OSCE ACADEMY in Bishkek

POLICY BRIEF

#111

Youth Engagement in Cybersecurity Governance: The Case of Digital Resilience in Uzbekistan

by Olimakhon Ergasheva

MAY
2026

The research underpinning this policy paper was conducted within the OSCE Conflict Prevention Centre's project "Youth Dialogue in South Caucasus and Central Asia" and was made possible through the generous support of the following OSCE participating States: the United States of America, Finland, and Switzerland.

OSCE ACADEMY in Bishkek
POLICY BRIEF
111, MAY 2026

Youth Engagement in Cybersecurity Governance: The Case of Digital Resilience in Uzbekistan

by Olimakhon Ergasheva

Executive summary

Uzbekistan's rapid digital transformation has expanded access to education, economic opportunity, and civic participation. At the same time, it has increased exposure to cyber risks – particularly for young people, who make up more than 60 percent of the population and are among the most active internet users. Despite their central role in the digital ecosystem, youth remain insufficiently prepared for cybersecurity threats and largely excluded from cybersecurity governance processes.

This policy brief draws on a mixed-methods study conducted in May 2025, combining a nationwide online survey of young people aged 18–27 (n=61) with semi-structured interviews with youth governance actors and cybersecurity experts. The findings reveal a pronounced skills-to-use gap: While 93 percent of respondents are online daily, fewer than one-quarter have received any formal cybersecurity education. Phishing, misinformation, and online fraud are the most commonly recognized threats. These risks are compounded by gendered disparities in access to devices, training opportunities, and confidence in online participation, leaving young women particularly vulnerable.

At the same time, youth willingness to engage in cybersecurity policymaking is high. Seventy-two percent of respondents expressed interest in participating in consultations, hackathons, or advisory mechanisms. However, only 18 percent have ever been involved in such activities. Key barriers include limited access to reliable information, perceptions that policy outcomes are pre-determined, technical intimidation, and uncertainty surrounding legal and institutional "red lines" as the boundaries of permissible online expression remain unclear and enforcement is inconsistent.

This policy brief argues that excluding youth from cybersecurity governance represents a missed opportunity for strengthening digital resilience and social stability. It proposes a shift from ad hoc consultation toward structured youth co-governance, including targeted cyber-literacy initiatives, predictable participation pathways, and transparent feedback mechanisms. By equipping and empowering young people as trusted partners rather than passive beneficiaries, Uzbekistan can enhance national cyber resilience while advancing inclusive development and confidence-building objectives in line with OSCE commitments.

Olimakhon Ergasheva is a cybersecurity consultant and researcher with professional experience in IT audit, cybersecurity, and digital risk assessment. She is currently pursuing a master's degree in Cybersecurity in Germany, with an academic focus on security testing, network security, and human-centred approaches to cyber resilience. Her professional and research work has engaged closely with youth-focused initiatives on digital resilience, cybersecurity awareness, and inclusive governance in Central Asia. She has contributed to regional dialogues on youth participation in security policy and has experience working with international and intergovernmental organizations. Her research interests include youth engagement in cybersecurity governance, digital inclusion, and the societal dimensions of cyber threats. She can be reached at olimaxonergasheva@gmail.com

Introduction & Policy Challenge

Uzbekistan's rapid digitalization over the past decade has transformed how citizens learn, work, and participate in public life. Expanded internet access, digital public services, and social media platforms have opened new opportunities for education, entrepreneurship, and civic engagement, particularly for young people. As the country positions itself as a regional digital hub in Central Asia, cybersecurity has become a central pillar of national development and stability.[1]

Yet, the pace of technological adoption has outstripped the development of human-centred cyber resilience, leaving significant segments of society—especially youth—exposed to growing digital risks.[2]

Young people represent both the backbone of Uzbekistan's digital future and one of its most vulnerable groups. Making up more than 60 percent of the population, youth are among the most active users of online platforms for communication, study, and income generation. However, increased connectivity has been accompanied by heightened exposure to phishing, misinformation, online fraud, cyberbullying, and data misuse. These risks are reflected in the findings of a mixed-methods

[1] International Telecommunication Union (ITU), *Digital Skills in Central Asia* (Geneva: ITU, 2022), https://www.itu.int

[2] United Nations Development Programme (UNDP), *Digital Literacy and Youth Empowerment in Central Asia* (New York: UNDP, 2021), https://www.undp.org

study conducted in May 2025, combining a nationwide online survey of young people aged 18–27 (n=61) with semi-structured interviews with youth governance actors and cybersecurity experts, which highlight phishing and misinformation as the most commonly reported cyber threats among young people (Figure 1).

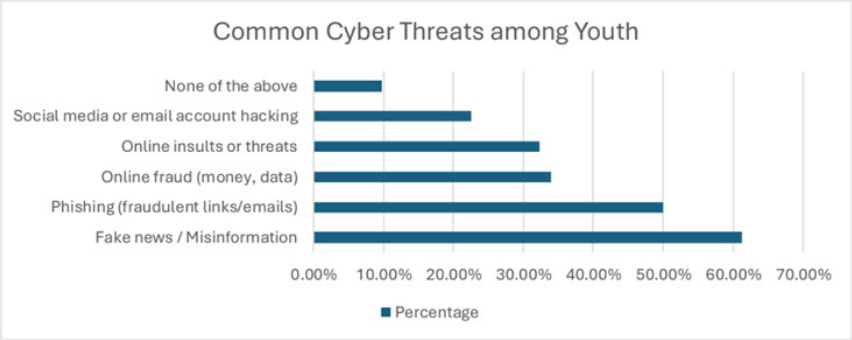

Figure 1: Most Commonly Encountered Cyber Threats Among Youth in Uzbekistan.

These risks are not only technical in nature; they carry broader social and political implications, including erosion of trust in institutions, amplification of disinformation, and potential for social instability. In this context, cybersecurity is not merely a technical challenge but a governance issue that intersects with education policy, youth engagement, and confidence-building efforts.

Despite this reality, youth remain marginal actors in cybersecurity governance. National cybersecurity strategies and regulatory frameworks in Uzbekistan have largely been developed through expert-driven and institutional processes, with limited structured input from young people. Limited awareness of existing cybersecurity laws and strategies further compounds this challenge, with a majority of respondents reporting either no awareness or uncertainty regarding current policy frameworks (Figure 2).

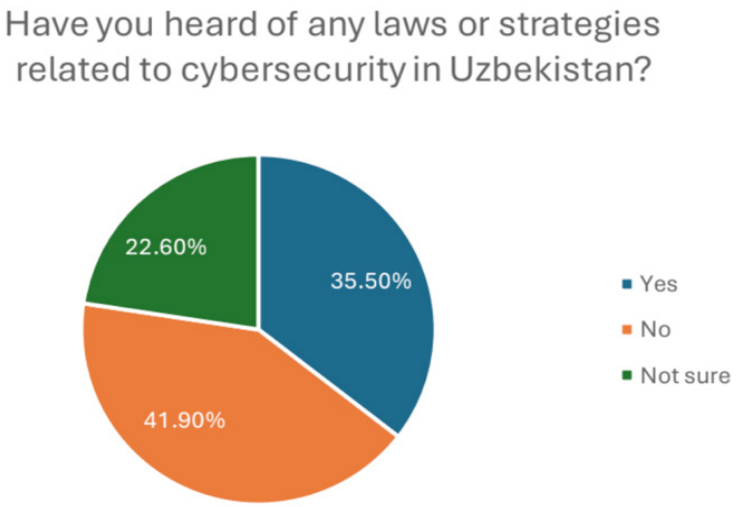

Figure 2: Youth Awareness of Cybersecurity Policies in Uzbekistan.

While awareness campaigns and capacity-building initiatives exist, they tend to position youth primarily as recipients of information rather than as contributors to policy design. As a result, policies risk overlooking everyday digital behaviours, emerging online trends, and gender-specific vulnerabilities that shape how cyber threats are experienced in practice.

Evidence from this study highlights a pronounced skills-to-use gap. Although most young people are online daily, fewer than one-quarter report having received formal cybersecurity education. This gap is particularly stark for young women, who often face delayed access to devices, fewer opportunities for ICT-focused education, and higher social costs for visible online participation.[3] These gendered disparities compound cyber risks and reinforce unequal access to digital opportunities. Without targeted intervention, the digital transformation risks reproducing existing inequalities rather than mitigating them.

[3] United Nations Children's Fund (UNICEF), *Girls' Digital Inclusion Report: Uzbekistan* (New York: UNICEF, 2023), https://www.unicef.org

Figure 3 summarizes how high youth digital exposure, when combined with a skills-to-use gap and governance and trust deficits, translates into heightened vulnerability to cyber threats. The diagram highlights that cyber risk is not driven by exposure alone, but by the interaction between technical skills gaps and structural governance constraints.

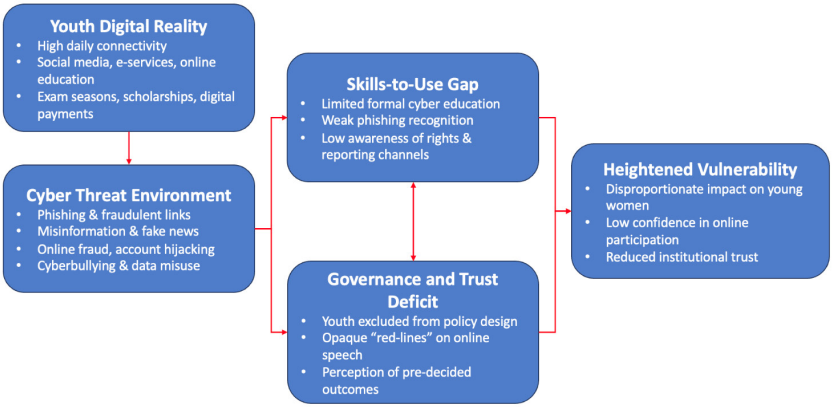

Figure 3: Pathways from Youth Digital Reality to Heightened Cyber Vulnerability.

At the same time, youth willingness to engage in cybersecurity policymaking is high: seventy-two percent of survey respondents[4] expressed interest in participating in consultations, hackathons, or advisory mechanisms. However, this interest rarely translates into practice, as only eighteen percent reported having ever participated in any cybersecurity-related policy or governance activity. These include limited access to clear and trustworthy information about participation opportunities, perceptions that policy decisions are finalized in advance, and the use of technical or legal language that intimidates non-specialists. In addition, uncertainty surrounding institutional "red lines" – caused by unclear boundaries around what is permissible online speech alongside inconsistent enforcement – creates a chilling effect, discouraging open participation, particularly among young women.

[4] Author's data, nationwide online survey of youth aged 18–27, conducted in Uzbekistan, May 2025.

If these challenges remain unaddressed, Uzbekistan risks several losses. First, cybersecurity policies may fail to resonate with or protect the population most exposed to digital threats, reducing their effectiveness. Second, continued exclusion of youth from governance processes may deepen distrust in institutions and weaken compliance with cybersecurity measures. Third, the country risks missing an opportunity to cultivate a generation of digitally skilled, civically engaged citizens who could contribute innovative, locally grounded solutions to cyber challenges.

The policy challenge, therefore, is how to move from *ad hoc* youth consultation toward predictable, inclusive, and meaningful youth participation in cybersecurity governance. This requires not only expanding cyber-literacy initiatives, but also establishing clear participation pathways, safeguarding mechanisms, and feedback loops that demonstrate how youth input informs policy outcomes. Addressing this challenge in the near term is essential for ensuring that Uzbekistan's digital transformation strengthens, rather than undermines, long-term security and social cohesion.

Proposed Policy Changes

Strengthening national cyber resilience in Uzbekistan requires a shift from awareness-based interventions toward structured youth co-governance in cybersecurity policy. While existing strategies focus on technical safeguards and institutional capacity, they insufficiently reflect the perspectives and everyday digital experiences of young people, who are among the most active and exposed users of digital technologies.

Current approaches largely position youth as end-users rather than contributors to cybersecurity governance, resulting in misalignment in terms of managing lived risks such as phishing, misinformation, online fraud, and gendered digital harms. This study highlights how high digital exposure, combined with limited cyber-literacy and unclear governance frameworks, increases vulnerability and undermines institutional trust.[5] This policy brief proposes a youth-centred cybersecurity governance model that embeds youth participation in decision-making, mainstreams cyber-literacy, strengthens local engagement, and clarifies institutional "red lines." Figure 4 illustrates how these coordinated measures can enhance cyber resilience and long-term security.

[5] Author's interview with international expert, conducted May 2025.

Importantly, the proposed policy change is designed to be **incremental and implementable**, building on existing institutional mandates, education systems, and youth structures rather than creating parallel or burdensome governance mechanisms. By leveraging ministries, district-level youth councils, educational institutions, and civil society actors already engaged in digital policy and youth affairs, this model prioritizes coordination over expansion. In doing so, it seeks to strengthen policy coherence, reduce participation barriers, and ensure that youth engagement is sustained rather than project based. Embedding youth co-governance within existing frameworks not only enhances feasibility but also increases the likelihood that youth input will meaningfully inform policy outcomes, reinforcing trust, accountability, and long-term cyber resilience.

Beyond institutional design, this shift also represents a normative reorientation of cybersecurity governance—from a state-centric, reactive model toward a participatory and preventative framework. By recognizing young people not merely as beneficiaries of protection but as strategic partners in shaping digital norms, early-warning mechanisms, and awareness ecosystems, Uzbekistan can better anticipate emerging risks and foster a culture of shared responsibility. In this sense, youth co-governance is not only a mechanism for inclusion, but a resilience strategy that enhances adaptability, legitimacy, and long-term societal stability in an evolving digital landscape.

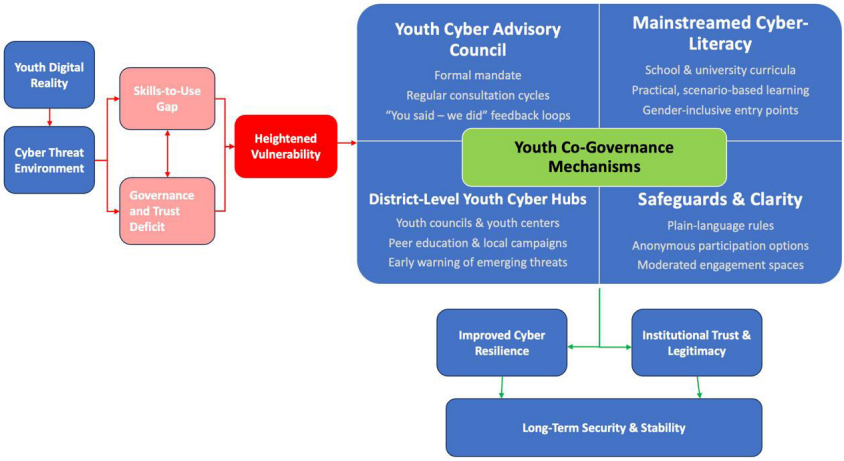

Figure 4: Youth-Centred Cybersecurity Governance Model and Policy Outcomes.

From *Ad Hoc* Consultation to Structured Youth Co-Governance

Strengthening cybersecurity governance in Uzbekistan requires moving beyond *ad hoc* and awareness-driven engagement toward structured youth co-governance. Current interactions with young people remain largely project based or consultative, often lacking clear mandates, continuity, and feedback mechanisms. This limits both the influence of youth input and trust in policy processes. Institutionalizing youth participation – such as through a Youth Cyber Advisory Council under the Ministry of Digital Technologies – would provide predictable engagement channels and ensure that youth perspectives inform cybersecurity policy at early stages. Transparent selection criteria, regular consultation cycles, and public "you said–we did" summaries are essential to demonstrate impact and legitimacy.

A second priority is closing the skills-to-use gap through systematic cyber-literacy integration. Despite high connectivity, many young people lack formal cybersecurity education. Embedding practical cyber-literacy modules into secondary and tertiary education curricula – focusing on digital hygiene, phishing recognition, misinformation resilience, and awareness of rights and reporting mechanisms – can reduce vulnerability at scale. Targeted entry points for girls and young women are necessary to address persistent gender disparities and avoid reinforcing existing inequalities.

Decentralizing engagement through district-level youth councils and youth centres represents a third policy change. These structures already enjoy higher trust and local reach than national institutions but remain underutilized for cyber-resilience. With basic training, standardized toolkits, and modest operational support, they can function as local hubs for peer education, awareness campaigns, and early identification of emerging digital risks, while feeding insights into national policy discussions.[6]

Finally, clearer communication of legal and institutional "red lines" governing online expression is essential to reduce uncertainty and encourage participation. Plain-language explanations of existing regulations, combined with safeguards such as moderated forums and

[6] **Organization for Security and Co-operation in Europe (OSCE),** *Comprehensive Security and Youth Engagement*, (2023).

options for anonymous input, can help transform youth engagement from a perceived risk into a legitimate civic practice.[7] Together, these measures form a realistic, youth-centred cybersecurity governance model that strengthens resilience, trust, and long-term security.

Recommendations

To translate youth willingness into meaningful participation and strengthen national cyber resilience, the following recommendations propose concrete, implementable actions for key stakeholders. Each recommendation builds on the findings of the study and aligns with existing institutional mandates, ensuring feasibility within current governance frameworks.

Government of Uzbekistan

- **Embed cybersecurity modules into secondary and tertiary education curricula**, with oversight by the Ministry of Preschool and School Education and the Ministry of Higher Education, Science and Innovation, in coordination with the Ministry of Digital Technologies. These modules should prioritize practical digital hygiene, phishing recognition, misinformation resistance, and awareness of reporting channels, rather than advanced technical skills. Special attention should be given to inclusive delivery, including targeted entry points for girls and young women to address gendered access gaps.

- **Clarify and communicate existing cybersecurity and online conduct regulations in plain language**, led by the Ministry of Digital Technologies in cooperation with relevant legal authorities. Plain-language summaries, FAQs, and scenario-based explanations should accompany legal texts and be disseminated through platforms widely used by youth. Clearer communication of "red lines" can reduce uncertainty, encourage lawful participation, and rebuild trust without requiring legislative reform.

[7] **United Nations Children's Fund (UNICEF),** *Girls' Digital Inclusion Report: Uzbekistan*, (2023).

Authorities of Uzbekistan

- **Establish a Youth Cyber Advisory Council under the Ministry of Digital Technologies** with a formal advisory mandate. The Council should include diverse youth representatives selected through transparent criteria and meet on a regular schedule aligned with cybersecurity policy cycles. To ensure credibility, the Ministry should publish brief feedback summaries demonstrating how youth input has informed policy decisions ("you said–we did").

- **Institutionalize youth consultation mechanisms in cybersecurity awareness campaigns and strategy reviews**, ensuring that youth engagement occurs at early stages of policy development rather than after decisions are finalized. This can be achieved through structured online consultations, moderated forums, and time-bound micro-tasks that lower participation barriers.

- **Leverage district-level youth councils and youth centres as local cyber-resilience hubs**, supported by the Youth Affairs Agency and local administrations. These structures should be equipped with standardized cyber-safety toolkits, basic training, and modest operational budgets to conduct peer education, local awareness campaigns, and early identification of emerging digital risks. Insights gathered locally should be systematically reported upward to national institutions to strengthen coordination.

- **Develop accessible, Uzbek-language cyber-safety content using story-based and peer-learning formats**, including short videos, podcasts, comics, and case studies. Universities, NGOs, and research institutions should collaborate to ensure that content reflects real-life digital behaviours and is suitable for non-specialist audiences. Female peer educators should be actively involved to encourage participation by young women.

- **Host regular youth hackathons and policy labs focused on practical cybersecurity challenges**, linking technical problem-solving with governance questions. These events should result in concrete outputs – such as policy briefs, campaign prototypes, or educational tools – that can be shared with government stakeholders.

OSCE and International Partners

- **Provide small-scale micro-grants to support youth-led cybersecurity initiatives**, including local awareness campaigns, peer education programs, and pilot reporting tools. These grants should prioritize projects that demonstrate inclusivity and scalability.

- **Facilitate regional youth exchanges and dialogue platforms on cybersecurity governance in Central Asia**, building on existing OSCE confidence-building measures. Such exchanges can promote peer learning, benchmark good practices, and strengthen regional cooperation on human-centred cyber resilience.

Together, these recommendations offer a realistic pathway for integrating youth as trusted partners in cybersecurity governance. By combining education reform, institutionalized participation, local engagement, and international support, policymakers can transform youth digital exposure from a source of vulnerability into a foundation for long-term security, trust, and stability.

Bibliography

"Comprehensive Security and Youth Engagement," Organization for Security and Co-operation in Europe (OSCE), (2023), retrieved from https://www.osce.org/

"Digital Literacy and Youth Empowerment in Central Asia," United Nations Development Programme (UNDP), (2021), retrieved from https://www.undp.org/

"Digital Skills in Central Asia," International Telecommunication Union (ITU), (2022), retrieved from https://www.itu.int/

"Girls' Digital Inclusion Report: Uzbekistan," United Nations Children's Fund (UNICEF), (2023), retrieved from https://www.unicef.org

"Strengthening Youth Resilience to Cybercrime in Uzbekistan," United Nations Office on Drugs and Crime (UNODC) and United Nations Development Programme (UNDP), (2025), retrieved from https://www.unodc.org/

"Youth & Digital Innovation Framework," International Telecommunication Union (ITU), (2020), retrieved from https://www.itu.int/

"Youth Population in Uzbekistan," United Nations Population Fund (UNFPA), (2024), retrieved from https://www.unfpa.org/

"Youth2030: The United Nations Youth Strategy," United Nations, (2018), retrieved from https://www.un.org/youthenvoy/youth2030/

Vesterbye, S. D., Dzhuraev, S. and Marazis, A., "Socio-economic Impact of COVID-19 and Media Consumption among Vulnerable Communities in Central Asia," Internews and European Neighbourhood Council, (2020).

OSCE Academy in Bishkek
1A, Botanichesky pereulok
Bishkek, Kyrgyz Republic 720044

Tel: +996 (312) 54-32-00, 54-12-00
E-mail: rtd@osce-academy.net
Website: www.osce-academy.net