Study Guide

for

Organization for Security and Co-operation in Europe

Topic Area: Information and Communication Technology (ICT) and Artificial Intelligence in the era of geopolitical instability: the role of OSCE's strategy in conflict prevention

Table of Contents

1. Welcoming Letter

Distinguished Delegates,

It is with great pleasure that we welcome you to the Organization for Security and Co-operation in Europe (OSCE) at this year's RhodesMRC. We feel honored and excited to serve on the board of our committee. The topic of "Information and Communication Technology (ICT) and Artificial Intelligence in the era of geopolitical instability: the role of OSCE's strategy in conflict prevention" is both urgent and complex. The rapid integration of AI into military systems, the emergence of Autonomous Weapon Systems, and the proliferation of hybrid threats through digital means have altered the international security landscape. Our discussion will not be a theoretical exercise; it is a direct response for updated CBMs and a cohesive preventive strategy. In this study guide, we aim to provide you with all the relevant background information necessary to understand the complexities of electoral interference. Additionally, we encourage you to conduct your own research, as a comprehensive grasp of this issue requires exploring multiple perspectives and case studies. The bibliography and further reading sections at the end of the guide will serve as valuable starting points for your investigation.

On a special note, we kindly ask that you not only read this study guide carefully but also familiarize yourselves with the Rules of Procedure (RoP). On behalf of the Organizing Team and the Secretariat, we welcome you to RhodesMRC 2026. We look forward to witnessing your insightful debates and diplomatic initiatives!

Best regards,

Margarita Theodora VASILEIADOU, *Chairperson-in-Office*

Aliki Aikaterini KOLIOPOULOU*, Secretary General*

2. Introduction to the Committee

2.1. History of the Committee[1]

The Organization for Security and Co-operation in Europe (OSCE) traces its origins to the détente period of the early 1970s, when the Conference on Security and Co-operation in Europe (CSCE) was established as a multilateral forum for dialogue between East and West. Following two years of negotiations in Helsinki and Geneva, the participating States signed the Helsinki Final Act on 1 August 1975. With the fall of the Iron Curtain, the 1990 Paris Summit marked a turning point, transforming the CSCE into a more structured institution. The institutionalization process culminated in the 1994 Budapest Summit, where the CSCE was officially renamed the OSCE. Today, the OSCE is the world's largest regional security organization, encompassing 57 participating States from North America, Europe, and Asia.[2] However, in 2024, the Russian Federation formally suspended its participation in the Parliamentary Assembly.

2.2. Political decision-making bodies[3]

The Organization for Security and Co-operation in Europe (OSCE) operates through a network of internal bodies and institutions that support its mandate in promoting security, democracy, and human rights across its 57 participating States. These bodies focus on conflict prevention, democratic development, media freedom, and dispute resolution.[4] The OSCE's decision-making structure is organized through several key bodies that operate at different levels of political authority. At the highest level, Summits bring together the Heads of State or Government of the participating States in order to set the Organization's long-term priorities and provide strategic guidance for its future work. At the ministerial level, the Ministerial Council, composed of the Ministers for Foreign Affairs of the participating States, serves as the OSCE's highest governing body. The Permanent Council, functions as the principal regular decision-making body and oversees the

[1] OSCE, "History," www.osce.org https://www.osce.org/history
[2] OSCE, "Who We Are | OSCE," Osce.org, 2018, https://www.osce.org/who-we-are.
[3] OSCE , "Institutions and Structures," www.osce.org, n.d., https://www.osce.org/institutions-and-structures
[4] Ibid

day-to-day operational work of the Organization. In the politico-military dimension, the Forum for Security Co-operation plays a central role in strengthening military security and stability in Europe.

2.3. Mandate, Functions, and Capacities of the Simulated Body

The OSCE Ministerial Council is the central decision-making and governing body of the Organization for Security and Co-operation in Europe (OSCE). It convenes annually in the country holding the OSCE Chairmanship and serves as a platform for Foreign Ministers of participating States to discuss key security issues, review the Organization's work, and adopt new decisions and declarations.

3. Introduction to the Topic Area

The rapid diffusion of information and communication technologies (ICTs) and artificial intelligence (AI) has altered the conditions under which conflict prevention is now conceived and practised. Digital systems shape strategic competition, crisis perception, political influence, and the resilience of critical infrastructure. In this environment, risks emerge not only from conventional military action, but also from cyber operations, AI-assisted disinformation, data-driven surveillance, and the manipulation of digital dependencies across borders. For the OSCE, this transformation is especially significant because its security model has long rested on the prevention of escalation, the reduction of miscalculation, and the maintenance of stability through co-operative and rules-based mechanisms.[5] This topic therefore focuses on the intersection of several dimensions of security that the OSCE recognises as interdependent rather than separate. In the politico-military dimension, ICTs create new pathways for coercion, disruption and ambiguity, especially where attribution remains uncertain and decision-making timelines are compressed.[6] In the human dimension, AI raises questions of privacy, freedom of expression, accountability and non-discrimination. In the economic and environmental dimension, digital dependence generates vulnerabilities that can be exploited through attacks on energy grids, financial systems, transport networks and other essential services.[7]

[5] Organization for Security and Co-operation in Europe, "*Our Mandate on Conflict Prevention and Resolution.*" 2026, www.osce.org/node/660052

[6] Organization for Security and Co-operation in Europe, "Cyber/ICT Security." December 9, 2016, www.osce.org/field-of-work/Cyber-ICT-security.

[7] "Annual OSCE-Wide Conference on Cyber/ICT Security Underscores the Importance of Strengthening National Cyber Resilience." *Osce.org*, 2024, www.osce.org/chairpersonship/573043.

The OSCE's cyber/ICT-security work reflects this multidimensional logic: its participating States have agreed sixteen confidence-building measures intended to make cyber activity more predictable and to prevent misunderstandings and miscalculations, while recent OSCE-wide discussions have explicitly addressed related issues. Against this background, the present topic asks whether the OSCE's existing strategy remains adequate for an era in which generative AI, autonomous systems, hybrid threats and widening digital inequalities increasingly affect regional security.[8]

4. Key- Words and Definitions

Artificial Intelligence: AI is a technology that enables computers and machines to simulate human learning, decision making, comprehension, creativity and autonomy. It can act independently, replacing the need for human intelligence or intervention.[9]

Information and Communication Technology: ICT covers all technical means used to handle information and aid communication. This includes both computer and network hardware, as well as their software.[10]

Generative AI: GenAI is a technology that can create original text, images video and other content in response to a user's prompt or request.[11]

Deepfakes: They are AI-generated synthetic media intended to convincingly depict a person saying or doing something they never did. Many deepfakes use tactics like voice cloning, synthetic video calls, and AI-generated content to mimic the way individuals communicate.[12]

[8] Organization for Security and Co-operation in Europe (OSCE), *"Conflict Prevention and Resolution,"* accessed April 21, 2026, https://www.osce.org/field-of-work/conflict-prevention-and-resolution

[9] Cole Stryker and Eda Kavlakoglu, "What Is Artificial Intelligence (AI)?," IBM, August 9, 2024, https://www.ibm.com/think/topics/artificial-intelligence.

[10] "Glossary:Information and Communication Technology (ICT)," ec.europa.eu, n.d., https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT).

[11] Ibid

[12] proofpoint, "Deepfake Technology," Proofpoint, August 26, 2024, https://www.proofpoint.com/us/threat-reference/deepfake.

***Cyberattacks*:** It refers to an unwanted intrusion by a malicious actor into a system, device or process. It usually leads to an incident such as malware infection, e.g. ransomware, a data breach, or a scam.[13]

***Hybrid threats*:** They usually refer to coordinated harmful activities that are planned and carried out with malign intent, aiming to undermine a target, through a variety of means, including information manipulation, cyberattacks, economic coercion, political manoeuvring etc. They are used by both state and non-state actors.[14]

***Confidence-Building Measures*:** CBMs are defined as measures that address, prevent, or resolve uncertainties among states, and are designed to prevent wanted and especially unwanted escalations of hostilities and build mutual trust.[15]

Points of Contact: PoCs are usually a person, system or device that serves as a communication interface between entities in a cyber incident. They act as a hub for info exchange and coordination.[16]

Early Warning Systems: It refers to an integrated system of hazard monitoring, forecasting and prediction, that enables individuals, governments etc. to take timely action to reduce risks in advance.[17]

5. Legal Framework

The Helsinki Final Act (Decalogue of Principles)

[13] "What Are Cyberattacks - Bitdefender InfoZone," Bitdefender, 2024, https://www.bitdefender.com/en-us/business/infozone/what-is-a-cyber-attack.
[14] "Hybrid Threats," Consilium, 2019, https://www.consilium.europa.eu/en/policies/hybrid-threats/.
[15] "Confidence-Building Measures | Cross-Strait Security Initiative | CSIS," www.csis.org, n.d., https://www.csis.org/programs/international-security-program/isp-archives/asia-division/confidence-building-measures.
[16] "What Does Point of Contact Mean?," Bizmanualz, October 30, 2023, https://www.bizmanualz.com/library/what-does-point-of-contact-mean?srsltid=AfmBOopsMMubmDBu0vWOE89-JXKKJoWXQ-n_aSJ2-mbCBn1wZkG_yu-P.
[17] United Nations Office for Disaster Risk Reduction, "Early Warning System," www.undrr.org, 2024, https://www.undrr.org/terminology/early-warning-system.

The Helsinki Final Act is the outcome of a collective effort that took place during the Conference on Security and Cooperation in Europe, signed by 35 nations and adopted on 1 August 1975.[18] This agreement is considered as the cornerstone of OSCE'S function, as it established the fundamental principles guiding the relations between Member States and their commitments during the Cold War.[19] The focus area of agreement has been divided into four pillars, called "baskets": the first one includes ten principles, emphasised in political and military issues, peaceful settlement of disputes and the implementation of CBMs; the second focuses on economic issues such as but not limited to trade and scientific cooperation; the third is centralised in human rights; and last but not least, the fourth established and formalised the details for follow-up meetings and implementation procedures.[20] However, the Helsinki Act, instead of a legally binding treaty, is a political binding code of conduct, as it relies on the voluntary compliance of the member states.[21]

OSCE Charter for European Security (Istanbul Summit 1999)

One of the most important documents establishing the security provisions associated with OSCE's mandate is the Charter of European Security. This agreement aims to empower the organisation's ability to prevent conflicts and aid societies ravaged by war to rehabilitate. The participating states had formulated and defined OSCE's role in peace keeping operations, creating Rapid Expert Assistance and Co-operation Teams and expanding OSCE policing activities. In addition, they committed themselves to strengthen co-operation with other international organizations via a new instrument called "the Platform for Co-operative Security".[22]

Permanent Council Decision No. 1106: Cyber/ICT Security CBMs

Following this decision, a set of voluntary Confidence Building Measures (CBMs) adopted to maintain the stability and safety in cyberspace between participating states from the use of

[18] Office of the Historian, U.S. Department of State, *"The Helsinki Final Act, 1975,"* accessed April 21, 2026, https://history.state.gov/milestones/1969-1976/helsinki

[19] Organization for Security and Co-operation in Europe, *"Principles and Commitments,"* accessed April 21, 2026, https://www.osce.org/node/650180

[20] Ibid

[21] "Library Guides: Government Sources by Subject: Helsinki Accords," n.d., https://guides.lib.uw.edu/research/govpubs-quick-links/helsinki-accords.

[22] Organization for Security and Co-operation in Europe, *"Helsinki Final Act,"* August 1, 1975, https://www.osce.org/mc/17502

Information and Communication Technologies (ICTs).[23] Some key aspects of the Decisions are the clauses of transparency, sharing information about cyberthreats, ensuring a secure and reliable internet, data about national ICT security strategies and in general cooperation between states of the OSCE region regarding emergencies and the development of partnerships to enhance cybersecurity.[24]

UN GGE (Group of Governmental Experts) Norms on Responsible State Behavior in Cyberspace

The UN GGE norms on responsible State behaviour in cyberspace constitute one of the most important normative reference points for contemporary cyber governance. Their principal formulation emerged in the 2015 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), and was later reaffirmed and further elaborated in the 2021 report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135). Although these norms are voluntary and non-binding, they have acquired considerable authority and their function is preventive.[25] Alongside with the GEE, the OEWG is another important UN mechanism which plays a pivotal role in cyber security, confidence-building measures, capacity-building, and the implementation of responsible State behaviour in cyberspace[26].

Tallinn Manual

It is a non legally binding scholarly work by international law academics aiming to provide a framework for the appliance of international law in the cyber context, more specifically issues like

[23] NATO Cooperative Cyber Defence Centre of Excellence, *"OSCE Confidence-Building Measures for Cyberspace,"*accessed April 21, 2026, https://ccdcoe.org/incyder-articles/osce-confidence-building-measures-for-cyberspace/

[24]NATO Cooperative Cyber Defence Centre of Excellence, *"OSCE Expands Its List of Confidence-Building Measures for Cyberspace: Common Ground on Critical Infrastructure Protection,"* accessed April 21, 2026, https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/

[25] United Nations, *"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,"* UN Doc. A/70/174 (July 22, 2015), https://digitallibrary.un.org/record/799853

[26] United Nations "Open-Ended Working Group on Ageing | Division for Inclusive Social Development (DISD)," n.d., https://social.desa.un.org/issues/ageing/oewga

sovereignty, use of force and state responsibility.[27] It was developed at the request of the NATO Cooperative Cyber Defence Centre of Excellence.[28]

OSCE Code of Conduct on Politico-Military Aspects of Security

The OSCE Code of Conduct on Politico-Military Aspects of Security is a key normative instrument within the OSCE's politico-military framework. Adopted in Budapest in 1994 and in force since 1995, it establishes politically binding commitments on democratic control over armed, paramilitary, internal security, intelligence, and police forces. Its relevance lies in the fact that it links military security with the rule of law, human rights, international humanitarian law, and accountability.The Code provides an important normative basis for arguing that the face must remain under effective human, legal and democratic control. In addition, by linking modern security risks and hybrid threats with existing OSCE principles on responsible military conduct and state accountability, it aids to empower the Organisation's legal framework.[29]

Budapest Convention on Cyber Crime

The Convention's primary objective is to promote cross-border collaboration, enhance investigative techniques, and harmonize national laws in the fight against cybercrime. It covers a broad spectrum of crimes, including but not limited to illegal access, data and system manipulation, computer-related fraud, copyright infringement, and network security violations, all of which could be possible vectors for upsetting political processes. Apart from its formal framework, the Budapest Convention has developed into an active forum for operational cooperation. It enables direct contact and relationship-building among practitioners, including law enforcement, prosecutors, and cybercrime units, across its more than 60 signatory countries.[30]

[27]CCDCOE, "Tallinn Manual 2.0," Ccdcoe.org, 2017, https://ccdcoe.org/research/tallinn-manual/.
[28]IRIS – BH, *"Tallinn Manual and the Use of Force,"* accessed April 21, 2026, https://irisbh.com.br/en/tallinn-manual-and-the-use-of-force/.
[29] OSCE "CODE OF CONDUCT ON POLITICO-MILITARY ASPECTS OF SECURITY," *Https://Cdn.Osce.Org/Sites/Default/Files/f/Documents/5/7/41355.Pdf*, 3 December 1994
[30] Council of Europe, "Budapest Convention and Related Standards.",2025. https://www.coe.int/en/web/cybercrime/the-budapest-convention

6. Main Discussion

6.1. Confidence-Building Measures (CBMs) in the Digital Era

Decision No. 1106 of OSCE first introduced Confidence-Building Measures, which were later enhanced in 2017 by Decision 1202, as non-binding measures.[31] The 16 CBMs can be divided in two main sets, transparency measures and cooperation measures, with the goal being the prevention of conflict and malicious use of Information and Communication Technologies (ICTs).[32]

As cyberspace is expanding, technical malfunctions, bugs or legitimate activities may be misinterpreted as hostile by national security systems. As a result, States may be unable to clearly distinguish accidental incidents from deliberate cyber operations. In response, CBMs 3, 13 and 16 constitute the core of OSCE's Crisis Management Mechanism in Cyberspace.[33]

CBM 3 establishes diplomatic groundwork for de-escalation by encouraging States to voluntarily participate in consultation of the appropriate level, in order to reduce the risks of misperception and military escalation.[34] In practice, this measure helps to avoid premature retaliation responses when there is an unverified cyber contact. CBM 3 ensures that negotiations may begin before tensions can escalate in confrontation of a larger scale, allowing state-members to act with good faith. CBM 13 inserts the importance of protected and authorized communication channels.[35] This measure reinforces the Clarification Mechanism of OSCE by providing a secure way for State officials and experts to verify the nature of the cyber event via these channels, attributing the problem accurately, avoiding the cycle of unilateral attribution. CBM 13 allows communication between technical experts, securing channels of cooperation and avoiding the politicization of incidents.[36]

[31] Permanent Council of the OSCE, "OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Decision No. 1202, 10 March 2016.
[32] OSCE. (2023). "Cyber Incident Classification: A Report on Emerging Practices within the OSCE region." Transnational Threats Department, OSCE Secretariat
[33] Martino, L. (2018). "Give Diplomacy a Chance: OSCE's Red Lines in Cyberspace." Center for Cyber Security and International Relations Studies (CCSIRS), Commentary
[34] Martino, ibid
[35] Permanent Council of the OSCE, "Initial set of the OSCE confidence-building measures to reduce the risks of the conflict stemming from the use of information and communication technologies.", Decision No.1106, 3 December 2013
[36] Permanent Council of the OSCE, "OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Decision No. 1202, 10 March 2016.

The above, compliment CBM 16, which focuses on transparency regarding technical weaknesses. States are encouraged to report such vulnerabilities and seek available remedies. In practice, voluntary disclosure fosters a secure environment of cooperation within the OSCE region and discourages the weaponization of infrastructure gaps.[37] Another important point is the maintenance of regional ICT infrastructure.[38]

CBM 15 recognizes the transnational character of the digital space.[39] The "Cyber Incident Classification" published in 2022, helps States adopt national arrangements to measure the scale and seriousness of incidents to prevent any militarization acts. This specific CBM focuses on evading criminal activity, espionage, use of force, permitting proportional legal and political responses.[40] Moreover, a plethora of CBMs stated by OSCE establish the importance of sharing national guidelines, risk assessments and expectations of behavior, establishing "red lines".[41] As a result, CBMs reduce the likelihood of aggression and deescalation aiding the creation of a uniform and secure framework promoting cooperation and communication regarding cyber security within the OSCE region.

An incident that highlighted the need for bilateral defensive frameworks was the Ukrainian "cyber affair". Ukrainian power grids were the target of major cyberattacks which from a political and technical perspective the involvement of Russia could not be proved. The anonymity tested OSCE's crisis management mechanism bringing forth the issue of the voluntary character of CBMs.[42]

6.1.1. Information Sharing and Points of Contact (PoCs) between Participating States

Points of Contact are established in CBM 8 and remain one of the most widely implemented mechanisms out of OSCE's toolbox.[43] States are required to aid communications and dialogue of ICT security by providing at least one PoC. During any concerning activity which could lead to a national

[37] OSCE. "Cyber Incident Classification System in Focus of OSCE Workshop." *Osce.org*, 2024, www.osce.org/secretariat/567034.
[38] Permanent Council of the OSCE, "Initial set of the OSCE confidence-building measures to reduce the risks of the conflict stemming from the use of information and communication technologies.", Decision No.1106, 3 December 2013
[39] OSCE CBMs, 2023, ibid
[40] OSCE. *CYBER INCIDENT CLASSIFICATION a Report on Emerging Practices within the OSCE Region 2 Published by the Organization for Security and Co-Operation in Europe*. 2022.
[41] Martino, ibid
[42] OSCE CBM, ibid
[43] OSCE CBM, ibid

level crisis, experts and bodies of each State are able to enable direct dialogue and rapid communication in order to resolve the issue at hand.[44] In practice, this measure helps avoid diplomatic crises. Without a PoC, States risk relying on assessments and speculated data, which in turn can lead to politicization and escalate otherwise manageable incidents. In negotiations, PoCS remain a valuable function creating trust-building anchors and depoliticized points promoting diplomacy and dialogue.[45] Participating States have to update contact information annually and notify OSCE for any changes within 30 days. Additionally, the OSCE Secretariat initiated conducting communication checks in 2017. The tasks range from administrative questions to complex scenarios.[46] Collectively, these mechanisms ensure productive crisis prevention and reinforce the OSCE's goals of stability and cooperation within the cyberspace.

The "OSCE Communities" platform[47] functions as a dedicated workspace in which participating States can edit country profiles and provide information regarding national legislation, cybersecurity strategies. Making these policies accessible within the States helps to avoid misperceptions rooted in ignorance regarding cyber security infrastructure of other States.

6.1.2. Transparence in National Cybersecurity doctrines

National Doctrines rely on OSCE's transparency framework, established in CBMs 1. CBM 1 focuses on States providing national views and threats related to ICTs, avoiding strategic ambiguity and undermining a State's capacity of cyber security mechanisms.[48] Through CBM 7, States share detailed information regarding national organizations, strategies, programs and policies. Both measures aim to strengthen the Information Sharing Mechanism of OSCE, reducing the risk of cooperative negotiations stalling.

CMB 9 enhances the aforementioned framework by addressing the risk of miscalculation due to linguistic ambiguity. States should voluntarily provide a list of national terminology and definitions to prevent diplomatic or military misunderstanding by a misinterpreted technical report. In practice,

[44]CCDCOE. "Tallinn Manual 2.0." *Ccdcoe.org*, 2017, ccdcoe.org/research/tallinn-manual/.

[45] Permanent Council of the OSCE, "Initial set of the OSCE confidence-building measures to reduce the risks of the conflict stemming from the use of information and communication technologies.", Decision No.1106, 3 December 2013

[46] OSCE CBM 2023, ibid

[47] OSCE CBM 2023, ibid

[48] Nye, Joseph. "Deterrence and Dissuasion in Cyberspace." *International Security*, vol. 41, no. 3, 2017

CBM 9 helps avoid situations where the issue could escalate due to definition problems. Similar terms allow state-members to even and thorough negotiations and a shared understanding. Serbia is a prime example of CBM 9 Glossary, having developed a publicly available website which hosts over 2.000 terms found in official technical documents and translated into the official OSCE languages.[49]

The Informal Working Group on Cyber/ICT Security has been encouraging the voluntary commitments of States through the Adopt-a-CBM Initiative. The Initiative categorizes certain CBMs as "champion specific". As of 2023, 23 States are actively participating, mostly focusing on CBMs 9, 14, 15 and 16 through e-learning courses and good practice tools.

6.2 The Impact of AI on Early Warning Systems

AI technologies are playing a pivotal and a leading role in Early Warning Systems (EWSs). In contemporary frameworks, EWS includes four interconnective pillars; disaster risk knowledge and management (Pillar I), detection, observation, monitoring, analysis, and forecasting (Pillar II), warning dissemination and communication (Pillar III) and preparedness and response capabilities (Pillar IV).[50] Artificial Intelligence has marked a new direction in the advancement of early warning mechanisms by enhancing the real-time processing of large-scale and multi-source data.

AI-driven EWS in contrast with the conventional mechanisms, have the privilege to integrate structured and unstructured inputs such as but not limited to conflict-event datasets and satellite imagery that are based in machine-learning models, centralised in detecting patterns and classifying anomalies. In addition, AI-driven EWS enhances faster triage of very large data flows and enables a continuous and more effective monitoring procedure and identification of conflict hotspots. Considering the importance of early detection and prevention mechanisms in cases of political and geopolitical tension, OSCE in terms of security and stability shed light on the aforementioned capabilities.

[49] Permanent Council of the OSCE, "Initial set of the OSCE confidence-building measures to reduce the risks of the conflict stemming from the use of information and communication technologies.", Decision No.1106, 3 December 2013

[50] United Nations. "Early Warnings for All." *United Nations*, 2023, www.un.org/en/climatechange/early-warnings-for-all.

Nevertheless, within the OSCE's conflict prevention framework there are also some important risks that must be addressed closely associated with the functionality and the accountability of such mechanisms. First and foremost, AI can magnify escalation risks.[51] Moreover, according to recent evidence conflict-forecasting models still perform better in already unstable environments than in previously peaceful settings.[52] Emphasising OSCE's mandate, this is particularly sensitive: Ministerial Decision No. 3/11 and the Conflict Prevention Centre place the systematic collection, analysis, and assessment of early warning signals at the heart of preventive action. OSCE publications on AI and freedom of expression also warn that AI can compromise safeguards and make human oversight and rights-based safeguards indispensable in any AI-supported warning chain.[53]

6.2.1 Autonomous Weapon Systems., Human Control and Accountability Gaps

For the OSCE, this debate is not peripheral. The governance of autonomy directly relevant to regional stability, military predictability, and the prevention of escalation in periods of geopolitical instability.

Automation and autonomous systems are widely used for a range of functions in weapons. The shift from autonomous systems from supportive functions, such as logistics, navigation and surveillance, to critical functions of identifying, selecting, and engaging targets.[54] Following the 2019 Group of Governmental Experts that highlighted the role of autonomous functions in the identification, selection, or engagement of targets, OSCE have likewise described autonomy as a spectrum defined by differing levels of human input and analytical capability.[55] Therefore, the matter of concern is

[51] Ioana Puscas, *"AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures,"* Geneva: United Nations Institute for Disarmament Research (UNIDIR), October 12, 2023, https://unidir.org/wp-content/uploads/2023/10/UNIDIR_AI-international-security_understanding_risks_paving_the_path_for_confidence_building_measures.pdf

[52] Max Murphy, Ezra Sharpe, and Kayla Huang, *"The Promise of Machine Learning in Violent Conflict Forecasting,"*Cambridge University Press, *Data & Policy* 6 (2024): e35, published August 30, 2024, https://www.cambridge.org/core/journals/data-and-policy/article/promise-of-machine-learning-in-violent-conflict-forecasting/40D559ADA18FF7308915B08956B4E8F3

[53] Organization for Security and Co-operation in Europe, *"Ministerial Council Decision No. 3/11: Elements of the Conflict Cycle Related to Enhancing the OSCE's Capabilities in Early Warning, Early Action, Dialogue Facilitation and Mediation Support, and Post-Conflict Rehabilitation,"* Vilnius, December 7, 2011, https://cdn.osce.org/sites/default/files/f/documents/6/b/86621.pdf

[54] United Nations Office for Disarmament Affairs, *"Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems,"* UN Doc. CCW/GGE.1/2019/3 (2019), https://documents.unoda.org/wp-content/uploads/2020/09/CCW_GGE.1_2019_3_E.pdf

[55] Organization for Security and Co-operation in Europe, *"Decision No. 3/18: Strengthening Efforts to Prevent and Counter Terrorism,"* Milan, December 7, 2018, https://cdn.osce.org/sites/default/files/f/documents/d/6/487054.pdf

not whether a system is autonomous, but whether human judgement is replaced by such technologies.

Human control has become the normative centre of the debate. In particular, there is a discordance whether human intervention should be characterised as "meaningful human control" or as "appropriate human judgement". Human control remains essential for legal accountability and operational oversight.[56] The potential replacement of the human actor by Automated Systems increases the accountability gap. There is also the difficulty to assign responsibility for war crimes, in cases of an unlawful attack, based on AWS miscalculation.[57]

These concerns resonate strongly with existing commitments about the emerging technologies and threats.[58] OSCE aims to strengthen human oversight and fill the accountability gaps over the insecurity caused by the AWS technologies.[59] For this purpose, the organization has released the "OSCE Code of Conduct on Politico-Military Aspects of Security"[60], safeguards against accidental or unauthorized use of military means, instruction in IHL, and the individual accountability of armed forces personnel and commanders under national and international law.

The real issue is whether emerging military autonomy can be incorporated into security governance. Current multilateral discussions increasingly suggest a two-tier logic: uncontrollable systems should be prohibited; systems with narrower autonomous functions may only be tolerated under strict conditions of predictability, limited mission parameters, responsible command, effective supervision, weapons review, incident investigation, and human accountability across the entire life

[56] Paul Scharre and Kelley Sayler, *"Autonomous Weapons and Human Control,"* Center for a New American Security (CNAS), n.d., https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS_Autonomous_Weapons_poster_FINAL.pdf

[57] Future of Life Institute, *"A Diplomat's Guide to Autonomous Weapons Systems,"* August 5, 2024 (updated September 17, 2024), https://futureoflife.org/wp-content/uploads/2024/08/AWS-Guide-for-Diplomats_17-September-2024.pdf

[58] Organization for Security and Co-operation in Europe, *"Conflict Prevention and Resolution,"* accessed April 21, 2026, https://www.osce.org/field-of-work/conflict-prevention-and-resolution

[59] Organization for Security and Co-operation in Europe, *"The OSCE Forum for Security Co-operation,"* Vienna, n.d., https://cdn.osce.org/sites/default/files/f/documents/5/a/77535_1.pdf

[60] Organization for Security and Co-operation in Europe, *"Code of Conduct on Politico-Military Aspects of Security,"*Budapest, December 3, 1994, https://cdn.osce.org/sites/default/files/f/documents/5/7/41355.pdf.

cycle. Defining what minimum legal and institutional safeguards are, is necessary to ensure that human judgement remains operationally real, politically meaningful, and legally answerable.[61]

6.2.2 Ethical and Legal Constraints on Autonomous Systems in Conflict Zones

Article 36 of the additional Protocol of the Geneva Conventions[62] implicitly presumes human oversight in weapons deployment.[63] By introducing systems that process data without contextual moral comprehension, dissolve the aforementioned foundation. For instance, when an autonomous drone misidentifies a civilian convoy as a military target, accountability fractures across the chain of development and deployment.[64]

Within the OSCE framework, the clearest normative anchor is the OSCE Code of Conduct on Politico-Military Aspects of Security, which requires effective guidance and control by constitutionally established authorities, and obliges participating States to guard against accidental or unauthorized use of military means.[65] Read together with the OSCE's role in early warning, conflict prevention and risk reduction, these commitments sit uneasily with weapons systems whose operation is opaque. The Forum for Security Co-operation has discussed AI and autonomous systems as part of the challenges of "new generation warfare". The OSCE's emerging position focuses on strong preference for accountability, democratic oversight, IHL compliance, and co-operative dialogue.[66]

---

[61] United Nations Office for Disarmament Affairs, *"Convention on Certain Conventional Weapons (CCW): Group of Governmental Experts on Lethal Autonomous Weapons Systems – Rolling Text (Status as of 18 December 2025),"* UN Doc. CCW/GGE/LAWS (2025), https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_%282026%29/CCW_GGE_LAWS_Rolling_Text_-_status_18_December_2025.pdf

[62] Natalia Jevglevskaja, *"Weapons Review Obligation under Customary International Humanitarian Law: The Case of Article 36 of Additional Protocol I," International Law Studies* 94 (2018), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1231&context=ils

[63] International Committee of the Red Cross (ICRC), *"Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977 – Article 36,"* accessed April 21, 2026, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977?activeTab=

[64] Jie Guo, *"The Ethical Legitimacy of Autonomous Weapons Systems: Reconfiguring War Accountability in the Age of Artificial Intelligence," Ethics & Global Politics* 18, no. 3 (2025): 27–39, https://www.tandfonline.com/doi/full/10.1080/16544951.2025.2540131.

[65] Ibid

[66] Organization for Security and Co-operation in Europe, *"Factsheet of the OSCE Forum for Security Co-operation,"* January 21, 2020, https://www.osce.org/forum-for-security-cooperation/factsheet

6.3 Information Integrity and Hybrid Threats

6.3.1 Combatting AI-driven Disinformation and Deepfakes

AI-driven disinformation and deepfakes are capable of destabilising societies. AI-enabled tools play a key role in the creation of highly realistic synthetic content that can convincingly imitate real individuals and events. Within the OSCE framework, information integrity is a core security issue, as the aforementioned phenomenon poses a direct challenge to democratic processes and distorts political environments and erode public trust.[67]

Fighting against AI-driven Disinformation and Deepfakes is a multifaceted challenge that demands a multilateral approach. Early detection of disinformation and deepfakes is not feasible. Besides, technical solutions such as watermarking and algorithmic detection are still not consistent enough and accurate.[68]

In the scope of the OSCE mandate, the regulatory framework is quite blurred.[69] Within the OSCE framework, the RFoM plays a pivotal role in combating deepfakes and disinformation, as it is recognised as the central institutional actor in safeguarding media freedom and addressing emerging challenges posed by AI-driven tools. The RFoM Policy Manual stresses that information spaces require inclusive and meaningful multi-stakeholder processes.[70] Besides, RFoM recommends efforts to demonetize disinformation and fraudulent actors, while avoiding politically captured interventions that could undermine media freedom.

6.3.2 Protecting Critical Infrastructure from ICT-based Attacks

ICT-based attacks have become emerging hybrid threats, targeting critical infrastructure and sectors. ICT-based attacks have become a major pillar of international security and stability. Cyber threats have significantly intensified and thus, ICT-based attacks are no longer isolated technical

[67] Anastasiia Romanishyn, *"AI-Driven Disinformation: Policy Recommendations for Addressing Emerging Threats,"Frontiers in Communication* (2025), accessed April 21, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12351547/

[68] Springer Nature, *"Article Collection,"* accessed April 21, 2026, https://link.springer.com/collections/diiijiiibh.

[69] Organization for Security and Co-operation in Europe, *"Project PROTECT: Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks,"* Vienna: OSCE Secretariat, October 29, 2025, https://cdn.osce.org/sites/default/files/f/documents/d/c/508292.pdf

[70] Organization for Security and Co-operation in Europe, *"OSCE Representative on Freedom of the Media,"* accessed April 21, 2026, https://rfom.osce.org/

incidents, but strategic tools capable of undermining state stability and institutional functionality.[71] Especially in terms of geopolitical instability, ICT-based attacks are the major source of disruptiveness and public trust erosion that leads to gradual destabilisation. The ICT-based attacks, carried out by malware, ransomware, distributed denial-of-service (DDoS) operations and intrusions into industrial control systems, are characterised as "hybrid".[72]

Protecting critical infrastructure is one of the major priorities of the OSCE. Via Confidence-Building Measures on ICT security, the Organisation promotes transparency and cooperation, aiming to reduce the risk of escalation,[73] The "OSCE Ministerial Council decision no.5/16 on the risks of conflict stemming from the use of ICT" declares that "*efforts by OSCE participating States to reduce the risks of conflict stemming from the use of information and communication technologies will be consistent with: international law, including, inter alia, the UN Charter and the International Covenant on Civil and Political Rights; the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms".*[74] OSCE should focus on capacity-building initiatives, technical cooperation and the development of coordinated incident response mechanisms that are necessary for strengthening cyber resilience and protecting critical infrastructure.[75]

6.3.3 Cyber-enabled economic coercion

The relevant OSCE framework is distributed across its digital-economy, cyber/ICT, and governance instruments. OSCE understands digital transformation as simultaneously creating opportunities, particularly where the private sector, small and medium-sized enterprises, and critical services become deeply dependent on ICTs. The 2018 Ministerial Declaration on the Digital Economy is

[71] Anastasiia Romanishyn, *"AI-Driven Disinformation: Policy Recommendations for Addressing Emerging Threats,"Journal of Information Security and Applications* (2025), https://www.sciencedirect.com/science/article/pii/S2199853125000824

[72] CrowdStrike, *"12 Most Common Types of Cyberattacks,"* accessed April 21, 2026, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

[73] Organization for Security and Co-operation in Europe, *"Our Mandate on Cyber/ICT Security,"* accessed April 21, 2026, https://www.osce.org/node/660054

[74] Organization for Security and Co-operation in Europe, *"Decision No. 5/16: OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies,"* Hamburg, December 9, 2016, https://www.osce.org/cio/288086.

[75] Organization for Security and Co-operation in Europe, *"Cyber/ICT Security,"* accessed April 21, 2026, https://www.osce.org/field-of-work/Cyber-ICT-security

especially important here, because it links digital transformation to co-operation, security, connectivity, transparency, and accountability.[76]

Cyber-enabled economic coercion refers to the use of malicious cyber activity, digital dependence, or technology-mediated pressure to impose economic costs on a state, society, or sector. OSCE material on cyber incidents underscores that such incidents now frequently threaten critical infrastructure and cause significant financial and societal harm.[77] Cyber disruption can function as pressure without crossing into declared armed conflict. The cyber/ICT CBMs establish contact points, consultation channels, platforms for best-practice exchange, critical-infrastructure co-operation, and responsible vulnerability reporting with business and industry.[78] These instruments make it harder for malicious actors to exploit institutional fragmentation.

6.4. The Human Dimension of AI and its impact on Regional Stability

6.4.1. Safeguarding Human Rights and Privacy in AI-enabled Surveillance

Facial recognition, smart city platforms and forms of policing, challenge fundamental human rights regarding privacy and consent.[79] Within the OSCE region, these issues take on a regional security dimension since they do not only concern individual privacy but also civil participation and democracy.[80] The "Chilling Effect" leads individuals to self-sensor and modify their behavior, especially when used in politically sensitive circumstances such as journalism, minority communities and political protests.[81] The normalization of automated monitoring can also lead to the emergence of the Digital Panopticon.[82]

---

[76] Organization for Security and Co-operation in Europe, *"Declaration on the Digital Economy as a Driver for Promoting Co-operation, Security and Growth,"* Milan, December 7, 2018, https://cdn.osce.org/sites/default/files/f/documents/a/5/405920.pdf

[77] Organization for Security and Co-operation in Europe, *"National Cyber Incident Classification Handbook,"* Vienna: OSCE Secretariat, 2025, https://cdn.osce.org/sites/default/files/f/documents/e/a/600455.pdf

[78] Organization for Security and Co-operation in Europe, *"Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,"* Vienna, March 10, 2016, https://cdn.osce.org/sites/default/files/f/documents/d/a/227281.pdf

[79] Nandy, D. "Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns." Journal of Current Social and Political Issues, 1(1), 2023

[80] OSCE, "Protecting Civic Space from Growing Digital Threats Requires Sustained Efforts, Leading OSCE Officials Say." *Osce.org*, 11 May 2026, www.osce.org/chairpersonship/664069

[81] Matar, R., & Murray, D. "Identity and the Right to Privacy in the Age of AI Surveillance." Human Rights Law Review,2026,

[82] Raees Malik, M. "Artificial Intelligence and the Right to Privacy: A Human Rights Dilemma in the Age of Surveillance." Dialogue Social Science Review, 3(9),2025

Other existent standards are the GDPR[83], the basis of date protections, as well as the findings of the European Court of Human Rights (ECtHR). ECtHR requires surveillance to be necessary, proportionate, and regulated.[84] On one hand, AI algorithms monitor and profile individuals to certain groups but on the other, it may be done without their awareness. As a result, regional inequalities can be deepened due to disproportionate monitoring from AI-enabled surveillance. In order to mitigate this issue, courts have sometimes allowed the *in abstracto* claims, where the existence of surveillance law is a threat by default.[85] For the OSCE, its wider human-security concerns remain the central point in the rise of AI systems, with the issue being of humanitarian nature and not only a matter of technological advancements.[86]

6.4.2. Ensuring Bias-free AI Technologies and the maintenance of Democracy in the OSCE Region

One of the main pillars of the function of OSCE is the respect and protection of human rights. From democratization to promoting non-discrimination, OSCE members focus on co-operating for the protection of human dignity.[87] In the age of AI, databases do not only reflect gathered information, but values and realities that end up misinterpreted when applied to other regions within the OSCE framework.[88] The above issue can create a feedback loop which will only fuel biases and highlight social inequalities if not moderated. For example, facial recognition technologies exhibit gender and racial biases.[89] Meanwhile, predictive policing algorithms target over-policed neighbourhoods, reinforcing structural biases. AI surveillance can target vulnerable groups to distort behavior, pressuring towards societal conformity in disregard of political and cultural activities that may challenge the status quo.[90] Within the OSCE region, this is a matter of high importance because any discriminatory function of AI systems weakens the human dimension of security by limiting the public's trust both against authorities and marginalized communities.

---

[83] Bakeer, H., et al. "AI and Human Rights." International Journal of Academic Engineering Research (IJAER), 8(10), 2024

[84] Ibid

[85] Kosta, E. "Algorithmic state surveillance: Challenging the notion of agency in human rights." Regulation & Governance, 2020

[86] OSCE, "Protecting Civic Space from Growing Digital Threats Requires Sustained Efforts, Leading OSCE Officials Say." *Osce.org*, 11 May 2026, www.osce.org/chairpersonship/664069

[87] OSCE. "Fields of Work." *Osce.org*, 2025, www.osce.org/fields-of-work

[88] OSCE ODIHR. *Think Again: Freedom of Thought in the Age of Artificial Intelligence POLICY BRIEF*, 2025.

[89] Feldstein, S. "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace, Working Paper, 2019

[90] Kosta, ibid

In order to combat the above, actors within the OSCE region have taken a plethora of actions. While the EU AI Act is binding within the European Union, it functions as a regional point of reference for the OSCE region since it is able to link issues of AI governance with the protection of fundamental human rights.[91] The EU AI Act restricts real-time biometric identification in order to minimize AI systems categorizing individuals. Developers must conduct human rights protections via Fundamental Rights Impact Assessments (FRIA) before implementing high-risk AI systems. As a result, AI tools will be trained by diverse databases, prioritizing bias mitigation and transparency regarding the nature of AI monitoring. Independent Oversight and Multi-Stakeholder Collaboration have been proposed to ensure compliance with human rights through technical expertise. The Privacy by Design rule ensures that AI systems are built on privacy safeguards rather than implementing them afterwards as an afterthought.[92] All in all, international collaboration is essential to harmonize standards with OSCE remaining a pioneer in the international community with its transparency framework, harboring dialogue, trust building and reciprocation of good practices among member-states.

6.4.3. Democratic oversight and Civil Participation

Modern AI systems rely on privatized knowledge from corporations who do not share such information with the public, which in the context of the OSCE regulations highlights the dangers regarding access to information and public expression shaped by private actors and not the transparency of public institutions.[93] The EU Digital Services Act (DSA) mandates transparency within the algorithms to protect citizens from political propaganda.[94]

Major networks still disregard the aforementioned concerns and moderation criteria, side lining the role of human oversight.[95] The Italian Supreme Court ruled that consent for data is contingent upon

[91] EU AI Act. "High-Level Summary of the AI Act." *EU Artificial Intelligence Act*, Future of Life Institute, 27 Feb. 2024, artificialintelligenceact.eu/high-level-summary/.
[92] Bakeer, ibid
[93] Zuboff, S. "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization." Organization Theory, 2022, OSCE, Shaping Europe's Digital Future." *Europa.eu*, 2024, digital-strategy.ec.europa.eu/en/policies/digital-services-act.
[94] Steffen, B. (Ed.). Bridging the Gap Between AI and Reality: First International Conference, AISoLA 2023, 2025
[95] Azgin, B., & Kiralp, S."Surveillance, Disinformation, and Legislative Measures in the 21st Century: AI, Social Media, and the Future of Democracies." Social Sciences, 13(10), 2024

transparency.[96] Governments often exploit "legal gray zones" by renaming them as "High risk zones" and deploying invasive AI systems to bypass existing privacy protections. Therefore, in the OSCE region the issue of transparency is a pillar for the protection of democracy and public trust.

Scholars argue that allowing activities that codify human behavior and later moderations the content or labels goes inherently against democratic principle. The alternative response proposes the institution itself to be ended. In contrast, the EU AI Act represents the effort by policy makers to assess the risk and impose standards accordingly.[97]

Civil Society Organizations (CSOs) remain the primary defenders of human rights in the digital age. Many campaigns have taken place all around the globe highlighting universal fatigue regarding biometric mass surveillance. "Reclaim Your Face" and "People's Declaration" are two examples of campaigns that managed to be delivered to the European Parliament and demanded an end to surveillance advertising. Nevertheless, civil society groups critique the EU AI Act. By allowing national security exemption the Act allowed mass surveillance to continue under a different name but with the same harmful purpose.[98] The aforementioned, highlight the OSCE's role in protecting universal human rights. Without campaigns, researchers and communities, AI-governance would have evolved as a state-driven function, disregarding public trust and informational self-determination.

6.5. Bridging the Digital Divide for Regional Stability

6.5.1. Capacity Building and Technical Cooperation among OSCE Participating States

Capacity building is the OSCE's primary method for translating the effort to maximize the benefits of digital transformation. The 16 CBMs aim to make cyber activity more predictable and to reduce misunderstandings and miscalculations. The 2024 Annual Report[99] records that the Transnational Threats Department supported participating States with study visits, workshops, annual meetings

[96]Carter, C."The Digital Surveillance of Workers: A Human Rights Perspective." European Labour Law Journal, 16(2), 2025

[97] Atif, M., & Alamgir, A. "The Illusion of Security: How AI-Powered Surveillance Erodes Privacy, Amplifies Inequality, and Redefines Democracy in the Digital Age." Social Science Review Archives, 3(4), 2025

[98] Bakeer, ibid

[99] Organization for Security and Co-operation in Europe, *"Annual Report 2024,"* Vienna: OSCE Secretariat, February 13, 2026, https://www.osce.org/sites/default/files/documents/publications/2026/02/Annual%20Report%202024%2010.02.2026%20REV1%20docx.pdf.

of national cyber points of contact, expert sessions, and practical training events. The OSCE also offers e-learning on cyber/ICT security CBMs and on coordinated vulnerability disclosure.[100]

In 2025, the OSCE convened experts from Moldova and Ukraine to work on threat-information sharing, critical-infrastructure protection, and vulnerability and joint crisis response.[101] A workshop in Ukraine focused on incident classification to prioritize incidents consistently. In Turkmenistan, the OSCE ran a cyber-diplomacy course that brought together multiple stakeholders. In Central Asia, the OSCE convened senior representatives from law-enforcement educational institutions to discuss systematic education on cybercrime and digital evidence.[102] This directly supports the prevention of misunderstanding, misattribution, and escalation. When stakeholders train together, they reduce the likelihood that a future cyber incident will be harmful.[103]

Participating States also need legal and policy frameworks that make co-operation sustainable. The OSCE's Handbook on incident classification emphasizes statutory mandates, reporting pathways, incentives for information sharing, data-protection safeguards, and legal limits on the re-use of shared data. Similarly, OSCE cyber diplomacy and CBM practice shows that national resilience depends on institutional clarity and political trust as much as on technology. Technical capacity without legal certainty and interagency co-ordination will not produce lasting cyber resilience.[104] Digital inclusion is a prerequisite for participation in modern society, economy, and public life, and that states should address digital divides.[105] Earlier OSCE economic-forum discussions likewise emphasized that training on digital skills is necessary to prevent the gender digital divide. Capacity building consists of the hard-security layer of cyber preparedness and incident response, and the societal layer of digital access, skills, and inclusion.

Since the CBMs are voluntary, their effectiveness depends on sustained implementation, recurring exercises, networks of practitioners, and institutional memory across the region. OSCE turns

[100] Ibid
[101] Organization for Security and Co-operation in Europe, *"OSCE Promotes Classification System for Cyber Incidents to Strengthen Cyber Security in Ukraine,"* January 30, 2025, https://www.osce.org/secretariat/585169
[102] Organization for Security and Co-operation in Europe, *"Cyber Diplomacy in Focus of OSCE-Organized Course in Turkmenistan,"* November 27, 2025, https://ashgabat.osce.org/centre-in-ashgabat/602870
[103] Ibid
[104] Ibid
[105] Organization for Security and Co-operation in Europe, "Recommendations on the Effective Participation of National Minorities in Social and Economic Life & Explanatory Note," The Hague: OSCE High Commissioner on National Minorities, October 2023, https://cdn.osce.org/sites/default/files/f/documents/2/3/553783.pdf

technical co-operation into preventive diplomacy by helping participating States build shared resilience.

6.5.2. Promoting Multi-stakeholder Governance (State, Private Sector, Academia)

Public-private collaboration is recognized as a common practice to increase cyber resilience and strengthen national preparedness. The private sector is indispensable for two reasons; first, much of the region's critical infrastructure is privately owned or operated, which means that governments cannot realistically secure essential services without trusted channels to operators, vendors, and digital-service providers; second, in the information space, digital platforms exercise immense gatekeeping power over visibility, reach, and monetization. The OSCE's Public-Private Partnerships's work explicitly links public-private co-operation to critical-infrastructure protection.[106]

Academia occupies a distinct place within this model. The OSCE Academy in Bishkek[107] is a strong illustration; the 2025 OSCE-wide Youth, Peace and Security Roadmap describes it as a flagship project in education and research. In Central Asia, OSCE-supported meetings on cybercrime education brought together universities, police colleges, prosecutors, and international training bodies.[108] OSCE media-literacy work in Kosovo includes evidence-based recommendations on AI-driven misinformation, fact-checking, and ethical reporting.[109] This is exactly the kind of knowledge ecology a resilient OSCE region requires.

Civil society and the journalistic community are equally important.[110] The OSCE has also explored practical models that could deepen such co-operation. Its PPP recommendations include secondment schemes and technical co-operation.

---

[106] Organization for Security and Co-operation in Europe (OSCE), Representative on Freedom of the Media, *"Safeguarding Media Freedom in the Age of Big Tech Platforms and AI,"* Vienna, October 6, 2025, https://rfom.osce.org/sites/default/files/f/documents/e/3/598525_1.pdf

[107] Organization for Security and Co-operation in Europe Academy, *"OSCE Academy in Bishkek,"* accessed April 21, 2026, https://osce-academy.net

[108] Organization for Security and Co-operation in Europe, *"OSCE-wide Roadmap for Strengthening OSCE Efforts on Youth, Peace and Security (YPS),"* Vienna: OSCE Chairpersonship, December 3, 2025, https://www.osce.org/sites/default/files/documents/publications/2025/12/OSCE%20YPS%20Roadmap.pdf

[109] Organization for Security and Co-operation in Europe, *"Education of Criminal Justice Actors in Central Asia on Cybercrime and Digital Evidence Discussed at Regional Meeting in Tashkent,"* March 10, 2023, https://www.osce.org/secretariat/538713

[110] Organization for Security and Co-operation in Europe (OSCE), Representative on Freedom of the Media, *"Outcome Report: The RFoM's Media Freedom Literacy Roundtable,"* Vienna, December 6, 2022, https://cdn.osce.org/sites/default/files/f/documents/a/3/535905_0.pdf

6.6 Reassessing the OSCE Strategy for the 21st Century

6.6.1 Updating the Cyber CBM Framework to Include Generative AI

Generative AI could enhance CBMs connected to the human dimension of the measures. AI could aid the detection of forms of intolerance and help identify online hate speech.[111] This framework has been established with the Vienna and Moscow mechanisms which were designed to address human rights violations, by promoting the obligation of exchange of information and the response of an expert mission.[112]

Updated CBMs could focus on moving on a purely technical perspective to respond to AI-driven cyberattacks, Zero-fault safeguards and updating risk-control protocols.[113] Moreover, CBMs could apply common norms of AI governance by implementing human oversight or even hybrid models of monitoring. The first option can protect fundamental rights by rendering human monitoring mandatory, while the concept of a hybrid model focuses on efficient data processing by AI but the decision and finalization comes from the human counterpart.[114]

6.6.2 Developing a Regional Code of Conduct for AI Security of the Region

CBMs and frameworks can benefit safeguarding against system failure and manipulation, standards to prevent malicious actors from interfering with the AI algorithms and any misuse of training data.[115] The 2005 Code of Conduct for Election Observers by OSCE serves as a document that can determine the nature of AI within the Organization´s framework.[116] Developing a consensus based Code would be a project of great significance amidst the current geopolitical climate. Russia´s war in Ukraine has called OSCE´s cooperative security in question. Moreover, it is important to take into account the opinion of critics who recognize the rapid rhythm of the evolution of AI. AI legislation

[111] Organization for Security and Co-operation in Europe, "*Artificial Intelligence Poses Risks but Can Also Contribute to More Open and Inclusive Societies, Say Participants at ODIHR Event*." October 6, 2023, odihr.osce.org/odihr/554413.
[112] Strohal, Christian, Very Unfinished Business: The OSCE and Human Rights, 50 years on. Part 3, 2026
[113] Dutton H., *A Decade of Research on Cybersecurity Capacity: Reflections on Themes and Issues for our Emerging Cyber Future. Notes on the Global Cyber Security Capacity Centre´s 2024 Annual Conference,* Global Cyber Security Capacity Centre (GCSCC), 2024
[114] Luordo D. *et al*., Application of Artificial Intelligence as an Aid for the Correction of the Objective Structured Clinical Examination (OSCE), Applied Sciences , Vol. 15, No. 1153, 2025
[115] Permanent Council of the OSCE, "Initial set of the OSCE confidence-building measures to reduce the risks of the conflict stemming from the use of information and communication technologies.", Decision No.1106, 3 December 2013
[116] OSCE, Declaration of principles for international election observation and code of conduct for international election observers, 2005

and Codes are often characterized as "chasing a moving object".[117] Even though the creation of the Code appears a challenge, it is in the best interest of OSCE to commence laying the base work for the creation of rules and red lines concerning the usage of AI. A Code of Conduct regarding AI Security could focus on reinforcing the legal tests and criteria used to identify unlawful manipulation as well as the exploitation of cognitive biases.

6.6.3 OSCE's role in mediating tech related disputes

It is important to point out that OSCE operates in a consensus, one veto can halt missions or budgets.[118] OSCE's RFoM brings forth the need for proper negotiations and mediation between States. A prime example is the Danish Press Publications' Collective Management Organisation (DPCMO) which has initiated mediation against Open AI for unauthorized use of journalism content.[119] Moreover, OSCE supports bargaining Codes like Australia and Canada advocating negotiations and the choice of arbitration when voluntary agreements are not fruitful,[120] especially regarding cyber-related disputes that escalate to violation of human rights, such as surveillance or disinformation propaganda.

Taking into account the evolution of cyberspace, it is possible to expect OSCE to expand to digital transnational aggression and information warfare. Either through transparency and information sharing or regional cooperation with OSCE as the forum of developing shared norms for activities within cyberspace.[121]

[117] Ibid
[118] OSCE. "Decision-Making in the OSCE." *Osce.org*, 2026, www.osce.org/decision-making.
[119] CMO." A united Danish media industry takes OpenAI to court, 2026, dpcmo.dk/a-united-danish-media-industry-takes-openai-to-court
[120] Schiffring *et al*., Safeguarding Media Freedom in the age of Big Tech Platforms and AI, , Office of the Representative on Freedom of the Media Organization for Security and Co-operation in Europe (OSCE), 2025
[121] OSCE. "Cyber/ICT Security." *Osce.org*, 9 Dec. 2016, www.osce.org/field-of-work/Cyber-ICT-security.

6.7 Case Studies

6.7.1 Asian Partners

Engagement in cyberspace and digital resilience among its Asian Partners for Cooperation[122], such as Japan[123], South Korea, and Australia[124], reflects the regional and multi-stakeholder dimension of modern cyber governance in the context of OSCE[125]. These global technology leaders, which are often subject to targeted cyber operations by states or their proxies involving state-of-the-art AI technology, play a vital role in shaping norms and rules concerning responsible state behavior in cyberspace. An example of such inter-regional cooperation and collaboration includes cooperation between OSCE and ASEAN Regional Forum (ARF), which is related to the development of PoC networks as well as the implementation of CBMs aimed at minimizing risks of miscalculation. Another strength is that Asian Partners for Cooperation has demonstrated strong capabilities in terms of multi-stakeholder governance, effectively bridging the divide between the realm of foreign policy decision-making and private sector companies. This is because most advanced AI algorithms, semiconductor supply chains, and other technologies are designed and developed by tech companies, whose headquarters are located in these regions. Hence, countries such as South Korea or Japan demonstrate an important ability to combine private security protocols with official foreign policy doctrines.

6.7.2 OSCE Special Monitoring Mission in Ukraine (SMM)

The OSCE Special Monitoring Mission in Ukraine serves as a primary case study for the operational use of ICT and AI tools in conflict prevention. The mission relied on advanced technological infrastructure, which also exposed the vulnerabilities of modern ICTs in unstable environments. The SMM underscores that while AI and modern technologies play a pivotal role in decision-making and

[122] "Asian Partners for Co-Operation," Osce.org, 2026, https://www.osce.org/partners-for-cooperation/asian.
[123] "Japan: The OSCE's First Asian Partner for Co-Operation," Osce.org, November 15, 2024, https://www.osce.org/magazine/372946.
[124] "Organization for Security and Co-Operation in Europe GRANTING of the STATUS of PARTNER for CO-OPERATION to AUSTRALIA," 2009. https://cdn.osce.org/sites/default/files/f/documents/d/5/40712.pdf
[125] EEAS, "EU Statement on Financial Technology Innovations: Challenges to Cyber/ ICT Security and Opportunities for Securing SDGs," June 18, 2018, https://www.eeas.europa.eu/sites/default/files/osce_asian_contact_group_eu_statement_on_financial_technology_innovations.pdf.

rapid response, if no safeguards are in place, regional stability can be heavily compromised. The mission was discontinued on 31 March 2022.[126]

7. Conclusion

In conclusion, the OSCE's framework on Cyber/ICT security demonstrates a promising and solid yet evolving approach in an increasingly complex digital environment. Through mechanisms promoting cooperation, transparency and communication, reducing the various issues that cause risks in cyberspace. On the face of the rise of artificial intelligence, hybrid threats and important gaps in human rights protection and accountability, OSCE remains emphatic on developing a system of trust and multi-stakeholder engagement albeit the voluntary nature of its measures. Ultimately, OSCE's framework operates as the bas is for security models in the 21st century,reinforcing human oversight, updating the system to match emerging technologies and overall ensuring cooperation and security in the area.

8. Points to be addressed (PtbA)

1. How can participating States enhance and improve secure communication channels and procedures in order to prevent deescalation during ambiguous incidents?
2. To what extent can OSCE States create shared practices against a cyber use of force, despite the non-binding nature of the CBMs?
3. What is the impact of the AI implementation on the Early Warning Systems and how can the Member States strengthen their national status against the possible threats within OSCE's framework?
4. In conflict zones, which are the ethical and legal constraints of Autonomous Systems and what measures can be implemented to combat the issue?

[126] OSCE, "OSCE Special Monitoring Mission to Ukraine (Closed)," www.osce.org, n.d., https://www.osce.org/special-monitoring-mission-to-ukraine-closed.

5. How can the existing PoC system be strengthened and be able to respond efficiently to real-life crises?
6. Which are the main consequences of AI-driven Disinformation and Deepfakes and what actions can the OSCE Member States take to address the issue?
7. How important is the protection of critical infrastructure from ICT-based Attacks and how can the Member States shape the future strategy of the organisation?

9. Bibliography

OSCE. "Cyber/ICT Security." *Osce.org*, 9 Dec. 2016, www.osce.org/field-of-work/Cyber-ICT-security.

OSCE, Declaration of principles for international election observation and code of conduct for international election observers, 2005

OSCE. "Cyber Incident Classification System in Focus of OSCE Workshop." *Osce.org*, 2024, www.osce.org/secretariat/567034.

OSCE. "Decision-Making in the OSCE." *Osce.org*, 2026, www.osce.org/decision-making.

CMO, A united Danish media industry takes OpenAI to court, 2026, dpcmo.dk/a-united-danish-media-industry-takes-openai-to-court

OSCE, Shaping Europe's Digital Future." *Europa.eu*, 2024, digital-strategy.ec.europa.eu/en/policies/digital-services-act.

Permanent Council of the OSCE, "Initial set of the OSCE confidence-building measures to reduce the risks of the conflict stemming from the use of information and communication technologies.", Decision No.1106, 3 December 2013

Schiffring *et al*., Safeguarding Media Freedom in the age of Big Tech Platforms and AI, , Office of the Representative on Freedom of the Media Organization for Security and Co-operation in Europe (OSCE), 2025

OSCE, "History," www.osce.org https://www.osce.org/history

OSCE, "Who We Are | OSCE," Osce.org, 2018, https://www.osce.org/who-we-are.

OSCE , "Institutions and Structures," www.osce.org, n.d., https://www.osce.org/institutions-and-structures

OSCE , "Partners for Co-Operation," www.osce.org, n.d., https://www.osce.org/partners-for-cooperation.

OSCE, "Protecting Civic Space from Growing Digital Threats Requires Sustained Efforts, Leading OSCE Officials Say." *Osce.org*, 11 May 2026, www.osce.org/chairpersonship/664069

OSCE. "Fields of Work." *Osce.org*, 2025, www.osce.org/fields-of-work

U.S. Mission OSCE, "The OSCE Ministerial Council," U.S. Mission to the OSCE, December 2, 2016, https://osce.usmission.gov/osce-ministerial-council/.

Organization for Security and Co-operation in Europe, "*Our Mandate on Conflict Prevention and Resolution.*" 2026, www.osce.org/node/660052

EU AI Act. "High-Level Summary of the AI Act." *EU Artificial Intelligence Act*, Future of Life Institute, 27 Feb. 2024, artificialintelligenceact.eu/high-level-summary/.

Organization for Security and Co-operation in Europe, "*Cyber/ICT Security.*" December 9, 2016, www.osce.org/field-of-work/Cyber-ICT-security.

"Annual OSCE-Wide Conference on Cyber/ICT Security Underscores the Importance of Strengthening National Cyber Resilience." *Osce.org*, 2024, www.osce.org/chairpersonship/573043.

OSCE. *CYBER INCIDENT CLASSIFICATION a Report on Emerging Practices within the OSCE Region 2 Published by the Organization for Security and Co-Operation in Europe*. 2022.

Organization for Security and Co-operation in Europe (OSCE), *"Conflict Prevention and Resolution,"* accessed April 21, 2026, https://www.osce.org/field-of-work/conflict-prevention-and-resolution

OSCE ODIHR. *Think Again: Freedom of Thought in the Age of Artificial Intelligence POLICY BRIEF*, 2025.

10 Years of OSCE Cyber/ICT Security Confidence-Building Measures, A Brochure by OSCE

Nye, Joseph. "Deterrence and Dissuasion in Cyberspace." *International Security*, vol. 41, no. 3, 2017

Organization for Security and Co-operation in Europe, *"Principles and Commitments,"* accessed April 21, 2026, https://www.osce.org/node/650180

Office of the Historian, U.S. Department of State, *"The Helsinki Final Act, 1975,"* accessed April 21, 2026, https://history.state.gov/milestones/1969-1976/helsinki

Organization for Security and Co-operation in Europe, *"Helsinki Final Act,"* August 1, 1975, https://www.osce.org/mc/17502

NATO Cooperative Cyber Defence Centre of Excellence, *"OSCE Confidence-Building Measures for Cyberspace,"*accessed April 21, 2026, https://ccdcoe.org/incyder-articles/osce-confidence-building-measures-for-cyberspace/

NATO Cooperative Cyber Defence Centre of Excellence, *"OSCE Expands Its List of Confidence-Building Measures for Cyberspace: Common Ground on Critical Infrastructure Protection,"* accessed April 21, 2026, https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/

United Nations, *"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,"* UN Doc. A/70/174 (July 22, 2015), https://digitallibrary.un.org/record/799853

European Commission, *"AI Act (Regulatory Framework for Artificial Intelligence),"* accessed April 21, 2026, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

CCDCOE. "Tallinn Manual 2.0." *Ccdcoe.org*, 2017, ccdcoe.org/research/tallinn-manual/

IRIS – BH, *"Tallinn Manual and the Use of Force,"* accessed April 21, 2026, https://irisbh.com.br/en/tallinn-manual-and-the-use-of-force/.

Permanent Council of the OSCE, "OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Decision No. 1202, 10 March 2016.

OSCE. (2023). "Cyber Incident Classification: A Report on Emerging Practices within the OSCE region." Transnational Threats Department, OSCE Secretariat

Martino, L. (2018). "Give Diplomacy a Chance: OSCE's Red Lines in Cyberspace." Center for Cyber Security and International Relations Studies (CCSIRS), Commentary

United Nations. "Early Warnings for All." *United Nations*, 2023, www.un.org/en/climatechange/early-warnings-for-all.

Ioana Puscas, *"AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures,"* Geneva: United Nations Institute for Disarmament Research (UNIDIR), October 12, 2023, https://unidir.org/wp-content/uploads/2023/10/UNIDIR_AI-international-security_understanding_risks_paving_the_path_for_confidence_building_measures.pdf

AlgorithmWatch. "A Guide to the Digital Services Act, the EU's New Law to Rein in Big Tech." *AlgorithmWatch*, 21 Sept. 2022, algorithmwatch.org/en/dsa-explained/.

Max Murphy, Ezra Sharpe, and Kayla Huang, *"The Promise of Machine Learning in Violent Conflict Forecasting,"*Cambridge University Press, *Data & Policy* 6 (2024): e35, published August 30, 2024, https://www.cambridge.org/core/journals/data-and-policy/article/promise-of-machine-learning-in-violent-conflict-forecasting/40D559ADA18FF7308915B08956B4E8F3

Organization for Security and Co-operation in Europe, *"Ministerial Council Decision No. 3/11: Elements of the Conflict Cycle Related to Enhancing the OSCE's Capabilities in Early Warning, Early Action, Dialogue Facilitation and Mediation Support, and Post-Conflict Rehabilitation,"* Vilnius, December 7, 2011, https://cdn.osce.org/sites/default/files/f/documents/6/b/86621.pdf

United Nations Office for Disarmament Affairs, *"Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems,"* UN Doc. CCW/GGE.1/2019/3 (2019), https://documents.unoda.org/wp-content/uploads/2020/09/CCW_GGE.1_2019_3_E.pdf

Organization for Security and Co-operation in Europe, *"Decision No. 3/18: Strengthening Efforts to Prevent and Counter Terrorism,"* Milan, December 7, 2018, https://cdn.osce.org/sites/default/files/f/documents/d/6/487054.pdf

Paul Scharre and Kelley Sayler, *"Autonomous Weapons and Human Control,"* Center for a New American Security (CNAS), n.d., https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS_Autonomous_Weapons_poster_FINAL.pdf

Future of Life Institute, *"A Diplomat's Guide to Autonomous Weapons Systems,"* August 5, 2024 (updated September 17, 2024), https://futureoflife.org/wp-content/uploads/2024/08/AWS-Guide-for-Diplomats_17-September-2024.pd

Organization for Security and Co-operation in Europe, *"Conflict Prevention and Resolution,"* accessed April 21, 2026, https://www.osce.org/field-of-work/conflict-prevention-and-resolution

Organization for Security and Co-operation in Europe, *"The OSCE Forum for Security Co-operation,"* Vienna, n.d., https://cdn.osce.org/sites/default/files/f/documents/5/a/77535_1.pdf

Organization for Security and Co-operation in Europe, *"Code of Conduct on Politico-Military Aspects of Security,"*Budapest, December 3, 1994, https://cdn.osce.org/sites/default/files/f/documents/5/7/41355.pdf.

United Nations Office for Disarmament Affairs, *"Convention on Certain Conventional Weapons (CCW): Group of Governmental Experts on Lethal Autonomous Weapons Systems – Rolling Text (Status as of 18 December 2025),"* UN Doc. CCW/GGE/LAWS (2025), https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_%282026%29/CCW_GGE_LAWS_Rolling_Text_-_status_18_December_2025.pdf

Natalia Jevglevskaja, *"Weapons Review Obligation under Customary International Humanitarian Law: The Case of Article 36 of Additional Protocol I," International Law Studies* 94 (2018), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1231&context=ils

International Committee of the Red Cross (ICRC), *"Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977 – Article 36,"* accessed April 21, 2026, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977?activeTab=

Jie Guo, *"The Ethical Legitimacy of Autonomous Weapons Systems: Reconfiguring War Accountability in the Age of Artificial Intelligence,"* *Ethics & Global Politics* 18, no. 3 (2025): 27–39, https://www.tandfonline.com/doi/full/10.1080/16544951.2025.2540131.

Organization for Security and Co-operation in Europe, *"Factsheet of the OSCE Forum for Security Co-operation,"*January 21, 2020, https://www.osce.org/forum-for-security-cooperation/factsheet

Anastasiia Romanishyn, *"AI-Driven Disinformation: Policy Recommendations for Addressing Emerging Threats,"Frontiers in Communication* (2025), accessed April 21, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12351547/

Springer Nature, *"Article Collection,"* accessed April 21, 2026, https://link.springer.com/collections/diiijiiibh.

Organization for Security and Co-operation in Europe, *"Project PROTECT: Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks,"* Vienna: OSCE Secretariat, October 29, 2025, https://cdn.osce.org/sites/default/files/f/documents/d/c/508292.pdf

Organization for Security and Co-operation in Europe, *"OSCE Representative on Freedom of the Media,"* accessed April 21, 2026, https://rfom.osce.org/

Anastasiia Romanishyn, *"AI-Driven Disinformation: Policy Recommendations for Addressing Emerging Threats,"Journal of Information Security and Applications* (2025), https://www.sciencedirect.com/science/article/pii/S2199853125000824

CrowdStrike, *"12 Most Common Types of Cyberattacks,"* accessed April 21, 2026, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

Organization for Security and Co-operation in Europe, *"Our Mandate on Cyber/ICT Security,"* accessed April 21, 2026, https://www.osce.org/node/660054

Organization for Security and Co-operation in Europe, *"Decision No. 5/16: OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies,"* Hamburg, December 9, 2016, https://www.osce.org/cio/288086.

Organization for Security and Co-operation in Europe, *"Cyber/ICT Security,"* accessed April 21, 2026, https://www.osce.org/field-of-work/Cyber-ICT-security

Organization for Security and Co-operation in Europe, *"Declaration on the Digital Economy as a Driver for Promoting Co-operation, Security and Growth,"* Milan, December 7, 2018, https://cdn.osce.org/sites/default/files/f/documents/a/5/405920.pdf

Organization for Security and Co-operation in Europe, *"National Cyber Incident Classification Handbook,"* Vienna: OSCE Secretariat, 2025, https://cdn.osce.org/sites/default/files/f/documents/e/a/600455.pdf

Organization for Security and Co-operation in Europe, *"Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,"* Vienna, March 10, 2016, https://cdn.osce.org/sites/default/files/f/documents/d/a/227281.pdf

Matar, R., & Murray, D. "Identity and the Right to Privacy in the Age of AI Surveillance." Human Rights Law Review,2026

Kosta, E. "Algorithmic state surveillance: Challenging the notion of agency in human rights." Regulation & Governance, 2020

Feldstein, S. "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace, Working Paper, 2019

Zuboff, S. "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization." Organization Theory, 2022

Steffen, B. (Ed.). Bridging the Gap Between AI and Reality: First International Conference, AISoLA 2023, 2025

Carter, C."The Digital Surveillance of Workers: A Human Rights Perspective." European Labour Law Journal, 16(2), 2025

Atif, M., & Alamgir, A. "The Illusion of Security: How AI-Powered Surveillance Erodes Privacy, Amplifies Inequality, and Redefines Democracy in the Digital Age." Social Science Review Archives, 3(4), 2025

Organization for Security and Co-operation in Europe "*Confidence Building in the OSCE*."September 24, 2012, www.osce.org/secretariat/106440

Organization for Security and Co-operation in Europe, *"Annual Report 2024,"* Vienna: OSCE Secretariat, February 13, 2026, https://www.osce.org/sites/default/files/documents/publications/2026/02/Annual%20Report%202024%2010.02.2026%20REV1%20docx.pdf.

Organization for Security and Co-operation in Europe, *"OSCE Promotes Classification System for Cyber Incidents to Strengthen Cyber Security in Ukraine,"* January 30, 2025, https://www.osce.org/secretariat/585169

Organization for Security and Co-operation in Europe, *"Cyber Diplomacy in Focus of OSCE-Organized Course in Turkmenistan,"* November 27, 2025, https://ashgabat.osce.org/centre-in-ashgabat/602870

Organization for Security and Co-operation in Europe (OSCE), Representative on Freedom of the Media,*"Safeguarding Media Freedom in the Age of Big Tech Platforms and AI,"* Vienna, October 6, 2025, https://rfom.osce.org/sites/default/files/f/documents/e/3/598525_1.pdf

Organization for Security and Co-operation in Europe, *"OSCE-wide Roadmap for Strengthening OSCE Efforts on Youth, Peace and Security (YPS),"* Vienna: OSCE Chairpersonship, December 3, 2025, https://www.osce.org/sites/default/files/documents/publications/2025/12/OSCE%20YPS%20Roadmap.pdf

Organization for Security and Co-operation in Europe, *"Education of Criminal Justice Actors in Central Asia on Cybercrime and Digital Evidence Discussed at Regional Meeting in Tashkent,"* March 10, 2023, https://www.osce.org/secretariat/538713

Organization for Security and Co-operation in Europe (OSCE), Representative on Freedom of the Media,*"Outcome Report: The RFoM's Media Freedom Literacy Roundtable,"* Vienna, December 6, 2022, https://cdn.osce.org/sites/default/files/f/documents/a/3/535905_0.pdf

Organization for Security and Co-operation in Europe, *"Recommendations on the Effective Participation of National Minorities in Social and Economic Life & Explanatory Note,"* The Hague: OSCE High Commissioner on National Minorities, October 2023, https://cdn.osce.org/sites/default/files/f/documents/2/3/553783.pdf

Organization for Security and Co-operation in Europe Academy, *"OSCE Academy in Bishkek,"* accessed April 21, 2026, https://osce-academy.net

Strohal, Christian, Very Unfinished Business: The OSCE and Human Rights, 50 years on. Part 3, 2026

Dutton H., *A Decade of Research on Cybersecurity Capacity: Reflections on Themes and Issues for our Emerging Cyber Future. Notes on the Global Cyber Security Capacity Centre's 2024 Annual Conference,* Global Cyber Security Capacity Centre (GCSCC), 2024

Luordo D. *et al*., Application of Artificial Intelligence as an Aid for the Correction of the Objective Structured Clinical Examination (OSCE), Applied Sciences , Vol. 15, No. 1153, 2025

Organization for Security and Co-operation in Europe, "*Artificial Intelligence Poses Risks but Can Also Contribute to More Open and Inclusive Societies, Say Participants at ODIHR Event*." October 6, 2023, odihr.osce.org/odihr/554413.

Bitdefender. "What Are Cyberattacks - Bitdefender InfoZone," 2024. https://www.bitdefender.com/en-us/business/infozone/what-is-a-cyber-attack.

Bizmanualz. "What Does Point of Contact Mean?," October 30, 2023. https://www.bizmanualz.com/library/what-does-point-of-contact-mean?srsltid=AfmBOopsMMubmDBu0vWOE89-JXKKJoWXQ-n_aSJ2-mbCBn1wZkG_yu-P.

Consilium. "Hybrid Threats," 2019. https://www.consilium.europa.eu/en/policies/hybrid-threats/.

proofpoint. "Deepfake Technology." Proofpoint, August 26, 2024. https://www.proofpoint.com/us/threat-reference/deepfake.

Stryker, Cole, and Eda Kavlakoglu. "What Is Artificial Intelligence (AI)?" IBM, August 9, 2024. https://www.ibm.com/think/topics/artificial-intelligence.

United Nations Office for Disaster Risk Reduction. "Early Warning System." www.undrr.org, 2024. https://www.undrr.org/terminology/early-warning-system.

www.csis.org. "Confidence-Building Measures | Cross-Strait Security Initiative | CSIS," n.d. https://www.csis.org/programs/international-security-program/isp-archives/asia-division/confidence-building-measures.

ec.europa.eu. "Glossary:Information and Communication Technology (ICT)," n.d. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT).