POLICY RECOMMENDATIONS

Study Group Regional Stability in the South Caucasus (RSSC SG)

"Emerging Technologies in Conflict Prevention: Leveraging Cyber Technologies for Peacebuilding in the South Caucasus"

29th RSSC SG Workshop
10 – 13 April 2025
Istanbul, Türkiye

PfP Consortium of Defense Academies and Security Studies Institutes

Selected Recommendations

- All stakeholders should explore **peaceful use of emerging technologies**. External stakeholders like the PfP-C could support this with their extensive network of security experts and practitioners.
- All stakeholders, especially international donors, could fund projects to gather cultural material from the South Caucasus to **train conflict-sensitive and culturally aware AI tools** (especially generative AI) in order to reduce bias and reflect social realities.
- The regional governments should **use emerging technologies and AI to address the "problems without borders"** in the South Caucasus, like building trust through shared environmental data and common goals, data-driven water management or public health data exchange.
- **Sharing first-hand life experiences in conflict zones through digital tools** fosters empathy and mutual understanding. Local civil society actors and media could create these platforms. The EU could fund such projects.

Overview of Political and Security Situation in South Caucaus

The 29th workshop of the "Regional Stability in the South Caucasus" Study Group was held at Bahçeşehir University in Istanbul, Türkiye on 10–13 April 2025. The workshop once again highlighted the fact that the South Caucasus remains a volatile region shaped by the legacy of former empires (Russia, Iran, Ottoman Empire). Despite some cautious optimism, the notion that peace equals security is substantially challenged in this region. Georgia's struggle with internal political issues, persistent Russian influence, and the unresolved conflicts in Abkhazia and South Ossetia/Tskhinvali Region mark just the latest major security-political shift. The Armenia-Azerbaijan conflict, while no longer marked by large-scale hostilities, has not yet yielded a final peace treaty. Key obstacles include contentious language in Armenia's Constitution interpreted in Baku as territorial claims to Karabakh, Azerbaijan's demand for a land passage to the Nakhchivan exclave through Southern Armenia, and the dissolution of the OSCE Minsk Group. Azerbaijan insists on these preconditions before any treaty is signed. Though Armenia's Prime Minister Pashinyan is perceived as a pragmatic figure aiming to move past historical grievances, reservations on further concessions towards Azerbaijan persist within Armenian society. In essence, both Azerbaijan and Armenia fear future aggressions from the other side could undermine their ongoing peace efforts.

Security Sector Reform and Governance and Emerging Technology Governance

Security Sector Reform and Governance (SSR/G) is essential to sustaining peace. It is not just about military structures, but about transforming institutions to better serve society, reduce corruption, and respond to citizen needs. SSR/G includes state actors (military, police) as well as civil society, academia, and NGOs. Therefore, SSR/G is foundational to foster peace and stability in the South Caucasus through emerging technologies (ETs). The digital transformation of the South Caucasus governments should be inclusive as inclusivity and participation are central principles of good governance. Failing to include voices from all levels of governance and participation risks fuelling further griev-

ances. Notably, all governance actors (as distinct from government) must establish norms that ensure trust, inclusion, and transparency in the digital age.

In addition, digital technologies can support SSR/G by improving transparency and accessibility. E-governance platforms can reduce bureaucracy and opportunities for corruption. However, the digital divide remains stark, as about 32% of the global population lacks internet access, which disproportionately affects marginalized groups and women.

Emerging Technologies in Warfare and Society

Emerging technologies (ETs) play a disruptive, enabling, and force-multiplying role in modern warfare. Data has become a key asset, creating a sensor ecosystem where every soldier or device becomes a data point. The driving force behind this rapid technological advancement is no longer the military but the private sector. At the same time, innovation is exponential and not linear.

Loitering munitions and drone swarms, used both by state and non-state actors, have become essential in modern armed conflicts. Facial recognition, like Clearview AI, has already been used by Ukraine to identify Russian soldiers. The gathered information has been exploited in order to reduce morale both at home and at the frontline.

Social media enables marginalized groups, including politically extremist movements, to organize effectively. Populism, polarization, and disinformation thrive in fragmented digital spaces. Algorithms reinforce echo chambers, making shared realities increasingly rare. “Truth” has become relative, and the capacity for critical engagement is declining, especially among younger generations raised on micro-targeted content.

Deep fakes and generative AI fuel information warfare already, affecting the cognitive domain of populations at war and at peace. AI-driven misinformation (“Weapons of Mass Disinformation”) undermines trust and social cohesion. In a few years, brain-computer interfaces will potentially drive cognitive warfare.

The challenge is exacerbated by unregulated proliferation of ETs. What was once exclusive to great powers is now cheap and widely available to middle powers, small states and even non-state actors. Ethical dilemmas include biased AI systems, data quality issues, and concerns about autonomy in nuclear decision-making.

Emerging Technologies and Peacebuilding

Technology is not inherently positive or negative. Peace technologies (“peace tech”) aim to use digital tools to foster empathy, dialogue, and understanding. AI-based content moderation might help transforming divisive content into neutral language. On the one hand, digital storytelling may support efforts to counter generational indoctrination and historical bias. On the other hand, AI could better detect disinformation and even improve early warning capabilities to prevent escalation of conflicts in the South Caucasus.

ETs also support monitoring missions like the EUMM Georgia, using drones, satellite imagery, and acoustic sensors. AI-powered monitoring agents and more integrated, databased communication systems (e.g., upgrading hotlines to accept data, not just voice) could boost the efficiency of these missions. However, training and procurement bottlenecks remain, and the local communities often fear surveillance technologies.

Cybersecurity and Regional Resilience

Cybersecurity is a growing concern across the South Caucasus. In Georgia, Russian cyber operations target public infrastructure, morale and test national defences. Georgia has responded with strong international partnerships (e.g., NATO, EU, and United Kingdom) and by investing in cyber resilience and public awareness. Armenia, meanwhile, lacks specific legal frameworks to combat cybercrime and has not effectively integrated cyber security into its national security strategies. Azerbaijan has adopted its first national cybersecurity strategy (2023–2027), establishing centralized agencies and emphasizing infrastructure protection. Despite Azerbaijan’s active integration of digital technologies into governance and cybersecurity, the peacebuilding potential of these tools is underexplored.

Strategic Foresight and Ethical Challenges

There is a strong call for strategic foresight, especially in the South Caucasus, where reactive politics dominate. Think tanks and civil society actors could vastly benefit from access to affordable foresight tools. The challenge lies in the imbalance between private sector capabilities and public interest – how can peaceful applications of ETs become as profitable as its exploitative counterparts?

Abusing ETs to control societies is not science fiction. Facial recognition or AI systems disrupting both governance processes (e.g., by overwhelming public petition systems) and civic agency (e.g., by discrediting civil society activists through deep fakes) indicate the negative use of ETs and pose grave ethical challenges. Therefore, governance must be proactive: ethical frameworks (like the EU AI Act) are essential to ensure that AI remains human-centric. But above all, there is a need for meaningful partnerships with the private sector, civil society, and international organizations in order to channel these powerful technologies toward inclusive peacebuilding.

Recommendations

To all Stakeholders (Governments, Civil Society, International Organisations, Academia, and Private Sector)

- **Distinction between negative and positive peace:** When developing any tech solution or policy each actor should determine whether their endeavour aims for negative peace (i.e., the absence of direct violence), or positive peace (i.e., the presence of just, inclusive, and equitable social conditions). Negative peace solutions should focus on rapid detection of escalation risks, deployment of preventive diplomacy, and humanitarian readiness. In contrast, measures targeting positive peace should prioritize structural reforms, inclusive governance, dialogue mechanisms, and long-term social cohesion.

- **Explore peaceful use of emerging technologies:** Regional civil society actors and academia should initiate workshops and discussions on the peaceful use of emerging technologies. The PfP-Consortium could support regional think tanks and civil society, e.g. as proposed by participants from Azerbaijan, with identifying distinguished experts through its Study and Working Groups.

- **Context-aware, locally co-developed and ethical technology:** All actors, public and private, should ensure that tech solutions are context-aware, co-developed locally and ethically implemented. This builds trust and confidence, maintains human rights standards and avoids harm. It further reduces friction and increases relevance, inclusivity and agency in peace processes. AI solutions that fail ethical or legal scrutiny should be rejected.

- **Regional cooperation for innovation:** The stakeholders, especially the private sector and tech start-ups in particular, should create platforms for PeaceTech to stimulate practical and creative solutions. Engage youth and civil society in creative problem solving. Run national contests to crowdsource tech ideas for peace (e.g., hackathons, innovation challenges).

- **Harmonize tech regulation:** The governments of the South Caucasus republics should develop a region-wide regulatory framework to encourage the responsible use of emerging technologies in all domains and uphold human-centric and transparent principles using international legal and ethical benchmarks. External partners like the EU could support them.

- **AI-powered, region-specific early warning systems:** All stakeholders could develop and implement AI-powered tools to monitor early warning signals across digital and physical environments and enable timely and proactive responses to conflict risks.

- **Oversight of AI peacebuilding tools:** To prevent abuse of digital tools, as well as their illegal or unethical applications and thus build public trust and accountability, an oversight body to vet these tools should be created (e.g., by regional or international organisations like the OSCE or the UN). This recommendation should not be limited to the South Caucasus.

- **Public-private cooperation in developing new tools:** As emerging technologies are driven by the private sector, national frameworks (e.g. cybersecurity strategies) should be developed in close cooperation of the public and private sector. This helps blending expertise to achieve scalable, sustainable solutions and strengthen collective resilience across sectors. Legislation should define clear institutional roles to ensure accountability.

- **AI-based media monitoring and public awareness campaigns:** Both governmental and non-governmental actors, and in particular civil society-academic-private sector coalitions, could use AI to detect and counter disinformation. Public and private stakeholders should run media literacy and public awareness campaigns against disinformation and the impact of AI. This enhances society's ability to resist manipulation and strengthen information integrity.

- **Diverse, inclusive, and representative AI training data:** All stakeholders, especially international donors, could fund projects to gather cultural material from the South Caucasus (i.e., language, pictures, narratives, etc.) to train AI tools (especially generative AI) in order to reduce bias and reflect social realities. Create a database of material for training conflict and narrative sensitive local AIs.

- **Digital literacy, critical thinking, and civic education:** All governments and civil societies should empower citizens to participate responsibly in digital life. Invest in educational campaigns. Train public and security sector staff in AI, data ethics, and cybersecurity to increase institutional readiness and adaptability. International partners could support funding such measures.

For the South Caucasus Region (Armenia, Azerbaijan, Georgia)

- **Academic cooperation on tech applications for conflict resolution:** Governments should support academic exchange to accelerate peaceful tech innovation through shared research, while the academic institutions should establish the actual cooperation.

- **Digital ceasefire monitoring platforms and real-time data sharing:** This technology enhances transparency and accountability in border zones. Missions on the ground could implement digital monitoring tools. Data sharing could be established by every stakeholder (governments, missions, NGOs, etc.)

- **Digital storytelling platforms to share experiences:** Sharing first-hand life experiences in conflict zones through digital tools fosters empathy and mutual understanding. Local civil society actors and media could create these platforms. The EU could fund such projects.

- **Promote cooperative platforms to jointly address climate, resource and other cross-border issues:** All stakeholders should use emerging technologies and AI to address the "problems without borders" in the South Caucasus, like building trust through shared environmental data and common goals, data-driven water management or public health data exchange.

- **Impact of the young and future generations Z, Alpha and Beta, on resolving conflicts:** Civil society and regional academia should explore the role of the young generations and create a scientific basis for policies and frameworks that will fit the needs of the future users.

For Armenian Government

- **South Caucasus Technology Alliance for hybrid threat response:** Encourage joint regional solutions and security collaboration.

- **Invest in a tech-savvy workforce through global university partnerships:** Build the implementation capacity for Armenia's digital transformation and enable to develop a profitable service industry sector.

- **Invest 2–3% of GDP in tech R&D and partner with NATO/EU states:** Strengthen national capacity in AI, cybersecurity, and digital innovation through financial commitment and knowledge transfer.

- **Establish a Cyber Command, mandate cybersecurity standards for critical infrastructure and fill legal gaps regarding cybersecurity and data protection:** Establishing a clear regulatory and governance framework ensures national systems are protected, resilient against digital threats and privacy is safeguarded.

For Armenia and Azerbaijan Governments

- **Sign the peace treaty under the agreed terms without further delay and focus on long-term strategic benefits:** The lack of mutual trust makes it difficult to address risks and chances of ETs in Armenia and Azerbaijan properly. Capitalizing on current advantages now can secure regional influence and future cooperation. Implementing emerging technologies could safeguard the adherence to the treaty from both sides.

For European Union

- **Deregulate equipment procurement to equip CSDP missions with modern technology:** Speed up access to necessary tools for field effectiveness. Adapt mandates to allow quick implementation of new technologies. Make use of drones, sensors and the EU Satellite Centre to enhance conflict surveillance and early warning capabilities. Transfer authority from Brussels to field missions to streamline decision-making and improve operational agility and responsiveness.

These policy recommendations reflect the findings of the 29th RSSC workshop on "Emerging Technologies in Conflict Prevention: Leveraging Cyber Technologies for Peacebuilding in the South Caucasus", convened by the PfP Consortium Study Group "Regional Stability in the South Caucasus" in Istanbul/Türkiye, 10 – 13 April 2025. They were prepared by Christoph Bilban, Dr. Elena Mandalenakis and by Dr. George Vlad Niculescu on the basis of the proposals submitted by the participants. Valuable support in proofreading and page-setting came from Miriam Zeug.

Pictures: Beyza Sari/Bahçeşehir University Istanbul