Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination.

The Use of Technology by Mercenaries, Mercenary Related Actors, and PMSCs in the Services, Operations, and Activities.

Annex – Glossary of Terms

Advertising-technology (Ad-tech) ecosystems: Ad-tech describes tools that process and organise information (including personal data) for online advertising purposes and automate the handling of advertising transactions.[1] In this context, 'ecosystems' refers to the variety of actors involved in this process, e.g. advertisers, publishers, Data Management Platforms (DMPs), Demand Side Platforms (DSPs), Supply Side Platforms (SSPs), and Consent Management Platforms (CMPs).[2]

Artificial intelligence: a "constellation" of processes and technologies that enable computers to perform tasks traditionally carried out by humans, such as decision-making and problem-solving.[3] The European Union's AI Act defines an AI system as a machine-based system designed to operate with varying levels of autonomy, capable of adapting after deployment, and able to generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.[4] ICoCA and ICT4Peace Toolkit for the Responsible Use of Technologies by Private Security Services, in Tool 8, define artificial intelligence as "The development of computer systems that can perform tasks typically requiring human intelligence, such as visual perception, speech recognition, decision-making, and language translation."[5]

Autonomous or semi-autonomous platforms: 'Autonomous' and 'semi-autonomous' refers to the level of human control employed during the operation of such platforms6, for example, use the term 'platform' in the context of airborne platforms and weapons platforms, indicating that it refers to a physical carrier of capability.[7]. Autonomous platforms can transport supplies and ammunition to soldiers and offer in-theatre mobility".[8]

Automated security robots: autonomous machines (ground-based or flying) that are primarily used to enhance the safety and security of various spaces through surveillance and monitoring. They combine self-navigation with visual and thermal imaging to collect and analyse data

[1] ICO, Update report into adtech and real time bidding, https://ico.org.uk/media2/migrated/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf para 2.1.
[2] ICO, Update report into adtech and real time bidding, https://ico.org.uk/media2/migrated/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf para 2.5.
[3] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/73/348), https://docs.un.org/en/A/73/348 para 3.
[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 Article 3(1).
[5] ICoCa, Tool 8: Emerging Technologies and Future Trends in Private Security, https://icoca.ch/wp-content/uploads/2024/11/Tool-8-Emerging-Technologies-and-Future-Trends-in-Private-Security.pdf para 3.1.
[6] DoD Directive 3000.09, Autonomy in Weapon Systems, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf p 21 and 23; ICoCa, Tool 8: Emerging Technologies and Future Trends in Private Security, https://icoca.ch/wp-content/uploads/2024/11/Tool-8-Emerging-Technologies-and-Future-Trends-in-Private-Security.pdf Glossary, p 47.
[7] DoD Dictionary of Military and Associated Terms, Joint Publication 1-02, https://edocs.nps.edu/2014/December/jp1_02.pdf p 117 and 209; Defence and Security Accelerator, Guidance on Affordable and Adaptable Unmanned Air Systems Autonomy, https://www.gov.uk/government/publications/competition-affordable-and-adaptable-unmanned-air-systems-autonomy/affordable-and-adaptable-unmanned-air-systems-autonomy.
[8] EDA Action Plan on Autonomous Systems, https://eda.europa.eu/docs/default-source/brochures/eda---apas-brochure---final-(1).pdf p 5.

while patrolling indoor and outdoor spaces. The data goes back to a central control hub in real-time which uses artificial intelligence to assess and report any credible threats or safety risks.[9]

Autonomous systems: systems that can perform tasks or make decisions independently, without direct human control or intervention.10

Autonomous weapon systems: any weapon system with autonomy in its critical functions - that is, a weapon system that can select (search for, detect, identify, track or select) and attack (use force against, neutralize, damage or destroy) targets without human intervention.11

Cloud infrastructure: comprises the hardware (e.g. servers, storage and networks) and software (e.g. APIs, cloud security features and AI-powered management tools) that enables the delivery and operation of cloud computing services, such as processing, storage or networking of resources.[12]

Data brokerage: 'data brokerage' is the (often covert) collection and reselling or sharing of consumers' personal information by companies as a business model, e.g. for verification of an individual's identity, marketing of products, or detection of fraud.[13]

Digital surveillance: d in an operational definition, digital surveillance is a pervasive ecosystem of digital and data infrastructures operated by both State and non-State actors that work in concert to track, identify, and monitor individuals. This system is characterised by a lack of transparency and a remote, invisible nature that prevents subjects from knowing when or how they are being watched, creating significant power asymmetries.[14]

Information operations: the integrated deployment of information-related capabilities (IRCs), alongside other operational activities to influence, disrupt, corrupt or usurp the decision-making capability of adversaries, potential adversaries, and audiences in support of mission objectives while safeguarding one's own understanding and capability.[15] Information operations can be conducted in times of peace, crisis and conflict.[16]

---

[9] SASA Surveillance, Why Automated Security Robots are the Next Big Thing, https://sasasurveillance.com/why-automated-security-robots-are-the-next-big-thing/.

[10] ICoCa, Tool 8: Emerging Technologies and Future Trends in Private Security, https://icoca.ch/wp-content/uploads/2024/11/Tool-8-Emerging-Technologies-and-Future-Trends-in-Private-Security.pdf Glossary, p 47.

[11] ICRC Position on Autonomous Weapons, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

[12] ISO Information technology — Cloud computing — Overview and vocabulary (ISO/IEC 22123-1:2023), https://www.iso.org/standard/60544.html para 3.5.3; ITU Recommendation ITU-T Y.3500 - Information technology – Cloud computing – Overview and vocabulary, https://www.itu.int/epublications/publication/itu-t-y-3500-2014-08-information-technology-cloud-computing-overview-and-vocabulary para 3.2.25; See also IBM, What is cloud infrastructure?, https://www.ibm.com/think/topics/cloud-infrastructure; Microsoft, What is cloud infrastructure?, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-infrastructure.

[13] Federal Trade Commission, Data Brokers, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf p i.

[14] Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights: report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, Gina Romero, https://digitallibrary.un.org/record/4113878?ln=en&v=pdf pp 3 and 4.

[15] Joint Publication 3-13 Information Operations, https://informationsecurity.info/wp-content/uploads/2021/04/jp3_13.pdf p ix; Allied Joint Publication-10.1 Allied Joint Doctrine for Information Operations, https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf p 25; NATO Military Policy on Information Operations, https://shape.nato.int/resources/3/images/2018/upcoming%20events/MC%20Draft_Info%20Ops.pdf para 9.

[16] Allied Joint Publication-10.1 Allied Joint Doctrine for Information Operations, https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf p xix.

Intelligence, Surveillance and Reconnaissance (ISR): the organized gathering, analysis and sharing of information that helps decision-making in defense, security, and crisis response operations and it provides for the situational awareness in modern military and civil protection efforts, providing the necessary insights to detect threats, track movements, and respond effectively to evolving scenarios.[17] It is also described as information provided to decision-makers and action-takers for better situational awareness of the conditions on the ground, air, sea, space and in the cyber domain. Allies work together to collect, analyse and share information to maximum effect.[18]

Machine learning: machine learning constitutes a core subset of AI, that focuses on the development of algorithms that enable computer systems to learn and improve their performance on a specific task over time, without being explicitly programmed.19 It refers to a category of AI techniques through which algorithms are trained on datasets in order to recognise patterns and solve problems. These methods underpin many contemporary applications of AI, including predictive analytics, surveillance systems, and autonomous decision-making tools.[20]

Open Source Investigations (OSINT): can be broadly defined as the systematic collection, verification, analysis and preservation of information that any member of the public can observe, purchase or request, without requiring special legal status or unauthorized access.[21] OSINT differs from traditional evidence gathering processes as it relies on legally accessible and open materials over covert operations or classified channels.[22]

Predictive analytics: the use of data, statistical algorithms, and machine learning techniques to identify the likelihood of future outcomes based on historical data.[23]

Satellite, geospatial, and signals intelligence: Information derived from satellite imagery, remote sensing, geospatial analysis and intercepted electronic signals to support monitoring, assessment and decision-making. Geospatial Intelligence provides for the exploitation and analysis of imagery and geospatial information to assess, and visually depict the physical features and geographically referenced activities on the earth.[24]

Synthetic media: artificially generated or manipulated images, audio, or video produced through machine learning techniques, often with a high degree of realism.[25]

---

[17] Elistair Intelligence, Surveillance and Reconnaissance, https://elistair.com/glossary/intelligence-surveillance-reconnaissance/.
[18] NATO Intelligence, Surveillance and Reconnaissance Force (NISRF), https://www.nato.int/en/what-we-do/deterrence-and-defence/nato-intelligence-surveillance-and-reconnaissance-force-nfpvf.
[19] ICoCa, Tool 8: Emerging Technologies and Future Trends in Private Security, https://icoca.ch/wp-content/uploads/2024/11/Tool-8-Emerging-Technologies-and-Future-Trends-in-Private-Security.pdf para 3.1 and Glossary, p 47.
[20] ICoCa, Tool 8: Emerging Technologies and Future Trends in Private Security, https://icoca.ch/wp-content/uploads/2024/11/Tool-8-Emerging-Technologies-and-Future-Trends-in-Private-Security.pdf para 10.1; See also ICRC Artificial intelligence and machine learning in armed conflict: A human-centred approach, https://www.icrc.org/sites/default/files/document_new/file_list/ai_and_machine_learning_in_armed_conflict-icrc.pdf para 1.
[21] United Nations Berkley Protocol on Digital Open-Source Investigations, https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf p 7.
[22] United Nations Berkley Protocol on Digital Open-Source Investigations, https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf p 7.
[23] ICoCa, Tool 8: Emerging Technologies and Future Trends in Private Security, https://icoca.ch/wp-content/uploads/2024/11/Tool-8-Emerging-Technologies-and-Future-Trends-in-Private-Security.pdf Glossary, p 47.
[24] Geospatial Intelligence Basic Doctrine, https://www.nga.mil/assets/files/170901-038_GEOINT_Basic_Doctrine_Pub_1.pdf p 3.
[25] ICO, Synthetic media and its identification and detection, https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-and-ico-tech-futures/tech-horizons-report-2025/synthetic-media-and-its-identification-and-detection/; UN, Artificial intelligence: What are deepfakes?, https://unric.org/en/artificial-intelligence-what-are-deepfakes/; INTERPOL, Beyond Illusions, https://www.interpol.int/content/download/21179/file/BEYOND%20ILLUSIONS_Report_2024.pdf p 7.

Uncrewed aerial systems (UAS): uncrewed aerial systems as an overarching term for a system whose component includes one or more unmanned aircraft, the supporting network and all the equipment and personnel necessary to control the unmanned aircraft.[26]

Digital surveillance: d
Spyware: umbrella term for intrusive monitoring software which enables covert monitoring by secretly accessing and penetrating a device without the user's awareness and allows the operator to monitor the location, read communication, extract data, and control hardware, software and features of the device (e.g camera and microphone).[27]

Crypto-assets: a type of private asset that depends primarily on blockchain to secure digital value or contractual rights; they can be transferred, stored or traded electronically.[28] According to the EU Markets in Crypto Assets Regulation (2023/1114), it means "a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology."[29]

Cloud computing: a delivery model for information technology (IT) services which permits remote access to shared computing services and data storage capacity typically through the internet.[30] , over the internet, including servers, storage, databases, networking, software, and analytics.31

Cyber operation: the employment of cyber capabilities to achieve objectives in or through cyberspace.[32] Under international humanitarian law, certain cyber operations may qualify as 'attacks' where they are reasonably expected to cause – directly or indirectly –damage, destruction of objects (such as infrastructure and, arguably, data) or injury or death of people. It does not include cyber operations aimed at obtaining unauthorized access to information.

Dual-use technology (such as e.g. uncrewed aerial devices, also referred to as drones, or as 'unmanned aerial vehicles'): refers to items, including software and technology, that can be used for both civilian and military purposes. This typically includes items that can be used for

[26] United Nations Use of Unmanned Aircraft System Capabilities Guidelines, https://resourcehub01.blob.core.windows.net/training-files/Training%20Materials/042%20PKISR%20RTP/042-023%20Ref%202%20-%202019.05%20UAS%20Guidelines%20February.pdf p 4 para 5.
[27] Venice Commission, Report on a rule of law and human rights compliant regulation of spyware, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)043-e para 7; Belgrade Center for Security Policy, Policy Paper/1, https://bezbednost.org/wp-content/uploads/2026/06/PPaper-1-eng-fin.pdf p 3; United Nations Spyware and surveillance: Threats to privacy and human rights growing, UN report warns, https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.
[28] European Parliament, Understanding crypto assets An overview of blockchain technology's uses and challenges, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757580/EPRS_BRI%282023%29757580_EN.pdf p 5; See also OECD, International Standards for Automatic Exchange of Information in Tax Matters, https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/international-standards-for-automatic-exchange-of-information-in-tax-matters_ab3a23bc/896d79d1-en.pdf Section IV A. (1).
[29] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114 Article 3(1)(5).
[30] ICoCa, Tool 8: Emerging Technologies and Future Trends in Private Security, https://icoca.ch/wp-content/uploads/2024/11/Tool-8-Emerging-Technologies-and-Future-Trends-in-Private-Security.pdf Glossary, p 47.
[31] ICoCa, Tool 8: Emerging Technologies and Future Trends in Private Security, https://icoca.ch/wp-content/uploads/2024/11/Tool-8-Emerging-Technologies-and-Future-Trends-in-Private-Security.pdf Glossary, p 47.
[32] ICRC Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Glossary#C.

the design, development and production of nuclear, chemical, or biological weapons, as well as other weapons of mass destruction.[33]

Geospatial intelligence (GEOINT): a discipline that comprises the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on Earth. It combines several disciplines such as mapping, charting, imagery analysis, and imagery intelligence. The basic principle of GEOINT is to organize and combine all available data around its geographical location on Earth and then exploit it in order to prepare products that can be easily used by planners, emergency responders and decision makers.[34]

Information and communications technology (ICT) systems - are defined, for example in Article 2(a) of the UN Cybercrime Convention, as interconnected devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data.[35]

[33] Centre for Future Generations, https://cfg.eu/double-edged-tech/; Wassenaar Arrangement, https://www.wassenaar.org/the-wassenaar-arrangement/.
[34] United Nations Geospatial and Location Data, https://www.un.org/geospatial/mapsgeo.
[35] UN Cybercrime Convention, https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html Article 2(a).