Band 16 / 2025

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

Christoph Bilban, Elena Mandalenakis and George Niculescu (Eds.)

Study Group Information

UNSER HEER

Study Group Information

Christoph Bilban, Elena Mandalenakis and George Niculescu (Eds.)

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

29th Workshop of the PfP Consortium Study Group "Regional Stability in the South Caucasus"

16/2025
Vienna, December 2025

Imprint:

Copyright, Production, Publisher:
Republic of Austria / Federal Ministry of Defence
Roßauer Lände 1
1090 Vienna, Austria

Edited by:
National Defence Academy
Command
Stiftgasse 2a
1070 Vienna, Austria

In co-operation with:
PfP Consortium of Defense Academies and Security Studies Institutes
Garmisch-Partenkirchen, Germany

Study Group Information

December 2025
ISBN 978-3-903548-23-7

Printing:
ReproZ W 26-0179
Stiftgasse 2a
1070 Vienna, Austria

Table of Contents

Acknowledgments

This edited volume reflects the proceedings of the 29th workshop of the Regional Stability in the South Caucasus Study Group (RSSC SG) of the PfP Consortium of Defense Academies and Security Studies Institutes held in Istanbul, Türkiye, from the 10th to the 13th April 2025. The success of this meeting is attributed to our host Prof. Dr. Esra Hapitoğlu, Rector of Bahçeşehir University in Istanbul, who welcomed us and accommodated all our needs. This meeting and its product would not have been feasible without the continuous commitment, the financial and technical support of the Austrian National Defence Academy, specifically of Mag. Benedikt Hensellek, as well as of the Austrian Ministry of Defence, especially Mag. Andreas Wannemacher. We would also like to thank Lieutenant Colonel Olaf Garlich, Deputy Executive Director of the PfP Consortium Secretariat as well as Mr. Bernd Speckhardt, for their appreciation of the RSSC SG work, their logistical and financial support as well as for the dissemination of the RSSC SG products to the PfP Consortium stakeholders and the international community.

The editors and co-chairs wish to extend their gratitude to all individuals who have contributed to the realization of this volume. This includes the distinguished participants and speakers who have contributed their work, policy recommendations, and constructive exchange of opinions during the discussions, which are included at the end of this volume. Finally, the editors would like to express their gratitude to Ms. Miriam J. Zeug for providing invaluable assistance during the proofreading and compilation of this volume.

Abstract

Emerging technologies such as AI, machine learning, robotics, and digital platforms are increasingly integrated into security sectors, promising enhanced capabilities. This volume examines the role of these technologies in promoting peace, resilience, and regional stability in the South Caucasus. The papers explore how digital innovations intersect with national security strategies, societal resilience, and conflict resolution mechanisms. They discuss challenges and applications in the South Caucasus, highlighting the need for legal frameworks, oversight, and technological adaptation for peacebuilding and security resilience. The role of the digital divide, cyber threats, drone surveillance, blockchain, and big data analytics is explored in the context of conflict prevention, peacekeeping, and regional stability. The papers also analyse the EU civilian monitoring missions' technological modernisation and the geopolitical implications of technology in conflict zones. The volume concludes that while technological tools offer immense promise for conflict prevention, their success depends on governance, participation, and commitment.

Introduction

Christoph Bilban, Elena Mandalenakis, George Vlad Niculescu

The South Caucasus remains a region defined by enduring geopolitical volatility, complex interethnic tensions, and a protracted legacy of unresolved conflicts. Situated at the crossroads of Europe and Asia, it continues to experience the intersecting pressures of regional rivalries and global strategic competition. In an era increasingly shaped by exponential technological transformation, the influence of emerging technologies, particularly in the domains of digital communication, data analysis, and artificial intelligence (AI), has become relevant in shaping both conflict dynamics and peacebuilding initiatives.

Given the recent hostilities, including the 2023 escalation between Armenia and Azerbaijan, whose formal conclusion through a signed peace agreement remains pending, it is both timely and imperative to examine how technological innovation can support the peaceful resolution of disputes, mitigate future escalations, and revitalize stalled negotiation processes. This volume responds to such a demand, building on earlier initiatives while advancing new perspectives on the use of innovative technologies for peace and security.

The Partnership for Peace Consortium's (PfPC) Regional Stability in the South Caucasus Study Group (RSSC SG) has taken a leading role in this discourse. At its April 10–13, 2025 meeting in Istanbul, titled *Emerging Technologies in Conflict Prevention: Leveraging Technology for Peacebuilding in the South Caucasus*, regional experts and international scholars convened to explore how emerging technologies – such as AI, cyber capabilities, and digital communication tools – can be harnessed not as instruments of warfare, but as enablers of peace and reconciliation. The present Study Group Information volume reflects the outcomes of these expert discussions and policy exchanges.

This is not the first time the RSSC SG has addressed the intersection of technological innovation and regional security. Previous volumes published in 2015 and 2017 considered the role of cyber technologies in combating

disinformation and promoting information integrity. Such concerns remain relevant in the South Caucasus where the weaponization of disinformation, manipulation of media networks, and the orchestration of influence operations continue to threaten democratic resilience, erode societal trust, and destabilize political systems. These efforts seek to undermine regional balance through the erosion of social cohesion and institutional legitimacy.

This volume builds upon that foundation by expanding the analytical lens beyond information warfare to the broader scope of *PeaceTech*, a term that refers to the intentional application of technological innovations to support conflict prevention, management, and resolution. The central objective is to investigate how emerging technologies can serve as enablers for de-escalation, dialogue, reconciliation, and inclusive peacebuilding. Specific attention is paid to technologies such as generative AI, large language models (LLMs), big data analytics, blockchain, and cyber monitoring systems.

What distinguishes PeaceTech from other technological applications is its explicit normative orientation as its purpose is not to project power or enhance military capabilities, but rather to enable participatory peace processes, improve early warning systems, foster transparency, and empower marginalized stakeholders. Technologies that were once deployed for offensive purposes – such as drones, cyber capabilities, and algorithmic targeting systems – can now be repurposed to support ceasefire monitoring, secure negotiation platforms, counter disinformation, and protect channels of communication for mediators and civil society actors.

Accordingly, this volume deliberately excludes analyses that focus on the militarization of emerging technologies or their application in warfare. Instead, it questions how the same tools, if appropriately governed and normatively framed, can be leveraged to foster long-term regional stability.

Emerging technologies have had transformative effects across sectors such as defence, governance, economy, and civil society, fundamentally altering power structures and ways of interaction between states and non-state actors. Their dual-use nature, however, presents both opportunities and challenges. While these tools have enhanced human capability and institutional responsiveness, they also carry risks related to misuse, algorithmic bias, ethical ambiguity, and structural inequality.

PeaceTech, as defined in recent literature, refers to the deliberate deployment of digital tools and technological innovations for the purpose of peacebuilding. AI and big data analytics, for instance, can be deployed to identify socio-political trends, forecast outbreaks of violence, and provide predictive insights into fragile contexts. These early warning systems are invaluable in pre-empting escalation and allowing for timely, targeted interventions.

Moreover, the application of PeaceTech can facilitate inclusive dialogue through online platforms that transcend geographical barriers. Such technologies allow for the integration of marginalized voices (particularly women, youth, and rural populations) into peace negotiations. Drone and satellite imagery, for example, can support ceasefire monitoring and humanitarian needs assessments, while virtual and augmented reality tools may play a role in reconciliation and post-conflict education efforts.

The South Caucasus, marked by unstable borders, historical grievances, and intermittent violence, represents a critical testing ground for PeaceTech. AI-driven foresight tools, real-time data processing for conflict mapping, and secure digital communication infrastructures could significantly enhance the resilience of peace processes in the region.

Nonetheless, technology alone cannot generate the political will necessary to resolve conflict. PeaceTech is a facilitative tool; its success depends on human agency, inclusive governance, and contextual sensitivity. The application of such technologies must be grounded in an understanding of local cultures, languages, and values to ensure legitimacy and efficacy. Nevertheless, AI systems often risk oversimplifying moral reasoning and neglecting deeply held cultural narratives, particularly in conflicts rooted in sacred values or identity-based claims.

AI tools can support peace practitioners by aggregating situational data from conflict zones, identifying blind spots, and generating policy options. Yet their outputs must be critically evaluated and ethically curated. The same holds true for early warning technologies and humanitarian logistics systems that depend on the availability, accuracy, and representativeness of underlying data. Algorithmic decisions must be scrutinized to avoid reproducing systemic biases or overlooking nuanced socio-political dynamics.

Digital platforms for dialogue must also contend with infrastructural disparities and the digital divide. Weak connectivity, lack of digital literacy, and low trust in virtual engagement may limit participation and reinforce exclusion. Moreover, the risk of surveillance, cyber intrusion, and disinformation remains a significant barrier to building trust in online peace processes.

This edited volume is organized into four interrelated parts:

Part I explores the Role of Emerging Technologies in Conflict Resolution and Peacebuilding as well as how having a peace agreement between Armenia and Azerbaijan concluded sooner rather than later would benefit the whole of the South Caucasus region. More specifically, Lui & Lazar analyse how digital technologies intersect with security sector governance (SSG), emphasizing their dual-use nature. While AI, surveillance systems, and predictive analytics can improve early warning and operational oversight, they also pose risks of authoritarian misuse, bias, and exclusion. They emphasize the need for human rights-based regulation and responsible as well as inclusive digital governance. Badridze presents a policy perspective from Georgia, emphasising the geopolitical urgency of an Armenia-Azerbaijan peace agreement. He argues that regional integration, economic connectivity, and long-term stability are only achievable if the peace deal is immediately signed, with Georgia serving as a mediator. Kuznetsov discusses "algorithmic geopolitics," highlighting how AI and big data are transforming power dynamics. He claims that Russia lags behind Western states in AI integration for geopolitical influence and suggests that without significant reform, it risks strategic irrelevance in the algorithmic age.

Part II explores existing frameworks governing cyber technologies in Armenia, Azerbaijan and Georgia based on their geopolitical position and therefore their relations with their neighbouring states. Gotsiridze presents Georgia's evolving cybersecurity architecture, shaped by its confrontational history with Russia. He reviews legal, institutional, and international initiatives to strengthen resilience, arguing for a cyber defence posture focused on Russia given the ongoing hybrid threats. Huseynov discusses Azerbaijan's digital modernization, from the success of ASAN services to green tech in Karabakh reconstruction. He critiques the underutilization of PeaceTech in Azerbaijan's policy discourse and urges for more structured efforts integrating emerging technologies in the reconciliation and dialogue

efforts with Armenia. Melikyan explores how Armenia could harness AI, big data, and blockchain to counter hybrid threats. He finds gaps in Armenia's cybersecurity legislation and strategic planning, and proposes a forward-looking integration of emerging technologies into Armenia's defence and foreign policy to ensure resilience and sovereignty.

Part III provides an analysis of the existing and future challenges and opportunities for using PeaceTech in the South Caucasus. Hence, Wathen assesses the EU's monitoring mission and the potential of AI and Unmanned Aerial Vehicles to improve observation accuracy and conflict de-escalation. He outlines both logistical and political challenges to modernization, including local resistance and technological gaps. Yılmaz proposes an AI-driven crisis early warning system tailored to the South Caucasus. Drawing from global models, he emphasizes the need for inter-agency cooperation, standardized data, and ethical algorithms to create a predictive and responsive PeaceTech infrastructure. Poghosyan analyses Armenia's contemporary relations with Azerbaijan, in anticipation of the conclusion of a peace deal, and Türkiye. He provides a political forecast of Armenia's diplomatic strategy in 2025, and argues that Armenia's Western alignment requires careful navigation to avoid regional isolation or renewed conflict.

Overall, the authors of the first three parts demand the responsible use of cyber capabilities and innovative technologies for the advancement of peace especially in light of regional instability due to historical tensions and conflicts in the South Caucasus.

Part IV, outlines the RSSC Study Group's reflections in the form of relevant, comprehensive and actionable policy recommendations. The Study Group calls for technological accountability and human rights; digital literacy and inclusion; institutional capacity building for cybersecurity; multilateral frameworks for AI ethics and algorithmic governance; and support for PeaceTech entrepreneurship and civil society engagement.

The editors believe that the analysis presented in the Study Group Information contributes to the debate regarding the value of innovative technologies as tools in the attainment of peace and will stimulate further research and discussions by policy-makers and practitioners in the South Caucasus.

The integration of emerging innovative technologies into the peacebuilding efforts in the South Caucasus would represent a transformative opportunity to address longstanding conflicts and build a more secure, resilient and inclusive future. The RSSC SG's aim to foster dialogue around PeaceTech is critical for ensuring that technological innovation serves as a facilitator for peace.

The included policy recommendations suggest that the South Caucasus should consider the valuable albeit vigilant use of innovative technologies for sustainable peacebuilding and as an inclusive and transparent form for cooperation among stakeholders within and among the regional states. By grounding PeaceTech initiatives in ethical principles, robust governance frameworks, and inclusive multi-stakeholder engagement, the region can harness the power of technology to prevent conflict, support reconciliation, and promote sustainable development. Continued investment in capacity building, research, and cross-border cooperation will be essential for realizing the full potential of PeaceTech in the South Caucasus and beyond.

PART I: The Role of Emerging Technologies in Conflict Resolution and Peacebuilding

New Technologies and Good Security Sector Governance: Linkages with Conflict Prevention and Sustaining Peace

Alexandru Lazar, Dawn Lui[1]

Introduction

In the past two decades, emerging digital technologies have transformed how security institutions approach governance of the security sector. Moreover, at a time of proliferating conflicts and a shrinking civic space, emerging technologies come across as attractive solutions in supporting efforts towards the prevention of violent conflicts and in sustaining peace. Nevertheless, this digital shift has also expanded the threat landscape, empowering non-state actors, cybercriminals, and even hostile state entities to exploit digital vulnerabilities, disrupt governance structures, and undermine citizen trust. As a result, security institutions around the world find themselves in a position where they are compelled to embrace digitalisation, while simultaneously ensuring that core good governance principles – including accountability, transparency, participation, effectiveness, and respect for human rights – are upheld, with the goal of preventing violent conflict and sustaining peace.

Russia's war of aggression in Ukraine, the war in Gaza, civil war in Sudan, coups d'état in West Africa – these are only some recent instances of a multiplying number of wars and violent conflicts, democratic reversals, and state capture of the security sector. Around the world, we see an increase in defence spending and a return to hard security, which, in turn, demands a greater focus on effective oversight and checks and balances.[2] The latest Global Peace Index, which measures peace nationally and globally, confirms this trend also reported in the past years.[3] The world has plunged into

---

1 This contribution draws upon: D. Lui and A. Lazar, Digitalization and SSG/R: Projections into the Future, (Geneva: DCAF, 2023). See also: DCAF – Geneva Centre for Security Sector Governance, Digitalization and Security Sector Governance and Reform (SSG/R). SSR Backgrounder Series (Geneva: DCAF, 2022); DCAF – Geneva Centre for Security Sector Governance, Artificial Intelligence (AI) and the Defence Sector. SSR Backgrounder Series, (Geneva: DCAF, 2025).

2 F. McGerty, 'Global defence spending soars to a new high' (IISS, 2025).

3 Institute for Economics & Peace, 'Global Peace Index 2024' (IEP, 2024).

a less peaceful era than at any point in the past decade, with a growing 'peace inequality' gap between countries.

In this context, emerging technologies offer novel avenues to monitor crises, engage stakeholders remotely, and predict or even pre-empt outbreaks of violence.[4] For example, artificial intelligence (AI) technologies can contribute towards the prevention of violent conflict through early warning systems and mechanisms that analyse satellite imagery, social media data, and historical trends to detect emerging threats.[5] In this vein, AI-powered platforms such as the new model of the Global Conflict Risk Index employs machine learning algorithms to predict political instability and violence.[6] Such an approach is strategic, as the ability to anticipate the potential outbreak of conflict is the first step towards identifying entry points towards prevention. Although AI-driven early warning systems provide crucial information, their effectiveness remains dependent on the availability of reliable data. To this end, it is essential that state institutions have the capacity to ensure that these tools are used responsibly, ethically, and in line with international and national human rights norms and standards.

As highlighted in the Geneva Centre for Security Governance's (DCAF's) report *Digitalization and SSG/R: Projections into the Future*, there is a "shared understanding that digital technologies will reshape governance structures, while prompting new patterns of coordination and cooperation".[7] Nonetheless, digitalisation introduces a dual-use dilemma: the same tools that enhance security provision and good governance can also be repurposed to violate rights, conduct mass surveillance, or spread disinformation. Ensuring that the security sector's adoption of technology upholds democratic values is therefore a critical challenge for governments and oversight institutions around the world. Good security sector governance (SSG) refers to the application of democratic principles to the management and oversight

4 A. Makri, 'Can Tech Tip the Balance Towards Peace?', (Rotary Action Group for Peace, 2025).

5 J. Y. Ndzana, 'The Role of Artificial Intelligence in Conflict Prevention and Management in Africa', (Accord, 2025).

6 European Commission, The Global Conflict Risk Index: Artificial intelligence for conflict prevention, (EU, 2019).

7 D. Lui and A. Lazar, Digitalization and SSG/R: Projections into the Future, (Geneva: DCAF 2023).

of security institutions – including the armed forces, law enforcement, border authorities, and intelligence services, among other actors – as well as the bodies responsible for their governance and oversight.[8]

The aim of this written contribution is thus to explore the impact of emerging technologies in shaping good SSG in relation to the prevention of violent conflict and to sustaining peace. Rather than focusing on the technologies themselves, this paper instead investigates how they intersect with core governance principles, with a focus on (1) effectiveness, (2) accountability and transparency, as well as (3) participation and inclusion. Drawing upon DCAF's research in this area,[9] this paper highlights both the opportunities and challenges of digitalisation in the security sector – challenges and opportunities that, by nature of the overarching goal of good SSG – also apply to conflict prevention and peacebuilding efforts.

By focusing on the impact of emerging technologies on the good governance of the security sector in terms of effectiveness, accountability, and participation, this paper aims to contribute towards current debates on digital transformation in the security sector. It highlights how governance frameworks must evolve to remain resilient and responsive in the face of rapidly advancing technologies, while offering insights into how security sector actors, policymakers, and civil society can collaboratively harness the potential of digital innovation to build more accountable, inclusive, and rights-respecting landscape that can contribute towards the prevention of violent conflict and ensure lasting peace.

Digitalisation of the Security Sector

Digital transformation of the security sector has profoundly reshaped the mechanisms through which security is delivered, managed, and overseen.

---

8 DCAF – Geneva Centre for Security Sector Governance. Security Sector Governance. SSR Backgrounder Series. (Geneva: DCAF, 2019).

9 DCAF – Geneva Centre for Security Sector Governance. Digitalization and Security Sector Governance and Reform (SSG/R). SSR Backgrounder Series. (Geneva: DCAF, 2022); D. Lui and A. Lazar, Digitalization and SSG/R: Projections into the Future, (Geneva: DCAF 2023); DCAF – Geneva Centre for Security Sector Governance. Artificial Intelligence (AI) and the Defence Sector. SSR Backgrounder Series, (Geneva: DCAF, 2025).

Emerging digital technologies offer unprecedented opportunities for enhancing operational efficiency. However, they also introduce complex challenges that can undermine democratic principles, human rights, and accountability mechanisms. Drawing upon existing research, this section will examine these key dynamics, focusing on five interrelated thematic areas: *new technologies*, *technical capacity*, *regulation and oversight*, *human rights*, and *the digital divide*.[10] This section delves into each thematic area, incorporating some of the findings from DCAF's report with more recent developments and data to provide a comprehensive understanding of the current landscape.

New Technologies

Emerging technologies such as artificial intelligence (AI), machine learning, robotics, quantum computing, and digital communication platforms are increasingly integrated into the security sector. These tools promise enhanced operational capabilities, including improved situational awareness, efficient resource allocation, and advanced threat detection.[11] Concrete examples of the digitalisation of the security sector can be observed in various areas. For instance, law enforcement agencies are increasingly making use of AI-powered facial recognition systems to identify and track suspects, improving their capabilities in investigations and maintaining public safety.[12] Moreover, machine learning algorithms are employed to analyse large volumes of data from diverse sources to identify patterns and potential threats, aiding in intelligence and counterterrorism efforts.[13]

The increasing prevalence of autonomous processes, such as machines using AI agents, performing tasks with minimal or no human supervision are becoming more common. Uses can range from virtual assistants in everyday life to precision targeting by the military in armed conflict.[14] Every

---

10 D. Lui and A. Lazar, Digitalization and SSG/R: Projections into the Future, (Geneva: DCAF 2023).

11 DCAF – Geneva Centre for Security Sector Governance. Artificial Intelligence (AI) and the Defence Sector. SSR Backgrounder Series, (Geneva: DCAF, 2025).

12 National Institute for Standards and Technology, 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software' (2019).

13 D. Van Puyvelde, S. Hossain and S. Coulthart, 'National Security Relies More and More on Big Data. Here's Why', The Washington Post (2017).

14 N. Davison, 'A Legal Perspective: Autonomous Weapon Systems Under International

action taken within digital systems can be logged and audited, providing transparency and accountability in security operations. This feature is particularly beneficial for oversight bodies, as it facilitates the tracking of decision-making processes and resource utilisation. Nonetheless, the effectiveness of digital paper trails hinges on the integrity and security of the underlying systems. Without robust cybersecurity measures, these records are susceptible to tampering, potentially compromising accountability mechanisms.

Despite their benefits, the deployment of these technologies raises significant governance concerns. AI and automated decision-making systems can perpetuate biases present in training data, leading to discriminatory outcomes.[15] The opacity of algorithms can obscure the rationale behind critical decisions, challenging transparency and accountability.[16] To mitigate these risks, it is imperative to implement ethical guidelines and regulatory frameworks that ensure human oversight, algorithmic transparency, and the protection of human rights.

Technical Capacity

The rapid integration of digital technologies necessitates a corresponding enhancement in the technical capacity of security sector personnel. Proficiency in areas such as cybersecurity, information management, data analysis, and AI is essential to effectively leverage new technologies and safeguard against emerging threats.[17] Research shows that there is an acute need for comprehensive training programs tailored to the unique demands of the security sector.[18] Special emphasis is placed on AI and cybersecurity training, given their pervasive impact. AI training should encompass not only technical aspects or best practices, but also ethical considerations, ensuring that personnel can critically assess and manage emerging technologies responsibly.

Humanitarian Law', ICRC (2018).

15 A. Jonker & J. Rogers, 'What is algorithmic bias?', (IBM, 2024).

16 M. Valderrama, M. P. Hermosilla & R. Garrido, 'State of the Evidence: Algorithmic Transparency', (Open Government Partnership, 2023).

17 K. Kohler, 'Estonia's National Cybersecurity and Cyberdefense Posture', Cyberdefense Report, ETH Zurich (2020).

18 European Union, 'Regulation (EU) 2024/1689 of the European Parliament and of the Council – Artificial Intelligence Act', (Brussels: EU 2024).

Moreover, fostering a culture of continuous learning is essential. The digital landscape is in constant flux, with new technologies, actors, and threats emerging regularly. Security institutions should establish partnerships with academic institutions, private sector entities, and civil society organisations to stay abreast of developments and share best practices. These collaborations can facilitate knowledge exchange, joint training initiatives, and the development of standardised protocols, thereby enhancing the overall technical capacity of the security sector.

Regulation and Oversight

Despite the growing reliance on AI and other emerging technologies by security sector actors, there remains a notable absence of comprehensive, binding international or regional regulatory frameworks that specifically govern the use of such technologies in the security domain. While the EU Artificial Intelligence Act (EU AI Act) represents a milestone in digital regulation, it explicitly excludes from its scope AI systems used exclusively for military, defence, or national security purposes, as stated in Article 2, paragraph 3.[19] As such, many core applications of AI in intelligence services or military operations fall outside the reach of this legislation.

Similarly, although the Act does apply to AI systems used in law enforcement and public safety, concerns remain regarding the practical enforcement of these provisions and the transparency of their implementation by domestic security actors. In many jurisdictions, including across the EU, domestic oversight mechanisms have yet to be fully equipped (both technically or legally) to audit and guide the use of high-risk AI systems in policing, surveillance, or border control.[20] This lack of tailored governance creates the space for a regulatory grey zone, where powerful technologies are deployed in security operations without a clear legal basis, standardised ethical criteria, or mandatory risk assessments. For instance, there is currently no binding international agreement regulating the development or deployment of lethal autonomous weapons systems (LAWS), despite growing concerns regarding their compatibility with international humanitarian law.

---

19 R. Powell, 'The EU AI Act: National Security Implications', Alan Turing Institute (Centre for Emerging Technology and Security, 2024).

20 C. Dumbrava, 'Artificial intelligence at EU borders: Overview of applications and key issues', European Parliament (European Parliamentary Research Service, 2021).

At the national level, some countries have issued non-binding guidelines or principles for the use of AI in the public sector, but these often lack the specificity or enforcement mechanisms required for the security context.[21] This fragmented landscape therefore highlights the urgent need for dedicated legal frameworks that address the unique risks and governance demands posed by emerging technologies in security provision. In the absence of comprehensive regulation, experts emphasise the importance of strengthening internal oversight mechanisms, establishing transparency protocols, and enhancing parliamentary and civil society scrutiny of digital technologies used in the security field.[22] Building institutional capacity to assess and audit new technologies remains essential to ensure their deployment aligns with the rule of law, fundamental rights, and democratic governance.

Human Rights

The integration of digital technologies into the security sector has profound implications for human rights. While these technologies can enhance security operations, they also pose risks related to privacy, freedom of expression, and protection from surveillance. Existing research highlights concerns regarding the potential for digital tools to be used in ways that infringe upon civil liberties, such as mass surveillance, data exploitation, and suppression of dissent.[23] To safeguard human rights in the context of digitalisation it is essential to establish clear legal and institutional frameworks that prevent misuse. Guidelines need to be rooted in international human rights law to ensure that surveillance and data collection are lawful, necessary, and proportionate. Oversight mechanisms, such as data protection authorities, Ombudsman institutions, and parliamentary committees, must be empowered to scrutinise how digital technologies are deployed.

---

21 Canada has implemented several frameworks and proposed legislation concerning the use of AI in the public sector, including areas related to security. For example, the Directive on Automated Decision-Making provides a framework for the responsible use of AI in federal institutions. While it sets out requirements for transparency and accountability, it is a policy instrument rather than a legally binding regulation, and its applicability to high-risk areas like national security is limited.

22 C. Kavanagh, 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?' (Washington, D.C.: Carnegie Endowment for International Peace, 2019).

23 A. Shahbaz, 'The Rise of Digital Authoritarianism', Freedom House (2018).

Another pressing concern relates to the spread of disinformation campaigns, often amplified through social media algorithms and AI-generated content.[24] These campaigns can manipulate public opinion, stigmatise communities, and fuel political instability, while threatening national security. Tools such as deepfakes and bot networks make it increasingly difficult for users to distinguish credible sources from fabricated narratives.[25] In fragile contexts, this can lead to violence and suppression of dissenting voices.[26] Security actors must tread carefully, ensuring that responses do not infringe on freedom of expression or enable censorship under the guise of cybersecurity. A threshold for what is considered as disinformation – and what it is not – in a national security context still needs to be developed. For example, the European Court of Human Rights (ECtHR) regulates how security institutions can interfere with human rights. A foundational case is *Handyside v. United Kingdom (1976)*, where the Court emphasized that: security institutions can interfere with human rights only if the interference is lawful, justified, necessary, and proportionate, and the State remains accountable through the ECtHR.[27]

Bias in AI systems is another risk. Predictive policing algorithms, for instance, may disproportionately target certain ethnic or socioeconomic groups based on flawed historical data.[28] Digital tools must be carefully audited for discriminatory outcomes, and that human oversight must remain central to decision-making in all security applications. In response to these issues, an intersectional and multi-stakeholder approach must be adopted, involving civil society, private sector actors, legal experts, and affected communities in shaping ethical and inclusive policies. Transparency, digital literacy, and independent journalism are key to resisting digital authoritarianism and preserving civic space.

---

24 D. Fallis, 'What Is Disinformation?', Library Trends, Vol. 63: No. 3 (2015), pp. 401–26.

25 M. Westerlund, 'The Emergence of Deepfake Technology: A Review', Technology Innovation Management Review (2020).

26 Amnesty International, "A Digital Prison" – Surveillance and the suppression of civil society in Serbia (2024).

27 European Court of Human Rights, 'Case of Handyside v. The United Kingdom', (1976).

28 European Union Agency for Fundamental Rights, 'Bias in Algorithms – Artificial Intelligence and Discrimination', (2022).

The Digital Divide

Digitalisation offers transformative potential, but uneven access to technology threatens to exacerbate inequality and marginalisation. The 'digital divide' refers to disparities in access to the Internet, digital devices, and the skills needed to use them.[29] For security sector governance to be genuinely participatory and accountable, digital inclusion must be a foundational principle.

Based on the latest data available:

- Nearly 2.6 billion people – or 32% of the world population – remain offline, according to the International Telecommunication Union (ITU).[30]
- In the least developed countries, just 36% of people use the Internet.[31]
- Globally, women are 17% less likely than men to use mobile internet in low- and middle-income countries.[32]
- Rural and older populations also face disproportionate barriers to digital access.[33]

These divides are not only issues within the development sphere, but they also have direct implications for security governance and prevention of violent conflict. Exclusion from digital tools can prevent communities from accessing reporting mechanisms, participating in consultations, or receiving timely alerts in crisis situations. Moreover, if oversight processes increasingly depend on digital tools, unequal access undermines their democratic legitimacy.

Security sector actors should collaborate with tech companies and local public institutions to create accessible platforms and digital literacy pro-

---

29 International Telecommunication Union, 'Digital inclusion of all', (2022).

30 International Telecommunication Union, 'Population of global offline continues steady decline to 2.6 billion people in 2023', (2023).

31 United Nations Development Programme, 'Committing to bridging the digital divide in least developed countries', (2023).

32 GSMA, 'The Mobile Gender Gap Report 2024', (2024).

33 Age Action, 'Digital Inclusion and an Ageing Population Ensuring Equality and Rights for All of Us as We Age', (2021).

grams targeting marginalised communities. Initiatives such as public technology hubs, mobile learning apps, and multilingual cybersecurity awareness campaigns can foster a more inclusive digital environment. A gender-sensitive approach is particularly crucial. The report calls for frameworks to close the digital gender gap, empower women in digital security policymaking, and ensure their participation in security oversight structures.[34] Digital inclusion, in short, is not a luxury. It is a prerequisite for the fair, transparent, and accountable governance of digitalised security institutions.

Prevention of Violent Conflict and Sustaining Peace

The prevention of violent conflict and the long-term sustainability of peace depend heavily on the principles of good SSG, including effectiveness, accountability, transparency, and inclusive participation, to name a few. When guided by strong governance frameworks, emerging technologies can support these aims by enabling more timely, informed, and targeted responses to early warning signals, enhancing oversight, and facilitating broader societal engagement in peace efforts. However, the success of such digital interventions is not guaranteed by technological availability alone. Their preventive and peace-sustaining potential also hinges on equitable access, institutional readiness, and the capacity of users to apply these tools responsibly. While the previous section outlined how emerging technologies intersect with key dimensions of the security sector, it is equally important to examine how these dynamics translate into the broader goals of preventing conflict and sustaining peace.

Effectiveness

Digital technologies can significantly enhance the conflict prevention capacity of the security sector by enabling more anticipatory, targeted, and evidence-based responses to emerging threats. When applied proactively, these tools allow security institutions to identify patterns of risk and intervene before violence escalates, thereby contributing to the sustainability of peace. Predictive analytics, for instance, can process large and diverse datasets to forecast when and where tensions may arise, ranging from cyber

[34] Organisation for Economic Co-operation and Development, 'Bridging the Digital Gender Divide – Include, Upskill, Innovate', (2018).

intrusions and disinformation campaigns to inter-communal unrest or electoral violence.[35] When integrated with geospatial information systems (GIS), these insights can guide early warning systems, humanitarian deployment, and conflict-sensitive policing strategies.[36] Security institutions in fragile and conflict-affected settings have begun employing drones, satellite imagery, and sensor technologies to monitor movements, assess local grievances, and detect environmental or logistical conditions that may lead to unrest.[37]

Meanwhile, AI-powered tools help intelligence and peacebuilding agencies filter noise from meaningful patterns, identifying flashpoints and actors of concern more efficiently. Advanced data systems can gather and process vast amounts of Publicly Available Information (PAI) – from satellite images to social media posts – allowing to detect warning signs of violence or ceasefire violations in real time.[38] Up to 80% of the information processed by intelligence analysts in UN peace operations, for example, now originates from open sources (Open Source Intelligence – OSINT), representing a dramatic shift that underscores the value of big data for situational awareness.[39] Similarly, AI-driven analytics are used to flag patterns in reports of human rights abuses, helping investigators focus on credible leads and hold perpetrators accountable.[40] These tools have been employed to monitor ceasefires via satellite (e.g., detecting troop movements) and to scan social media for hate speech that could incite violence.[41]

---

35 A. Duursman & J. Karlsrud, 'Predictive Peacekeeping: Strengthening Predictive Analysis in UN Peace Operations', Stability - International Journal of Security and Development, 8(1), pp. 1–13, (2018).

36 E. Convergne & M. R. Snyder, 'Making Maps to Make Peace: Geospatial Technology as a Tool for UN Peacekeeping', International Peacekeeping, 22(5), pp. 565–586, (2015).

37 A. W. Dorn, 'Smart Peacekeeping: Towards Tech-Enabled UN Operations', International Peace Institute (2016).

38 S. Grand-Clément, 'What role can technology play in enabling remote ceasefire monitoring and verification?', (TechPops, 2022).

39 D. Kolb & P. Starz, 'Real-time conflict monitoring using artificial intelligence for peace operations', (TechPops, 2022).

40 M. Giovanardi, 'AI for peace: mitigating the risks and enhancing opportunities', (Cambridge University Press, 2024).

41 M. Giovanardi, 'AI for peace: mitigating the risks and enhancing opportunities', (Cambridge University Press, 2024).

Beyond prediction, technology also enhances the effectiveness of direct conflict mitigation and de-escalation efforts. Diplomatic actors are increasingly using digital communications to manage crises in real time. For instance, during tense stand-offs or incidents, messaging apps and encrypted channels allow envoys to pass clarifications or concessions between parties within minutes, helping to prevent misunderstandings that could lead to escalation.[42] There have been cases where WhatsApp groups were established between community leaders and security forces in conflict zones to quickly dispel rumours and calm flashpoints, essentially serving as digital 'hotlines' for de-escalation.[43] Moreover, social media analysis has been turned into a conflict prevention tool in its own right: peace-builders monitor platforms not just for warning signs but also to inject counter-narratives and calming messages when they see hate speech trending.[44]

Nevertheless, technology alone does not ensure effectiveness in sustaining peace. Data quality, institutional culture, and digital literacy among staff are all determining factors. Moreover, interoperability challenges, especially in fragmented or post-conflict systems, can limit information sharing and coordination across agencies. Addressing these barriers requires investment not only in digital tools but also in inclusive governance processes, cross-sectoral collaboration, and long-term institutional strengthening.

Accountability and Transparency

Effectiveness alone, however, is not sufficient. For digital tools to contribute meaningfully to peace, their use must be embedded in transparent and accountable governance structures that cultivate trust and legitimacy. Trust in security institutions is a cornerstone of violence prevention and durable peace. In contexts where the social contract is weak – due to past abuses, corruption, or exclusionary practices – digital technologies can provide mechanisms for oversight, transparency, and redress, helping to rebuild public confidence and reduce the likelihood of renewed violence.

---

42 A. W. Dorn, 'Smart Peacekeeping: Towards Tech-Enabled UN Operations', International Peace Institute (2016).

43 J. Beck, 'When disaster strikes, the world opens WhatsApp', Rest of World (2024).

44 Centre for Humanitarian Dialogue, Digital Conflict (HD, 2025).

Logs of decisions, operations, and communications can support after-action reviews and post-crisis evaluations, creating opportunities for institutional reform and capacity development. In peacebuilding contexts, this also strengthens institutional memory, which is critical for non-recurrence of violence. By improving the evidence base and timeline of information, technology can make interventions more transparent – decisions can be backed by concrete data, and the international community can respond more quickly and visibly to emerging crises.[45] At the same time, the growing accessibility of smartphones has empowered individuals to document and share questionable actions by security actors, including human rights abuses by police or military personnel.[46] Coupled with the proliferation of Closed-Circuit Television (CCTV) and other low-cost surveillance systems, these developments have transformed the accountability landscape. Digital platforms now facilitate not just the exposure of misconduct, but also the mobilisation of public opinion and international scrutiny, helping to deter future abuses and foster a culture of rule-based governance.

In the absence of clear legal safeguards, digital tools can be misused for political repression, targeting dissent, or undermining minority rights. Policy vacuums and ambiguous mandates further exacerbate these dangers, particularly when data is weaponised to intimidate or marginalise. As DCAF's report highlights, strong regulatory frameworks, human rights impact assessments, and independent oversight bodies are essential to mitigate these risks and ensure that digital tools uphold rather than erode the principles of democratic security governance.[47]

Participation and Inclusion

Even the most transparent systems can fall short if they fail to reflect the voices of those most affected by insecurity. Inclusive participation in security governance is not just a democratic value; it is a core strategy for preventing violence and sustaining peace. In fragile or conflict-affected settings, where

---

45 P. Engelke, A. Agachi and I. Bayoumi, 'The future of multilateral peacebuilding and conflict prevention', (Atlantic Council, 2023).

46 A. W. Dorn, 'Smart Peacekeeping: Towards Tech-Enabled UN Operations', International Peace Institute (2016).

47 D. Lui and A. Lazar, Digitalization and SSG/R: Projections into the Future, (Geneva: DCAF 2023).

governance institutions may be contested and mistrust widespread, digital technologies offer innovative pathways to inclusion, enabling engagement even when physical presence is unsafe or logistically challenging. Mobile surveys, crowdsourcing platforms, and remote consultations can amplify the voices of communities most affected by insecurity, displacement, or exclusion, by providing them with an active role in shaping local security responses, setting peacebuilding priorities, and co-designing technology deployments.[48] This participatory approach helps identify early grievances, build local legitimacy, and prevent the escalation of tensions by fostering a sense of ownership over peace and security processes.

Digital tools enable remote or marginalised groups to take part in dialogues and decision-making that would otherwise be geographically or socially inaccessible. For instance, mediators have used Zoom and other conferencing platforms to include diaspora members or conflict-affected communities in peace consultations without requiring travel or safe passage.[49] Mobile messaging apps and online forums allow youth, women, and minorities – who might be sidelined in formal negotiations – to voice their perspectives and organise collective action for peace.[50]

However, the benefits of digital inclusion come with caveats, principally the reality of the digital divide. Large segments of the global population still lack reliable internet access or even basic telecommunications, meaning they are effectively cut off from these new avenues of participation.[51] As illustrated in the previous section, digital divides – whether infrastructural, economic, or educational – continue to exist and to exclude large segments of the population, especially women and young girls, in rural areas, or among elderly populations. Even where access exists, participation may be superficial or symbolic, lacking influence over real decisions.

In addition, women and minority communities often face harassment, hate speech, and targeted abuse in digital forums, which can intimidate and si-

48 S. Agathe, 'New Technologies and the Protection of Civilians in UN Peace Operations', (IPI, 2023).

49 Centre for Humanitarian Dialogue, Digital Conflict (HD, 2025).

50 PeaceDirect, Digital Pathways for Peace (PeaceDirect, 2020).

51 International Telecommunication Union, 'Global Internet use continues to rise but disparities remain, especially in low-income regions', (2024).

lence them. Studies have found that women and marginalised groups are the most likely to be targeted by online harassment and hate speech, sometimes driving them out of digital spaces where they are already underrepresented.[52] For example, female peace activists might endure trolling or doxxing campaigns when they speak up on conflict issues, discouraging their continued participation.[53] Similarly, ethnic or religious minorities may find social media flooded with hostile rhetoric against them, undermining the promise that technology would level the playing field. These threats can lead to self-censorship and a retreat from online engagement by those voices the peace process most needs.[54] Inclusive digital engagement can therefore help identify grievances early, prevent marginalisation, and create a shared stake in peace. It enables societies to move from reactive crisis management toward proactive, participatory governance, laying the foundation for a more resilient, just, and inclusive peace.

Policy Recommendations

- **Adopt responsive and effective use of digital technologies**: Digital technologies can prevent conflict by enabling more anticipatory, targeted, and evidence-based responses to emerging threats and sustain peace by identifying patterns of risk and intervening before the escalation of violence.

- **Develop training and capacity building programmes**: Security sector actors need to be prepared for the transformative impact of new technologies on the delivery of security provision and oversight. Training programmes should focus on cybersecurity, AI ethics, information management, and data analysis.

- **Implement rights-based regulatory frameworks**: Institutional safeguards such as independent oversight bodies and complaints mechanisms can prevent the potential misuse or abuse of digital tools by security sector actors.

---

52 PeaceDirect, Digital Pathways for Peace (PeaceDirect, 2020).

53 Amnesty International, "Being Ourselves is too Dangerous" – Digital violence and the silencing of women and LGBTI activists in Thailand, (2024).

54 Centre for Humanitarian Dialogue, Digital Conflict (HD, 2025).

- **Ensure accountability and transparency in decision-making**: Opacity of algorithms can obscure the rationale behind critical decisions and may weaken trust in security sector institutions. Decisions made by digital tools and processes must be held to the same standards as human decision-makers.

- **Promote an inclusive and participatory approach to governance**: Invest in digital literacy, civic education, and rights awareness so that digital participation is informed and empowered. Civil society, academia, and the private sector should be involved in the design and review of digital tools.

- **Ensure gender-sensitive and intersectional AI training data**: To avoid biases, AI systems must be trained on diverse, representative, and inclusive datasets that reflect the lived experiences of different individuals and communities, including women and youth. Efforts should be made to ensure that structural, offline barriers faced by marginalised communities are not replicated online.

Concluding Comments

Emerging technologies are transforming the security sector in ways that are both profound and complex. The future of peace and security in the digital age will depend not only on which technologies are adopted, but on the governance frameworks that shape their use. Good SSG, grounded in principles of accountability, transparency, effectiveness, and inclusion, must underpin every stage of technological design, deployment, and evaluation. Without such principles, technological innovation may reinforce structural inequalities, erode civil liberties, or exacerbate conflict rather than prevent it.

Insights from DCAF's report *Digitalization and SSG/R Projections into the Future* underline the importance of regulating the digitalisation of security institutions with foresight and responsibility. Technology can support prevention and sustaining peace, but only when embedded within ethical frameworks, guided by inclusive processes, and subjected to robust oversight. Digital tools can contribute to more efficient and evidence-based security delivery, enabling improved situational awareness, early warning, and operational coordination. Governance gains are also possible: digital

paper trails and open data initiatives can enhance transparency, while mobile platforms and online engagement tools can widen participation in oversight and accountability processes. However, without appropriate safeguards, the deployment of such technologies can also lead to surveillance overreach, biased outcomes, and the exclusion of vulnerable populations.

To ensure that digital transformation contributes to peace and security, security institutions should adopt a principled approach to technology use. This involves:

- Investing in both digital infrastructure and human capacity;
- Developing and enforcing rights-based regulatory frameworks;
- Promoting inclusive, accessible digital tools that reduce inequality;
- Ensuring alignment with international standards on data protection, transparency, and digital rights.

The decisions made today regarding how technologies are governed will shape the legitimacy, resilience, and peacebuilding potential of security institutions for the years to come. With thoughtful implementation, emerging technologies can become critical enablers of accountable governance and sustainable peace.

A Critical Time for the Future of the South Caucasus – A View from Georgia

Giorgi Badridze

Introduction

Georgia, Armenia and Azerbaijan regained their independence as a result of a profound geopolitical shift in the early 1990s. More than three decades later, the South Caucasus, together with the rest of the world, is entering a new phase of geopolitical changes and the way the three countries prepare themselves for the new realities will determine their fate for the years to come. In this regard, the peace deal between Armenia and Azerbaijan, providing the basis for a lasting settlement of the decades-old territorial conflict, would play a key role.

A Troubled Start

The early 1990s were marked with great expectations and often illusions. Many believed that it was a dawn of a new, more peaceful and fairer world in which democracy had convincingly demonstrated its superiority and the peoples of Central and Eastern Europe, as well as Central Asia, formerly dominated by the Soviet empire, would now gain a chance at building their free and prosperous societies. And this is exactly what most of these countries, especially in Central Europe did. However, as it turned out, the history did not end, it only took a break.

Georgians were perhaps the first nation which found out that the Soviet empire was not going to give up as easily as many thought, and that its successor Russia was not parting ways with its traditional imperial instincts as the new Western friends and supporters of Russian democracy hoped. From day one, Georgia found itself at the receiving end of what would later be called "hybrid warfare".

Armenia and Azerbaijan also felt the "brotherly" embrace of the Kremlin. If in Georgia Russia actively enticed internal conflicts (between the first

democratically elected government and its opposition, as well as the conflicts in Abkhazia and South Ossetia), in their case Russia invested in the territorial dispute between the two. For three decades the Karabakh conflict constituted Russia's main leverage, especially over Armenia, which considered Russia as an ally and the sole guarantor of its security. Russia made Armenia pay a high price for its support – that price was a considerable share of Armenia's political and economic sovereignty. However, the moment the Kremlin felt that Armenians strayed from total obedience and wanted a better government than a Moscow-approved corrupt regime, the "security guarantees" suddenly vanished. Armenia lost the second Karabakh War.

The End of the War with No Peace

Azerbaijan's victory had many other reasons: the most fundamental one was the gradual change in the balance of power. After completion of the Baku-Tbilisi-Ceyhan oil pipeline (a project initiated and brought to fruition by the United States) which allowed it to export oil directly to the international markets (bypassing Russia), followed by a similarly important natural gas pipeline, Azerbaijan accumulated enough economic strength that allowed it to profoundly transform its armed forces and gain decisive military superiority over Armenia. It must be emphasised that Azerbaijan's victory was not predetermined only by better armaments, but by taking advantage of modern training and highly effective tactics while Armenia relied on the outdated Soviet/Russian military school.

Russia's lukewarm reaction to the renewed military hostilities in 2020 (known as the second Karabakh War) and several later clashes raised questions about whether Russia changed its sympathies. Even its "peacekeeping force", deployed in parts of Karabakh, did next to nothing to prevent the subsequent exodus of Armenians. This should have surprised no one, as long before, their conduct in Georgia's occupied Abkhazia region produced a sad joke: "Russians are here not to keep peace but the pieces of the Soviet Union". Karabakh produced a gloomy joke of its own that is based on reality: "In the conflict between Armenia and Azerbaijan Russia supports ... the conflict." Indeed, up to a certain point, Russia did support Armenia militarily but it never seriously promoted or brokered peace with Azerbai-

jan when Armenia commanded a position of strength. Such peace deals in the late 1990s or the early 2000s would have been incomparably more favourable to Armenia. And this is something that victorious Azerbaijan should keep in mind when it is making its calculations on how to extract more concessions from the Armenian side before agreeing to a peace deal.

The Breakthrough that Almost Happened

A peace deal was indeed announced in March 2025 when Armenia and Azerbaijan agreed on the terms of the treaty. It was also said that Azerbaijan expected Armenia to meet some additional conditions before signing the document: elimination of the territorial claims from the Armenian constitution and disbandment of the Minsk Group – a format created under the OSCE and co-chaired by Russia, US and France. Azerbaijan wants to ensure a stable agreement and also feels particularly negatively about the Minsk format which has not delivered any meaningful results in more than three decades of existence. Azerbaijan has had a profound distrust of individual outside brokers, as Baku viewed them as biased and preferred to negotiate with Armenia without any mediators. Such direct contacts have actually produced more tangible results than other formats.

Apparently, since March, Azerbaijan's stance has hardened, and it appears that the number of preconditions to sign the deal have grown. It has been clear that Armenia, after decades of reluctance, showed greater eagerness to finalise the deal. Prime-Minister Pashinyan's government has invested all its political capital in trying to leave the conflict with Azerbaijan behind and concentrate on Armenia's pivot toward the West. So far, Pashinyan, who faced a strong opposition for his readiness to make peace with Azerbaijan has survived several attempts to oust him. However, his position might not remain stable if he could not show results to his own core supporters who, like him, prioritised peace and the opportunity to build a viable Western-integrated democracy over nationalistic aspirations. Pashinyan's Civil Contract Party already experienced a major setback in early April 2025, when a communist candidate with the support of other opposition parties won the mayoral election in Armenia's second largest city, Gyumri (which also houses a major Russian military base).

The Risks of Not Finalising the Deal

In other words, the window of opportunity for the Armenia-Azerbaijan peace deal is narrowing and this does not necessarily mean bad news just for Prime-Minister Pashinyan. Azerbaijan might feel it was in a commanding position and that it could afford to wait for better conditions for the agreement or even aspire for more territories in case the current ceasefire arrangements broke down altogether. However, this is exactly how Armenians had felt a couple of decades ago when they had not agreed on a deal (in the late 1990s the two sides were particularly close to a breakthrough) as they refused to offer Azerbaijan any territorial concessions because of their military superiority status and the security assurances from Russia.

Armenia clearly made a grave mistake when its leaders did not seize the opportunity to make a peace deal from a position of strength. Azerbaijan might want to make sure it is not repeating this mistake today. While there is no immediate prospect of the decline of Azerbaijan's military superiority, the return to power of the pro-Moscow forces in Yerevan might endanger the prospects of any peace deal without which lasting stability in the region cannot be achieved. Azerbaijan has most to gain if, after 34 years of independence, the South Caucasus finally became a proper region, with its constituent countries actively cooperating instead of waging wars or attracting rival external forces in order to balance one another. One such force – Russia – has a proven track record of working toward preventing all three countries become stable sovereign states, not just ones with rival (democratic) political systems or with pro-Western geopolitical predispositions.

As mentioned above, the world order is experiencing profound and unpredictable changes, which might once again be bringing great geopolitical turbulence, and the best way for the South Caucasus to be ready for it is to have stable and cooperative relations among the three regional countries, which cannot be achieved without a viable peace arrangement between Armenia and Azerbaijan.

Why a Peace Deal would be a Win for Both Parties

To ensure a more stable and prosperous future in the emerging new world, the countries of South Caucasus must work together to make sure that

their region can play a joint international function, as a hub and a bridge between the Greater Caspian and Black Sea regions, connecting Europe and Central Asia. Azerbaijan and Georgia have already performed this function by providing Caspian energy with an outlet toward the international markets. With the settlement of the conflict with Azerbaijan, Armenia could join the cooperation format which would provide not only additional opportunities for international trade but it would dramatically reduce the risks of destabilisation of the region (a factor that has been keeping many investors away) by depriving the Kremlin of its main leverage against both countries and the whole region.

If Russia's unprovoked war on Ukraine has demonstrated anything is that the Kremlin continued to act upon its leaders' fantasy to restore the Russian control over the "lost imperial possessions". This represents a clear and present danger to all of Russia's neighbours, not least in the South Caucasus. However, this also represented an opportunity: Russia's reckless behaviour has resulted in its international isolation and has severed many international transportation routes that had run via Russia. This has created a greater demand for the Middle Corridor and the alternatives to Russian energy supplies, particularly natural gas. This should create an additional incentive for Azerbaijan to expedite the finalisation of the peace deal as it would be the primary beneficiary of increased trade between the wider Caspian Sea region with the Greater Black Sea region.

Potential International Ramifications of the Peace Deal

The neighbours of the South Caucasus region are in need of greater connectivity both in the East and the West. Central Asia has long been dependent upon Russian-controlled transport and energy infrastructure for many years. Russia's near monopoly has started to weaken as China started building economic partnerships with Central Asian countries. This partnership included new pipelines and land transport infrastructure. By doing so, China has somewhat balanced the Russian dominance and thus has provided a greater degree of security from Russian threats, especially for Kazakhstan, which had been concerned about its security and territorial integrity for quite a while. However, without stable access to the Western markets, the Central Asian countries would not be able to fully utilise their economic potential or consolidate their national sovereignty.

From the West, the European Union and Türkiye, have been looking for new sources of energy. Türkiye could most likely be both an important participant of such future projects, and one of its main beneficiaries, as a consumer of extra energy as well as a provider of transit to European customers. It must be stressed that just like the odds to achieving a peace deal between Armenia and Azerbaijan, the above mentioned economic and energy opportunities, will not last forever, as China is methodically working to expand its influence in Central Asia.

The successful experience accumulated by Georgia and Azerbaijan in cooperating on major international projects, particularly that of the Baku-Tbilisi-Ceyhan (BTC) pipeline (which many in the 1990s deemed a "pipe dream"), has shown that working together for mutually beneficial goals, unhindered by the zero-sum game mentality, could deliver impressive results.

Of course, one of the preconditions for attracting major partners and investors to join projects designed to increase regional connectivity is to make sure that the South Caucasus is not viewed as a volatile region, as it has been seen for decades. Today, fostering greater regional stability has better chances than ever since lasting peace between Armenia and Azerbaijan is within their grasp. Georgia could play a greater role in peacebuilding by providing mediation, or at least a platform, for the ongoing peace talks between Armenia and Azerbaijan.

Armenia too must be offered a role in regional projects that can deliver the economic dividends of peace and leave less room for the revanchism inevitably fuelled by Russia. Georgia has its own stake in the final resolution of the conflict and of lasting peace in its neighbourhood, as it will be one of the beneficiaries of greater stability in the South Caucasus.

Conclusion

This is a moment of historic significance – Armenia and Azerbaijan have an opportunity to leave the conflict behind and help the South Caucasus develop into a stable region with a valuable international function – a region that connect its Eastern and Western neighbours. This opportunity must be seized now as it might not be there for much longer. The time for a peace deal is now.

Russia and the Future of Algorithmic Geopolitics

Boris Kuznetsov

Mankind is entering an era in which artificial intelligence (AI) is no longer merely an auxiliary technology but a foundational element in the global governance system. Its influence extends beyond accelerating routine processes – it actively shapes decision-making, creates alternative trajectories of action, and redefines the dynamics of international relations. Algorithms now participate in geopolitics not just as analytical tools but as mechanisms of influence that determine what is considered rational, beneficial, or acceptable. This transformation is particularly evident in the strategies of states vying for global leadership.

We are living an informational era characterised by a post-industrial society in which the innovative sector takes precedence over traditional industries. The knowledge industry has undergone radical transformations, shifting from standard manufacturing to a digitalised economy heavily reliant on the transfer and analysis of information. In a landscape where information confrontation has evolved into an algorithmic war, dominant nations have transitioned from simply producing content to creating structural frameworks powered by advanced algorithms and neural networks. The integration of AI into global governance and diplomacy has given rise to a new paradigm: algorithmic geopolitics.

Unlike traditional power struggles, where military might and economic leverage were the primary tools of influence, today's geopolitical landscape is increasingly shaped by AI-driven decision-making, predictive modelling, and automated influence operations. This shift marks a fundamental transformation in how states compete, cooperate, and assert dominance in the 21st century. AI is no longer just a tool for efficiency – it has become an architect of geopolitical strategy. Governments now deploy machine learning and big data analytics to:

- **simulate policy outcomes**: AI models predict the consequences of trade wars, sanctions, or military interventions, allowing states to optimise their strategies and actions;

- **digitalize diplomacy**: chatbots and AI-driven assistants analyse vast datasets to suggest optimal diplomatic responses in real time;
- **manage information flows**: algorithms curate and amplify narratives, shaping public perception domestically and abroad.

For example, China's "Social Credit System" uses AI to monitor and influence citizen behaviour, while the U.S. employs AI in intelligence analysis through platforms like Palantir, enabling predictive assessments of global instability.

In contrast, Russia appears to be lagging behind, sticking to outdated strategies reminiscent of the early 2000s. The nation appears more as an object within the information domain rather than a proactive subject, as confirmed by reports indicating that, towards the end of 2024, the Kremlin engaged in discussions about adapting AI for political projects. However, substantial systemic solutions remain elusive, with efforts primarily focused on digesting vast amounts of data through platforms like Medialogy. The major concern is that Russia lacks hybrid model systems, where AI could serve dual roles in both foreign and domestic policy. Unfortunately, what is currently branded as "information warfare" in Russia often comprises fragmented projects that lack coordination and technological robustness. While other nations are leveraging AI and algorithms, Russia continues to rely on human resources for its strategic communications.

While some countries utilise neural networks to model social behaviours, others cling to "information special operations" rooted in past methodologies. AI is no longer a futuristic concept; it is an immediate reality that necessitates consideration of advancements in neural network technologies from corporations like Yandex or Sberbank for applications in political contexts, rather than limiting their use to commercial advertising.

Globally, AI is progressing beyond mere algorithms to become a critical element of decision-making architectures, spanning domains from electoral analytics to crisis management. In contrast, in Russia, discussions about AI remain confined to the realm of technological novelty – a topic sparking enthusiasm among panellists but lacking operational application.

The Russian political landscape continues to function along a vertical hierarchy of meaning, characterised by strict narrative control, manual audience

engagement, and traditional campaigning methods. Within this framework, AI may serve as an assistant – utilised for personalising content, automating reports or managing chatbots – but it is not yet viewed as a partner in public governance. In this context, AI poses a challenge given that any deviation from established hierarchies is often perceived as a threat rather than a step towards innovations. Moreover, AI is seen as a rival to political consultants whose influence on decision-making remains significant. Instead, it represents a tool that can liberate consultants from the constraints of traditional templates, over-reliance on personal intuition, and sluggish analytical processes. However, if the political machinery is predicated on the fear of relinquishing manual control, then no neural network will be able to integrate into its operations.

In the West, information warfare has morphed from traditional discussions into a sophisticated form of algorithmic warfare, which employs AI as a central tool. It encompasses intricate data networks that shape audience engagement, raising questions about who constructs reality for these audiences and, more critically, how semantic structures are formed. The contemporary challenge is not about determining who is right in a debate; rather, it is about who has effectively integrated into the algorithms that govern information perception, algorithms meticulously crafted by AI and directed toward specific users. The concept of "algorithmic warfare" has emerged, where AI is used as weapon not just in cyber operations but in psychological, economic, and political domains. Key developments include:

- **AI-powered disinformation**: Deepfake technology and bot networks manipulate elections and social unrest;
- **autonomous military systems**: AI-driven drones and decision-support tools in defence (e.g., Israel's "AI targeting systems" in Gaza Strip);
- **economic coercion via AI**: predictive sanctions and trade barriers.

Paradoxically, Russia's current disunity within the AI landscape may present unique advantages. Centralised AI platforms in the West are potentially susceptible to disruptions stemming from technological, ideological, or political upheavals. In an age marked by algorithmic hyper-dependence, resilience may hinge not on sheer computational power but on adaptability. Russia has

the opportunity to construct its own architecture of influence, not as a mere imitation of existing models but as a multifaceted system characterised by cognitive flexibility – one that recognises regional diversity, caters to loyal audiences, and can strategically utilise even limited resources.

The initial steps toward this ambition are already emerging: the AI infrastructure of corporations such as Yandex and Sberbank, the implementation of meaning-recognition models in major media enterprises, and pilot projects of generative systems within the Ministry of Foreign Affairs and the Ministry of Defence. The objective is not merely to catch up to the West but to create a unique developmental trajectory that does not adhere to Western paradigms, but instead aligns with the principles of digital sovereignty. Thus, there is a pressing need not just for technological development but for cultivating a mode of thinking that is resilient against external influences.

The 21st century's defining conflict is no longer over resources but over interpretations of reality. AI stands at the forefront of a new era in geopolitics, influencing the fundamentals of power, security, and governance. As nations strive to become leaders in AI, the global landscape will continue to evolve, shaped by technological advancements and competitive dynamics. AI has become a pivotal actor in this struggle, shaping perceptions, influencing decisions, and redefining power structures. States that fail to recognise AI as a strategic sovereignty issue risk losing more than technological ground – they forfeit the right to define their own future. In this algorithmic era, the question is no longer who holds the truth but who controls the neural networks that shape it. The nations that thrive will be those that harness AI not as a tool but as a foundational pillar of their geopolitical strategy.

Understanding the multifaceted implications of AI as a geopolitical game-changer is essential for policymakers, scholars and public influencers. It is imperative to navigate this landscape thoughtfully, balancing the pursuit of technological progress with ethical considerations, international cooperation, and a commitment to preserving democratic values. Ultimately, how countries choose to wield the power of AI will determine not only their own futures but also the shape of global affairs in the years to come.

PART II: Existing Frameworks for Governance of Cyber Technologies for Peace in the South Caucasus Countries

Securing Georgia in the Cyber Age: National Security, Threats, and Resilience

Andro Gotsiridze

Cyber Threats Impacting Georgia

Over the past two decades, cyber security has become more and more important as a part of national security. Cyber has established itself as a fifth domain of confrontation. Political, military, social and criminal processes have mostly migrated to cyberspace. That means that the cyber domain is constantly used for reaching political, economic or military goals. Well-developed cyberattack potential enables many states to successfully use cyberspace during wars, conflicts or peacetime to obtain geopolitical superiority.

Cyber, today, has already become an important part of any war, conflict or confrontation. So, what is the geography of destructive cyber operations? Chinese state-backed tech companies are Trojan horses for Chinese intelligence, Russia's disinformation campaigns try to turn our citizens against one another, and Iranian cyberattacks plague Middle East computer networks.

Russia, China, Iran, North Korea successfully developed its offensive cyber capabilities. From the beginning of the 21st century, fields such as state structures, media and communications, industry, energy, political organizations have become the targets for cyber operations by destructive actors of varying difficulty and intensity in tens of countries.

Iran's cyber capabilities may be a threat to Georgia insofar as the infrastructure of the states that Iran considers hostile to itself is placed on our territory. Also, it is entirely realistic for the Tehran-backed terrorist organizations to use the Georgian cyber network for recruiting and propaganda purposes. Cyber espionage is another tool for Iran to conducting a terrorist attack. It can be used both for determining real-time geolocation, resulting from surveillance through a cell phone company, as well as for tracking of a potential target to preparing a terrorist act.

While Iran's cyber activities pose a distinct challenge, Georgia must also be cautious of cyber threats originating from China. Unlike Iran, whose cyber operations often focus on espionage and terrorist facilitation, China integrates its cyber strategy with broader geopolitical and economic ambitions.

China has been advancing its cyber-attack capabilities by integrating its military cyber-attack and espionage resources in the Strategic Support Force, which it established in 2015. Targets of China's cyber operations vary from national security related information to sensitive economic data and intellectual property. Furthermore, Georgia should pay significant attention to the cyber security of the national or commercial projects, which involves US and other strategic partners, whom Beijing sees as adversaries.

Regardless that China, Iran, and North Korea state and non-state actors have offensive cyber capabilities, Georgia remains most concerned about Russia. Cyber threats from Russia and its proxies will remain acute. Additionally, many capable hackers and profit-oriented cybercriminal groups maintain mutually beneficial relationships with the Kremlin that offer them safe haven or benefit from their activity.

Russian Cyber Operations:
Strategies, Tools, and Implications for Georgia

Since the cyberattacks of 2008, the scale and sophistication of Russian cyber threats have significantly increased due to several factors.

- First, Russia has not altered its aggressive cyber policy, and even more, it has increased its offensive cyber capabilities.
- Second, Russia extended the fields of usage of cyber operations in both directions: information-technical and information-psychological.
- Third, Georgia's dependence on information and communication technologies (ICT) is much higher now, which increases the scale of the expected damage.

The Kremlin regards information as a key domain in modern military conflict and has successfully advanced its offensive cyber capabilities to achieve political, economic, and military objectives, as well as broader geopolitical leverage. Considering Georgia as part of its sphere of influence, Russia persistently targets the country with hybrid warfare. Consequently, Russian cyber operations remain the primary threat to Georgia, posing both technical and psychological effects. Therefore, Georgia's cyber defence policy must be "Russo-centric".

How far, with what means and to what extent, intentionally or unintentionally, can Russia reach into information systems?

From the use of such tools as NotPetya to SolarWinds, or to Yandex and Kaspersky, what are the means of frustration?

Can the Kremlin score an unexpected success in cyber warfare if we are insufficiently prepared?

The negative effects of cyber operations conducted by Russia are diverse and could serve different purposes:

- **Various Levels of Disruption or Disablement of Critical Infrastructure through DDoS or Defacement Type Attacks**

  In terms of a weakly protected infrastructure, even low-tech Distributed Denial-of-Service (DDoS) or defacement attacks could result in disproportionately high damage. The cyber operations during the 2008 Russia-Georgia war were a direct and well-coordinated complement to conventional military actions. However, due to the relatively low internet penetration in Georgia at the time (7–8%), these attacks did not significantly facilitate the Russian armed forces' military objectives. Instead, they aimed to create an information vacuum, establish informational superiority, and reinforce the Russian narrative of the conflict – namely, that the Georgian government initiated the war, prompting Russia to launch its so-called **"Operation to Compel Georgia to Peace"** to protect Ossetian citizens.

- **Compromising the Supply Chain and Disabling Industrial Control Systems (ICS)**

  Russia has been refining its supply chain attack capabilities for years. In 2016, Russian military intelligence launched one of the most devastating supply chain attacks to date – the **NotPetya** ransomware campaign. This operation targeted financial institutions, government agencies, and energy firms, causing widespread disruption and billions of dollars in damages. **NotPetya**, initially disguised as ransomware, was in fact a destructive wiper malware, permanently crippling the systems it infected.

  Georgia has also been a frequent target of Russian cyber operations, with tactics ranging from website defacements and DDoS attacks to sophisticated supply chain compromises. For instance, in 2019, a large-scale cyberattack attributed to Russian intelligence defaced thousands of Georgian websites, including government portals, media outlets, and private organizations. This attack mirrored elements of supply chain compromises by exploiting trusted digital infrastructure to amplify its impact.

  A few years after **NotPetya**, another large-scale supply chain attack emerged – the **SolarWinds** breach. This incident represented a classic supply chain compromise, in which attackers, Russian state actors, infiltrated **SolarWinds**, a company that provides network management software called **Orion**, to gain access to clients further down the supply chain

  This method proved highly effective, impacting a vast number of organizations simultaneously – approximately **18,000** entities, including government agencies, military organizations, high-tech firms, and commercial enterprises, were infected through the compromised Orion software. This attack underscored the evolving sophistication of Russian cyber operations, demonstrating their ability to exploit trusted software providers to penetrate high-value targets.

- **Cyber Espionage and Destructive Malware**

  Georgian authorities, with the assistance of FireEye, uncovered a large-scale cyber espionage operation known as Georbot, attributed to the hacker group APT28 (Russian GRU). This operation targeted Georgian government networks, stealing sensitive data, including information on NATO-Georgia relations, and exfiltrating it through remotely deployed malware. The campaign not only compromised Georgian systems but also extended to other Eastern European countries and international organizations. APT28, which has been active since at least 2007, primarily conducts intelligence-gathering operations aligned with Russian geopolitical objectives. Beyond espionage, Russia has demonstrated its capacity to deploy advanced malware for disruptive and destructive purposes. For instance, during its military intervention in Ukraine (2014–2016), Russia used malware such as BlackEnergy and Ouroboros to target critical infrastructure, causing significant disruptions including power grid failures. This dual-use approach – combining cyber espionage and destructive malware – suggests that Russia's future cyber operations will likely focus not only on covert intelligence collection but also on high-impact attacks designed to disrupt and damage critical infrastructure, further underscoring the evolving nature of modern cyber warfare.

- **Insider Threats**

  One of the most effective ways to infiltrate a system is through insiders. In the context of Russian cyber operations, insiders are often used as entry points in larger cyber espionage campaigns or supply chain attacks, where trusted individuals within targeted organizations facilitate or unwittingly aid in the compromise of sensitive data or critical infrastructure. This threat is particularly pronounced in post-Soviet countries, where there is a high level of Russian penetration across various sectors, combined with a developing cybersecurity culture and low awareness. The absence of a strong cybersecurity framework in these countries increases vulnerability, making it easier for malicious actors to exploit insider access for espionage, sabotage, or data theft. Russian cyber actors commonly use phish-

ing as a method to exploit this weakness, posing significant risks to organizational security.

- **Cyber Operations with Psychological and Informational Impact**

  Russia's cyber operations often aim to shape public perception, reduce pro-Western sentiment, and foster the rise of a **pro-Russian elite**, creating conditions for potential conventional action. A notable example of such a **cyber-enabled influence operation** targeting Georgia's sovereignty occurred on **October 28, 2019**, when a large-scale **Russian-backed cyberattack** defaced thousands of Georgian websites, including government portals, courts, media outlets, and NGOs. The attackers replaced these sites' landing pages with electronic graffiti featuring images of former President **Mikheil Saakashvili** and the phrase "I'll be back!" This act was intended to sow division and incite internal discord among Georgian citizens. Additionally, the attack served as an intelligence-gathering effort, testing Georgia's cyber defenses, vulnerabilities, and overall resilience. The attack was attributed to **Russian Intelligence Service**, with numerous states and organizations, including the **European Union**, **NATO**, and the **United States**, publicly condemning the operation.

Georgia's Cyber Ecosystem: Legal Frameworks and Institutional Responses

Cybersecurity has become a state priority after 2008 Russia-Georgia war, when the country has experienced a wide-scale cyberattack on its governmental, as well as banking and media sectors. The Digital Governance Agency under ministry of Justice was established to protect information and cybersecurity of critical infrastructures in 2010. In the following years, the whole of organizational structures have been formed – among such organizations are Cybersecurity Bureau of the Ministry of Defence of Georgia, Operative-Technical Agency under the State Security Service of Georgia, and the division to fight against cybercrime within the Central Criminal Police Department.

The main legal framework for this cyber architecture is the *Law on Information Security*, originally adopted in 2012. Since the last amendments in 2022, the State Security Service has been responsible for the cybersecurity of government networks and e-communication services, including Internet Service Providers and telecommunications. Digital Governance Agency covers e-governance, data exchange infrastructure and some important awareness raising activities. The Cyber Security Bureau of the MoD remains responsible for cybersecurity of defence agencies and the Criminal police department covers the cybercrime investigation activities.

The high rate of private ownership of critical information systems in Georgia makes close collaboration between private infrastructure operators and government security stakeholders crucial. Exchange of information between domestic stakeholders was formally unregulated. This was largely since the Law on Information Security identified only public institutions as Critical Infrastructure and therefore, the private organisations, including Internet Service Providers (ISPs) were not obliged to cooperate or report cyber security incidents.

Following the changes made in 2020, the list of Critical Infrastructure (CI) has been updated and includes three groups of subjects:

- state agencies and networks;
- e-Communication companies incl. ISPs;
- business actors identified as CI. Financial institutions and Banking sector.

State security services are responsible for the first two points and the third is the responsibility of the Digital Governance Agency.

Georgia's first cyber security strategy and action plan was developed in 2013. The second edition of Cyber Security Strategy (2016–2018) was developed at the end of 2015. It covers new projects and necessary events to provide cyber security. The third-generation National Cyber Security Strategy is bringing together components aimed at improving not only the country's cyber security environment but also strengthening capabilities to combat cybercrime and effectively make the use of cyber defence techniques.

The main goals and objectives of new strategy are:

- Bolster the development of cyberculture among information society and organizations, to support resilience to threats and incidents in cyberspace;
- Sustainability of cybersecurity governance system and enhancement of the public-private cooperation;
- Strengthening cyber capabilities and development of strong cyber workforce;
- Strengthen Georgia's position as a net contributor to international cyber security at an international scale.

International Collaboration: Strengthening Georgia's Cyber Resilience

Organizing an effective cyber defence without an international cooperation is inefficient; no state has yet managed to ensure effective cybersecurity without it. Thus, Georgia, together with its allies, is trying to increase cyber capabilities in crucial areas using diverse projects, such as information sharing, public-private partnership, capacity building, and awareness raising:

- **NATO-Georgia Joint Training and Evaluation Centre (JTEC)**
  Launched as part of the Substantial NATO-Georgia Package (SNGP) that began around 2014, this Centre organizes regular cyber defence exercises, simulations, and training sessions. It strengthens the interoperability between the Georgian Defence Forces and NATO partner nations while enhancing practical cyber defence skills.

- **NATO's Malware Information Sharing Platform (MISP) Membership**
  In March 2020, the Georgian Cyber Security Bureau joined NATO's MISP. This membership enables Georgia to exchange threat intelligence with NATO and its partners, thereby enhancing its ability to detect, prevent, and respond to cyberattacks in a coordinated manner.

- **UK-Georgia Cyber Partnership Project**
  Announced in recent years, this initiative – jointly funded by the UK and the Georgian government – focuses on boosting Georgia's cyber resilience. Its activities include capacity-building measures, joint training sessions, and the sharing of best practices for countering cyber threats.

- **EU Twinning Project: Strengthening Cybersecurity Capacities in Georgia**
  Active since around 2020, this EU-funded project is designed to modernize Georgia's cybersecurity legal and institutional framework. It helps align national regulations with EU directives (such as the NIS[1] Directive) and supports capacity building through both technical and regulatory assistance.

- **US-Supported Cybersecurity Capacity Building**
  Over the past four years (roughly 2019–2023), Georgia has received approximately $68 million in US aid aimed at improving its cybersecurity capabilities. These investments cover training programs, technology upgrades, and infrastructure improvements that bolster Georgia's overall digital resilience.

- **USAID Critical Infrastructure Cybersecurity Project**
  Launched in 2021, this USAID-funded project is focused on strengthening the cybersecurity posture of Georgia's critical infrastructure. With particular attention to the energy and telecommunications sectors, it supports enhanced incident response capabilities and risk management frameworks to safeguard vital national systems.

- **USAID-supported Elections Cybersecurity Initiative**
  Beginning in 2022, this initiative partners with USAID to bolster the cybersecurity of Georgia's electoral systems. Its measures include technical support and capacity building for election officials, as well

[1] Network and information systems.

as the deployment of tools to detect and counter cyber threats and misinformation during electoral processes.

- **Energy Sector Cybersecurity Enhancement Project**
  Also initiated around 2022, this project (supported by USAID and other international partners) aims to secure Georgia's energy infrastructure against cyber threats. The project involves conducting risk assessments, implementing advanced monitoring systems, and upgrading cybersecurity protocols in critical energy installations.

Future Outlook: Preparing for Evolving Cyber Threats

The evolution of Russian cyber capabilities demonstrates a clear trajectory toward increasing sophistication and strategic integration with conventional military operations. The 2007 cyberattack on Estonia marked the first politically motivated cyber operation aimed at provoking public unrest. A year later, in the Russia-Georgia War, cyber operations were deployed as a complementary tool to traditional warfare, facilitating an information vacuum, spreading disinformation, and obstructing international support for Georgia. Russia's ability to secure informational superiority enabled it to manipulate narratives, falsely portraying its military intervention as a response to alleged Georgian aggression.

In subsequent conflicts, Russian cyber tactics became even more advanced. The exploitation of telecommunications networks for covert surveillance and psychological operations, along with the use of malware to disable critical infrastructure, underscored the growing role of cyber warfare in modern conflicts. The ability to track individuals, intercept communications, and utilize this intelligence for targeted operations demonstrated a shift toward more integrated and precise cyber-enabled military strategies. Additionally, disabling critical infrastructure through sophisticated cyberattacks further illustrated how cyberspace is being leveraged to disrupt essential services and exert strategic pressure on adversaries.

Beyond military applications, Russia employs cyber-enabled influence operations to undermine democratic institutions, erode public trust, and manipulate political processes. Russia seeks to destabilize democratic governance

and impede the aspirations of countries striving for closer ties with the West. To achieve this, it actively interferes in elections through manipulation, aiming to secure a strategic advantage by installing pro-Russian elites and governments. These operations often aim to sow division within societies, weaken alliances with strategic partners, and obstruct the Euro-Atlantic integration of neighbouring states. Through a combination of disinformation campaigns, election interference, and the weaponization of social media, Russia seeks to destabilize democratic governance and impede the aspirations of countries striving for closer ties with the West.

To counter such threats, states must develop comprehensive cybersecurity architecture supported by clear strategic documentation, international partnerships, intelligence sharing, and robust public-private collaboration. Additionally, volunteer-based cyber reserves and awareness-raising initiatives are essential components of national cyber resilience. Given that human security is a fundamental aspect of cybersecurity, efforts to enhance public awareness and preparedness should be prioritized.

Moving forward, Georgia must continue strengthening its cybersecurity architecture through a combination of legal frameworks, institutional coordination, and international partnerships. Given the evolving nature of cyber warfare, investing in cybersecurity education, public-private cooperation, and proactive threat intelligence sharing will be essential to mitigating emerging threats. Only through a comprehensive and adaptive approach can Georgia maintain its digital resilience against increasingly sophisticated adversaries.

References

Defence Intelligence Agency. China Military Power – Modernizing a Force to Fight and Win. Washington D.C.: 2019 (DIA-02-1706-085).

Defence Intelligence Agency. Iran Military Power – Ensuring Regime Survival and Securing Regional Dominance. Washington D.C.: 2019 (DIA_Q_00055_A).

Defence Intelligence Agency. Russia Military Power – Building a Military to Support Great Power Aspirations. Washington D.C.: 2017 (DIA-11-1704-161).

Fireeye special report, 2014. APT28: A Window into Russia's Cyber Espionage Operations. Available online: https://www.fireeye.com/content/dam/fireeyewww/global/en/current-threats/pdfs/rpt-apt28.pdf.

Giles, Keir. "Handbook of Russian Information Warfare". NATO Defense College Fellowship Monograph Series, No. 9. Rome: 2016. ISBN: 978-88-96898- 16-1.

Gotsiridze, Andro; Petriashvili, Maka. "Rebooting Security – An innovative plan for protecting Georgia's critical infrastructure". Per Concordiam – Journal of European Security and Defense Issues, Vol. 9, Issue 1, 2018.

International Monetary Fund. Monetary and Capital Markets Department. Georgia: Technical Assistance Report-Cyber Risk: Regulation, Supervision and Testing. International Monetary Fund, Vol. 2024, Issue 107, 2024. https://doi.org/10.5089/9798400296154.019.

Tikk, Eneken; Kaska, Kadri; Vihun, Liis. International Cyber Incidents: Legal Considerations. CCD COE, Tallinn: 2010.

Harnessing Emerging Technologies for Peacebuilding: Azerbaijan's Experience and Untapped Potential

Vasif Huseynov

In recent years, Azerbaijan has made considerable strides in the integration of emerging and cyber technologies across various sectors of governance and the economy. Like many other nations, the country views these innovations as essential tools not only for modernization and efficiency, but also for ensuring national security and long-term development. In this context, one of the most pressing needs is protecting the country and its population from both internal and external cyber threats. Additionally, digital innovation plays a key role in Azerbaijan's strategic objective of diversifying its economy and reducing reliance on oil and gas.

Azerbaijan's citizens began experiencing the tangible benefits of these technologies through the advancement of e-governance. According to international evaluations, Azerbaijan has emerged as a global leader in this domain. In 2024, the United Nations E-Government Development Index (EGDI) placed Azerbaijan 74th out of 193 countries, a nine-place improvement from 2022. Notably, the country entered the "Very High EGDI" group for the first time – an achievement that reflects the steady progress in digitizing governance.

Among the most prominent achievements is the *ASAN Service* ("Easy Service"), a flagship initiative representing the country's efforts to simplify state-citizen interactions. Based on a "one-stop-shop" digital model, ASAN has reduced bureaucracy, improved transparency, and brought public services closer to the population. More than a matter of convenience, ASAN empowers citizens and exemplifies how digital transformation can foster more inclusive and efficient governance.

Innovation in Azerbaijan also extends to the economic domain, particularly the energy sector – a historic cornerstone of the national economy. The integration of artificial intelligence and smart technologies has enhanced efficiency and sustainability in energy management. These tools now handle

in seconds what once required months, drastically improving planning and operations. Simultaneously, Azerbaijan is investing in green energy, integrating solar and wind infrastructure with digital solutions to optimize performance and resilience.

Emerging technologies are also central to the reconstruction of territories liberated from Armenian occupation. Projects such as smart villages and green zones are being launched to revitalize the Karabakh region, with the ambition of transforming it into a hub for renewable energy and digital innovation. As this transformation proceeds, ensuring cybersecurity becomes increasingly critical. As more aspects of society – from banking to critical infrastructure – go digital, the risk of cyber threats grows.

This was acutely evident during the Second Karabakh War in 2020, when Azerbaijan faced not only physical attacks but also cyber offensives targeting government institutions, media outlets, and essential infrastructure, including the Central Bank. These experiences underscored a modern reality: in the 21st century, national security hinges as much on data protection and network resilience as on territorial defense.

In response, Azerbaijan adopted its first **National Strategy on Information Security and Cybersecurity for 2023–2027**. This comprehensive strategy aims to elevate cybersecurity standards across the public and private sectors, including critical infrastructure. It provides a framework for the secure and responsible use of modern information and communication technologies (ICT), and mandates regular coordination among key state agencies to implement the designated objectives. The potential use of these technologies for conflict prevention and peacebuilding has not been, however, part of the public debates or government programs for the time being.

Yet, this absence of discussion should not be mistaken for a lack of relevance. On the contrary, it is commonly agreed amongst the political experts that emerging technologies have enormous potential to support the Azerbaijan-Armenia peace process – both now and in the post-conflict period. These tools can create vital platforms for people-to-people engagement and societal reconciliation. They can help curb the spread of hate speech, fake news, and revanchist narratives in both traditional media and social networks.

The first step is to recognize these technologies not only as tools for administrative efficiency or cybersecurity, but also as instruments for peace. Technologies such as artificial intelligence, data analytics, and digital communication platforms can be harnessed to detect early warning signs of conflict, promote inclusive dialogue, counter disinformation, and foster mutual understanding between long-divided communities.

The workshop of Partnership for Peace Consortium in Istanbul (April 2025) should not be seen as a routine academic event. It represented a starting point – a path forward for thinking differently, for building bridges across political and historical divides, and for taking concrete steps and exploring the potential of emerging technologies in this process. The promise of technology is not only in what it can do, but also in how we choose to use it. In the case of Azerbaijan and the broader South Caucasus, it offers a unique opportunity to turn innovation into reconciliation.

Armenia's Resiliency in the Age of Hybrid Threats: Leveraging Emerging Technologies for Security and Regional Stability

Gevorg Melikyan

Abstract

Armenia's geopolitical position exposes it to an intricate web of hybrid threats, ranging from military escalation to cyberattacks and disinformation campaigns. This paper examines how emerging technologies such as artificial intelligence (AI), cybersecurity tools, big data analytics, and blockchain can enhance Armenia's security and resilience against multifaceted challenges. By analysing Armenia's current capabilities, vulnerabilities, and regional dynamics, the study explores how these technologies can counter hybrid threats, strengthen defence, intelligence, and governance, and contribute to regional stability. While these advancements offer unprecedented opportunities to bolster national security, they also introduce new risks that require careful management. To address these complexities, the paper proposes actionable policy measures to effectively integrate these technologies into Armenia's national security framework, ensuring greater stability and strategic advantage in the South Caucasus.

Introduction

Armenia faces an increasingly complex security environment characterized by hybrid threats that relentlessly challenge its national resilience and exploit its vulnerabilities. These threats encompass a high likelihood of military escalation by Azerbaijan, cyberattacks disrupting critical systems, disinformation campaigns eroding public trust, economic coercion weakening national stability, cognitive warfare increasingly reliant on advanced technology, lawfare, weaponized narratives enhanced by AI and other innovations, and diplomatic efforts aimed at isolating the country.[1] State and non-

[1] https://emerging-europe.com/opinion/how-armenia-can-defend-itself-against-hybrid-warfare/.

state actors target Armenia's fragile governance, outdated technological infrastructure, and societal divisions, anticipating its collapse. Yet, Armenia's resilience – its capacity to withstand and adapt to such pressures – has yet to be fully realized, offering the potential to become its greatest asset through strategic governance, an innovative approach, and rational calculations.[2] By harnessing advanced technologies to fortify its defense and employing astute foreign policy to counter these threats, Armenia has the need to transform its exposed position into a demonstration of enduring strength. Central to this resilience is the strategic deployment of emerging technologies, including AI, cybersecurity mechanisms, big data analytics, and blockchain applications.

This article explores these challenges and opportunities through the following sections: (1) *Understanding Hybrid Threats in Armenia's Context*, which examines the nature and scope of hybrid threats facing Armenia; (2) *Armenia's Current Capabilities and Vulnerabilities*, which assesses the nation's strengths and weaknesses in confronting these threats; (3) *Emerging Technologies as Force Multipliers*, which explores how Al, cybersecurity, and other innovations can enhance Armenia's resilience; (4) *Regional Stability and Armenia's Role*, which analyzes Armenia's position in the broader geopolitical landscape; and (5) *Policy Recommendations*, which offers actionable strategies to bolster Armenia's defense and stability.

Understanding Hybrid Threats in Armenia's Context

Hybrid threats represent a fusion of conventional and unconventional tactics designed to destabilize a target state without escalating into full-scale war. For Armenia, these threats manifest across multiple domains, each exploiting specific weaknesses. The persistent risk of military escalation from Azerbaijan, bolstered by its oil revenues and Turkish and Russian support, remains a primary concern, as evidenced by the 2020 Nagorno-Karabakh war and subsequent border skirmishes.[3] Armenia's heavy structural dependence

---

2 Abrahamyan, E. & Melikyan, G, 2025. A New Comprehensive Security System Concept for the Republic of Armenia: Obstacles, Opportunities, Strategy. [Unpublished manuscript].

3 https://www.rand.org/pubs/commentary/2024/03/the-us-cant-guarantee-armenias-security-despite-azerbaijans.html.

on Russia is another major source of threats and vulnerability.[4] Simultaneously, Armenia's critical infrastructure – such as its energy grids and government systems – faces vulnerabilities to cyberattacks, potentially orchestrated by hostile neighbors or their proxies. Disinformation and cognitive warfare further complicate the landscape, with Azerbaijan and Russia employing weaponized narratives to exploit historical grievances and sow division, increasingly amplified by AI-driven tools.[5] Economic coercion, including blockades by Azerbaijan and Türkiye and Armenia's dependence on Russian hydrocarbons, undermines its economic stability.[6] Additionally, diplomatic efforts to isolate Armenia in regional forums exacerbate its geopolitical fragility.[7] These threats collectively target Armenia's structural weaknesses – limited resources, outdated technology, and societal cohesion.

Armenia's Current Capabilities and Vulnerabilities

Armenia's resilience is rooted in a combination of historical adaptability and contemporary challenges. The country benefits from a strong diaspora, a tech-savvy youth population, and a growing renewable energy sector, which provide a foundation for potential growth. The domestic events of 2018 showcased societal cohesion and a capacity for reform, signaling Armenia's ability to mobilize in times of crisis. However, significant vulnerabilities persist. Governance inefficiencies, a military budget of $1.7 billion in 2025 compared to Azerbaijan's $3.9 billion,[8] societal polarizations,[9] and aging infrastructure[10] constrain Armenia's ability to respond effectively to imminent security threats.

Despite the presence of a number of organisms specifically dealing with digital threats and cyberspace issues such as Armenia's MoD's specialized

4 https://rcds.am/en/armenia-s-structural-dependence-on-russia-trade-energy-security.html.
5 https://www.researchgate.net/pzblication/390192011_Cognitive_Warfare_and_Cybersecurity_Strategic_Implications_for_Global_Security.
6 https://www.iea.org/reports/armenia-2022.
7 https://countercurrents.org/2024/04/armenias-escape-from-isolation-lies-through-georgia/.
8 https://www.azatutyun.am/a/33136331.html.
9 https://www.euractiv.com/section/global-europe/news/armenia-grapples-with-political-polarisation/.
10 https://euneighbourseast.eu/news/publications/ebrds-armenia-country-strategy-2025-2030/#:~:text=The%20Armenia%20Country%20Strategy%2C%20developed,working%20to%20improve%20trade%20routes.

unit dedicated to cybersecurity, CyHub Armenia,[11] which operates as a private cybersecurity hub, Media Diversity Institute – Armenia, which aims to safeguard Armenia against digital threats,[12] and "Nork" social services technology and awareness center,[13] Armenia' cybersecurity framework remains significantly underdeveloped, with limited investment in advanced defenses leaving critical systems exposed. Compounding this vulnerability, Armenia has not yet adopted any law or bill regulating cybersecurity, leaving its digital landscape without a formal legal framework to enforce standards or coordinate responses to cyber threats. However, general rules concerning the processing of personal data are set out in the Republic of Armenia's (RA) Law on Protection of Personal Data, adopted in 2015, which is the main legal act regulating the sphere. In contrast, when it comes to cybersecurity, there is only a legislative project of the Law on Cybersecurity,[14] which aims to create a cyber-safe environment in information systems and critical information infrastructures used to provide vital services in Armenia,[15] but it remains non-adopted by the parliament. There is also a draft version of the Cybersecurity Strategy of the Republic of Armenia was developed by the Government of the Republic of Armenia in 2023. If adopted, the law would aim to create a cyber-safe environment in information systems and critical information infrastructures used to provide vital services in the Republic of Armenia. It would also regulate relations related to the detection of cyber incidents, their notification, prevention and resolution, monitoring, control, and cyber security audit of compliance with the requirements of this law, as well as would define the scope of the subjects who are obliged to ensure the information systems and critical information they use, cyber security of infrastructures, their continuous, uninterrupted, and safe use. There are also suggestions for making corresponding amendments to other Armenia's laws containing data protection regulations, as well as the approaches to the creation of the Cybersecurity Centre. The text of that Strategy is still under discussion.[16]

---

11 https://www.cyhub.am/.

12 https://mdi.am/en/home.

13 https://nork.am/en/about/.

14 https://www.e-draft.am/projects/6970/about.

15 https://www.dialog.am/storage/files/posts/posts_1696440980651_Armenia-Data-Protection-Cybersecurity.pdf.

16 https://www.dcaf.ch/sites/default/files/publications/documents/ArmeniaCybersecurityGovernanceAssessment.pdf.

A significant disconnect persists between Armenia's traditional conceptions of security and the transformative potential of emerging technologies, particularly AI and cybersecurity, within its strategic thinking and policy-making. Neither the National Security Strategy (2020)[17] nor the New Concept for the Transformation of the Army (2024)[18] adequately addresses the profound ways in which these technologies are reshaping the security landscape. These foundational documents lack comprehensive references to or analyses of how new technologies, such as AI, advanced cybersecurity measures or electronic warfare influence Armenia's security environment – whether by amplifying hybrid risks such as disinformation campaigns and sophisticated cyberattacks or by providing innovative tools to enhance national resilience. This analytical gap reflects a broader lag in integrating technological advancements into Armenia's security doctrine, particularly in the critical domain of cybersecurity, where the absence of a robust framework exacerbates vulnerabilities to digital incursions. This oversight limits Armenia's ability to proactively leverage these capabilities to strengthen defense and contribute to regional stability. Bridging this divide is imperative, as the absence of a forward-looking, technology-informed strategy – encompassing both AI and cybersecurity – risks perpetuating Armenia's exposure to hybrid threats in an era where adversaries increasingly weaponize such tools to undermine sovereignty and stability.

While Armenia's IT sector is burgeoning – evidenced by companies like PicsArt and Krisp demonstrating innovation – its application to national security lags behind commercial achievements. This disparity between Armenia's latent potential and its current state underscores the urgent need for technological integration to bridge these gaps.

Emerging Technologies as Force Multipliers

Emerging technologies offer Armenia a dynamic toolkit to asymmetrically counter hybrid threats, turning potential vulnerabilities into strategic leverage points. These tools – ranging from AI to quantum computing –

---

17 https://www.mfa.am/filemanager/security%20and%20defense/Armenia%202020%20National%20Security%20Strategy.pdf.

18 https://mil.am/files/lib1/CONCEPT%20TRANSFORMATION%20OF%20THE%20ARMY.pdf.

can empower Armenia to punch above its weight in a geopolitically volatile region. The key lies in not just adopting these technologies, but in tailoring them to Armenia's unique security challenges, such as its contentious borders, weaponized narratives from adversaries, lawfare, cognitive threats, and economic pressures exerted by aggressive neighbors like Azerbaijan and Russia, and to some extent, Türkiye. AI stands out as a versatile and transformative asset with far-reaching applications. Beyond its ability to enhance intelligence analysis by predicting adversary moves, AI can shift Armenia's posture from reactive to proactive. For example, machine-learning algorithms could be trained on historical data – combining military maneuvers, diplomatic rhetoric, and media patterns – to forecast hybrid threats with greater precision.[19] A number of research highlights how AI-driven platforms can monitor social media and web content to detect and debunk disinformation,[20] a tactic that could neutralize Azerbaijan's and Russia's cognitive warfare campaigns, which increasingly rely on technological sophistication.[21] Imagine an AI system that not only identifies an impending disinformation campaign but also generates counter-narratives tailored to specific demographics, deploying them across platforms like Telegram or VK (VKontakte) before the adversary's message gains traction. The process of pre-bunking in combating disinformation and malign campaigns can also be integrated[22] into the plethora of new technology. This preemptive capability could disrupt Azerbaijan's and Russia's efforts, which often target Armenia's vulnerabilities and lead to surrender.

Moreover, AI's potential in autonomous systems could revolutionize border security. Drones equipped with AI-driven facial recognition and thermal imaging could patrol Armenia's rugged terrain, distinguishing between hostile cross-border activity and incursions. A report from the Atlantic Council notes how Human Machine Teaming (HMT) systems or

---

19 https://www.iso.org/artificial-intelligence/machine-learning#:~:text=Predictive%20analytics%3A%20Machine%20learning%20algorithms,demand%20prediction%20and%20risk%20management.

20 https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1517726/full.

21 https://eng.globalaffairs.ru/articles/artificial-intelligence-and-new-threats-to-international-psychological-security/.

22 https://www.acice-asean.org/files/information%20centre%20reports/jul_24_info.pdf.

Human-robot interactions (HRI) have been used in conflict zones (e.g., Ukraine),[23] reducing reliance on overstretched human resources while providing real-time data to military command. However, adversaries, depending on the situation, could exploit similarly sophisticated technologies – such as AI-generated deepfakes impersonating Armenian leaders to sow confusion – underscoring the need for counter-AI defenses, such as anomaly detection algorithms to flag synthetic media. The dual-use nature of AI demands a delicate balance: Armenia must harness its benefits while anticipating its weaponization by others.

As mentioned, cybersecurity is another linchpin in Armenia's technological arsenal. The nation's critical infrastructure – energy grids, financial systems, and government databases – remains vulnerable to cyberattacks, a tactic Russia has honed in conflicts with Ukraine or Georgia. Azerbaijan is also on the same page with Russia launching cyberattacks against Armenia's critical infrastructures. Examples include the alleged hacking of strategically important documents from Armenia's nuclear power plant during 2020 war,[24] the hacking of governmental database,[25] including the "Mulberry Groupware" electronic document management system used for inter-departmental communication within the Armenian government[26] and civil society organizations' (CSOs) websites during the 2020 war,[27] the use of Pegasus spyware against individuals,[28] and the alleged breach of Yerevan's street CCTV network, among others.

Advanced firewalls and intrusion detection systems are table stakes, but Armenia could jump to next-generation defenses by integrating AI-based threat analysis. This can be a system that learns from every attempted breach, adapting its protocols to neutralize novel attack vectors in real time.

---

23 https://www.atlanticcouncil.org/in-depth-research-reports/report/how-modern-militaries-are-leveraging-ai/.

24 https://evnreport.com/magazine-issues/the-cyber-battlefield-is-just-as-important-armenia-s-cybersecurity/.

25 https://oc-media.org/russian-hackers-reportedly-attack-armenian-government-database/.

26 https://evnreport.com/magazine-issues/the-cyber-battlefield-is-just-as-important-armenia-s-cybersecurity/.

27 https://mdi.am/wp-content/uploads/2021/02/Digital%20security%20incidents%20against%20the%20Armenian%20Civil%20Society%20in%202019%20-%202020_Artur%20Papyan.pdf.

28 https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.

Certainly, the financial burden of such systems could strain Armenia's budget, and a lack of cybersecurity talent risks leaving these tools underutilized. One original solution might be a regional tech-sharing pact with like-minded states, such as Georgia or even India, pooling resources to build a collective cyber shield. This cooperative approach could offset costs while fostering diplomatic ties – a strategic bonus in a neighborhood dominated by hostile powers. Still, Armenia must grapple with the risk of overreliance on foreign partners, which could expose it to new vulnerabilities if alliances shift. **Big data analytics** offers Armenia a lens to pierce the fog of hybrid warfare. By synthesizing vast datasets – social media trends, satellite imagery, trade flows, and even weather patterns – Armenia could uncover hidden correlations that signal impending threats. Predictive analytics could, for instance, detect an economic coercion campaign by tracking subtle shifts in Azerbaijan's export policies or Russia's gas pricing, giving policymakers a head start to diversify supply chains or secure alternative funding. Some research and reports show the role predictive analytics can play in detecting and preventing different threats[29] and anticipate military escalations by monitoring troop movements, an increase in lethal weapons procurement and the defense spending, or economic indicators, providing early warnings to decision-makers. On the military front, analyzing drone footage alongside open-source intelligence could reveal troop buildups cloaked as "exercises", a tactic Azerbaijan has employed in the past.

The originality here lies in combining big data with Armenia's cultural and historical context. Algorithms could be tuned to recognize propaganda themes rooted in the Armenian-Azerbaijani conflict – say, references to Nagorno-Karabakh conflict or the 1915 Armenia Genocide – flagging them for rapid response. However, this approach demands robust data governance. A breach exposing citizen data to adversaries could erode public trust, while storage limitations in Armenia's modest tech infrastructure might necessitate cloud solutions – introducing yet another dependency on foreign providers. Striking this balance will test Armenia's strategic foresight. **Blockchain's** potential extends beyond economic resilience to the very fabric of governance. By securing land registries, voting records, and even military supply chains, blockchain could thwart attempts

[29] https://www.researchgate.net/publication/384018715_The_role_of_predictive_analytics_in_cybersecurity_Detecting_and_preventing_threats.

to undermine Armenia's sovereignty through corruption or sabotage. Ukraine's wartime use of blockchain for transparent aid distribution is instructive, as noted in a 2023 report about the use of Blockchain technology in Russia-Ukrainian war, which details how Ukraine managed funds during the 2022 invasion.[30] Armenia could take it further, and launch a decentralized platform for diaspora fundraising, ensuring donations reach frontline defenses without bureaucratic leakage – a powerful counter to economic strangulation by hostile neighbors. This could also bolster public confidence, a psychological edge in hybrid conflicts where morale is a battlefield.

Blockchain's energy-intensive nature and Armenia's limited digital infrastructure pose logistical hurdles. A phased rollout – starting with pilot projects in Yerevan – might mitigate this, but scaling up would require foreign investment or partnerships, potentially with blockchain hubs like Switzerland or Singapore. The strategic payoff could justify the effort: a tamper-proof system that signals to adversaries that Armenia's institutions are resilient, even under pressure. Looking further ahead, **quantum computing** could redefine Armenia's technological edge. Though still nascent, its ability to crack encryption or simulate complex systems could one day neutralize cyber threats or optimize resource allocation in real time.

Collectively, these technologies form a force multiplier only if deployed as an integrated ecosystem. AI could power cybersecurity and analytics, blockchain could secure the data they rely on, and quantum computing could future-proof the entire framework. Armenia's challenge is to prioritize based on immediate needs – border security and weaponized narratives – while laying groundwork for long-term gains. Originality lies in blending these tools with Armenia's strengths: a nimble tech sector, a mobilized diaspora, and a national ethos of survival entrenched in high resilience. Unlike bigger states, Armenia cannot outspend its rivals, but it can outsmart them by turning emerging technologies into a shield and a sword. This expanded arsenal, if wielded with precision, could elevate Armenia's capacity to deter hybrid threats, assert sovereignty, and reshape its security narrative. The stakes are

[30] https://www.elliptic.co/resources/crypto-in-conflict#:~:text=Since%20Russia's%20full%2Dscale%20invasion,to%20crypto%20pre%2Dpaid%20cards.

high, but so is the potential reward: a small nation leveraging the cutting edge to secure its place in a turbulent world.

Regional Stability and Armenia's Role

Armenia's resiliency is not a solitary pursuit; it is intricately linked to the stability of the South Caucasus, a region perpetually at risk of destabilization. Hybrid threats – ranging from disinformation campaigns to economic coercion and cyberattacks – undermine the region as a whole, often serving the interests of larger powers such as Russia and Türkiye, who exploit the ensuing disorder to maintain influence.[31] Azerbaijan, too, plays a malign role in this dynamic, leveraging its military assertiveness and energy-driven leverage to pursue territorial ambitions and projecting aggressive intentions towards Armenia, further complicating regional harmony. By harnessing advanced technologies to counter aggression, Armenia can thwart the malign intentions of adversaries, reducing their incentives to escalate tensions into full-scale military confrontations. This approach could lower the risk of broader conflict, fostering a more predictable and manageable regional environment.

The integration of cutting-edge tools like cybersecurity defenses, blockchain systems, and big data analytics may offer Armenia a dual advantage: diminishing the cost of peace and increasing that of war.[32] A technologically fortified Armenia can deter attacks by raising the price of aggression for its adversaries – be it through disrupting hybrid operations or exposing disinformation in real time – thus avoiding the devastating human and economic toll of armed conflict. Simultaneously, these innovations can streamline governance, secure supply chains, and enhance transparency, making peacekeeping efforts more efficient and less resource-intensive. For instance, blockchain could safeguard critical infrastructure against sabotage, while data-driven intelligence could preempt threats, reducing the need for costly military build-ups. This resilience could set a precedent for the South Caucasus, promoting a model of cooperation over confrontation and encouraging neighbors to adopt similar stabilizing measures.

---

31 https://www.gisreportsonline.com/r/turkey-russia-caucasus/.

32 https://williamspaniel.com/2016/03/14/does-increasing-the-costs-of-conflict-decrease-the-probability-of-war/.

Economically, a stable Armenia bolstered by technological advancements could become a magnet for Western investment, countering diplomatic isolation and diversifying its partnerships beyond traditional allies. By showcasing a robust defense against hybrid threats and a modernized economy, Armenia could appeal to European and American stakeholders, offsetting the influence of regional powers like Russia, Türkiye, and Azerbaijan, who often seek to dominate through chaos or coercion. However, Armenia must tread carefully in balancing its historical reliance on Russia with its aspirations for Western integration. Missteps in this delicate dance could embolden Azerbaijan's opportunism or provoke retaliatory measures from Moscow, risking escalation.

Policy Recommendations

To effectively integrate emerging technologies into its security framework, Armenia must pursue a comprehensive strategy that addresses both opportunities and challenges.

The first policy recommendation is to prioritize investment in technological infrastructure. The government should allocate 2–3% of its Gross Domestic Product (GDP) annually to research and development in AI, big data analytics, blockchain technology, quantum computing cybersecurity, and IT, potentially supplemented both by local and international private funds and contributions from its influential diaspora. Partnerships with NATO and EU states could facilitate training and technology transfers, accelerating Armenia's capacity-building efforts and aligning it with Western standards.

The second recommendation focuses on establishing a robust national cybersecurity framework. Armenia should create a Cyber Command within the Ministry of Defense, drawing inspiration from Estonia's, Israel's and/or Sweden's successful models, which emphasize public-private collaboration. Additionally, mandating cybersecurity standards for operators of critical infrastructure would ensure a baseline of protection across key sectors, reducing vulnerabilities to cyberattacks that could undermine the nation's functionality. Creating an advisory group under the Prime Minister's Staff to help build capabilities in emerging technologies would be a meaningful step forward. This group could also co-

operate with the legislative body to ensure direct access to legal processes and support the development of forward-looking regulatory frameworks.

The third recommendation involves harnessing artificial intelligence to counter disinformation and weaponized narratives. Armenia should develop a dedicated media monitoring unit, working in tandem with civil society organizations, to identify, debunk and pre-bunk false narratives propagated by adversaries. Complementing these efforts, the government should launch public awareness campaigns to enhance media literacy and critical thinking among citizens, empowering them to discern truth from manipulation and thereby strengthening societal resilience.

The fourth recommendation targets military resilience. Armenia should procure AI-enabled drones and counter-drone systems from allies such as France or the United States to bolster its defensive capabilities along contested borders. Concurrently, leveraging big data analytics to optimize resource allocation would maximize the efficiency of its limited military budget, ensuring that scarce resources are directed where they are most needed.

The fifth recommendation addresses economic defenses. Armenia should pilot blockchain technology for secure trade and financial transactions, reducing its reliance on vulnerable intermediaries and enhancing transparency. In parallel, diversifying energy sources through investments in solar and wind projects, guided by data-driven analytics, would mitigate the risks posed by economic coercion and external resource dependencies.

The sixth recommendation emphasizes fostering regional cooperation. Armenia should propose a South Caucasus technology al-liance, initially with Georgia and potentially expandable to include Western partners, to share intelligence and best practices for countering hybrid threats. Engaging its diaspora to amplify diplomatic efforts on the global stage would further enhance Armenia's influence and counter attempts at isolation.

The seventh recommendation is to mitigate the risks associated with these technologies. Armenia must enact comprehensive data protection laws to govern the use of AI and analytics, safeguarding citizens' privacy

and preventing misuse. Simultaneously, investing in workforce development through university partnerships with global tech hubs like Silicon Valley would ensure a steady supply of skilled professionals capable of implementing and maintaining these advanced systems.

The eighth recommendation addresses the critical gap in cybersecurity legislation. Armenia should expedite the adoption of the proposed Law on Cybersecurity and the Cybersecurity Strategy, currently stalled in parliament, to establish a legal framework that ensures a cyber-safe environment for information systems and critical infrastructures. This legislation should define clear responsibilities, enforce compliance across public and private sectors, and align with international cybersecurity standards, thereby closing the regulatory void that currently undermines national resilience.

And last but not least, to ensure a holistic approach to national security, Armenia should establish a comprehensive security system that integrates emerging technologies, human expertise, and cross-sector collaboration. This system should include a formalized private-public partnership (PPP) framework, bringing together state and non-state institutions, private tech companies, and academic institutions to co-develop and implement security solutions. Drawing on models like the US' Cybersecurity and Infrastructure Security Agency (CISA), Armenia could create a joint task force to coordinate efforts in threat detection, incident response, and technology innovation. This approach would not only enhance Armenia's ability to respond to cyber, military, economic and all other threats but also foster a resilient ecosystem capable of adapting to evolving challenges.

Conclusion

Armenia stands at a pivotal juncture where hybrid threats test its resilience, yet emerging technologies provide a pathway to enduring strength. By strategically adopting artificial intelligence, cybersecurity mechanisms, big data analytics, and blockchain, among others, Armenia can fortify its multi-faced security system, counter eminent threats and challenges, and contribute to regional stability. This transformation demands bold investment, governance reform, and international collaboration. The stakes are im-

mense: failure risks collapse under mounting pressures, while success could redefine Armenia as a resilient, technologically adept state in a volatile region, setting a precedent for others to follow.

A technologically resilient Armenia, therefore, holds transformative potential as a stabilizing force in the South Caucasus. By mitigating the incentives for malign activities from Russia, Türkiye or Azerbaijan, and by lowering the economic and strategic burdens of maintaining peace, Armenia could reshape regional dynamics in its favor. This vision hinges on strategic investments in innovation, positioning Armenia not just as a survivor of regional volatility, but as a proactive architect of a more secure and prosperous South Caucasus.

PART III: What Way Ahead: Challenges and Opportunities for Future PeaceTech in the South Caucasus

Modernizing the Observation Equipment of EU Monitors and Observers? – Challenges and Prospects

Henry Wathen

Introduction

In this paper, I explore the modernisation of observation equipment and digital tools used in unarmed civilian monitoring missions over the past decade, with a particular focus on the European Union Monitoring Mission (EUMM) in Georgia and a secondary focus on the EU Mission in Armenia (EUMA). Specifically, I analyse the implementation and effectiveness of advanced surveillance technology in conflict observation contexts, focusing on EUMM Georgia. I share brief lessons learned from the use of High-Lifted Camera Systems and vehicle-mounted mast cameras in Georgia since 2017, assessing their operational impact and effectiveness. Furthermore, I examine how the proliferation of quadcopters and other Unmanned Aerial Vehicles (UAVs) has affected the monitoring activities in EUMM Georgia's area of operations.

Looking ahead, this study explores options for future technological enhancements, including the potential integration of acoustic sensors for detecting small arms fire and radar systems for airspace monitoring and UAV tracking in European Union (EU) missions across Georgia and Armenia. Insights and experiences from the Organization for Security and Cooperation in Europe (OSCE) Special Monitoring Mission in Ukraine include the employment of Unmanned Aerial Vehicles (UAVs) as well as stationary cameras and acoustic sensors on masts-integrated in their monitoring. This analysis seeks to provide food-for-thought to EU policymakers and field practitioners on optimising observation capabilities in complex security environments influenced by recent technological advancements.

These key technological developments that, I would argue, have had the most significant impact on the operational environment for EU monitors and observers from 2015 to the present are the following: (1) the widespread availability of drones/quadcopters to all actors, and (2) the rise of

social media as a dominant force in the information sphere. The deployment of quadcopters by conflict parties, media and activists has contributed to the emergence of a more dynamic operational context, posing challenges to EU monitors and observers in the field. While national and *de facto* security actors, journalists, and activists have incorporated camera-equipped quadcopters into their arsenals,[1] EU monitors and observers continue to rely on binoculars and handheld cameras. Additionally, the prominence of social media and the resulting hyperconnectivity have increased the demand for timely updates from monitoring and observation missions. In years to come we can also expect AI to affect the operational environment of the EU missions further.

My core assumption is that EU monitors and observers deployed to the field need to have equipment with similar capabilities as the other actors in the operational environment, otherwise, they risk becoming irrelevant, instrumentalised or vulnerable targets. Technological upgrades would improve the impact and efficiency of monitors and observes, whether the emphasis is on observation/monitoring or by just being a proactive ground presence.

Another underlying assumption for this study is that the main function of the two EU missions in the South Caucasus is to prevent any unintentional escalation on the ground. Both EUMM Georgia and EUMA are unarmed

---

1 Reports of unidentified Unmanned Aerial Vehicles have since around 2017 featured regularly in the field level talks of the Incident Prevention and Response Mechanism (IPRM), where EUMM Georgia and the OSCE facilitate with participants from Georgian, Russian and *de facto* South Ossetian authorities. See European Union Monitoring Mission in Georgia. "79th Meeting under the Incident Prevention and Response Mechanism (IPRM) Held in Ergneti", *EUMM Press Release*, July 11, 2017, https://eumm.eu/en/press_and_public_information/press_releases/5938/?year=2017&month=12 and "Chorchana Checkpoint, Drones, and Cigarette Smuggling Discussed During the Meeting in Ergneti", *Sakartvelos Ambebi*, https://sakartvelosambebi.ge/en/news/chorchana-checkpoint-drones-and-cigarette-smuggling-discussed-during-the-meeting-in-ergneti, both accessed 18 March 2025. In 2019 a South Ossetian and a Georgian quadcopter collided, triggering reports in the media see; "KGB of South Ossetia, 'Quadcopter of the Prosecutor General's Office of South Ossetia Shot Down by Georgian Security Forces'", Cominf.org, https://cominf.org/en/node/1166525028 and "Georgian Vigilante Group 'Downs South Ossetian Drone'", *OC Media*, https://oc-media.org/georgian-vigilante-group-downs-south-ossetian-drone/, both accessed 18 March 2025.

civilian missions and have no means to counter any deliberate offensive actions, more than instantly alerting political decision-makers of any escalation on the ground.

As a research method, I have conducted interviews with former and current staff of EU and OSCE monitoring missions. My objective has been to explore options for modernising the equipment of EU monitors and observers in the South Caucasus and to assess both advantages and disadvantages of potential technological upgrades. Although broad and exploratory, the study does not constitute a full evaluation of the aforementioned modernisation initiated in EUMM Georgia since 2017.

While this article narrows in on the technical equipment of monitors and observers, the conclusions from my interviews and consultations aim to contribute to a larger examination by EU institutions and member states, evaluating the efficiency of our missions. I wish to add this case study to the larger discussion on how resources invested in EU's missions, such as EUMM and EUMA and the Common Security and Defense Policy (CSDP), serves EU interests. During my interviews with experienced mission managers about the equipment they had been provided with or wished to have, it became evident that the discussions would consistently broaden to encompass the administrative and organisational challenges inherent to CSDP missions.

Background, Terminology and Concepts

Terms and concepts specific to EUMM Georgia and to some extent EUMA and OSCE Special Monitoring Mission (SMM) are explained below. However, I will not attempt to define the generic terms and concepts of monitoring and observation in conflict management, instead I would recommend curious readers to study Aly Verjee of the University of Gothenburg's article "Ceasefire monitoring under fire: The OSCE, technology, and the 2022 war in Ukraine."[2]

[2] Aly Verjee, "Ceasefire Monitoring under Fire: The OSCE, Technology, and the 2022 War in Ukraine", *Global Policy* 13, no. S4 (August 2022): 78–88, accessed 15 April 2025 https://doi.org/10.1111/1758-5899.13123.

The **EU Monitoring Mission (EUMM) Georgia** was established after the conflict in 2008.[3] The EUMM monitors foremost observe the **administrative boundary lines (ABL)**[4] separating the *de facto* separatist entities Abkhazia and South Ossetia from Georgian government-controlled territory, with a mandate that stresses activities "throughout Georgia".[5] A considerable obstacle for the mission is not having access to Abkhazia and South Ossetia.

The **EU Mission in Armenia (EUMA)**[6] may at first glance seem like an operational cloning of the older EUMM Georgia but differs considerably in essence and modus operandi. While EUMM Georgia was established after the Six-Point Agreement in August 2008,[7] the EU mission in Armenia was launched to contribute towards reaching a peace agreement between Armenia and Azerbaijan.[8]

---

3 For a recent general description of EUMM Georgia and its context see; Manelle Lepoix, *EUMM Georgia following the 2022 Russian invasion of Ukraine* (Rondeli Foundation, June 2023), https://gfsis.org.ge/files/library/pdf/Eng--3529.pdf.

4 "Administrative Boundary Line" in the Georgian context refers to old Soviet internal administrative lines, which were not demarcated but reflected in land use and authority over collective farms and state enterprises. Georgian sources have for many years rather used the term "occupation line." Russian Federation and de facto authorities refer to the same line as a "state border." In other contexts, the term "Line of Control" is used to illustrate the dividing line in controlled territory in a disputed context. See; Tornike Turmanidze, *The Occupation Line – Russia's Foreign Policy Instrument Against Georgia* (Tbilisi: Georgian Foundation for Strategic and International Studies, 2017), https://gfsis.org.ge/files/library/pdf/Eng--3529.pdf and Ondrej Ditrych, *Karabakh's Twenty Years Crisis: The EU Should Do More*, Policy Paper (Prague: Institute of International Relations, May 2014), https://www.files.ethz.ch/isn/180657/PP_Ditrych_Karabakh.pdf, p. 2.

5 Council of the European Union, *Council Joint Action 2008/736/CFSP of 15 September 2008 on the European Union Monitoring Mission in Georgia, EUMM Georgia*, Official Journal of the European Union L 248, 17 September 2008, 26–31, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008E0736.

6 For a general description of EUMA and its context see; Onnik James Krikorian, "European Mission in Armenia Completes Its First Year Amid Regional Tensions", *Eurasia Daily Monitor*, Jamestown Foundation, March 11, 2024, https://jamestown.org/program/european-mission-in-armenia-completes-its-first-year-amid-regional-tensions/.

7 A comprehensive overview of the multiple signed versions of the Six-Point agreement and later agreed implementing measures is provided by the International Center on Conflict and Negotiation (ICCN). https://iccn.ge/index.php?article_id=301&clang=1. Accessed 19 March 20125.

8 Council of the European Union. "Statement Following Quadrilateral Meeting between

The **OSCE Special Monitoring Mission (SMM) in Ukraine** was established in 2014 and ceased its activities on the eve of Russia's full scale invasion of Ukraine in early 2022. A notable difference is that SMM Ukraine did have access to all the territory of Ukraine; the mission operated on both sides of the conflict divide/line of control, in contrast to the EU missions in the South Caucasus.[9]

EUMM Georgia participates in regular rounds of the **Geneva International Discussions for Security and Stability arrangements in the South Caucasus (GID)** since its launch on 15 October 2008. This format is co-chaired by UN, OSCE and EU with participation from the U.S., Russia, Georgia, as well from the *de facto* authorities of Abkhazia and South Ossetia. EUMM Georgia at each GID round (currently, three times a year) presents an overview of the security situation on the ground, reporting on any incidents since last GID session.[10]

Early in the process of GID rounds an agreement was reached to establish two **Incident Prevention and Response Mechanisms (IPRM)**, in the Abkhaz and South Ossetian contexts respectively, for security actors across the conflict divide (Georgian government, Russian Federation and the *de facto* authorities of Abkhazia or South Ossetia) to meet regularly on the operational level.[11] EUMM and the OSCE facilitate IPRM meetings in the village of Ergneti to discuss the security situation along the South Ossetian ABL. The UN has facilitated equivalent meetings for Abkhazia at the Unit-

---

President Aliyev, Prime Minister Pashinyan, President Macron, and President Michel, 6 October 2022", October 7, 2022, accessed 19 March 2025, https://www.consilium.europa.eu/en/press/press-releases/2022/10/07/statement-following-quadrilateral-meeting-between-president-aliyev-prime-minister-pashinyan-president-macron-and-president-michel-6-october-2022/.

9 See Aly Verjee, "Ceasefire Monitoring under Fire: The OSCE, Technology, and the 2022 War in Ukraine", *Global Policy* 13, no. S4 (August 2022): 78–88, https://doi.org/10.1111/1758-5899.13123.

10 The Geneva International Discussions are described in "The Caucasus Conflicts: Frozen and shelved?" Politorbis, No. 60, 2/2015. Accessed 19 March 2025. https://www.eda.admin.ch/dam/eda/mehrsprachig/documents/publications/Politorbis/Politorbis%2060_dfe.pdf.

11 European Union Monitoring Mission in Georgia. *The EUMM Monitor*, Issue No. 6, August 2018. Accessed 19 March 2025. https://www.eumm.eu/data/file/6440/The_EUMM_Monitor_issue_6_ENG.pdf.

ed Nations High Commissioner for Refugees (UNHCR) office in Gali, though such meetings have been paused since June 2018.[12]

As part of IPRMs, EUMM Georgia operates a **'hotline'** to convey early warning messages and prevent escalation between the security actors in their area of operations.[13] It is also used to identify and coordinate the release of detainees and to facilitate the transfer of Abkhaz residents to receive medical care on Georgian-government controlled territory. Despite the hotline standing out among best practices from the EU's long experience of conflict management in Georgia, EUMA does not have an equivalent function. At the time of drafting, EUMA did not communicate with Azerbaijani authorities, but shared pre-announcements of those patrols, which would be escorted by Armenian military or border guards through the Office of the EU Special Representative for the South Caucasus.[14]

Historically, a similar function of tele-liaison between Armenia and Azerbaijan has been filled by the Personal Representative of the OSCE Chairman-in-Office on the Conflict dealt with by the OSCE Minsk Conference. Ambassador Andrzej Kasprzyk[15] in that capacity from 1996 to 2021, held strong bonds and a capital of trust with both Baku and Yerevan and at times facilitated exchanges addressing occurrences similar to those defused by EUMM Georgia at the working level, such as cattle straying across the line of control/conflict divide.[16]

Method

Leveraging my own experience in EUMM Georgia (2012–2017 and 2018–2020) as well as in other EU missions in Iraq and the Western Balkans, I

---

12 Civil.ge, "Gali District de-Facto Head Says New Venue Being Prepared for Gali IPRM," December 5, 2023. Accessed 30 April 2025, https://civil.ge/archives/572459.

13 European Union Monitoring Mission in Georgia. *The EUMM Monitor*, Issue No. 3, December 2018. Accessed 19 March 2025, https://www.eumm.eu/data/file/5666/The_EUMM_Monitor_Issue_____December_____ENG.eBVExcNZkf.pdf.

14 Interview 5 March 2025 and email 26 April 2025.

15 See H.E. Ambassador Andrzej Kasprzyk, "Nagorno-Karabakh: Background and Recent Developments", guest lecture, College of Europe, Natolin, 17 January 2023, https://www.coleurope.eu/guest-lecture-nagorno-karabakh-background-and-recent-developments-he-ambassador-andrzej-kasprzyk.

16 Discussions on context 2016–2020.

was able to organize semi-structured in-depth interviews with four former and current staff of the three missions mentioned above. In addition, I consulted and corresponded with four other former mission members as well as with one career military officer and one private sector expert. My approach is one of "participatory action",[17] as I discuss ways to optimize the work of the EU missions with peers/colleagues. During these interviews we exchanged ideas on how to reach the common objective of improving the monitoring and observation tasks of EU missions. The method I employed throughout the interviews and consultations is 'reflexive', i.e. each discussion capitalises on the conclusions of the previous interviews and more topical consultations. Discussions were followed by specific questions and comments on the draft text at multiple stages.[18]

In the interviews, we discussed the operational context of EU missions in Georgia, as well as in Armenia, considering both their observation means and the political context, in order to explore options for modernisation. A central question arises, whether the primary purpose of the EU's staff in the field in Georgia and also Armenia is to be seen ("show the flag") or to see what is taking place (observe, analyse and report). Three of my discussants had insights into the operations of the former OSCE Special Monitoring Mission in Ukraine.

Assessment of Monitoring Equipment

EUMM Georgia's employment of new observation equipment in 2017 sought to partially compensate for the lack of access to Abkhazia and South Ossetia. Thus, the mission employed a **High-Lifted Camera System (HLCS) – an aerostat surveillance balloon** – for observation. It consists of a helium balloon (a.k.a. "blimp") raised from a ground station. Similar systems are employed *inter alia* by the US Border Patrol, French law enforcement and Azerbaijani security forces. In addition, EUMM Georgia employed **cameras on masts** mounted on the back of the vehicles for

[17] See for example Kindon, Sara, Rachel Pain and Mike Kesby, eds. (2007), *Participatory Action Research Approaches and Methods: Connecting people, participation and place*. Routledge, London and New York.

[18] See for example Larsson, Patrick. (2010). "Reflexive methodology: New vistas for qualitative research" (second edition), by Mats Alvesson and Kaj Sköldberg. *European Journal of Psychotherapy & Counselling*.

enhanced observation. EUMM's employment of HLCSs and masts on vehicles were a short-lived experiment, which begun in 2017, as since 2018, the use of the HLCS declined.

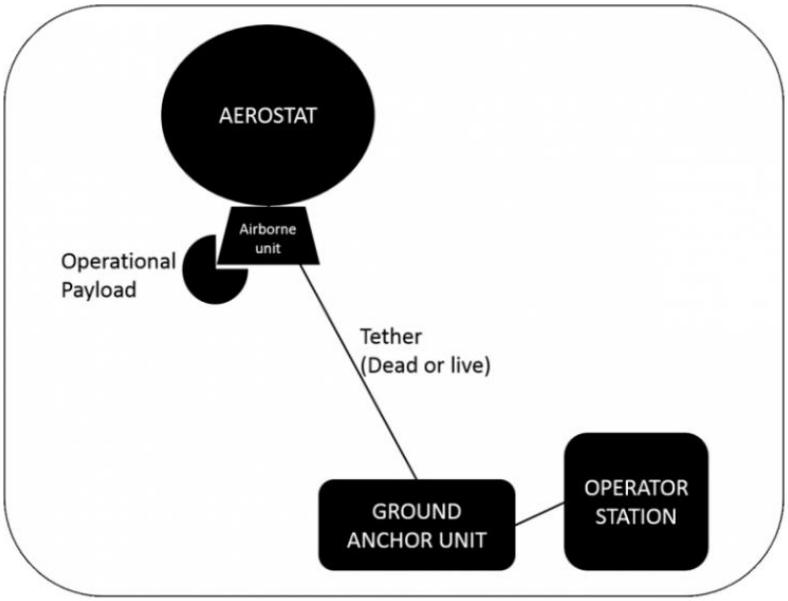

Figure 1: An aerostat system, including the balloon, aerial components, operation payload, tether and ground elements.
Diagram credit: Nir Tenenbaum[19]

Discussions with staff who were operating the systems shed light on multiple challenges. Cooperation with the commercial provider and maintenance were smooth in the beginning, but problems developed after personnel rotations in the mission. After discussing the topic with four former mission staff directly involved with the system, it appears the main challenge was to maintain the knowledge of operating the system among mission staff. Limited added value in relation to the personnel resources demanded led to the eventual decommissioning, before the HLCS ever becoming fully integrated into operations. Operations staff assessed that EUMM attempted to use the HLCS as mobile assets during limited time periods, whereas other actors (such as Azerbaijan) use them in stationary positions, only

[19] Image from "A Beginner's Guide to Aerostats", *Mongabay*, March 2016. Accessed 18 March 2025, https://news.mongabay.com/2016/03/a-beginners-guide-to-aerostats/.

pulling the aerostat/balloon down during heavy winds. In essence, the mission spent more resources (primary personnel working hours) on training staff for its use, than the added observation value, particularly with increased use of satellite imagery and open sources. Use of both the HLCS and vehicle-mounted masts were discontinued in 2020.[20]

The **EU Mission in Armenia** (EUMA) has not employed anything more than cameras and binoculars with lenses that can be carried. The EU toes a careful political line as EUMA is under a constant barrage of harsh rhetoric from Azerbaijani media outlets,[21] and Azerbaijani officials reiterate calls for its withdrawal.[22] Any bolstering of capacity would likely reduce any remaining hope for the mission to establish an interface with Azerbaijani authorities.[23]

The **OSCE Special Monitoring Mission (SMM)** in Ukraine employed a large number of technical means, including quadcopters operated by monitors, larger UAVs flown by contractors, and towers with acoustic sensors and cameras. The Mission utilised between 22 to 24 stationary **masts equipped with cameras**. These installations were strategically placed near disengagement areas, high-activity zones like the Donetsk airport, and at the five crossing points over the line of contact. The masts were highly effective for information collection, requiring a technical monitoring centre with staff working 12-hour shifts. However, setup required permission from the parties involved and areas had to be cleared of unexploded ordnance, a process lasting several months.

The SMM used **quadcopters** operated by technical monitoring teams, with each patrol hub having a team ready to respond to urgent requests. These mini-UAVs had a maximum flight time of 30 minutes and were effective despite some camera challenges. **Mid-range UAVs/drones** offered higher

---

[20] Interviews 16 February, 5, 6 and 14 March, 4 and 24 April 2025, followed by email correspondence.

[21] See for example Murad Abiyev, "The lord of binoculars: Unsettling logic of EU's reconnaissance mission", *Caliber.Az*, April 24, 2024, https://caliber.az/en/post/the-lord-of-binoculars-unsettling-logic-of-eu-s-reconnaissance-mission.

[22] Onnik James Krikorian, "Azerbaijan Seeks End to EU Mission in Armenia as Pashinyan Offers Border Compromise", *Eurasia Daily Monitor*, Jamestown Foundation, January 16, 2025, https://jamestown.org/program/azerbaijan-seeks-end-to-eu-mission-in-armenia-as-pashinyan-offers-border-compromise/.

[23] Interview 5 March 2025 followed by email correspondence.

altitude, better visibility, and superior cameras but were complex to operate, requiring additional training. The mission developed its own training programs for these drones. **Long-range UAVs**, with flight durations of 6 to 8 hours, covered the entire area up to the Russian Federation border. However, they faced significant issues like signal interference and shooting incidents, leading to the loss of three UAVs. The SMM also deployed **acoustic sensors** but did not fully operationalise them due to the complexity and cost of setting up a triangulation network.[24]

Key Points and Lessons Identified

EU procurement is slow – technological development is fast: From the establishment of EUMM Georgia in 2008 to the EU's latest establishment of missions in the field, overzealous legal safeguards and sluggish administrative processes hamper equipping EU's staff in the field with affordable modern tools. Despite the existence of methods for accelerating the acquisition process, it appears that the EU has cultivated a practice of awaiting the completion of "due process" rather than facilitating the expeditious execution of procurements. During the current long tendering processes, systems could potentially get outdated.[25]

Seconded staff are generalists – not technical specialists: The dominant mechanism for staffing EU Common Security and Defence Policy (CSDP) missions are member state secondments, primarily police or military officers, but also a number of varied civilian professionals. The EU has found this system to be an effective means of recruiting monitors, reporting officers, operations officers, managers and generalists. In situations where particular competencies or technical expertise have been required, the EU has been compelled to explore alternative approaches.[26] One option has been to contract staff directly to the mission, which burdens the budget. Consequently, since 2018, member states have made efforts to reduce the number of contracted staff and increase the share of second-

[24] Interviews 26 February and 14 March 2025, followed by email correspondence. See also Valerie Sticher and Aly Verjee, "How to Monitor a New Ceasefire in Ukraine", *ETH News*, ETH Zurich, April 24, 2025, https://ethz.ch/en/news-and-events/eth-news/news/2025/04/how-to-monitor-a-new-ceasefire-in-ukraine.html.

[25] Interviews 6 March and 4 April, topical consultation 24 April 2025.

[26] Interviews 26 February, 6 March, 4 and 20 April 2025.

ments.[27] Other examples are getting a limited time "Visiting Expert"[28] seconded by a member state. The EU also developed a concept with "Specialised Teams"[29] of experts joining forces with the missions, funded by willing member states. Specialised Teams have been deployed in EU missions in Moldova, Somalia and Palestine.[30]

Observing and collecting information vs. being seen and "showing the flag": In essence, the primary objectives of monitoring and observation missions are twofold. Firstly, they are tasked with providing accurate reporting to decision makers (or the public in the case of the OSCE SMM) from designated hotspots. Secondly, they are tasked with defusing tension through their proactive presence, thereby reducing the risk of armed escalation. It is debatable which of these two aspects takes primacy. Clearly, reports from the missions compete for the attention of readers these days with a multitude of other sources. For EU institutions and member states, the missions in the field are seldom first to report of any major new development, but rather constitute a tool for confirming or verifying the regular flow of allegations and reports from partisan sources.[31]

---

27 Interview 20 April 2025 and European Union, *Civilian CSDP Compact: Towards More Effective Civilian Missions* (Brussels: European External Action Service, May 22, 2023), https://www.eeas.europa.eu/sites/default/files/documents/2023/Civilian%20CSDP%20Compact%20Report_22.05.2023.pdf, p. 4 and 25.

28 Council of the European Union, *Draft Guidelines on the Use of "Visiting Experts" in the Context of Civilian CSDP Missions*, 8551/12, Brussels, 4 April 2012, https://data.consilium.europa.eu/doc/document/ST-8551-2012-INIT/en/pdf.

29 Council of the European Union, *Concept of the Use of "Specialised Teams" in Civilian CSDP Missions*, 11992/19, Brussels, 6 September 2019, https://data.consilium.europa.eu/doc/document/ST-11992-2019-INIT/en/pdf.

30 See for example Delegation of the European Union to the Republic of Moldova, "Newsletter of the Delegation of the European Union to the Republic of Moldova: April-June 2024" (April-June 2024), https://eu4moldova.eu/wp-content/uploads/2024/07/Newsletter-of-the-Delegation-of-the-European-Union-to-the-Republic-of-Moldova.pdf, p. 97, European Union. *Common Security and Defence Policy Missions and Operations: Annual Report 2022*. Luxembourg: Publications Office of the European Union, 2023. https://www.eutmsomalia.eu/wp-content/uploads/bsk-pdf-manager/2023/10/CSDP_Annual_Report_2022_2023_EN_v5-1.pdf, p. 46, and European External Action Service. "EUBAM Rafah: Statement by the Spokesperson on the Redeployment of the Mission at the Rafah Crossing Point." EEAS, January 31, 2025. https://south.euneighbours.eu/news/eubam-rafah-statement-by-the-spokesperson-on-the-redeployment-of-the-mission-at-the-rafah-crossing-point/.

31 In another study I have compiled insights on how staff in EU institutions and member

As for the aspect of field presence, other conflict zones such as Kosovo have been crowded with international actors, but EUMM Georgia since 2009 and EUMA since its inception are uniquely poised. The closest to complementary presences are those of the Russian Federation, to which EUMM Georgia has a mirroring role (each actor patrolling on their respective side of the ABL), and EUMA has since its inception operated through a somewhat awkward cohabitation with Russian security actors in Armenia.

The main conclusions from the interviews are that both, providing factual reporting as well as showing presence, are essential, and their importance varies over time on a case-to-case basis. Weighing the significance of observing versus being seen, both EUMM Georgia and EUMA's field presence as international monitoring/observing actors is unique. However, the missions' reporting faces intense competition for attention in the information sphere. In summary, prioritisation between providing information and showing presence deserves careful consideration before embarking on any technical upgrading that is costly in resources or carries any political risk. Interviewees/discussants with experience in both EUMM and EUMA, conveyed perceptions that presence was, in general, more important for "Brussels" than reporting. These perceptions may offer a partial explanation for the absence of any substantial technical upgrading of either EU mission. At the time of drafting, the prospect of such upgrading does not appear to have been considered.[32] Admittedly, the series of consultations supporting this study involved correspondence with only one interlocutor with EU institutions at the Brussel's headquarters. Furthermore, it does not take into account the perspective of member-state diplomats, thus precluding a strategic overview of the objectives of these CSDP missions.

Recommendations and Options to Consider

The modernisation of observation equipment in EU and OSCE monitoring and observation missions has achieved varying degrees of success. While technological advancements like UAVs and sophisticated software systems

state capitals view the reporting from the field. See Henry Wathen, "Lessons Learned for EU Reporting from Field Missions", Academia.edu, 2024, https://www.academia.edu/128719188/Lessons_Learned_for_EU_Reporting_from_Field_Missions.

32 Interviews 5 and 14 March 2025.

offer enhanced capabilities, challenges persist – such as equipment suitability, maintenance, and operational integration. Future efforts should focus on ensuring equipment compatibility with the operational environment and improving systems for data management, geolocation and analysis.

Stay out of the air – no drones or aerostats: For the primary reason that people in conflict zones fear quadcopters, EUMM Georgia and EUMA should not deploy any low-altitude drones. Secondly, as both missions face suspicion and disinformation, deployment of any air asset may be misconstrued. The political risks currently, outweigh any operational advantage of data/observations from drones/quadcopters. Further ahead, one can imagine a future where the general public is so used to drones/UAVs that additional ones from EU missions would not cause any adverse reaction. The first type of drones to employ could be tethered, i.e. secured to the controlling station with a cable, thus minimising risks of the craft going astray.[33]

Equipment and specialists as member state contributions? In the horizon, acoustic sensors present a viable option for monitoring and observation missions, particularly in environments such as the Armenia-Azerbaijan state border or along the ABLs in Georgia and the vicinity of Tskhinvali, South Ossetia.[34] The latter area frequently experiences noise disturbances due to the presence of an active training range in Dzartsemi, with regular artillery live fire drills.[35] This factor must be taken into account when considering the deployment of acoustic sensors. However, current software can easily differentiate gunshots from artillery. Additionally, the program has the capacity to differentiate automatically if the location of the artillery is at the training range.

Consequently, the system could be calibrated to react primarily to small arms fire – the likely factor in any potential unintentional escalation – pinpoint the location and alert the mission to both dispatch a patrol to the area and swiftly alert decision-makers of a potential escalation. A challenge to

---

33 Interviews 26 February and 6 March 2025.

34 Interview 5 March 2025.

35 See for example Ministry of Defence of the Russian Federation, "Bulletin of the Centre for Reconciliation of Opposing Sides and Refugee Migration Monitoring in the Syrian Arab Republic", accessed April 25, 2025, https://syria.mil.ru/en/syria/bulletins/bulletin/more.htm?id=12054798@egNews.

consider is the potential interference from hunting rifles.[36] However, envisioned sensors could be tactically placed in areas where hunting activities are minimal or non-existent. In addition, both EUMM Georgia and EUMA are well aware of all fixed positions of security actors in their respective areas of operations that are the primary risk zones for incidents involving small arms.

In a not-so-distant future, missions could employ a series of masts with acoustic sensors, as well as a number of complementary vehicle-mounted sensors – adding mobility and a temporary recourse should the mast mounted acoustic sensors malfunction or get destroyed. Considering the 'Game of Drones' affecting the operational context, radars for UAV tracking can be borrowed from a member-state's military or law enforcement agency. A team of trained operators could be re-hatted and integrated with a mission thus, adding this capability without exerting pressure on the mission budget or staffing levels.[37]

As mentioned above, EU missions struggle with long and cumbersome procurement processes as well with high staff turnover, advanced equipment and specially trained operators are best provided by one or more member-states, perhaps as a 'Specialised Team'[38] integrating with the missions on the ground. As member state priorities are diverse, such a flexible approach allows particular member states with more vested interests in a certain geographical area to contribute more within the framework of the

---

36 See for example the reported detention on 27 February 2021 in "Abduction, arrest and detention near occupation line South Ossetia", Occupied Eastwatch, accessed April 25, 2025, https://occupied.eastwatch.eu/south-ossetia/abduction-arrest-and-detention-south-ossetia/.

37 A system such as the latest low altitude radar the US Marine Corps acquisition can track quadcopters in a radius of 100km. However, the costs of such a system renders them currently improbable to be fielded in a monitoring and observation mission, given that member-states are prioritising national defence and support to Ukraine. See John Keller, "Northrop Grumman to Build 14 New G/ATOR Multi-Role Radar Systems to Protect Marines from Unmanned Aircraft", *Military & Aerospace Electronics*, April 11, 2024, https://www.militaryaerospace.com/sensors/article/14300920/radar-multi-role-unmanned.

38 Council of the European Union. "Concept of the Use of 'Specialised Teams' in Civilian CSDP Missions", Brussels, September 4, 2019, accessed 19 March 2025, https://data.consilium.europa.eu/doc/document/ST-11992-2019-INIT/en/pdf.

EU's broader efforts. However, deploying Specialised Teams always requires considerable administrative and managerial efforts on part of the hosting mission.[39] A careful assessment of added value versus invested resources is always paramount.

Rethink procurement: Acquiring advanced equipment through a direct member state contribution may stand out as a pragmatic option today. However, the need to circumvent the EU's financial and procurement regulations illustrate an institutional challenge that needs to be addressed rather than bypassed. Sluggish procurement was highlighted as the primary organisational hurdle already during the establishment and consolidation of EUMM Georgia from 2008 and onwards. The rapid launch of the mission was only possible by deploying a diverse mix of member state contributed teams and equipment. While attempts to address the issues have been made, member-states need to endorse bold reform of the EU's procurement rules in order to keep up with the developments in the field of technology as well as the operational needs of a fast-changing world. Consider shifting authority for the missions' procurement from Brussels to the principals in the field – delegated authority instead of central bureaucratic control.[40] Other best practices could be borrowed from NATO, as well as the OSCE whose procurement regulations mirror those of the former.[41] My informed interlocutors express the need for a change of paradigm and organisational culture in the EU. Acknowledging that handling a budget will always require a certain degree of safety-rails, the EU should at least aim at levelling-up to the efficiency achieved by other multilateral organisations.

---

39 Correspondence/comments on draft text 20 April 2025.

40 Henry Wathen, "Crisis is the New Normal: Adapting EU's Security and Defence Instruments", *Säkerhetsrådet* (Frivärld), April 15, 2024, accessed 19 March 2025 https://frivarld.se/sakerhetsradet/crisis-is-the-new-normal-adapting-eus-security-and-defence-instruments/.

41 Topical consultation 24 April 2025. See also; NATO International Staff, *NATO IS Procurement Manual*, EM(2010)0285-REV1 (Brussels: NATO, 2010), https://www.iddportugal.pt/wp-content/uploads/2015/12/EM20100285-REV1-NATO-IS-Procurement-Manual.pdf and Organization for Security and Co-operation in Europe (OSCE), "Key Procurement Documents", OSCE Procurement, accessed April 25, 2025, https://procurement.osce.org/key-procurement-documents both accessed 25 April 2025.

Reinforce EU Satellite Center[42] and develop an AI "Monitoring Agent": The most pertinent area of emerging technology identified in this study, is software development. Minor resources invested on the central level could be a force multiplier for all missions in the field. The EU should develop a dedicated AI agent to process a number of different types of data/observations, primarily from our own assets and our (security actor) partners, as well as from social media and, for example, websites tracking aircraft like flightradar24. The management of this AI agent should be centralised, for instance at the EU Satellite Centre, whilst maintaining dashboard interfaces at the EU Situation Centre in Brussels and at mission headquarters. Furthermore, the envisioned AI agent should be able to export data (reports) to Geographical Information System (GIS) applications.

The envisioned AI agent would provide a data processing tool both for the purpose of prompt reaction – activating the hotline in case of EUMM Georgia – and for the purpose of notifying key stakeholders in order to prevent an unintended escalation. In addition, the data analysis provides means for following up incidents, at both the field level meetings of the Incident Prevention and Response Mechanisms as well as the Geneva International Discussions for Security and Stability Arrangements in the South Caucasus – where, as mentioned, EUMM Georgia three times a year shares an update of the security situation on the ground.

Consequently, my primary recommendation is for member-states to ensure that the EU Satellite Centre has the resources to stay abreast with today's rapid technological developments. The second recommendation is to ensure that the missions have the skills and resources to capitalise on the support available from the EU Satellite Centre. The advantages of satellite imagery – an "eye in the sky" – far outweighs the images EUMM Georgia could produce with its aerostats/HLCS and vehicle mounted masts. Moreover, satellites are not seen as intrusive or provocative.

---

[42] The European Union Satellite Centre (EU SatCen) is an EU agency that supports the EU's crisis management missions and operations. It provides products and services, including satellite and aerial imagery. SatCen is headquartered in the Torrejón Air Base, in the vicinity of Madrid. European Union Satellite Centre. Accessed 19 March 2025, https://www.satcen.europa.eu/.

Concluding Remarks

By focusing on the recommendations above (staying out of the air for now, but bolstering satellite monitoring and developing use of AI for processing observations), monitoring and observation missions can enhance their capabilities without exacerbating the risks of public concern and operational interference. In today's hyperconnected and data-saturated operational context, EU Satellite Centre can be expected to have increasing volumes of data to process – with or without the specific proposals in this paper. Consequently, ensuring that this key agency has adequate staffing and resources seems increasingly important.

As digital images and videos take an ever-expanding place in public discourse and diplomacy, EU monitors and observers should have the training and tools for digital analysis – to geolocate imagery and to debunk fakes with confidence and credibility. Admittedly, staff in the mission have received some training over the years and exposure to modern tools and open-source techniques. EUMM Georgia has for many years successfully fused their own patrol observations, with various media reports and satellite imagery – such operational progress attracts the attention of principals and decision-makers.

Another area the EU has stressed as a priority is to harmonise cooperation between its various instruments and tools, achieving a so-called 'Integrated Approach.'[43] Progress made here for EUMM went beyond routine cooperation with the EU Delegation in Georgia and the EU Special Representative for the crisis in Georgia, as it came to entail cooperation with the EU's "East StratCom Task Force" in strategic communications, i.e. countering disinformation.[44] Beyond synergies among EU instruments, EU's Service for Foreign Policy Instruments (FPI) also funded satellite imagery support for SMM Ukraine.[45]

---

[43] Council of the European Union, *Council Conclusions on the Integrated Approach to External Conflicts and Crises*, 5413/18, Brussels, 22 January 2018, accessed 25 Apr. 2025 https://data.consilium.europa.eu/doc/document/ST-5413-2018-INIT/en/pdf.

[44] See for example EUvsDisinfo, "Georgian armed groups are using EUMM as an element that can provoke Tskhinval to inadequate behaviour", EUvsDisinfo, accessed April 25, 2025, accessed 25 April 2025, https://euvsdisinfo.eu/report/georgian-armed-groups-are-using-eumm-as-an-element-that-can-provoke-tskhinval-to-inadequate-behaviour/.

[45] European Commission, "Security Union: Commission Reports on Progress Made

In contrast to the subjects currently in vogue of open sources utilisation and satellite imagery, as well as the promotion of an Integrated Approach in operations, the systemic challenges in the domain of mission support do not receive adequate attention. The primary focus of my interviews and consultations on equipment. However, a pattern clearly emerged, indicating that the areas with the most room for improvement remain in the spheres of administration, finance, human resources (maintaining institutional memory/knowledge management) and procurement, as highlighted above. The most important factor in keeping up with modernisation may not lie in the equipment itself, but rather in the processes of day-to-day operations in EU institutions, as well as on the adoption of a comprehensive Integrated Approach at the headquarters level.

under the European Agenda on Security and on Countering Illegal Content Online", press release, March 13, 2017, accessed 25 April 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_17_729.

Armenian Foreign Policy in 2025 and Perspectives on Armenia-Azerbaijan Negotiations and Armenia-Türkiye Normalization Process[1]

Benyamin Poghosyan

In recent years, Armenia's foreign policy has undergone significant changes in response to the transformation of the global order from a unipolar world to a more complex, multipolar era and a shift in the regional balance of power.

The war between Russia and Ukraine, Azerbaijan's military takeover of Nagorno-Karabakh in September 2023, its incursions into Armenia proper and its continued promotion of concepts such as the so-called "Zangezur Corridor" and "Western Azerbaijan" have profoundly altered Armenia's security environment.

As the military balance has continued to favour Azerbaijan, and existing security guarantees based on bilateral Russia-Armenia agreements and Armenia's membership in the Collective Security Treaty Organization (CSTO) have proved ineffective, in 2022 Armenia developed a new foreign policy strategy based on two pillars:

1. **Foreign policy diversification** that aims to build and deepen diplomatic and military cooperation with both new and existing partners, notably India, France, the European Union, and the United States;

[1] Parts of this publication have already been published in the following publications – APRI Armenia, "Armenia and Azerbaijan Agreed on a Draft Peace Agreement: What Comes Next?", March 19, 2025: https://apri.institute/armenia-and-azerbaijan-agreed-on-a-draft-peace-agreement-what-comes-next/; Benyamin Poghosyan, *Armenian Foreign Policy in 2025: The Return of Geography*, Rondeli Foundation Expert Opinion 209, 2025: https://gfsis.org/wp-content/uploads/2025/03/229-expert-opinion-eng.pdf; Rusif Huseynov, Benyamin Poghosyan, and Hugo von Essen, *How Close Is Peace between Armenia and Azerbaijan?*, Stockholm Centre for Eastern European Studies (SCEEUS) Guest Report, April 17, 2025: https://sceeus.se/en/publications/how-close-is-peace-between-armenia-and-azerbaijan/.

2. Pursuing a **"peace agenda"** to normalise relations with Türkiye and Azerbaijan.

Foreign policy diversification was partly driven by the assumption that, given its military setbacks in Ukraine, Russia would be weakened and lose its capacity to continue exerting significant influence in the South Caucasus. Another underlying assumption was that enhanced engagement with the West could serve as a stronger deterrent against further Azerbaijani aggression and help ensure the security of Nagorno-Karabakh's Armenian population.

The "peace agenda" was based on the premise that accepting the post-2020 and post-September 2023 status quo would facilitate the normalising of relations with Azerbaijan and Türkiye and ensure Armenia's long-term security and prosperity.

These assumptions have not fully materialised. Despite significant efforts, Armenia entered 2025 without a peace agreement with Azerbaijan or normalisation of relations with Türkiye. Moreover, neither the United States nor the European Union was able to prevent Azerbaijan's military actions in Nagorno-Karabakh in September 2023.

Armenia-Azerbaijan Negotiations

Negotiations between Armenia and Azerbaijan are proceeding along three tracks: the signing of a peace agreement, the restoration of transport and communications links, and the delimitation and demarcation of borders.

Peace Agreement

Armenia and Azerbaijan failed to sign a peace agreement in 2024. Azerbaijan rejected[2] Armenia's offer[3] to sign a document containing 15 articles while negotiations continued to resolve remaining issues. To foster the

[2] Armenpress, "Azerbaijan Rejects Armenia's Proposal to Sign Peace Treaty Based on Agreed Provisions", September 9, 2024: https://armenpress.am/en/article/1199419.

[3] Siranush Ghazanchyan, Armenia Offers Azerbaijan to Sign a Peace Treaty Based on Already Agreed-Upon Articles –PM", Public Radio of Armenia, September 13, 2024: https://en.armradio.am/2024/09/13/armenia-offers-azerbaijan-to-sign-a-peace-treaty-based-on-already-agreed-upon-articles-pm/.

peace process, on March 13, 2025, Armenia accepted proposals by Azerbaijan on the two unresolved articles in the agreement and offered to initiate consultations on a time and venue for the signing of the agreement.[4] Azerbaijan rejected[5] this offer, arguing that an amendment to Armenia's Constitution was a prerequisite to the signing of the negotiated text and emphasising the need to formally abolish the Minsk Group and related Organization for Security and Cooperation in Europe (OSCE) structures. Following these pronouncements, Azerbaijan's Ministry of Defence issued multiple statements claiming that Armenian troops had opened fire on Azerbaijani positions, apparently seeking to create a pretext to justify a new Azerbaijani attack. These statements were refuted both by the European Union Mission in Armenia (EUMA)[6] and the Armenian Ministry of Defence.[7] Armenia's Office of the Prime Minister issued a statement[8] asserting that the Armenian Armed Forces had neither a reason nor orders to violate the ceasefire. Prime Minister Nikol Pashinyan reiterated[9] Armenia's readiness to sign the agreed text in a March 21 interview, and stated that Armenia would initiate the process of dissolving the OSCE Minsk Group. Meanwhile, Azerbaijani forces opened[10] fire on Armenian villages.

---

4 Ministry of Foreign Affairs of the Republic of Armenia, "MFA Statement", March 13, 2025:https://www.mfa.am/en/interviews-articles-and-comments/2025/03/13/mfa_statement/13114.

5 Republic of Azerbaijan Ministry of Foreign Affairs, "No. 105/25, Statement on the Conclusion of the Negotiations on the Text of the Draft Agreement on Peace and the Establishment of Interstate Relations between Azerbaijan and Armenia", March 13, 2025: https://mfa.gov.az/en/news/no10525.

6 European Union Mission in Armenia, "On 16–17 March #EUMA dispatched patrols to various locations along the AM-AZ border. The situation remains calm and quiet, with no unusual activity observed.", X, March 26, 2025: https://x.com/EUmARMENIA/status/1901385959717085355.

7 Armenpress, "Azerbaijan Again Falsely Accuses Armenia of Border Shooting", March 18, 2025: https://armenpress.am/en/article/1214692.

8 Armenpress, "Armed Forces Don't Have Reason or Order to Violate Ceasefire – Statement by Prime Minister's Office", March 18, 2025: https://armenpress.am/en/article/1214696.

9 The Prime Minister of the Republic of Armenia, "Prime Minister Nikol Pahinyan's Interview to Public TV", March 21, 2025:https://www.primeminister.am/en/interviews-and-press-conferences/item/2025/03/21/Nikol-Pashinyan-interview/.

10 Ministry of Defence of the Republic of Armenia, "Units of the Azerbaijani Armed Forces Opened Fire toward the Khnatsakh", March 31, 2025: https://www.mil.am/en/news/12696.

Restoration of Communications

Azerbaijan has demanded unrestricted passage through Armenia to Nakhichevan through the so-called "Zangezur Corridor", insisting on transit without an Armenian passport or customs control. This would effectively be an extraterritorial corridor, even though Baku already has access to Nakhichevan through Iran. Armenia has officially proposed[11] the reopening of rail connections to Azerbaijan and expressed a willingness to implement simplified control procedures, but Azerbaijan has called these suggestions irrelevant.[12]

Border Delimitation and Demarcation

In 2024, Armenia and Azerbaijan approved[13] the Border Delimitation and Demarcation Commission regulations. It has completed the demarcation of 12.7 kilometres of the border – approximately 1% of its total length – since Pashinyan announced that President Ilham Aliyev had issued an ultimatum threatening imminent military action unless Armenia withdrew from certain territories. In January 2025, both sides agreed[14] to continue the process from the northern section of the border to its southern edge. Some progress could be achieved on this track by the end of 2025. As Azerbaijan continues to occupy around 220 square kilometres of Armenian territory, the border delimitation process should logically result in the withdrawal of Azerbaijani troops and will hopefully proceed without duress.

---

11 The Prime Minister of the Republic of Armenia, "The Prime Minister's Article about Communication Routes between Armenia and Azerbaijan Published in Armenpress", March 4, 2025:https://www.primeminister.am/en/interviews-and-press-conferences/item/2025/03/04/Nikol-Pashinyan-article/.

12 Ministry of Foreign Affairs of the Republic of Azerbaijan, No: 086/25, Response by Aykhan Hajizada, Spokesperson of the Ministry of Foreign Affairs, to the local media inquiry regarding the article by Prime Minister of Armenia on communications published in Armenpress news agency, https://mfa.gov.az/en/news/no08625.

13 Ministry of Foreign Affairs of the Republic of Armenia, "Press Release", August 30, 2024: https://www.mfa.am/en/press-releases/2024/08/30/Delimitation/12775.

14 Ministry of Foreign Affairs of the Republic of Armenia, "Press Release on the Outcome of the 11th Meeting of the State Commission on the Delimitation of the State Border between Armenia and Azerbaijan", January 16, 2025: https://www.mfa.am/en/press-releases/2025/01/16/arm_az/13039.

Other Demands

Azerbaijan is demanding the establishment of "Western Azerbaijan" in Armenia. It argues that significant parts of the Republic of Armenia were historically Azerbaijani land and that Azerbaijanis travelling to Armenia should have special rights and security guarantees. Azerbaijan is also demanding that Armenia cancel arms supply contracts and return weapons already received.

What Comes Next?

Unless Azerbaijan adopts a more constructive approach to negotiations by dropping preconditions, meaningful progress on establishing peace and restoring communications is unlikely in 2025. Azerbaijan's reluctance to sign the agreed peace agreement appears to stem from its strategic interest in keeping the possibility of future military action against Armenia open. The absence of a peace agreement enables Azerbaijan's leadership to rally domestic support against "the external threat" that is supposedly Armenia. Maintaining the potential for military escalation is also aligned with Azerbaijan's broader geopolitical strategy of establishing a direct land connection to Nakhichevan and Türkiye and reinforces its vision of uniting the Turkic world.[15] In this context, Azerbaijan seeks to position itself as the key link between Türkiye and Central Asia. Given these dynamics, the primary objective of partners interested in peace and stable connectivity in the region should be to prevent a new escalation by Azerbaijan in 2025.

Armenia-Türkiye Normalisation Process

Armenia accelerated efforts to normalise relations with Türkiye in 2021,[16] recognising that reducing dependence on Russia and reshaping Armenia's security environment would be difficult without improved ties with Ankara.

---

[15] Ruslan Rehimov, "Azerbaijan's President Stresses Unity of Turkic World", AA, June 7, 2024: https://www.aa.com.tr/en/Turkey/azerbaijans-president-stresses-unity-of-turkic-world/3242657.

[16] Anu Meslumyan, "Turkey Armenia, to Appoint Envoys to Normalize Relations", Eurasianet, December 14, 2021: https://eurasianet.org/turkey-armenia-to-appoint-envoys-to-normalize-relations.

To advance this process, the Armenian government took many steps, such as opening up a debate on "Real vs Historical Armenia",[17] sending humanitarian aid to Türkiye following the 2023 earthquake, and completing the renovation of the Margara checkpoint on the Armenia-Türkiye border. The government also sought to cultivate the goodwill of the President of Türkiye, Recep Tayyip Erdoğan. Prime Minister Pashinyan attended Erdoğan's inauguration in 2023[18] and accepted his book as a gift during a meeting at the United Nations in 2024.[19]

Many analysts argue that Türkiye's strategic goal in the South Caucasus is to supplant Russia as the dominant power.[20] Normalising Armenia-Türkiye relations and reducing Armenia's reliance on Moscow would represent progress toward this objective. Despite this conjecture and Armenia's openness, Türkiye continues to insist that progress on Armenia-Türkiye relations is contingent on the signing of an Armenia-Azerbaijan peace agreement.[21]

There are various possible explanations for this. One factor might be the close personal relationship between President Aliyev and President Erdoğan, and the interests of the business circles connected with them. Another possibility is that Türkiye is not seeking to displace Russia in the South Caucasus but prefers to manage regional affairs in coordination with Moscow to avoid confrontation. Türkiye's insistence on tying Armenia-Türkiye normalisation to the Armenia-Azerbaijan peace agreement has created a diplomatic deadlock, reinforcing the status quo among the three countries.

---

17 The Prime Minister of the Republic of Armenia, "The Ideology of the Real Armenia: The Statement of the Prime Minister in Address to the Nation", February 19, 2025: https://www.primeminister.am/en/statements-and-messages/item/2025/02/19/Nikol-Pashinyan-Speech/.

18 The Prime Minister of the Republic of Armenia, The Prime Minister Attends the Inauguration Ceremony of the President of Turkey", June 3, 2023: https://www.primeminister.am/en/press-release/item/2023/06/03/Nikol-Pashinyan-ceremony-Turkey/.

19 Azatutyun, Erdogan, Pashinian Meet In New York, https://www.azatutyun.am/a/33133116.html.

20 Carnegie Endowment, https://carnegieendowment.org/posts/2023/10/how-turkiye-could-broker-peace-in-the-south-caucasus?lang=en.

21 Armenpress, "Turkey Again Says Normalization with Armenia Depends on Yereva-Baku Peace Process", November 6, 2024: https://armenpress.am/en/article/1204157.

Deepening Cooperation with Georgia and Iran

Relations with Georgia and Iran are vital for Armenia, as only these two neighbours serve as gateways to the broader world, economically and geopolitically.

Georgia provides land access to Russia and global markets via the Black Sea. At the same time, Iran ensures land access to the Middle East, Central Asia, and other regions through its Persian Gulf ports.

Iran is Armenia's only alternative natural gas supplier besides Russia today. The two countries launched a gas pipeline in 2007.[22] They established the "gas for electricity" scheme, under which Armenia imports gas from Iran and exports electricity at a ratio of 3 kilowatt-hours per cubic meter of natural gas. Armenia can also import natural gas from Iran for domestic consumption if necessary. As Armenia seeks to diversify its imports of key food staples – most of which currently come from Russia – Iran could play a role by, for example, facilitating wheat imports from Kazakhstan.

Relations with Georgia and Iran are also crucial to Armenia's participation in the Persian Gul-Black Sea Transport Corridor, which could connect Iran with Europe via Armenia, Georgia, and the Black Sea. Likewise, Armenia needs both countries' consent to be included in a potential International North-South Transport Corridor route, which aims to link India with Europe via Iran, Armenia, Georgia, and the Black Sea.

Iran and Georgia are important to Armenia not only economically but also geopolitically. Iran's firm opposition to establishing the so-called "Zangezur Corridor" or any change to regional borders has served as a key deterrent against Azerbaijan's potential use of force to invade Armenia.

Until recently, Georgia was seen as Armenia's gateway to the European Union, a market Yerevan is keen to enter, and its leading diplomatic partner in 2024. However, recent tensions in Georgia-EU relations will most likely hinder Georgia's ability to facilitate Armenia-EU political contacts. Still, Georgia's experience in navigating the shifting global order by engag-

---

[22] Azatutyun, Armenia, Iran open key gas pipeline, https://www.azatutyun.am/a/1587258.html.

ing with multiple geopolitical poles could provide valuable insights for Armenia. At the same time, Armenia's growing cooperation with the West could help Georgia narrow its differences with Western partners. Only in January 2024 did Armenia and Georgia sign a declaration on strategic partnership,[23] and much work is needed by the governments' policy and economic advisors to further substantiate the bilateral ties.

Establishing a New Modus Operandi with Russia

Russia remains one of the key forces shaping the balance of power in the South Caucasus.[24] Russia maintains its 102nd Military Base and border troops in Armenia, and remains Armenia's main economic partner. Bilateral trade grew from $2.5 billion in 2021 to $12.4 billion in 2024.[25] However, Armenia-Russia military-technical cooperation has declined significantly. By 2024, Russia accounted for less than 10% of Armenia's arms purchases.[26]

Since the start of the war between Russia and Ukraine, Moscow has concentrated much of its resources on Ukraine, reducing its ability to project power in other regions, including the South Caucasus. In the early stages of the war, Russia appeared close to defeat, bringing its regional influence to one of its lowest points since the collapse of the Russian Empire in 1917.

---

23 The Prime Minister of the Republic of Armenia, "The Strategic Partnership between Armenia and Georgia Will Open up New Opportunities for Further Deepening of Cooperation. Nikol Pashinyan", January 26, 2024: https://www.primeminister.am/en/press-release/item/2024/01/26/Nikol-Pashinyan-Session-ICEC/.

24 Giorgi Bardridze, Mahammad Mammadov, Sergei Melkonian, Murad Muradov, *Russia in the South Caucasus: Losing, Adapting, Overcoming*, SCEEUS Guest Report: https://sceeus.se/publikationer/russia-in-the-south-caucasus-losing-adapting-overcoming/.

25 ARKA News Agency, "Armenia's Foreign Trade in 2024 Exceeded $30 billion; Growth Had Been Slowing for Six Months", February 6, 2025: https://arka.am/en/news/economy/armenia-s-foreign-trade-t2024-exceeded-30-billion-growth-has-been-slowing-for-six-months/.

26 First Channel News, "Acquisition of Military Equipment from Russia Dropped from 96% to Less Than 10%: Secretary of Security Council", March 6, 2025: https://www.1lurer.am/en/2024/03/06/Acquisition-of-military-equipment-from-Russia-dropped-from-96-percent-to-less-than-10-percent-Secre/1089073.

However, recent battlefield developments and the launch of US-Russian bilateral talks[27] have signalled that conjectures around the "end of Russian presence in the South Caucasus" were premature. In this new geopolitical landscape, Armenia must establish a new modus operandi with Russia, based on several principles:

- Armenia must acknowledge that Russia has had – and is likely to continue to have – influence over the geopolitics of the South Caucasus.
- A purely adversarial approach to Armenia-Russia relations could harm Armenia's security and stability.
- Armenia should avoid unnecessary actions that could deteriorate relations with Russia. In particular, Armenian officials and Members of Parliament from the ruling party should moderate or abandon anti-Russian rhetoric.
- Armenia must prepare for a South Caucasus increasingly dominated by Russia and Türkiye, two powers with frequently competing and contradictory interests.

Exploring the Establishment of Minilateral Groupings

The current transformation of the global order is marked by the growing influence of ad hoc minilateral partnerships, while more formal multilateral organisations and alliances are in crisis. The primary multilateral institutions of the post-World War II order, such as the United Nations and the OSCE, have become largely dysfunctional due to increasing contradictions and disagreements among key members. Formal military alliances, such as the CSTO, are also facing difficulties. The CSTO failed to intervene after Azerbaijan's incursions into Armenia in 2021 and 2022, and took no effective measures to prevent military incidents between two of its member states – Tajikistan and Kyrgyzstan – in 2014,[28] 2021,[29] and 2022.[30]

---

27 US Department of State, "Secretary Rubio's Meeting with Russian Foreign Minister Lavrov", February 18, 2025: https://www.state.gov/secretary-rubios-meeting-with-russian-foreign-minister-lavrov/.

28 Joshua Kucera, "In Kyrgyzsta-Tajikistan Conflict, CSTO's Absence Is Conspicuous", Eurasianet, January 15, 2014: https://eurasianet.org/in-kyrgyzstan-tajikistan-conflict-cstos-absence-is-conspicuous.

29 BBC News, "Kyrgyzsta-Tajikistan: Images of Destruction after Border Clashes", May 2, 2021: https://www.bbc.com/news/world-asia-56963998.

Minilateral organizations, informal groupings, and military partnerships are on the rise. Notable examples include the Quadrilateral Security Dialogue (QUAD, with Australia, India, Japan, and the United States), I2U2 (India, Israel, United Arab Emirates, and the United States), and AUKUS (Australia, the United Kingdom, and the United States). As we have entered a more complex and unstable era of great-power competition, minilateral partnerships appear poised to at least partially assume the role once played by multilateral organisations and formal alliances.[31]

Armenia should note these developments and establish its strategic issue-based minilateral coalitions with like-minded countries to enhance its comprehensive power and deterrence capacity. Efforts could be made to form or strengthen economic partnerships such as Armenia-India-Iran, Armenia-Russia-Iran, Armenia-Greece-France, and Armenia-Greece-Cyprus. Armenia could also explore opportunities to involve Georgia in such initiatives, focusing on the realisation of the Persian Gul-Black Sea Transport Corridor project.

Readjusting Relations with the US and the EU, Building on the Recent Momentum

Armenia has taken significant steps to deepen its cooperation with the United States and the European Union, a strategy that APRI Armenia has termed "Western-focused diversification". Several factors motivated this approach. Given that the regional balance of power continued to favour Azerbaijan, Armenia saw closer ties with the West as a potential deterrent against further Azerbaijani aggression and as a means to facilitate normalisation with Azerbaijan and Türkiye. Another rationale behind this strategy was the belief that democratic states should prioritise cooperation with fellow democracies. Post-2018, Armenia has considered itself an aspiring

---

30 Aljazeera, "At Least 24 Killed in Clashes on Kyrgyzstan, Tajikistan Border", September 16, 2022: https://www.aljazeera.com/news/2022/9/16/kyrgyzstan-reports-heavy-fighting-with-tajikistan.

31 APRI Armenia, "APRI Armenia and ORF Collaborate on a Side Event at the 2025 Munich Security Conference", February 19, 2025: https://apri.institute/apri-armenia-and-orf-collaborate-on-a-side-event-at-the-2025-munich-security-conference/?fbclid=IwY2xjawIm3_NleHRuA2FlbQIxMAABHcvYFvD4bOqeHUKy8dsJ4u_pE3O_uPh_E0WuUUmqJEWoHMXrrIDITyHjCQ_aem_NYmov35yYceLJS6jPVPmIg.

democracy[32] and has been working toward strengthening its relations with the United States and the European Union.

There was also an expectation that the United States and the European Union would help Armenia modernise its state institutions, develop its economy, and support reforms. This Western-focused diversification led to the signing of a strategic partnership charter with the United States,[33] negotiations on a new partnership agenda with the European Union, and the renewed deployment of an EU mission along the Armenia-Azerbaijan border.

However, this approach has paved the way for more "carrots" focused on Armenia's development than "sticks" to address geopolitical risks emanating from Azerbaijan. It failed to prevent or generate a response to the forced displacement of Armenians from Nagorno-Karabakh, did not deter Azerbaijan from using the threat of force in 2024 to get a small section of the Armenia-Azerbaijan border demarcated to its liking, and has not led so far to normalisation with Azerbaijan and Türkiye.

Meanwhile, the start of direct US-Russia talks under the administration of President Donald J. Trump and rising tensions between Washington and Brussels have created a new geopolitical reality that may reduce US interest in the post-Soviet space as a theatre of competition with Russia. The European Union's deep internal struggles, the rise of right-wing political forces, and divisions among member states suggest that the EU will likely be unable to sustain involvement at the levels seen from 2022 to 2024. Consequently, in 2025, Armenia must prepare for a South Caucasus with reduced EU and US engagement.

This requires Armenia to adjust its Western-focused diversification strategy while maintaining positive momentum with the United States and the European Union. The focus should shift toward implementing the US-

[32] The Prime Minister of the Republic of Armenia, "Democracy Is the Main Brand of Armenia, and This Is Our Belief and Strategy. Nikol Pashinyan", May 31, 2023: https://www.primeminister.am/en/press-release/item/2023/05/31/Nikol-Pashinyan-Armenian-Forum-Democracy/.

[33] Armenpress, "Armenia Plans to Sign New Partnership Agenda with EU Soon", January 8, 2025: https://armenpress.am/en/article/1208982.

Armenia Strategic Partnership Charter (whose one expected action, of sending a US Customs and Border Patrol team, appears to have been postponed) and the EU-Armenia Comprehensive and Enhanced Partnership Agreement, which remains only partially implemented. The focus should be on where the EU has the strength and ability to substantially support Armenia – economic assistance, support in economic diversification, and public administration reforms – rather than on candidacy talks that complicate the already many layers of unfinished negotiations with Brussels.

Conclusion

The ongoing shifts in the global and regional order require Armenia to pursue a pragmatic foreign policy that avoids performative actions and embraces realistic, high-impact diplomacy. Armenia must continue to prepare for a South Caucasus shaped by an assertive Azerbaijan, an increasingly influential Russia and Türkiye, and diminished engagement from the United States and the European Union. The geopolitical engagement of other powers, such as Iran, France, India, Israel, and China, be it the same as or greater than in 2024, is not likely to replace the importance of the other powers.

In this era of growing regionalism and declining globalisation, Armenia should:

- Avoid further antagonising Russia,
- Intensify efforts to deepen cooperation with Iran and Georgia,
- Continue steps toward normalising relations with Azerbaijan and Türkiye,
- Prioritise establishing minilateral partnerships with like-minded partners interested in a peaceful and prosperous region.

With this approach, Armenia can better navigate shifting geopolitical realities while safeguarding its sovereignty and advancing its national interests.

PeaceTech in Practice: AI-Based Tailored Crisis Early Warning System for the South Caucasus Region

Atakan Yılmaz

Introduction

Conflict rarely erupts without warning. Long before violence breaks out, early signals – such as provocative rhetoric, disinformation, military posturing, and civic unrest – often emerge. Yet these indicators are frequently fragmented, indirect, and buried within routine political developments, making it difficult for policymakers to distinguish credible threats. This challenge contributes to what is known as strategic surprise/surprise attack, which is characterized by its unexpected occurrence in a given location and time, thereby raising concerns among policymakers.[1] In response, states, international organizations, and research institutions increasingly rely on tools like Conflict Early Warning Systems (CEWS) to detect risks and enable preventive action.

CEWS are designed to identify early signs of conflict and translate them into actionable insights for diplomacy, humanitarian preparedness, and security responses. Therefore, CEWS have become central to conflict mitigation, relying on systematic data collection and analysis.[2] Today, their effectiveness depends on integrating digital innovations – especially artificial intelligence (AI) – to keep pace with complex and fast-evolving conflict environments.

This integration, is part of a broader shift toward PeaceTech: the use of digital technologies to support conflict prevention, resolution, and recovery. Tools such as satellite monitoring, social media analytics and AI-based

1 Mark F. Cancian, 'Strategic Surprise', Avoiding Coping with Surprise in Great Power Conflicts (Center for Strategic and International Studies (CSIS), 2018), 30, https://www.jstor.org/stable/resrep22428.8.

2 Tim Sweijs and Joris Teer, 'Practices, Principles and Promises of Conflict Early Warning Systems', The Hague Centre for Strategic Studies, February 2022, 4, https://hcss.nl/wp-content/uploads/2022/02/Conflict-Early-Warning-Systems-HCSS-2022.pdf.

sentiment analysis are reshaping how conflict is detected and addressed.[3] In particular, AI-powered CEWS show promise in bridging the long-standing "warning-response gap" by delivering timely, high-resolution forecasts to inform effective interventions.[4]

One region where such innovation is urgently needed is the South Caucasus – a geopolitically sensitive area marked by unresolved territorial disputes, ethnic tensions, and great power rivalries. The prolonged Nagorno-Karabakh conflict, political polarization in Georgia and Russia's regional influence contribute to persistent instability, further aggravated by disinformation and environmental stressors like climate change.

This paper proposes that AI-based CEWS could serve as a critical PeaceTech tool for the South Caucasus. While no system can entirely prevent and predict conflict, well-designed CEWS can at least provide timely information to help mitigate the human and political costs of violence. To support this argument, this paper proceeds in three parts: first, outlining the conceptual foundations of PeaceTech and CEWS; second, assessing the strengths and limitations of AI-based early warning systems; and third, presenting a case-based analysis using event data of Integrated Crisis Early Warning System (ICEWS) data for Armenia and Azerbaijan. The paper concludes by emphasizing the potential of AI-enhanced CEWS to improve predictive capabilities and support more effective peacebuilding strategies in the region.

PeaceTech and Conflict Early Warning Systems (CEWS)

PeaceTech is widely accepted as an umbrella term for technologies – both hardware and software – developed or deployed to prevent, reduce, or transform violence and to support sustainable peace.[5] Christine

---

3 Andreas Timo Hirblinger et al., 'Digital Peacebuilding: A Framework for Critica-Reflexive Engagement', *International Studies Perspectives* 24, no. 3 (1 August 2023): 266, https://doi.org/10.1093/isp/ekac015.

4 Robert Muggah and Mark Whitlock, 'Reflections on the Evolution of Conflict Early Warning', *Stability: International Journal of Security and Development* 10, no. 1 (28 March 2022): 4, https://doi.org/10.5334/sta.857.mu.

5 Andy Carl, 'Understanding PeaceTech: A Think Piece to Support the Development of Peace Analytics', Peace Analytics Series (PeaceRep: The Peace and Conflict Resolution

Bell[6] provides a more functional definition, describing PeaceTech as the use of digital tools and innovation to enhance and extend peace-building practices. Its relevance today lies not only in the technologies themselves, but also in the expanding networks of researchers, developers, policy-makers, and peace-builders who are contributing to this growing field.[7]

Despite the increasing enthusiasm for PeaceTech in both policy and academic circles, some scholars caution against treating technology merely as a tool or an add-on to existing practices. Technologies are not simply neutral instruments serving predetermined goals; rather, they interact dynamically with peace processes, shaping how peace is defined, pursued, and experienced. Hirblinger et al. describe this as a co-constitutive relationship between peace and technology, where both evolve in tandem.[8] Glybchenko further emphasizes that PeaceTech implies a normative hierarchy – the "what" (peace) is often privileged over the "how" (technology) – but that both dimensions must be understood as interdependent and mutually influential.[9]

One of the most compelling applications of PeaceTech is the development of Conflict Early Warning Systems (CEWS). These systems draw conceptual inspiration from early warning mechanisms used in meteorology and natural disaster response – such as those designed to predict floods or hurricanes.[10] Similarly, CEWS aim to anticipate political crises by assessing risk through observable trends and event data. They monitor a broad spectrum of conflict-related activity, including protests, riots, armed clashes, targeted violence against civilians, and one-sided violence – perpetrated by both state and non-state actors for political purposes.[11] As Muggah and Whitlock emphasize, CEWS are

---

Evidence Platform, University of Edinburgh, 11 January 2024), 3, https://era.ed.ac.uk/handle/1842/42559.

6 Christine Bell, *PeaceTech: Digital Transformation to End Wars* (Cham: Springer International Publishing, 2024), 14, https://doi.org/10.1007/978-3-031-38894-1.

7 Yelyzaveta Glybchenko, 'Virtual Reality Technologies as PeaceTech: Supporting Ukraine in Practice and Research', *Journal of Peacebuilding & Development* 19, no. 1 (1 April 2024): 117, https://doi.org/10.1177/15423166231211303.

8 Hirblinger et al., 'Digital Peacebuilding', 267.

9 Glybchenko, 'Virtual Reality Technologies as PeaceTech', 118.

10 Bell, *PeaceTech*, 115.

11 Sweijs and Teer, 'Practices, Principles and Promises of Conflict Early Warning Systems', 5–6.

> first and foremost intended to identify and trigger action to reduce the onset, duration, intensity, and effects of multiple forms of political violence, from communal violence to outright war. [12]

By detecting these early indicators, CEWS serve a range of actors – including humanitarian agencies, diplomatic institutions, local communities, and military forces – by providing critical information that can inform targeted responses.[13] The core premise behind these systems is that enhanced forecasting enables better decision-making: when provided with timely, reliable insights into evolving threats, policymakers are better positioned to craft strategic responses. These may range from preventive diplomacy and civilian protection to deterrence strategies or coordinated peacekeeping interventions. In short, CEWS aim to give stakeholders time to act before crises escalate, thereby reducing harm and increasing the effectiveness of peacebuilding efforts.[14] In this way, the main goal is not only to predict the occurrence of conflict but also to provide the necessary lead time to take preventive or mitigating action.

Today, CEWS encompass a wide range of tools and platforms. For instance, the "Ushahidi"[15] platform developed in Kenya collects and visualizes citizen reports of violence in real time. Hala Systems' app "Sentry",[16] used in Syria, triangulates data from sensors, crowd-sourced reports, and flight tracking systems to provide early warnings of air raids during civil, "ViEWS",[17] a predictive tool created by the Uppsala Conflict Data Program to forecast fatalities in state-based conflict scenarios up to 36 months

---

12 Muggah and Whitlock, 'Reflections on the Evolution of Conflict Early Warning', 1.

13 Muggah and Whitlock, 'Reflections on the Evolution of Conflict Early Warning', 1–3.

14 Anna Knack, Nandita Balakrishnan, and Timothy Clancy, 'Applying AI to Strategic Warning Modelling Instability Risks and Stabilisation Factors for Intelligence and National Security', CETaS Research Reports, 27 March 2025, 7, https://cetas.turing.ac.uk/sites/default/files/2025-03/cetas-scsp_research_report_-_applying_ai_to_strategic_warning_1.pdf.

15 AK Njeru, B Malakwen, and M Lumala, 'Contribution of Social Media Platforms in Conflict Management: Case of Ushahidi Platform in Kenya', *International Academic Journal of Information Sciences and Project Management* 3, no. 2 (2018): 364–377.

16 Fabian Hofmann, 'Towards a Holistic Approach to PeaceTech Ethics', *Policy Perspectives* 13 (2025): 2.

17 Håvard Hegre et al., 'ViEWS: A Political Violence Early-Warning System', *Journal of Peace Research* 56, no. 2 (1 March 2019): 155–174, https://doi.org/10.1177/0022343319823860.

ahead. In addition to widely known public-facing tools, a diverse array of regional and international actors – including governments, international organizations, and research institutions – have developed or adopted Conflict Early Warning Systems (CEWS).[18]

Although prediction has long been a central aim of peace research and various CEWS offer significant promise, these systems continue to face notable limitations. Forecasting human behavior – particularly the outbreak and escalation of violent conflict – remains inherently complex and uncertain. As Knack et al. emphasize, no existing system can consistently and precisely predict geopolitical flash-points or fully anticipate their consequences. Issues such as randomness, dynamic political environments, and data quality continue to pose persistent challenges for conflict forecasting efforts.[19]

Nonetheless, promising advancements are emerging, particularly in AI, to strengthen early warning capabilities. With the anticipated development of artificial general intelligence (AGI), AI-powered CEWS may soon be able to significantly improve both the accuracy and speed of predictions. By integrating diverse data sources – including satellite imagery, open-source media, and mobility patterns – such systems could simulate unfolding scenarios in real time and offer tailored, strategic recommendations to decision-makers.[20]

A useful metaphor for understanding this shift comes from the world of Formula 1 racing. In high-speed motor sport, teams must constantly adapt to unpredictable developments – such as crashes or sudden weather changes – by running real-time simulations that test different strategic responses. Even when the ideal outcome is uncertain, informed decision-making based on rapid scenario modeling significantly increases the chances of success. In a similar way, CEWS enable peace-builders and policymakers to explore possible courses of action under evolving conflict conditions. Although such systems may not predict the exact timing or location of a crisis,

---

18 For more information about CEWS in practice, see: Sweijs and Teer, 'Practices, Principles and Promises of Conflict Early Warning Systems', 8.

19 Knack, Balakrishnan, and Clancy, 'Applying AI to Strategic Warning Modelling Instability Risks and Stabilisation Factors for Intelligence and National Security', 3, 19.

20 Knack, Balakrishnan, and Clancy, 3–4.

they significantly enhance preparedness and reduce the likelihood of reactive or poorly informed responses.

In this regard, AI-enhanced CEWS offer distinct advantages over traditional systems. These include real-time monitoring across diverse platforms, anomaly detection that identifies early signs of escalation, predictive modeling that simulates future conflict trajectories, and sub-national forecasting with greater geographic specificity. The value of these systems lies less in achieving perfect precision and more in providing timely, context-aware insights that support adaptive and pre-emptive decision-making. Based on this foundation, the next section turns to case study: the application of the Integrated Crisis Early Warning System (ICEWS) to the South Caucasus.

Mapping Conflict Signals: Dyadic Event Intensity Analysis in the South Caucasus

This section explores how AI-based early warning system, tailored to the region's unique geopolitical dynamics and risk patterns, could inform the design of a localized CEWS. In doing so, it offers practical insight into how PeaceTech can be operationalized to anticipate and mitigate conflict in one of the world's most complex and volatile regions.

Data as a Strategic Asset in Conflict Prediction

In today's data-driven world, information is no longer a passive by-product of policy – it has become the strategic terrain upon which geopolitical decisions are made. As The Economist famously declared, "The world's most valuable resource is no longer oil, but data".[21] This shift carries profound implications for peace-building and conflict prevention. The use of digital event datasets, enables analysts to identify patterns of rising tensions, to monitor evolving interstate dynamics, and to generate early warnings before crises escalate.

[21] The Economist, 'The World's Most Valuable Resource Is No Longer Oil, but Data', *The Economist*, 6 May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

One of the most sophisticated datasets available for this purpose is the Integrated Crisis Early Warning System (ICEWS) Coded Event Data, which provides event data capturing political interactions across time and space.[22] ICEWS operates by continuously scanning global news sources and coding political events using the Conflict and Mediation Event Observations (CAMEO) framework – recording "who-did-what" to "whom-when-where"[23] (Gerner et al., 2002). These coded events are converted into numerical intensity values reflecting quantitative interactions between political actors, making ICEWS a foundational input for AI-based CEWS.

To evaluate its applicability to the South Caucasus, this study draws on ICEWS dyadic event intensity data from 2015 to 2023, as provided via the Harvard Dataverse.[24] The analysis aims to assess how these dyadic trends reflect regional developments and explore the feasibility of using ICEWS as the foundation for a localized CEWS.

Leveraging for Real-Time Political Event Analysis in South Caucasus

The South Caucasus – comprising Armenia, Azerbaijan, and Georgia, and shaped by the involvement of regional powers like Türkiye, Russia, and Iran – has long been a hotspot of geopolitical instability. With unresolved territorial disputes, shifting alliances, and deep historical grievances, the region is both highly volatile and under-monitored in terms of predictive analytics.

A focal point of this volatility is the ongoing Armenia-Azerbaijan conflict over Nagorno-Karabakh. To assess the utility of ICEWS for early warning purposes, this study first correlates dyadic event intensity trends between these two states with key real-world developments over the past decade. Table 1 below summarizes major conflict-related events, while Figure 1: illustrates how these moments are reflected in the ICEWS dataset.

---

22 Elizabeth Boschee et al., 'ICEWS Coded Event Data' (Harvard Dataverse, 2015), https://doi.org/10.7910/DVN/28075.

23 D. J. Gerner et al., 'Conflict and Mediation Event Observations (CAMEO): A New Event Data Framework for the Analysis of Foreign Policy Interactions', 2002, https://www.semanticscholar.org/paper/Conflict-and-Mediation-Event-Observations-(CAMEO)%3A-Gerner-Abu-Jabr/775d7f7262ffb42972e5b87a245bc4b63c20396d.

24 Boschee et al., 'ICEWS Coded Event Data'.

Date	Event	Explanation
Aug-Sep 2015	Border Clashes	Deadliest spike since 1994 ceasefire
Apr 2016	Start of Four-Day War	Brief but intense escalation
Nov 2020	Ceasefire Signed	End of 2020 Nagorno-Karabakh War
Apr 2022	Brussels Peace Talks	EU-mediated normalization meeting
Sep 2022	Renewed Clashes	Major border skirmishes resume

Table 1: Timeline of Key Conflict Events between Armenia and Azerbaijan between 2015–2023

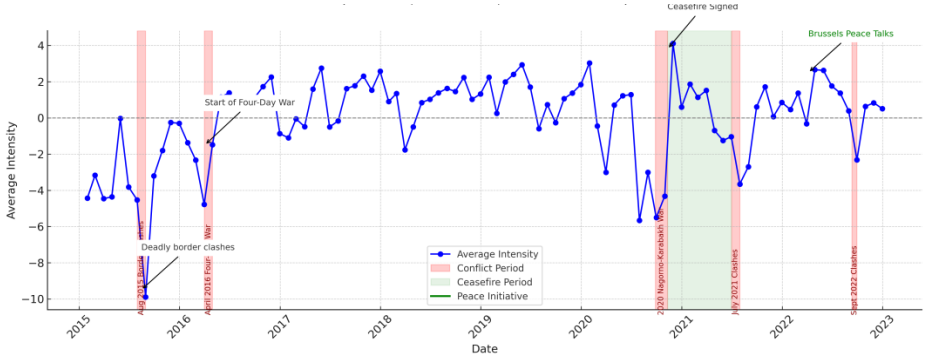

Figure 1: Monthly Average Intensity between Azerbaijan and Armenia 2015–2023 (Conflicts, Ceasefires and Peace Talks)

As illustrated in Figure 1, these dates in Table 1 correspond with pronounced negative shifts in ICEWS dyadic intensity scores – particularly in 2015, 2016, and late 2020 – suggesting that changes in the sentiment of interstate interactions often precede or accompany conflict escalation. This alignment reinforces the viability of using ICEWS as an early warning tool, particularly when integrated into an AI model trained to detect anomalies and sudden shifts.

However, focusing on a single dyadic relationship – such as Armenia and Azerbaijan – risks oversimplifying a region defined by asymmetric dependencies and multidimensional alliances. As in other regions, in the South

Caucasus, actors often maintain simultaneously cooperative and adversarial relations with multiple partners. Such patterns reinforce the importance of multi-actor monitoring for early warning systems. For example, as shown in Figure 2, while Armenia-Azerbaijan tensions escalate, Azerbaijan's relationship with Türkiye often strengthens, while Armenia-Türkiye relations deteriorate or remain tense. These intertwined dynamics highlight the importance of multi-actor monitoring for CEWS.

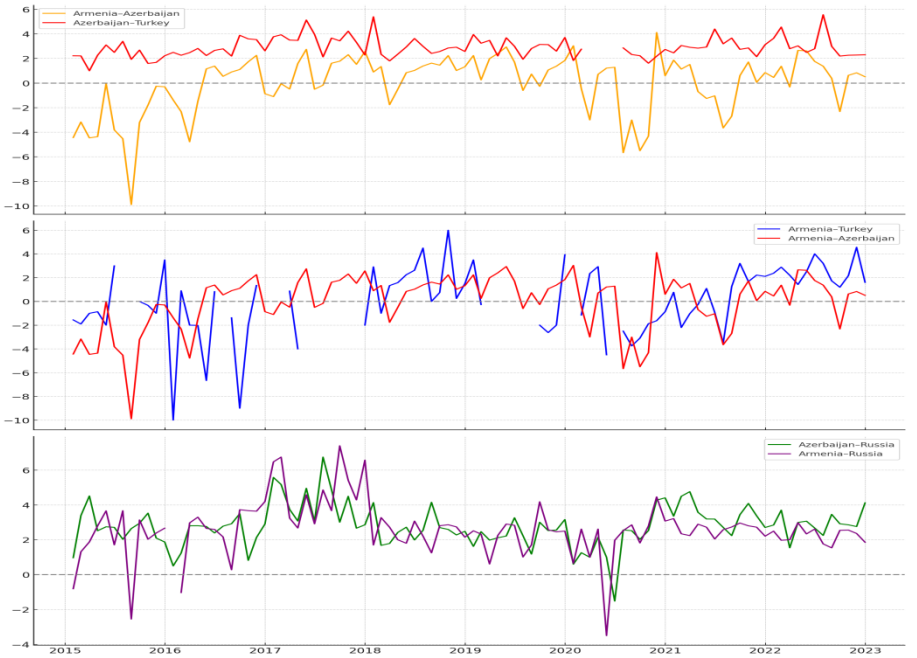

Figure 2: Dyadic Trends – Armenia-Azerbaijan, Azerbaijan-Türkiye, Armenia-Türkiye, Armenia-Russia, Azerbaijan-Russia (2015–2023)

On the other hand, the role of Russia should also be noted because Russia's role further exemplifies the multidimensional nature of regional politics in the South Caucasus. As illustrated in Figure 2, Russia's dyadic relationships with both Armenia and Azerbaijan exhibit similar patterns of fluctuation over time – rising and falling in tandem with broader geopolitical developments. These dual allegiances are not exceptions but rather defining features of the region's strategic landscape. Russia has long maintained a security alliance with Armenia, while simultaneously expanding

energy and military cooperation with Azerbaijan. This balancing act highlights the need for CEWS models that go beyond binary assessments of conflict or peace, and instead capture how third-party relationships can buffer, offset, or intensify bilateral tensions.

To capture the layered complexity of the South Caucasus, this paper emphasizes the importance of analyzing an aggregate overview of twelve bilateral relationships (dyads) among six key regional actors: Armenia (ARM), Azerbaijan (AZE), Georgia (GEO), Türkiye (TUR), Russia (RUS), and Iran (IRA). As Figure 3 presents monthly averages of event intensity scores across all dyads. This visualization clearly highlights the interdependence of regional relationships – showing that volatility in one dyad often coincides with, or even contributes to, shifts in others. Such patterns underscore the critical need for CEWS frameworks that move beyond dyad-specific analyses and instead monitor the broader network of regional dynamics. Only through this holistic, interconnected lens can early warning systems generate contextually grounded and operationally useful insights for conflict prevention and response.

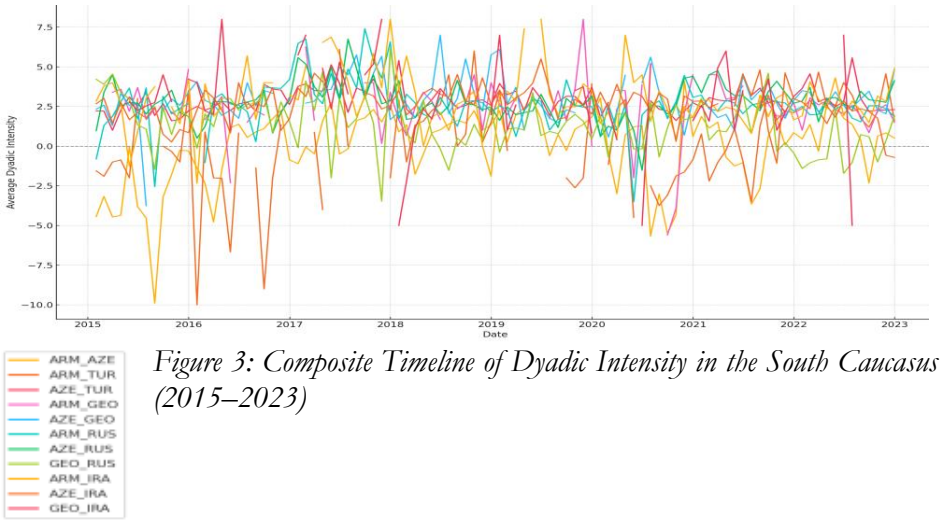

Figure 3: Composite Timeline of Dyadic Intensity in the South Caucasus (2015–2023)

Therefore, a model that incorporates the dyadic relationships among all regional states – and updates these dynamics in real time – offers significant

potential for conflict prediction. Given that datasets like Global Database of Events, Language, and Tone (GDELT)[25] update news-based event data in as little as 15-minute intervals, it is possible to track rapidly shifting interactions between states. By analyzing these live-changing dynamics, AI can detect how fluctuations in one bilateral relationship may influence the stability of others, particularly in relation to ongoing or emerging crises. Such a system could alert policymakers, NGOs, and international organizations to significant shifts, enabling them to simulate potential scenarios and identify effective preventive strategies. Where prevention is not possible, early alerts can support mitigation efforts, helping to protect civilians and reduce the impact of violence. Where conflict de-escalates, the same tools can enhance peace-building by identifying windows of opportunity for dialogue, cooperation, and reconciliation.

Conclusion

This paper aims to demonstrate that real-time analysis of dyadic event intensity – such as that enabled by ICEWS – can illuminate conflict dynamics and enhance regional situational awareness in the South Caucasus. The region's geopolitical landscape is characterized by overlapping alliances, adversarial partnerships, and interdependent relationships. As the data reveals, escalation between one pair of actors often coincides with, or triggers, shifts in other bilateral relationships. This complexity demands a CEWS that is not only AI-enabled, but also regionally adapted, context-aware, and capable of capturing multi-actor dynamics.

An AI-based CEWS designed specifically for the South Caucasus could provide valuable early alerts, simulate evolving risk scenarios, and identify windows of opportunity for conflict mitigation or peace-building. It would allow decision-makers, humanitarian actors, and civil society stakeholders to act with greater speed and strategic foresight. Furthermore, by involving local researchers and institutions in its development, such a system could promote ethical, inclusive, and sustainable peace technology. In sum, PeaceTech – when grounded in both innovation and local context – offers

[25] 'Data: Querying, Analyzing and Downloading: The GDELT Project', accessed 2 April 2025, https://www.gdeltproject.org/data.html.

a path toward more proactive, data-informed, and effective conflict prevention in the South Caucasus and beyond.

References

Bell, Christine. *PeaceTech: Digital Transformation to End Wars*. Cham: Springer International Publishing, 2024. https://doi.org/10.1007/978-3-031-38894-1.

Boschee, Elizabeth; Lautenschlager, Jennifer; O'Brien, Sean; Shellman, Steve; Starz, James and Ward, Michael. *ICEWS Coded Event Data*. Harvard Dataverse, 2015. https://doi.org/10.7910/DVN/28075.

Cancian, Mark F. *'Strategic Surprise'. Avoiding Coping with Surprise in Great Power Conflicts*. Center for Strategic and International Studies (CSIS), 2018. https://www.jstor.org/stable/resrep22428.8.

Carl, Andy. U*nderstanding PeaceTech: A Think Piece to Support the Development of Peace Analytics*. Peace Analytics Series. PeaceRep: The Peace and Conflict Resolution Evidence Platform, University of Edinburgh, 11 January 2024. https://era.ed.ac.uk/handle/1842/42559.

Data: Querying, Analyzing and Downloading: The GDELT Project. Accessed 02 April 2025. https://www.gdeltproject.org/data.html.

Gerner, D. J.; Abu-Jabr. Rajaa; Schrodt, Philip A. and Yilmaz, Ömür. C*onflict and Mediation Event Observations (CAMEO): A New Event Data Framework for the Analysis of Foreign Policy Interactions*. 2002. https://www.semanticscholar.org/paper/Conflict-and-Mediation-Event-Observations-(CAMEO)%3A-Gerner-Abu-Jabr/775d7f7262ffb42972e5b87a245bc4b63c20396d.

Glybchenko, Yelyzaveta. 'Virtual Reality Technologies as PeaceTech: Supporting Ukraine in Practice and Research'. *Journal of Peacebuilding & Development* 19, no. 1 (1 April 2024): 117–122. https://doi.org/10.1177/15423166231211303.

Hegre, Håvard; Allansson, Marie; Basedau, Matthias; Colaresi, Michael; Croicu, Mihai; Fjelde, Hanne; Hoyles, Frederick; et al. 'ViEWS: A Political Violence Early-Warning System'. *Journal of Peace Research* 56, no. 2 (1 March 2019): 155–174. https://doi.org/10.1177/0022343319823860.

Hirblinger, Andreas Timo; Hansen, Julie Marie; Hoelscher, Kristian; Kolås,

Åshild; Lidén, Kristoffer and Oliveira Martins, Bruno. 'Digital Peacebuilding: A Framework for Critical-Reflexive Engagement'. *International Studies Perspectives* 24, no. 3 (1 August 2023): 265–284. https://doi.org/10.1093/isp/ekac015.

Hofmann, Fabian. 'Towards a Holistic Approach to PeaceTech Ethics'. *Policy Perspectives* 13 (2025): 2.

Knack, Anna; Balakrishnan, Nandita and Clancy, Timothy. 'Applying AI to Strategic Warning Modelling Instability Risks and Stabilisation Factors for Intelligence and National Security'. *CETaS Research Reports*, 27 March 2025. https://cetas.turing.ac.uk/sites/default/files/2025-03/cetas-scsp_research_report_-_applying_ai_to_strategic_warning_1.pdf.

Muggah, Robert and Whitlock, Mark. 'Reflections on the Evolution of Conflict Early Warning'. *Stability: International Journal of Security and Development* 10, no. 1 (28 March 2022). https://doi.org/10.5334/sta.857.

Njeru, Abraham Kirea; Malakwen, Bernard and Lumala, Masibo. 'Contribution of Social Media Platforms in Conflict Management: Case of Ushahidi Platform in Kenya'. *International Academic Journal of Information Sciences and Project Management* 3, no. 2 (2018): 364–377.

Sweijs, Tim and Teer, Joris. P*ractices, Principles and Promises of Conflict Early Warning Systems*. The Hague Centre for Strategic Studies, February 2022. https://hcss.nl/wp-content/uploads/2022/02/Conflict-Early-Warning-Systems-HCSS-2022.pdf.

The Economist. 'The World's Most Valuable Resource Is No Longer Oil, but Data'. *The Economist*, 6 May 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Senior Advisor's Epilogue: Beware Technototalitarism

Frédéric Labarre

"If you campaign against Persia, a great empire will be lost." Thus spoke the Pythia to the King of Lydia, who promptly invaded the Achaemenid empire, and lost. Much like the Delphic Oracle of the Ancients, the reliance on technology and artificial intelligence is becoming commonplace. But whereas the Ancient Greeks lacked the necessary discernment to question the priestess' soothsaying (despite Plato and Aristotle's best efforts at fostering critical thinking among the Greeks), modern people should be intelligent enough to question whether AI technology can be trusted. After all, didn't Cleomenes, King of the Spartans, bribe the Pythia?

There is therefore ample grounds for prudence in the integration of AI technology as tools of security governance and monitoring. In principle, the idea of having AI, or AI-assisted machines support human agents in their tasks is appealing. In contexts where emotions are likely to run high, such as the challenges of finding a lasting peace between Armenia and Azerbaijan, or of reintegrating separatist territories in Georgia, or even NATO-Russia relations, mistrust will abound. The temptation to yield sensitive tasks to dispassionate and purely rational non-national machines could be blinding. There are many caveats to consider.

In September 2021, in Rome, the RSSC Study Group heard a presentation by a potential contributor to the Handbook "Understanding the Contemporary Information Landscape" which was then under production. One of the key insights from that presentation was that the task of technologists was to innovate, whereas it was the task of social scientists to draw attention to the ethical implications linked to innovation. In other words, it is not because Alfred Nobel was a callous individual that we ended up with dynamite being misused. It simply wasn't his job to care that it might be. If this is the case, then as a social scientist, I shall use these few pages to underscore the caution that should be shown in embracing technology and AI too readily in the pursuit of stability in conflict and post-conflict management, lest we wall ourselves into a technototalitarian GULag.

The ethical concerns are numerous and onerous. AI-assisted instruments appear neutral, and that makes them appealing in post-conflict contexts. However, they may not be impartial. Large Language Models (LLMs) that power AI search engines have to be taught by fallible humans. At its inception, AI (ChatGPT) leaned slightly to the left of centre politically. Three or four years hence, new LLMs have sprung up, each fed by its own community, leading to left-leaning and right-wing AI search engines. In other words, echo chambers are feeding information to bias LLMs. Similarly, expecting AI to incorporate concepts like gender-sensitivity, diversity, or inclusiveness into their algorithms seems equally hopeless. This is not because it would generate a "woke" AI search engine, but because AI does not do abstract concepts very well. Much like the Oracle, we expect LLMs to produce decisions for us, to relieve us of the effort of thinking, and from the pain of finding out the truth. But the truth sometimes resides in abstraction and ambiguity is often preferable to inconvenient facts.

For example, detecting, responding to, and curbing hate speech and disinformation content through the use of AI-assisted instruments sounds like a good idea, but what is the advantage when we know that AI models grow more biased as each week goes by? There are also the ethical and philosophical implications to consider when using AI to come up with normative solutions. When thinking and decision-making on what constitutes hate and untruth is outsourced to machines, what happens to human agency? Not only is human agency removed, but so is the possibility of freedom of speech, freedom of opinion and thought, since AI is acting as judge, jury, and executioner all in one. Indeed, AI prompts are formulated in such a way as to reveal wants and intentions. By flagging what a machine thinks (or rather has been told to think) is proscribed speech or thought, and by accepting its decision because it is convenient to hide our responsibility behind the machine's purported neutrality, we submit not to the law of the land, but to the will of the machine. We remove the need for competent courts, and we silence dissent as well as consent. In the pursuit of more perfect human rights, it is unreasonable to expect a machine to solve complex issues that have dogged diplomats and experts for decades, not because the solution would not be rational or reasonable, but because that solution would still be submitted to the passions of the people it would affect, and these people would have had no say in the outcome, either directly, or through their representatives. The use of AI technology absolves

us of responsibility for finding solutions to problems. As such, AI would not produce value-neutral solutions, because the beneficiaries of those solutions may yet disagree with the outcome. They would disagree with the outcome because they would not be mystified by the technology as the Ancient Greeks were by the Oracle. No one wants the solution to be imposed externally. There must be local ownership for stability to emerge.

To a certain extent, the unequal access to the technology – lamented by some commentators – hints at a lack of democracy, and more equal access would be harbinger of peace and stability. There is no concrete evidence of this statement, and if anything, the contrary is more likely to be true. In 1993, the Rwandan massacres were heavily facilitated by how the Rwandans were mystified by the radio – which encouraged the genocide. Unfamiliarity with technology may lead individuals to ascribe mystical powers to processes they do not comprehend. This lack of critical thinking is spread far and wide; the belief in "chemtrails" dusted by commercial airliners is one example. And this example grows in influence thanks to the internet, and its reach is multiplied by AI. In such contexts, pushing complex technology on unsuspecting populations at a moment when we ourselves do not fully grasp the implications of that innovation is imprudent and unethical.

That technology (even AI-assisted) could indeed be a capabilities-multiplier, but here too, prudence is essential. Certain physical activities in post-conflict situations could be supported by AI instruments; drone surveillance along a contact line could be carried out autonomously, with live video feed relayed to human-controlled stations. Such systems would be susceptible to hacking, and the imagery generated could be tampered with just like any other, and be used for sinister purposes. There could be a way to generate trust from conflicting parties, however. The inherent neutrality of the machinery would be one way. Another would be to commit fully to transparency. Sharing freely the product of autonomous monitoring instruments with the public (local and global) would force the parties to stick to their agreement, and to better police their own populations to avoid being seen as breaking a cease-fire or peace deal. Publish and be saved was the watchword at the beginning of the world wide web. The promise that transparency could bring peace was true only insofar as reality could not be tampered with, and could be accepted at face value, with no further interpretation. The world would be a much safer place if each country could see

and know where the neighbours' armed forces were, and their strength. In many ways, the early "neutral" aids to conflict management can be found in the GPS trackers installed on monitored nuclear warheads as part of the 1991 START treaty. Similarly, seismic sensors and passive SONARs help detect movement on land and water. Nowadays, free services like *FlightRadar24*, and similar services for maritime traffic enable the whole world to witness what is happening (even though these services can also be tricked, such as when some Ukrainian hackers made a figure of the An-224 *Mryia* appear on *FlightRadar24* well after it had been destroyed). These services are already complicating the ambitions of more authoritarian actors that put a premium on narrative control, and rely on opaque information. As was stressed during our workshop, international competition now revolves around conflicting interpretations of reality.

Doubt having been sown completely, the responsibility for outcomes has been abdicated. The use and abuse of technology, and the reliance on AI is killing critical enquiry, and with it the human ability to engage in constructive dialogue about the world, and on the crafting of solutions to social problems – what we've been calling politics for 2500 years. It is tempting to submit to the tropes that technology will enslave us all, and that some giant Terminator with an Austrian accent will machine-gun us into oblivion. Thankfully, there is already evidence that AI is reaching a plateau. LLMs rely on external feeding of information to learn. Their inability to sift through the mountain of informational chaff generated by the net means that it requires enormous amounts of energy to enable LLMs to distinguish fact from the avalanche of errors and fiction that pollute the data sphere. Several hundreds of nuclear reactors would be needed to enable an LLM to acquire even a marginal computing power improvement.

Apocalyptic scenarios may be far removed, but the march of innovation continues. In Antiquity, a clear distinction was made between the private and public spheres. Humanity in the 21st century may have missed the boat on keeping information distinct from entertainment, but there remains the opportunity to commit to keeping human affairs human, distinct from machines. A reasonable solution (one that is logical, but accounts for human passion) may appear sub-optimal, but only in comparison with the operation of a machine's pure rationality. Lest we forget, a machine's logical solution to the problem of war could be genocide. No humans, no war. We

should be wary of elevating AI technology to the rank of divinity – God has reputedly punished Man for his wickedness more than once, after all. Let us change our behaviour by ourselves instead on relying on *Deus ex Machina*.

PART IV: Policy Recommendations

Policy Recommendations

Regional Stability in the South Caucasus Study Group

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

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 Caucasus

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/Tskhin-

vali 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 grievances. 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 un-

derstanding. 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 dis-information 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.

List of Abbreviations

ABL	administrative boundary lines
AGI	artificial general intelligence
AI	artificial Intelligence
a.k.a.	also known as
APRI Armenia	Applied Policy Research Institute of Armenia
APT28	Advanced Persistent Threat 28 (hacker group of Russian GRU)
ARM	Armenia
ASAN	Azerbaijan Service and Assessment Network (ASAN Service/"Easy Service")
AUKUS	Australia, the United Kingdom, and the United States
AZE	Azerbaijan
BTC	Baku-Tbilisi-Ceyhan
CAMEO	Conflict and Mediation Event Observations
CCCTV	Closed-Circuit Television
CEWS	Conflict Early Warning Systems
CI	Critical Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CSDP	Common Security and Defence Policy
CSOs	Civil Society Organizations
CSTO	Collective Security Treaty Organization
DCAF	Geneva Centre for Security Sector Governance
DDoS	Distributed Denial-of-Service
ECtHR	European Court of Human Rights
e.g.	exempli gratia/for example
EGDI	E-Government Development Index
EU	European Union
EUMA	EU Mission in Armenia
EUMM	European Union Monitoring Mission
FPI	Foreign Policy Instruments

GDELT	Global Database of Events, Language, and Tone
GDP	Gross Domestic Product
GEO	Georgia
GID	Geneva International Discussions for Security and Stability arrangements in the South Caucasus
GIS	Geo Information System
GPS	Global Positioning System
HLCS	High-Lifted Camera System
HMT	Human Machine Teaming
HRI	Human-robot interactions
I2U2	India, Israel, United Arab Emirates, and the United States
ICEWS	Integrated Crisis Early Warning System
ICS	Industrial Control Systems
ICT	information and communication technologies
i.e.	id est/that is
IPRM	Incident Prevention and Response Mechanisms
IRA	Iran
ISPs	Internet Service Providers
IT	Information Technology
ITU	International Telecommunication Union
JTEC	Joint Training and Evaluation Centre
LAWS	lethal autonomous weapons systems
LLMs	large language models
MISP	Malware Information Sharing Platform
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organization
NIS	network and information systems
OSCE	Organization for Security and Cooperation in Europe
OSINT	Open Source Intelligence
PAI	Publicly Available Information

PfP Consortium/PfP-C	Partnership for Peace Consortium of Defense Academies and Security Studies Institutes
PPP	private-public partnership
QUAD	Quadrilateral Security Dialogue, with Australia, India, Japan, and the United States
RA	Republic of Armenia
RSSC SG	Regional Stability in the South Caucasus Study Group
RUS	Russia
SMM	Special Monitoring Mission
SNGP	Substantial NATO-Georgia Package
SONAR	Sound Navigation and Ranging
SSG	Security Sector Governance
SSG/R	Security Sector Governance and Reform
START Treaty	Strategic Arms Reduction Treaty
TUR	Türkiye
UAVs	Unmanned Aerial Vehicles
UK	United Kingdom
UN	United Nations
UNCHR	United Nations High Commissioner for Refugees
US/U.S.	United States of America
USAID	United States Agency for International Development
ViEWS	Violence & Impacts Early-Warning System
VK	VKontakte (Russian Social Media service)

List of Authors and Editors

Giorgi BADRITZE, Georgian Foundation for Strategic and International Studies, Tbilisi

Christoph BILBAN, Austrian National Defence Academy, Vienna

Andro GOTSIRIDZE, The University of Warwick, Tbilisi

Vasif HUSEYNOV, Center of Analysis of International Relations, Western Studies Department, Baku

Boris KUZNETSOV, Centre for International and Regional Policy, St. Petersburg

Frédéric LABARRE, Royal Military College of Canada, Kingston

Alexandru LAZAR, CyberPeace Institute, Geneva

Dawn LUI, Geneva Centre for Security Governance (DCAF)

Elena MANDALENAKIS, Independent Researcher and Lecturer, Heraklion

Gevorg MELIKYAN, Armenian Institute for Resilience and Statecraft, Yerevan

George Vlad NICULESCU, European Geopolitical Forum, Brussels

Benyamin POGHOSYAN, Center for Political and Economic Strategic Studies, Yerevan

Henry WATHEN, PeaceTalk, Geneva/Tbilisi

Atakan YILMAZ, Bahçeşehir University, Istanbul

Band 16 / 2025

How can digital innovation be leveraged to foster peace and prevent conflict in one of the world's most strategically sensitive regions – the South Caucasus? From algorithmic geopolitics and cyber resilience to smart infrastructure and AI-based early warning systems, this volume provides rigorous analysis and concrete recommendations. With its multidimensional insights and practical focus, it is an essential read for policymakers, security professionals, and scholars working on peace technology, regional security, and digital governance.

ISBN: 978-3-903548-23-7

29th Workshop of the PfP Consortium Study Group
"Regional Stability in the South Caucasus"