisation and strengthen cybersecurity. **Kazakhstan** has a wide range of public bodies working in these areas. The Ministry of Artificial Intelligence and Digital Development supervises cybersecurity and ICT, as well as leads the implementation of e-governance through its Information Security Committee. It shares expertise with the State Technical Service, which, through Kazakhstan’s national CERT, monitors internet developments and responds to breaches. In November 2025, Kazakhstan adopted an AI law that sets out responsibilities for developers, operators, and users, regulates applications, and prohibits unlawful data collection and identity-related theft. The law not only introduces regulatory provisions but also promotes the use of AI and the development of new infrastructure.

Since 2022, **Uzbekistan** has had a Ministry of Digital Technologies responsible for e-government policy, ICT, and information security, as well as for overseeing cybersecurity and investment in the digital sector. The Central Bank’s Cybersecurity Centre also contributes to cybersecurity in the financial sector. Together with UZCERT, which works to reduce cyber threats in state-managed internet activity, these bodies form the core of Uzbekistan’s institutional architecture.

Through the Digital Uzbekistan 2030 strategy, the country aims to further digitalise the public sector, expand ICT across the economy, and improve its e-government system. In 2025, the country adopted an AI strategy to guide the use of innovative technologies.

In *Kyrgyzstan*, the Ministry of Digital Development and Innovative Technologies is the main government body responsible for cybersecurity and digitalisation policy. Under the State Committee of National Security, the Coordination Centre on Cybersecurity drafts legislation, implements state policy, works to prevent cyber threats, and operates the national CERT, which is only partially functional. The institutional landscape therefore reflects the country's evolving position in this field. The most recent strategic document, Digital Kyrgyzstan 2019-2023, focuses on the digitalisation of public institutions, the development of ICT clusters, the strengthening of legislation on cybersecurity, e-commerce, and innovation, and the improvement of digital infrastructure.

Institutional development in *Tajikistan* has been slow, with relevant bodies emerging only in the past three years. The Communications Service under the government and the Agency for Innovation and Digital Technologies, established in 2024, are the only institutions with both strategic and operational responsibilities for cybersecurity and digital transformation, including the development of relevant legislation. Public information about their activities remains scarce. No operational CERT exists and there is no overarching national strategy, although a new cybersecurity strategy is currently under preparation.

In *Turkmenistan*, the Ministry of Communications is responsible for implementing policy on cybersecurity, the digital economy, and telecommunications. Public information remains limited. The Law on Cybersecurity was adopted in September 2019, and the Cybersecurity Service was established in the same month. In March 2022, the State Cybersecurity Programme was approved. Beyond these formal measures, however, little is known about the country's legislative framework or its broader approach to cybersecurity and digitalisation.

	Country	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)

*(Table 3 – Rankings on multiple international categorisations – taken from [Team Europe Initiative on Digital Connectivity in Central Asia: Cybersecurity Component Report](#) and reformatted by the author of this article)*

The cybersecurity and digitalisation landscapes in Central Asia thus appear both promising and ambiguous. The ITU Global Cybersecurity Index reveals a clear divide in national efforts to address cyber threats and develop regulatory and institutional frameworks. Kazakhstan and Uzbekistan are the frontrunners, while Kyrgyzstan, Tajikistan, and Turkmenistan remain at earlier stages of development. Nevertheless, legal and institutional progress is visible across all five states, together with a desire to adopt national strategies and establish CERTs. It remains to be seen whether this encouraging trend will endure and whether regional disparities will narrow as Central Asian countries improve their positions in international rankings.

## Article - Digital vigilantism in Kyrgyzstan

*Samir Sultanov, independent researcher (MA in Politics and Security, OSCE Academy in Bishkek), Kyrgyzstan*

In recent years, *Telegram* and *Instagram* channels have become increasingly visible in the digital feeds of Kyrgyz citizens, often promising to 'restore order' by portraying the state as inactive. Users publicly expose alleged offenders, post threatening videos, publish personal information, and call for justice. This practice is increasingly perceived as a normal means of achieving justice, particularly in a context of high distrust in the police and the courts.

Such campaigns are a manifestation of digital vigilantism, in which individuals assume the role of 'judge, jury, and executioner', using social media to track down, harass, and punish those they perceive as guilty. At first glance, this appears to be a quick and effective tool: a message is posted and society itself punishes the offender. However, this approach can have serious personal, ethical, and legal consequences. Here is why:

*First*, digital vigilantism undermines the foundations of the legal system by bypassing formal procedures and guarantees of due process. *Second*, it abolishes the presumption of innocence and deprives those targeted of the opportunity to defend themselves and be heard. *Third*, it increases the risk of mistaken identity, leading to disproportionate harm and the long-term stigmatisation of innocent individuals. In this way, digital vigilantism not only threatens the security of individual citizens but also undermines legal certainty in society, further eroding trust in state institutions.

Kyrgyzstan has a number of laws that partially address digital violence, including the law on false information, the law on personal data protection, and relevant provisions in the Criminal Code. However, significant gaps remain. There are no clear regulations governing phenomena such as digital vigilantism, doxing, online shaming, trolling, and cyberbullying. This creates legal uncertainty and makes it difficult to classify such acts as offences or crimes.

Another challenge is the persistent perception that what happens online is not real. Digital threats and harassment continue to be underestimated in comparison with physical violence. The Ombudsman's Office and local NGOs point to the limited digital literacy of law enforcement officials and the lack of specialised units capable of investigating online offences. This creates a permissive environment in which digital vigilantism can flourish with minimal risk for its organisers.

Combating digital vigilantism requires coordinated action in both the legislative and institutional spheres. *First*, clearer legal definitions of different forms of digital violence are needed. Even if the term 'digital vigilantism' is not used in legislation, regulations can be introduced to cover associated practices such as doxing, online shaming, and harassment. For example, in 2024 the Netherlands criminalised doxing. This enables victims to report cases through formal channels and allows the authorities to respond more rapidly. Proceedings can be initiated more quickly, perpetrators are more easily held accountable, and unlawfully published data can be removed faster.

*Second*, alongside the development of the legislative framework, priority should be given to strengthening the institutional capacity of government bodies involved in combating cybercrime. A national strategy for training law enforcement officers in the prevention and investigation of digital violence is essential. International models, such as the Europol Training Competency Framework for Digital Investigations and the joint Council of Europe-Interpol guide with step-by-step recommendations for national training strategies, can provide valuable guidance in this process.

*Third*, the response should not be limited to the state alone. The Ombudsman's Office, NGOs, human rights organisations, and independent media can play a vital role in monitoring online harassment and hate speech campaigns, providing legal assistance and psychological counselling to victims, and raising awareness of digital rights. Partnerships between government and civil society are crucial for building trust and ensuring that new regulations are implemented in line with human rights standards.

Digital lynching is a symptom of dissatisfaction with weak institutions rather than a viable alternative. Left unchecked, it risks developing into a persistent parallel system of justice based on fear, stigma, and arbitrary punishment. By addressing legal gaps and strengthening institutional responses, Kyrgyzstan now has the opportunity to better protect citizens' rights and to demonstrate that combating crime, including online, remains the sole responsibility of the state, not of anonymous mobs.

### **Article - Tajikistan's digital catch-up**

*Alisher Melikov, MA student in Politics and Security at the OSCE Academy in Bishkek, Kyrgyzstan*

Digital transformation in Tajikistan is reshaping public services, financial platforms, and communication systems. However, three fundamental elements of cybersecurity protection are missing: there is no national strategy, no modern data protection legislation, and no operational CERT. These institutional gaps create security risks for citizens, businesses, and state operations. Tajikistan faces multiple vulnerabilities as weak infrastructure operates under fragmented governance and remains dependent on foreign support.

Tajikistan relies on two main technological systems: Chinese companies, particularly through Huawei's Safe City surveillance systems, and Russian telecommunications infrastructure. The absence of national security standards, independent audits, and effective oversight mechanisms increases the vulnerability of these externally provided systems. These foreign technologies, especially surveillance platforms, create risks of data theft, political control, and physical disruption of critical infrastructure. The lack of domestic technical expertise to assess and protect these systems creates additional challenges for national digital sovereignty. Three challenges stand out:

*First*, Tajikistan does not have a national cybersecurity strategy. In the absence of such a framework, no single institution has clearly defined responsibilities for responding effectively to cyber threats. Ministries and agencies operate independently without shared reporting protocols, resulting in fragmented systems and inefficiency. This prevents the development of cyber defence strategies and incident-response protocols, leaving the country insufficiently prepared for significant cyber incidents.

Closing this gap requires the adoption of a national cybersecurity strategy that would define institutional mandates, establish emergency response systems, set security standards, and distribute financial resources. Such a strategy would provide a clear direction for both government agencies and digital service providers in enhancing their cybersecurity systems.

*Second*, Tajikistan lacks an official CERT, which prevents it from monitoring threats in real time and restricts its ability to join worldwide cyber information-sharing networks. As a result, there is no early-warning system for cyber incidents. Attacks targeting financial services and mobile operators are thus more likely to remain undetected and poorly coordinated at the national level. Establishing a national CERT under the Ministry of Digital Development would help to address this gap. A functioning CERT would enable real-time threat analysis, enhance national preparedness, and connect Tajikistan to regional and global cyber-response networks.

*Third*, Tajikistan's legal framework remains outdated and does not provide clear protection for personal data, resulting in insufficient safeguards for public institutions, businesses, and individuals. Existing legislation fails to establish specific guidelines for the protection of critical infrastructure or for modern cybersecurity standards, leaving public organisations and private businesses without legally-binding security protocols. At the same time, public safety initiatives have enabled the expansion of surveillance technologies which, according to Freedom House and Human Rights Watch, have been used to monitor journalists and opposition groups, thereby threatening both privacy and civil liberties.

The adoption of a personal data protection law in 2018 established only minimal protection standards and requires substantial modifications to meet modern international standards. Aligning the legal system with recognised data protection standards and establishing an independent supervisory body to monitor organisations and enforce regulations would strengthen the system.

More than three million people in Tajikistan access the internet through their mobile devices, yet awareness of basic cybersecurity protocols remains low. The practice of poor cyber hygiene through weak passwords, unlicensed software, and dependence on unregulated digital platforms expose users to fraud, identity theft, and privacy violations. Civil society organisations, including Freedom House and Access Now, have documented rising cyber fraud cases and unauthorised digital account intrusions in recent years.

Additionally, Tajikistan would benefit from digital literacy development. The human dimension requires public education institutions to implement cybersecurity awareness programmes, including within university curricula and civil service training. The development of IT and information security expertise at local universities and through specialised training programmes has started to create a foundation for future capacity building initiatives. International organisations such as the Organisation for Security and Cooperation in Europe (OSCE), the United Nations Development Programme (UNDP), and the World Bank should support these initiatives through technical assistance and capacity building programmes.

Tajikistan would benefit from launching cybersecurity governance reform without delay, as the financial and societal costs of inaction are likely to increase. Protecting citizens, strengthening institutions, and securing the country's digital future require a well-designed cybersecurity plan that international partners support, but that local experts develop.

## **Interview on Uzbekistan**

*Madina Tursunova, independent media lawyer and digital rights expert, Uzbekistan*

***What recent steps has Uzbekistan taken to enhance its digital and cybersecurity environment? Is current legislation sufficient?***

Uzbekistan is rapidly building cyber infrastructure and institutional capacity, but its legislative framework requires further reform to ensure that cybersecurity measures uphold human rights, transparency, and international best practices. The Digital Uzbekistan 2030 strategy envisages areas for the development of digital services, e-government, and the private sector. Meanwhile, the National AI Strategy adopted in 2025 serves as a policy document for strengthening both the legal framework and technology.

Despite these advances, current legislation remains insufficient when measured against international UN and OSCE standards and commitments. The regulatory landscape is fragmented, heavily enforcement-oriented, and lacks comprehensive legal safeguards related to privacy, data protection, digital rights, transparency, and due process. There is no formal mechanism through which independent stakeholders can shape priorities or oversee progress in digital transformation. Uzbekistan also lacks a unified digital literacy strategy, and cyber-prevention measures continue to rely on technical controls rather than on rights-based frameworks. Further gaps include the absence of a standalone cybercrime law (currently under development), limited judicial oversight in certain rapid-response mechanisms, weak accountability for state actors' data practices, the filtering and blocking of online content, and insufficient multistakeholder participation in digital and internet policy design.

***What are the trends in digital media literacy in Uzbekistan, and which areas still require attention?***

According to the May 2025 Asian Development Bank policy report *Harnessing Digital Transformation for Good*, Uzbekistan continues to face low levels of digitalisation and digital skills development. Only about 15 per cent of the population has basic digital skills, and 7-8 per cent has standard skills, which indicates a low level of digital literacy, especially in rural areas. The strategy *Digital Uzbekistan 2030* includes education and training in the field of information technology as a priority area. Thus, digital media literacy in Uzbekistan is advancing as a national priority amid rapid digitalisation, with initiatives emphasising critical thinking, disinformation countermeasures, and youth education.

Meanwhile, media and information literacy has also gained traction through multistakeholder efforts. UNESCO's AIM programme organised workshops in 2025 that brought together universities, media, and civil society to contribute to the development of a national strategy. Youth-focused projects, such as training courses by NGOs like 'Yuksalish' and 'Critical Lens', teach factchecking, instruct on cybersecurity and content analysis, and inspire participants to create awareness blogs. Digital inclusion is also expanding via World Bank-supported programmes targeting vulnerable groups, including people with disabilities, women, and rural youth, in line with the growing number of internet users.

***Is Uzbekistan affected by cyberattacks? If so, what response mechanisms are available in terms of cybersecurity?***

Uzbekistan faces frequent cyberattacks, with over 12 million attempts recorded in 2024 and ongoing threats targeting the government, financial, and IT sectors. Reported incidents include operations by the Bloody Wolf group, which used malicious PDF files and remote-access trojans (RATs) against financial systems, alongside surges in phishing, ransomware, and fraud.

Since 2020, the UZCERT under the Ministry of Internal Affairs has been handling threat monitoring, vulnerability elimination, and rapid incident response. The 2022 Cybersecurity Law requires the identification of vulnerabilities in critical infrastructure and establishes state oversight of compliance with security standards. Technical measures include the rollout of a centralised anti-fraud system; the integration of banking data into a unified platform; parental alerts for minors' transactions; nationwide caller-ID spoofing prevention; and requirements for banks to implement antivirus protection in mobile applications. Enhanced cybercrime investigation mechanisms include rapid-response procedures such as the immediate blocking of suspicious bank cards and the swift transmission of relevant data to law enforcement, along with expert cybersecurity assessments at the pre-investigation stage. Prosecutorial oversight has been expanded through the creation of specialised cybercrime units at both the central and regional levels. These are supported by the development of a secure data-exchange platform connecting the Ministry of Internal Affairs, the Prosecutor General's Office, and the Central Bank, enabling real-time coordination and faster disruption of cyber offenses.

Public awareness is promoted through an annual nationwide cyber hygiene and cybersecurity programme, featuring a dedicated 'Cyberculture Month' each November and targeted online campaigns to inform citizens about emerging risks. While these initiatives and projects have placed cybersecurity and digitalisation on the agenda, there is still a lot of work to do in terms of boosting digital literacy, fine-tuning the legal framework, and protecting citizens and institutions from cyberattacks.

### **Interview on Kazakhstan**

*Tlegen Kuandykov, programme coordinator, CAPS Unlock, Kazakhstan*

***Kazakhstan has recently embraced new digitalisation, cybersecurity, and artificial intelligence strategies and laws that set ambitious goals. How do you see these legislative and policy developments?***

In November 2025, Kazakhstan adopted a comprehensive AI law introducing risk-based regulation, transparency obligations, and provider accountability. In January 2026, a group of parliamentarians codified general digital provisions into a Digital Code covering digital assets, biometric data, and e-government systems. Institutional capacity was further strengthened with the creation of a Ministry of Artificial Intelligence and Digital Development in September 2025 to coordinate policy and implementation.

These measures signal political commitment and create an umbrella framework for digitalisation and AI adoption. Yet, from a legislative standpoint, the sequencing is unusual – first developing the law, then codifying it. Both the AI law and Digital Code lack clarity on procedures, enforcement mechanisms, and public oversight, all of which are essential for safe AI deployment in public services.

High-risk or otherwise forbidden AI applications, such as the online monitoring of citizens' behaviour or emotions, may still be used under broadly defined exceptions, including the protection of constitutional order, public security, or 'human rights'. This reflects recent amendments to the data protection law that were not publicly debated and raises questions about transparency and accountability.

Overall, these policies are an improvement: they simplify governance and offer legal clarity for public agencies and firms, enabling pilot projects and digital service expansion. At the same time, major incidents, such as the 2025 data breach affecting roughly 16 million citizens, highlight weaknesses in operational security. Enforcement efforts are increasing through anti-fraud campaigns and the blocking of fraudulent communications, but consistent application, investment in workforce skills, and the strengthening of public trust remain critical. While ambition is evident, the effectiveness of these laws will depend on precision, oversight, and enforcement, as well as on overall digital governance frameworks and public participation. Without these elements, the reforms risk remaining formal achievements rather than drivers of safer, inclusive digitalisation.

***What do you think are the biggest threats to Kazakhstan in the cyber domain? How does Kazakhstan confront cybersecurity threats, including from a governance perspective?***

The most common risks stem from data breaches, service disruptions, and cybercrime, especially fraud, phishing, malware, deepfakes, and disinformation campaigns. These threats thrive in an environment where digitalisation has moved faster than data protection practices, rule-of-law enforcement, and the development of cybersecurity skills. Limited institutional capacity and a shortage of trained professionals make both the state and citizens vulnerable.

Kazakhstan also faces state-linked cyber threats, including cyber espionage conducted by both domestic and foreign actors. Given its geopolitical position, the country is a potential target for covert operations aimed at accessing government data, critical infrastructure, and communication networks. These risks are compounded by structural dependencies, such as reliance on Russian internet transit routes and the widespread use of foreign cloud services, which increase exposure to external pressure and disruptions beyond national control. The growing use of facial recognition and AI-based urban monitoring systems further raises the stakes, as large volumes of sensitive biometric data become attractive targets.

In response, the government treats cybersecurity as a matter of national security. Alongside the introduction of new legislation, the authorities work with telecommunications operators to block fraudulent calls from foreign numbers, dismantle scam call-centre chains, and coordinate investigations across borders. Dedicated cybercrime and anti-fraud units have been expanded, while training programmes aim to upskill public servants and raise public awareness of cyber fraud. Unfortunately, the development of legal and policy frameworks has not been matched by improvements in enforcement and institutional capacity, limiting the overall effectiveness of these measures.

***How does Kazakhstan relate to its powerful neighbours, China and Russia, in terms of digitalisation? Is the EU able to play a role as a partner of Kazakhstan in terms of digitalisation?***

China plays a major role in the country's technology ecosystem. Chinese firms supply most telecommunications hardware, lay fibre-optic cables, and provide smart-city solutions, including surveillance systems such as Hikvision, which are widely deployed even in apartment building entrances. Brands such as Huawei, Xiaomi, and Oppo also hold a significant share of the smartphone market. This dependence on Chinese smart-industry services increases vulnerability to external pressure.

Russia's influence is equally pronounced, particularly through digital services and platforms such as Yandex, which remain widely used by both government agencies and citizens. Russian regulations and network requirements, including the mandatory deployment of SORM systems, shape both technical and governance practices. Kazakhstan also relies on Russia for high-bandwidth international connectivity, while Russian and Chinese firms dominate cloud and data infrastructure across critical sectors, creating structural dependencies that could be exploited in periods of geopolitical tension.

The EU's role is more normative and advisory. Although it is slower and more bureaucratic, and thus less attractive for rapid infrastructure deployment, the EU does offer guidance on standards, regulatory frameworks such as the AI Act or the General Data Protection Regulation (GDPR), as well as practical examples from countries like Estonia in e-government and public transport digitalisation. EU involvement can help Kazakhstan balance fast digital adoption with interoperability, transparency, and citizen-facing safeguards. However, given current technological and political priorities, the scope for deep cooperation remains limited.

### **Article - Turkmenistan can't go at it alone**

*Jos Boonstra, EUCAM coordinator, CESS and Matei Ciocan, intern, CESS, the Netherlands*

It is difficult to get a sense of where Turkmenistan stands in the cyber and digital realm, as the government provides almost no information on policies or strategies, and very little analysis is available from either local or international observers. What we do know is that people in Turkmenistan have limited access to internet and that state control over the digital domain is tight.

Estimates suggest that between 20 and 40 per cent of Turkmenistan's population has access to internet, compared with around 90 per cent in Kazakhstan, Kyrgyzstan, and Uzbekistan. The state-owned operator TurkmenTelekom holds a monopoly over the domestic market, and censorship is extremely prevalent, particularly affecting news websites and social media platforms. The use of VPNs to circumvent censorship is risky and can lead to arrest. A data protection law adopted in 2017 does little in terms of restricting data collection and sharing.

Of course, Turkmenistan is not immune to cyberattacks. In 2019, a law on cybersecurity was adopted and a State Cybersecurity Service was established under the Ministry of Communications. Moreover, in 2022, a State Cybersecurity programme was also developed, although the authors could not find further information about it. Turkmenistan has recently taken some steps towards international cooperation on cybersecurity and digital matters. One example is the OSCE's Centre in Ashgabat, which organises training in cyber diplomacy. In the area of digitalisation, cooperation with Estonia's e-Governance Academy focuses on knowledge exchange and support for the development of digital government services.

The European Union is one of the few partners working with Turkmenistan on digitalisation. This cooperation is primarily channelled through the Team Europe Initiative on Digital Connectivity that applies to all five Central Asian countries and focuses on improving access to broadband internet through investments in satellite connectivity, regulatory reforms, and capacity building. As one EU official interviewed by the authors noted, 'Cooperation includes efforts to enhance digital skills and promote good governance in the digital sector'. The same official added that 'good governance remains a concern, as Turkmenistan's restrictive environment and limited transparency pose challenges for open digital development. The EU's support aims to encourage reforms that improve regulatory transparency, foster public-private partnerships, and strengthen digital literacy, though progress is often slow due to Turkmenistan's cautious approach to international engagement'.

The Team Europe Initiative also promotes the development of cybersecurity frameworks. As one EU official noted, 'The country has expressed interest in cooperation on cybersecurity, particularly in combating cyber threats, terrorism, and extremism. However, Turkmenistan's closed political system and limited digital openness mean its direct role in regional cybersecurity is constrained compared to other Central Asian states.' The EU nevertheless seeks to involve Turkmenistan, as it 'is interested in Central Asia's cybersecurity landscape because of the region's strategic location between China and Russia – two major cyber powers. By supporting digital connectivity and cybersecurity capacity in Central Asia, the EU seeks to counterbalance the influence of these cyber giants and promote a more diverse, secure, and open digital ecosystem'.

Turkmenistan's digital environment can be characterised by limited public access and extensive state control, with many websites and applications blocked through the government's monopoly over data and its use. On cybersecurity, the country has taken some action, although little is known about the scale of cyberattacks and the quality of the country's defences. There does seem to exist a growing understanding among Turkmenistan's leadership that a 'go at it alone' approach will not suffice in cybersecurity and digitalisation, as reflected in the first cautious steps towards cooperation with European partners.

### **EU-Central Asia connectivity: Using all the pieces**

**EUCAM policy brief No. 39, October 2024**

*Jos Boonstra*

The EU has embarked on a geopolitics-inspired connectivity agenda with Central Asia. While energy security and transition, as well as transport and digitalisation, are prioritised, these issues are being developed separately from ongoing work in the field of democratisation and civil society engagement. The EU should beef-up and integrate human connectivity into its corridor plans, as pipelines, roads, and data cables are only as valuable as people make them.

### **European development cooperation with Central Asia: From abstract to concrete**

**EUCAM policy brief No. 40, December 2024**

*Jos Boonstra and Kamila Smagulova*

The European Union (EU) is a substantial development cooperation partner for Central Asia. As Central Asia has risen in prominence on the European foreign policy radar in recent years, there is increased interest among EU member states to be engaged with the region. But on what? This policy brief outlines eight connectivity project ideas that are characterised by human interaction, with long-term benefits for both Europe and Central Asia.

### **Should Kazakhstan power Europe?**

**EUCAM commentary No. 55, January 2026**

*Douwe van der Meer*

Kazakhstan wants to export green electricity to Europe through the 'Green Energy Corridor'. Electricity shortages in Kazakhstan, its continued reliance on coal, and the risk of export blockades across the Caspian Sea make this a flawed proposition. Instead, a green partnership should focus on integrating renewable energy into Kazakhstan's power grid, while Europe reduces its net emissions abroad.

## **EUCAM podcast**

### **A chat in the Yurt**

Step into our Yurt and join us for a monthly conversation on Europe-Central Asia developments. In the EUCAM podcast, *Yelena Kilina*, *Kamila Smagulova* and *Rashid Gabdulhakov* welcome guests from both regions to discuss exciting new research and the latest developments in Europe and Central Asia.

In 2025, the team chatted about connectivity, succession and legitimacy, education and dialogue, subjective well-being, the Caspian Sea, regional identity, climate change and (GO)NGOs. Join EUCAM in the Yurt via [SoundCloud](#), [Spotify](#), and [Apple](#) podcasts. Be part of the discussion by posing questions and sharing your thoughts on our social media platforms: [LinkedIn](#), [Bluesky](#), and [Mastodon](#).



## EUCAM

Established in 2008 by FRIDE as a project seeking to monitor the implementation of the EU Strategy for Central Asia, EUCAM has grown into a knowledge hub on broader Europe-Central Asia relations. As part of CESS, EUCAM will continue to raise the profile of European-Central Asian relations in general, and more specifically to:

- Critically, though constructively, scrutinize European policies towards Central Asia;
- Enhance knowledge of European engagement with Central Asia through top-quality research;
- Raise awareness on the importance of Central Asia and Europe's engagement, as well as discuss European policies among Central Asian communities;
- Expand the network of experts and institutions from Europe and Central Asia and provide a forum for debate.



## CESS

The Centre for European Security Studies (CESS) is an independent institute for research and training, based in Groningen, the Netherlands. CESS seeks to advance political development, democracy, human rights and in particular security, by helping governments and civil society face their respective challenges.

CESS is an international, multidisciplinary and inclusive institute. Its work is part of the European quest for stability and prosperity, both within and outside Europe. CESS encourages informed debate, empowers individuals, fosters mutual understanding on matters of governance, and promotes democratic structures and processes.