SIPRI Research Policy Paper
November 2025

THE MILITARIZATION OF TECHNOLOGY: PREVENTING DIVERSION AND MISUSE THROUGH EXPORT CONTROLS

MARK BROMLEY AND GIOVANNA MALETTA*

SUMMARY

● Processes associated with the militarization of technology are leading to a blurring of distinctions in the way civilian technologies and military and security equipment are developed and produced. As a result, technologies and systems that would previously have been classed as 'civilian' may need to be reclassified as 'dual-use items'. This SIPRI Research Policy Paper examines some of the diversion and misuse risks generated by these developments and assesses potential policy responses through an analysis of facial recognition technologies and their incorporation into military and security equipment. Export controls could be used to address or mitigate the risks that are being created but would need to be complemented by additional policy tools, including human rights due diligence.

I. Introduction

The 'militarization of technology' is a broad term that is used to refer to a range of interlinked processes that are eroding traditional distinctions between the ways in which civilian technologies and military and security equipment are produced and used. These processes include the deployment of 'data-intensive systems for military purposes', situations where companies and start-ups that have 'developed commercial and civilian infrastructure technologies' enter the defence sector, and the repurposing and adaption of technologies developed for use in conflict zones for commercial purposes.[1]

Among the areas where these distinctions are breaking down most clearly is in the production of military and security equipment—that is, equipment that is developed and deployed for military and security end-uses carried out by armed forces, law enforcement agencies, intelligence agencies and private security companies—and the increasing importance of civilian technologies and dual-use items in this domain. States and arms manufacturers are expanding the range of situations in which civilian technologies are used in the production of military and security equipment. As a result, technologies and systems that would previously have been classed as 'civilian' may need to be reclassified as 'dual-use items' (i.e. goods, software and technology that can be used for both civilian and military applications).[2] States are also encouraging companies and research and academic institutes to develop technologies and systems that are dual use 'by design', and that can be incorporated into military and security equipment or deployed as military and security equipment. These processes could create new categories of dual-use items.

These shifts create new risks for the governments, companies and research and academic institutes involved. Any expansion in the range of situations in which civilian technologies are incorporated into military and security equipment, as well as the creation of technologies and systems that are dual use 'by design', forms new pathways through which military and security equipment can be produced. It also increases the range of companies and research and academic institutes that are directly or indirectly involved in the production of military and security equipment. These shifts create

[1] Privacy International, 'What is militarisation of tech?', 12 Sep. 2025.
[2] European Commission, 'Exporting dual-use items', [n.d.].

* This paper forms part of SIPRI's contribution to a project on the Militarisation of Technology that is being led by Privacy International with funding provided by Luminate. See https://privacyinternational.org/campaigns/militarisation-of-tech

new avenues through which military and security equipment can reach criminals, terrorists or states that might use it in connection with violations of international human rights law (IHRL, 'human rights') or international humanitarian law (IHL).

These shifts and the risks that they generate are demonstrated in the case of facial recognition technologies (FRTs), which are a type of biometric technology that can be used to recognize an individual's identity based on their facial features. FRTs have mainly been developed in the civilian sector and have a wide range of civilian applications, but they are also being incorporated into military and security equipment. Companies and research and academic institutes are also being encouraged—and are seeking—to develop FRTs, and systems that employ FRTs, that are dual use by design. Finally, concerns about risks of diversion and misuse have been raised in connection with FRTs and military and security equipment that incorporates FRTs.

Export controls enable states to require companies and research institutes to request approval before exporting military and security equipment and dual-use items. This allows states to prevent exports that might be diverted to unauthorized end-users or used in ways that violate human rights or IHL. Certain types of FRTs and military and security equipment that incorporate FRTs are already captured by states' export controls. The European Union (EU) and the United States have also discussed creating new categories of export controls to capture FRTs. These controls and discussions highlight the possibilities and limitations of using export controls to address some of the challenges generated by the militarization of technology, and particularly the creation of new categories of dual-use items.

States are often unwilling to use export controls to regulate technologies that are widely used in commercially available civilian systems, as is the case with FRTs. States are also keen to achieve broad multilateral consensus before new export controls are adopted, and the systems for reaching these types of agreement are experiencing significant strain. Export controls operate most effectively when the exporters of controlled items are aware of their regulatory obligations, but many of the companies and research and academic institutes that are developing FRTs might not be familiar with these instruments. Finally, there are problems when it comes to implementing and enforcing controls on items that can be transferred by electronic means, as is the case with the software that enables FRTs to operate.

Export controls can mitigate some of the risks of misuse and diversion associated with FRTs and other categories of dual-use items that could be created by the militarization of technology. To operate effectively, however, states will need to think carefully about identifying the appropriate technical parameters to ensure that the controls are feasible and proportionate. There are also limits to what export controls can achieve without disrupting the trade in civilian technologies. These limits are likely to become more apparent as export controls are confronted with a progressive blurring of traditional distinctions in the way that civilian technologies and military and security equipment are developed and manufactured. To fully address risks of misuse and diversion, export controls will need to be complemented by other soft-law instruments, such as requiring companies to embed human rights due diligence processes in the conduct of their business.

This SIPRI Research Policy Paper examines some of the risks generated by the militarization of technology, and particularly by the creation of new categories of dual-use items, through a close analysis of FRTs and their incorporation into military and security equipment. Section II outlines ongoing efforts to incorporate civilian technologies into the production of military and security equipment and develop items and systems that are dual use by design. It focuses on the development of FRTs, their incorporation into military and security equipment and the concerns that have been raised about diversion and misuse. Section III examines the role of export controls in regulating the trade in military and security equipment and dual-use items. It focuses on the extent to which military and security equipment that incorporates FRTs is captured by existing export controls, US and EU discussions on creating new controls and the role that other regulatory instruments can play in preventing diversion and misuse. Section IV presents conclusions and recommendations for states, companies and academic and research institutes. It focuses on how to address gaps in export controls and maximize the synergies between these tools and other regulatory instruments.

II. Civilian technologies, the production of military and security equipment and the case of FRTs

The incorporation of civilian technologies into military and security equipment

The process by which civilian technologies are incorporated into the production of military and security equipment is complex and the dynamics vary depending on the types of technology, components and equipment involved and the specific ways in which incorporation takes place.[3] At the broader level, there is a general consensus that there has been a shift since the 1990s away from processes of 'spin off'—in which companies in the defence sector develop technologies that are of broader benefit to the civilian sector—towards processes of 'spin in', 'spin on' or 'spin together'—in which arms manufacturers use technologies developed in the civilian sector.[4] Key drivers have been falling research and development (R&D) spending in the defence sector since the end of the cold war and the emergence of a civilian sector that is a more important source of and location for R&D spending and technological innovation. As a result, companies and research and academic institutes in the civilian sector have been at the forefront of developing technologies, including in the fields of cloud computing, semiconductors and artificial intelligence (AI), that the defence sector has sought to incorporate into the systems they produce.

[3] See te Kulve, H. and Smit, W. A., 'Civilian–military co-operation strategies in developing new technologies', *Research Policy*, vol. 32, no. 6 (June 2003), pp. 955–70.

[4] Stowsky, J., 'From spin-off to spin-on: Redefining the military's role in technology development', *UC Berkeley: Berkeley Roundtable on the International Economy*, 27 Jan. 2005; Evron, Y., 'Military-civil fusion: A conceptual framework', *The Fourth Industrial Revolution and Military-Civil Fusion: A New Paradigm for Military Innovation?* (Cambridge University Press: Cambridge, 2023); and Reuven, N. and Shamir, E., 'The shift in technological dominance and the adaption of open innovation by the defence sector', *Defense & Security Analysis*, vol. 41, no. 3 (July 2025).

States have sought to both enable this shift and benefit from its consequences by encouraging the incorporation of civilian technologies into military and security equipment and removing the regulatory barriers that prevent this from taking place. China's policy of 'military-civil fusion' was adopted as a national strategy in 2014, aimed at enabling the Chinese military to benefit from developments in its civilian sectors.[5] The US Department of Defense (DOD) has been pursuing its own policy of civil-military integration since the 1994 'Perry Memorandum', which sought to reduce the barriers between the defence and civilian sectors.[6] However, these efforts have expanded in recent years, particularly in the field of AI where the US DOD is seeking to enable the US military to utilize advances made in the civilian sector.[7]

For the past decade, the EU has also been taking steps to encourage the incorporation of civilian technologies into military systems. The European Defence Fund (EDF), the EU's main tool for funding defence-related R&D, is seeking to encourage the use of technologies developed in the civilian sector in the development of military systems through its EU Defence Innovation Scheme (EUDIS). The EUDIS aims to enhance opportunities for small and medium-sized enterprises, start-ups and other 'non-traditional' actors in the defence sector to access EDF resources. Among the instruments offered by the EUDIS are 'spin-in' calls, which focus on enabling 'a faster uptake of innovative solutions from civil applications [for] defence use'.[8]

The development of items and systems that are dual use by design

In addition to encouraging the incorporation of civilian technologies into military and security equipment, states are also seeking to facilitate the development of technologies and systems that are dual use by design. Since the second world war, military spending has been one of the main sources of funding for key advances in the technologies that power modern economies. This has supported the emergence of a wide range of dual-use items and systems. Through the work of the Defense Advanced Research Projects Agency (DARPA)—founded in 1958—the USA has sought to use military R&D spending to support the development of foundational technologies with both military and civilian applications.[9] This approach has been far more prevalent in the USA than in Europe, where research funders and research and academic institutes have often been keen to maintain a distinction between civilian research and processes associated with the development and production of military and security equipment.[10] However, the security challenges generated by Russia's full-scale invasion of Ukraine in 2022 are leading the EU and

[5] National Bureau of Asian Research, 'Commercialized militarization: China's military-civil fusion strategy', 30 June 2021.

[6] Perry, W., 'Memorandum from the Secretary of Defense to the Secretaries of the Military Departments, "Specifications & standards: A new way of doing business"', US Department of Defense, 29 June 1994.

[7] See Apostoaie, E., 'What happened at America's own military-civil fusion fair', The Wire China, 12 May 2024.

[8] See European Union, EU Defence Innovation Scheme (EUDIS), 'Spin-in calls', [n.d.].

[9] See Mazzucato, M., *The Entrepreneurial State* (Penguin: London, 2013).

[10] Altmann, J. et al., 'Science for Peace and the need for civil clauses at universities and civilian research institutions', arXiv, 28 May 2025.

European funding agencies to seek to remove some of these distinctions and create new pathways for developing technologies and systems that are dual use by design.

Through the EDF, the EU is seeking to fund the development of systems that can serve both civilian and military functions. Examples include systems with potential civil applications that are able 'to inspect, repair, update, maintain or deorbit military satellites'.[11] The EU is also adjusting the guidelines around its R&D funding streams to create new pathways and incentives for research and academic institutes to conduct fundamental and applied research with potential military and security applications. In July 2025, the European Commission published a proposal for Horizon Europe for the period 2028–34 that would be 'able to support dual-use actions' and a shift to 'a DARPA-like approach dedicated to supporting defence and dual use startups'.[12] Individual EU member states are also seeking to create direct research funding for the development of items and systems that are dual use by design or establish new connections between civilian companies and defence procurement processes.[13]

In recent years, there has been a significant increase in global military spending linked to the deteriorating security situation at the global and regional levels.[14] Increases in spending are likely to further entrench and accelerate the shifts in the processes through which military and security equipment are produced and the ways in which R&D funding is allocated. Resources allocated to strengthen and develop military capabilities in the context of ongoing rearmament plans are focused on harnessing innovation from the civilian sector as well as engaging with various actors outside of traditional arms industry ecosystems.

The development of FRTs for civilian uses

The incorporation of civilian technologies into military and security equipment and the development of technologies and systems that are dual use by design are both trends that are visible in the case of FRTs. FRT is an umbrella term that encompasses a number of tools, mostly digital systems and software, that can be used for different tasks involving video or images. These include: facial detection (i.e. the ability to detect the presence of a face in an image), facial analysis (i.e. the ability to identify additional features in a detected face such as perceived gender) and facial recognition (i.e. the ability to compare facial features in multiple images for verification or identification purposes).[15] FRTs are generally considered to perform better on verification

[11] European Commission, 'Annex to the Commission Implementing Decision on the financing of the European Defence Fund and the adoption of the work programme for 2025, Part 2 and amending Implementing Decisions C(2023) 2296 final and C(2024) 1702 final as regards financial support to third parties', C(2025) 568 final, 29 Jan. 2025.

[12] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe, the Framework Programme for Research and Innovation, for the period 2028–2034 laying down its rules for participation and dissemination, and repealing Regulation (EU) 2021/695', COM(2025) 543 final, Brussels, 16 July 2025.

[13] See 'Civilian technology can solve military challenges', Vinnova, Updated 22 Oct 2025; and Cyber Innovation Hub, 'Your pitch for the CIHBw!', [n.d.], accessed 21 Oct. 2025

[14] Liang, X. et al., 'Trends in world military expenditure, 2024', SIPRI, Apr. 2025.

[15] Buolamwini, J., Ordóñez, V. and Learned-Miller, E., 'Facial recognition technology: A primer', MacArthur Foundation, 29 May 2020. pp. 2–6; and National Institute of Standards and Technology

tasks because these normally involve subjects who are aware that they are being scanned and participating willingly.[16] The use of facial recognition systems for identification processes tends to be less accurate because it often makes use of footage captured at a distance.[17]

The early development of FRTs was supported by the US government with the objective of harnessing its potential for security and law enforcement activities. Since the 2000s, however, most of the key advances have been made in the civilian sector and FRTs have been embedded in a wide variety of civilian systems.[18] FRTs are used to unlock cars and digital devices, such as smartphones and computers, to support financial services by means of verifying users' identities for online banking and payments or to verify the identities of individuals accessing public events, workplaces and other public spaces.[19] The commercial success of FRTs has been further driven by advances in AI and the incorporation of AI applications into facial recognition systems.[20] Today, FRTs are primarily powered by deep learning, a type of machine learning technique that uses artificial neural networks trained on labelled datasets to learn how to associate data features with specific labels.[21] These technological advances combined with a general and wider availability of large training datasets have significantly enhanced the ability of FRTs to perform at a higher scale and speed and their relevance for military and security uses.

The incorporation of FRTs into military and security equipment

Security-relevant applications of FRTs include their use by law enforcement in various activities, such as criminal investigations and surveillance.[22] In these contexts, FRTs are used to search images to identify individuals suspected of being involved in violations of the law. In the UK, for instance, live facial recognition systems have been used by the police to capture live footage of crowds and compare this with an already available list of suspects, generating an alert in case of a match.[23] A similar method used by the police

(NIST), 'Facial Recognition Technology (FRT)', 6 Feb. 2020.

[16] Crumpler, W., 'How accurate are facial recognition systems and why does it matter?', Strategic Technologies Blog, Center for Strategic and International Studies, 14 Apr. 2020.

[17] Crumpler (note 16).

[18] National Institute of Standards and Technology (NIST), 'Face recognition technology (FERET)', updated 26 Mar. 2025.

[19] European Parliament, Directorate General for Parliamentary Research Services, *Regulating Facial Recognition in the EU: In Depth Analysis*, Brussels, Sep. 2021, pp. 7–8.

[20] European Parliament (note 19), p. 2.

[21] AI is a 'broad field that refers to the use of technologies to create machines and computers that can mimic the cognitive functions associated with human intelligence'. Machine learning is 'a subset of artificial intelligence that allows a system to learn and improve autonomously using neural networks and deep learning…by acquiring large amounts of data'. See Google Cloud, 'What is deep learning?' [n.d.]; and Google Cloud, 'Artificial intelligence (AI) vs. machine learning (ML)', [n.d.].

[22] European Parliament (note 19), pp. 3–4; Buolamwini, Ordóñez and Learned-Miller (note 15), pp. 7–8; Simmler, M. and Canova, G., 'Facial recognition technology in law enforcement: Regulating data analysis of another kind', *Computer Law & Security Review*, vol. 56 (Apr. 2025); and US Department of Homeland Security et al., Biometric Technology Report, Submitted in fulfillment of Section 13(e) of Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety (EO 14074), Dec. 2024.

[23] UK Government, 'Police urged to double AI-enabled facial recognition searches', 29 Oct. 2023.

in New Orleans relied on FRTs to locate suspects by scanning city streets.[24] The Chinese government makes extensive use of FRTs in public spaces. The Chinese police use such tools to scan crowds to identify persons of interest against available datasets. Police officers have reportedly been equipped with glasses embedded with FRTs to identify suspected criminals.[25] China has also emerged as a leading supplier of FRT-enabled surveillance tools to police and law enforcement agencies around the world.[26]

States have also sought to incorporate commercial FRTs into military equipment or have used available systems for military purposes. Most recently, different militaries have been working to integrate FRTs into uncrewed aerial vehicles (UAVs) for reconnaissance and intelligence operations—and potentially for targeting.[27] For instance, in 2023 the US Army reportedly signed a contract with the company RealNetworks to adapt its SAFR facial recognition software and deploy it on an autonomous small unmanned aircraft system for use in special operations such as 'intelligence, surveillance, and target acquisition'.[28] The Ukrainian Armed Forces have made extensive use of FRTs developed by the US-based company Clearview AI to identify deceased Russian soldiers, and it is likely that the same technology has also directly supported military operations.[29]

The Israel Defence Forces (IDF) have been using FRTs in the occupied Palestinian territories for the past decade, progressively integrating this technology, including AI-powered systems, into existing applications for ID identification, video surveillance and security checks.[30] For instance, the IDF have deployed FRTs at security checkpoints in the West Bank and East Jerusalem to collect biometric data and scan individuals to compare their image against available information before permitting them to pass.[31] In this context, the IDF have reportedly relied on FRT systems supplied by private companies, such as AnyVision, an Israel-based start-up currently trading under the name of Oosto, which specializes in AI-powered FRT.[32] Israel has significantly expanded its use of FRTs during its military campaign in Gaza,

[24] MacMillan, D. and Schaffer, A., 'Police secretly monitored New Orleans with facial recognition cameras', *Washington Post*, 19 May 2025.

[25] *Wall Street Journal*, 'Next-level surveillance: China embraces facial recognition', YouTube, 27 June 2017; *The Economist*, 'China: Facial recognition and state control', YouTube, 24 Oct. 2018; and BBC News, 'Chinese police spot suspects with surveillance sunglasses', 7 Feb. 2018.

[26] Beraja, M. et al., *Exporting the Surveillance State via Trade in AI* (Center on Regulation and Marketing at Brookings: Washington, DC, Jan. 2023); and Jankovic, J. and Standish, R., 'Leaked files reveal Serbia's secret expansion of Chinese-made surveillance', Radio Free Europe/Radio Liberty, 13 Aug. 2025.

[27] Pivcevic, K., 'Biometrics planned for AnyVision JV's first drones for military use', Biometric Update, 4 Jan, 2021; Brewster, T., 'Drones with facial recognition are primed to fly, but the world isn't ready yet', *Forbes*, 15 Feb. 2021; Gault, M., 'US military signs contract to put facial recognition on drones', Vice, 27 Feb. 2023; and Wadhva, V. and Salkerver, A., 'Killer flying robots are here: What do we do now?', *Foreign Policy*, 5 July 2021.

[28] Gault (note 27).

[29] Hagerty, A., 'In Ukraine, identifying the dead comes at a human rights cost', Wired, 22 Feb. 2023; and Bergengruen, V., 'Ukraine's "secret weapon" is a controversial tech company', Time, 14 Nov. 2023.

[30] Weitzberg, K., 'Biometrics and counter-terrorism: Case study of Israel/Palestine', Privacy International, May 2021.

[31] Amnesty International, 'Automated apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT', 2 May 2023.

[32] Weitzberg (note 30); and Talbot, R., 'Automating occupation: International humanitarian and human rights law implications of the deployment of facial recognition technologies in the occupied Palestinian territory', *International Review of the Red Cross*, vol. 102, no. 914 (Aug. 2020).

which it launched in response to the Hamas attack of 7 October 2023.[33] The IDF has deployed a facial recognition system in Gaza that reportedly relies on technology developed by the Israel-based company Corsight AI to identify individuals in crowds and drone footage.[34] There have been allegations that data collected by these means has been used by the IDF to train and operate AI decision-support systems, particularly 'Lavender', which the IDF has reportedly deployed in Gaza to assist with targeting decisions.[35]

In some cases, companies market relevant products and services as being able to adjust to different environments and be used for multiple purposes. For instance, Herta promotes its 'BioSurveillance NEXT' solution facial recognition software, which can be used to identify subjects in crowded environments, as for use by government and law enforcement but also to regulate access at sporting events, in retail applications and for surveillance on public transport.[36] The FRT systems developed by Corsight AI, mentioned above, are also used for law enforcement and in various commercial applications, such as banking and retail, among other things.[37] Several universities and research centres around the world are also involved in research projects on the development of FRTs.[38]

Concerns about the misuse of FRTs

The use of FRTs for security and military purposes has raised a number of concerns, especially among civil society and non-governmental organizations (NGOs), that this could lead to violations of human rights and IHL. In the light of the structural biases in the AI-systems that underpin their functioning, there are risks that the use of FRTs could generate 'false positives', where the wrong person is deemed to be a match.[39] This is particularly problematic in contexts where such tools may be or are being used by law enforcement to, for instance, identify possible suspects in a criminal case. The use of FRTs by police forces has come under scrutiny for allegedly violating individuals' right to privacy, leading to cases of wrongful arrest and misidentification, and for substantially being operated in a legal vacuum.[40] The massive deployment of FRTs in China, in combination with other surveillance tools and

[33] Pusztaszeri, A. and Harding, E., 'Technological evolution on the battlefield', Center for Strategic and International Studies, 16 Sep. 2025.

[34] Andersin, E., 'The use of the "Lavender" in Gaza and the law of targeting: AI-Decision Support Systems and Facial Recognition Technology', *Journal of International Humanitarian Legal Studies*, 23 May 2025; and Frenkel, S., 'Israel deploys expansive facial recognition program in Gaza', *New York Times*, 27 Mar. 2024.

[35] Andersin (note 34); Yuval, A., '"Lavender": The AI machine directing Israel's bombing spree in Gaza', +972 Magazine, 3 Apr. 2024; and Human Rights Watch, 'Questions and answers: Israeli military's use of digital tools in Gaza', 10 Sep. 2024

[36] Herta, 'BioSurveillance NEXT: High performance facial recognition for crowded environments' [n.d.]; Herta, 'Government and law enforcement', [n.d.]; Herta, 'Sports and events', [n.d.]; Herta, 'Retail', [n.d.]; and Herta, 'Transportation', [n.d.].

[37] Corsight, 'The hidden cost of missing real time threats', [n.d.].

[38] See Tools for Innovation Monitoring (TIM), 'Cybersurveillance: Facial Recognition Dataset', [n.d.].

[39] United Nations High Commissioner for Human Rights, 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests', A/HRC/44/24, 24 June 2020, p. 9; and Privacy International, 'Facial Recognition', [n.d.].

[40] MacMillan and Schaffer (note 24); Whannel, K., 'Government expands police use of facial recognition vans', BBC News, 14 Aug. 2025; Privacy International, 'Revealed: "Skyrocketing" scale of UK police's secret facial recognition searches of passport and immigration databases', 7 Aug. 2025; and

practices, has been heavily criticized for enabling the systematic repression of the Uyghur ethnic minority.[41]

Several commentators have expressed concerns in relation to the possible misuse of FRTs in the context of an armed conflict. Some have argued that even in cases where FRTs could be used to identify whether an individual is a combatant, many factors affect the accuracy and reliability of the technology, generating the risk of a mismatch and violations of the principles of IHL.[42] One such factor is the environment in which FRT is deployed. In the context of an armed conflict, the presence of civilians, dust and poor lighting conditions would by definition create an uncontrolled environment, increasing the chances of misidentification.[43] Other factors relate to the opacity associated with the functioning of the AI systems on which FRTs rely and, more generally, the existing biases in military AI.[44]

III. The role of export controls and other relevant instruments in regulating the trade in FRTs

FRTs and multilateral export controls

Export controls are policy tools that states have developed to oversee and regulate the trade in military equipment and dual-use items through the imposition of licensing requirements and reporting obligations. The implementation and enforcement of these controls can mitigate the risks of dual-use and military items contributing to the proliferation of weapons of mass destruction, being misused in violation of international law or being diverted to unintended recipients. The scope of export controls is largely defined and agreed through the four multilateral export control regimes—the Australia Group, the Missile Technology Control Regime, the Nuclear Suppliers Group and the Wassenaar Arrangement.

The Wassenaar Arrangement is focused on preventing the proliferation and misuse of conventional arms. Of the four regimes, it is the most relevant when it comes to setting standards for regulating transfers of military and security equipment and their associated parts and components. The Wassenaar Arrangement maintains control lists for military items (the 'munitions list') and dual-use items (the 'dual-use list') that are 'major or key elements for the indigenous development, production, use or enhancement of military capabilities'.[45] The control lists include physical items as well as software and technology—defined as including both 'technical data' and 'knowledge and technical assistance'—that is 'specially designed' or 'necessary' for the 'development, production or use' of controlled items. The

Heilweil, R., 'Big tech companies back away from selling facial recognition to police: That's progress', Vox, 11 June 2020.

[41] Bhuiyan, J., 'How Chinese firm linked to repression of Uyghurs aids Israeli surveillance in West Bank', *The Guardian*, 11 Nov. 2023.

[42] Zwanenburg, M., 'Biometrics on the battlefield', Lieber Institute, West Point, 21 Oct. 2020.

[43] Andersin (note 34).

[44] Andersin (note 34); On the bias in military AI see Bruun, L. and Bo, M., *Bias in Military Artificial Intelligence and Compliance with International Humanitarian Law* (SIPRI: Stockholm, 2025).

[45] Fleuriot, V., 'The Wassenaar Arrangement Munitions List', 30 May 2018; and Wassenaar Arrangement, 'Criteria for the selection of dual-use items (Adopted in 1994 and amended by the Plenary in 2004 and 2005)', [n.d.].

Wassenaar Arrangement also encourages states to apply 'catch-all controls' to capture exports of items that do not appear on its control lists but which are being exported to a destination that is subject to an arms embargo and 'are intended, entirely or in part, for a military end-use'.[46]

If an FRT has been specifically developed to be incorporated into a type of military and security equipment described in the Wassenaar Arrangement munitions list, then its export would potentially be captured by the controls on software or technology. Moreover, if an FRT is being exported for a military end-use to a country that is subject to an arms embargo, then it should be captured by catch-all controls. However, there are no specific controls on FRTs in the Wassenaar control lists. A new control list category for FRTs would need to be proposed by a Wassenaar participating state and be agreed to by all 42 participating states. The process for creating new control list categories is often criticized for moving too slowly and failing to keep pace with the speed at which technological developments take place. However, lengthy negotiations are often required to draft controls that are sufficiently clear and well defined to enable a distinction between items that do and do not require an export licence.[47]

The likelihood of creating new controls on FRTs within the Wassenaar Arrangement seems limited at present. States have been wary about adding items to the Wassenaar dual-use list that are widely used in the civilian sector for fear of disrupting legitimate commercial production and trade. The Wassenaar guidelines state that '(g)eneral commercially applied materials or components should not be included' on the dual-use list.[48] Although FRTs are being incorporated into a variety of military and security equipment, the fact that they are also being widely used in commercial products is likely to be a barrier to the creation of new controls. Moreover, the process of adding new controls to the Wassenaar control lists has become more difficult due to the geopolitical tensions created by Russia's invasion of Ukraine. Russia is a member of the Wassenaar Arrangement and has reportedly used its veto powers to block the adoption of new control list categories for certain emerging technologies.[49]

The existing controls on FRTs within the Wassenaar Arrangement and any new ones that might be established would seek to capture the software that enables these tools to operate. Software and technology can take a non-physical—intangible—form or be transferred by non-physical or intangible means, including by being shared electronically or made available through

[46] Wassenaar Arrangement participating states are encouraged to 'require authorisation for the transfer of non-listed dual-use items to destinations subject to a binding United Nations Security Council arms embargo, any relevant regional arms embargo either binding on a Participating State or to which a Participating State has voluntarily consented to adhere, when the authorities of the exporting country inform the exporter that the items in question are or may be intended, entirely or in part, for a military end-use'. Military end-use is defined as 'use in conjunction with an item controlled on the military list of the respective Participating State'. Wassenaar Arrangement, 'Statement of Understanding on Control of Non-Listed Dual-Use Items', Agreed at the 2003 Plenary.

[47] Brockmann, K., 'Drafting, implementing, and complying with export controls: The challenge presented by emerging technologies', *Strategic Trade Review*, vol. 4, no. 6 (2018), p. 10.

[48] Wassenaar Arrangement (note 45).

[49] See: Brockmann, K., 'The multilateral export control regimes', *SIPRI Yearbook 2023: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2023).

cloud computing.[50] Effective implementation and enforcement of export controls on intangible transfers of technology requires licensing authorities to have specific knowledge of and capabilities in, for instance, digital forensics, which might not exist in less well-resourced states. FRTs are also being made available through a Software as a Service (SaaS) model, which involves vendors making software applications available to users through cloud computing without having to download them.[51] States have developed different views and practices on which action—the act of uploading the software, giving access to the software or downloading the software—should be subject to licensing requirements when controlled software is made available in a SaaS model.[52] This lack of harmonization could have a negative impact on the level of oversight over transfers of software that take place via SaaS models.

FRTs and US and EU export controls

States can and do adopt export controls at the national and regional levels that go beyond the scope of the lists adopted within the multilateral export control regimes. Both the USA and the EU have explored the possibility of using this avenue to control transfers of FRTs. The USA generally seeks to ensure that dual-use items are only added to its national control list, the Commerce Control List (CCL), if they have been included on the lists adopted by multilateral export control regimes. However, it is often willing to adopt unilateral national controls on items that are not captured by regime lists if there are economic, national security or human rights concerns.[53] Since the 1970s, the USA has included crime control and detection items on the CCL that are not controlled by the regimes because these items have raised human rights concerns.[54]

In July 2024, the US Department of Commerce Bureau of Industry and Security issued a proposal for the establishment of new list-based export controls 'for facial recognition systems specially designed for mass-surveillance and crowd scanning' and related software, technology, components and accessories.[55] The proposal indicates among the 'major components' of facial recognition systems 'input camera(s), data storage, processing computers, and the software algorithms needed to model facial images'.[56] The rationale for the proposed controls was to prevent 'foreign-

[50] Bromley, M. and Maletta, G., *The Challenge of Software and Technology Transfers to Non-Proliferation Efforts: Implementing and Complying with Export Controls* (SIPRI Research Report: Stockholm, 2018).

[51] Many companies offer cloud-based solutions for facial recognition software, such as Microsoft Azure AI Face, Amazon Rekognition and Clearview AI. See AWS, 'What is Amazon Rekognition?', [n.d.]; Microsoft, 'Azure AI Vision', [|n.d.]; and Clearview AI, [n.d.].

[52] Brockmann, K. and Héau, L., 'Spyware as a service: Challenges in applying export controls to cloud-based cyber-surveillance software', SIPRI Topical Backgrounder, 17 Feb. 2025.

[53] Bromley, M. and Brockmann, K., 'A tale of two systems: Alignment, divergence and coordination in EU and US dual-use export controls', IAI Paper no. 24/15, May 2024.

[54] Hart, N. M. and Casey, C. A., 'Transatlantic leadership in an era of human rights-based export controls', *Journal of International Economic Law*, vol. 27, no. 1 (Mar. 2024), pp. 134–35.

[55] US Department of Commerce, 'Commerce proposes restrictions on US persons' support for foreign military, intelligence, and security services and controls to protect national security and human rights', Press release, 25 July 2024; and US Federal Register, 'US Department of Commerce, Export Administration Regulations: Crime Controls and Expansion/Update of US Persons Controls', 29 July 2024.

[56] US Department of Commerce (note 55); and US Federal Register (note 55).

security end-users', including law enforcement agencies, from using these items in violations of human rights. The policy justification accompanying the proposal for controls notes how the progressive incorporation of FRTs and AI technologies has increased this risk by making it easier, cheaper and faster to draw inferences about individuals at scale and, consequently, to weaponize this capability to implement repressive tactics.[57] The proposal was opened for comments until September 2024 but there is no evidence that it was later approved.

The EU has established a common legal framework for controls on the export, brokering, transit and transshipment of dual-use items. The current version of the EU dual-use regulation entered into force in September 2021. The items covered by the EU dual-use regulation are listed in Annex I of the regulation (the EU dual-use list). The EU dual-use list is updated annually and matches the coverage of the regimes' control lists.[58] In September 2025, for the first time, the annual update of the EU dual-use list included items that have not been included in the regimes' control lists.[59] The European Commission delegated regulation adopting these updates was formally published and entered into force in November 2025.[60] Citing the ongoing difficulties with reaching agreement on the adoption of new controls within the regimes, the EU added several items that all EU member states had wanted to see added to their lists but which had been blocked for inclusion within the Wassenaar Arrangement, such as quantum computers, additive manufacturing tools and semiconductor-related technologies.

The EU has also adopted export controls that go beyond the coverage of the regimes because of human rights concerns. For example, the EU torture regulation establishes controls on the trade in certain goods that could be used for capital punishment, torture or other cruel, inhuman or degrading treatment.[61] The 2021 recast of the EU dual-use regulation added a new catch-all control that applies to non-listed cybersurveillance items that 'may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law'.[62] During the recast process, the European Commission proposed including 'biometrics' in the definition of cybersurveillance items, which would have created a path to bringing FRTs within the scope of member states' dual-use export controls.[63] However, the inclusion of this term provoked concern from industry and EU member

[57] US Department of Commerce (note 55); and US Federal Register (note 55).

[58] Bromley and Brockmann (note 53).

[59] European Commission, '2025 Update of the EU Control List of Dual-use Items', 8 Sep. 2025.

[60] Commission Delegated Regulation (EU) 2025/2003 of 8 September 2025 amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items, *Official Journal of the European Union*, OJ L, 2025/2003, 14 Nov. 2025.

[61] Regulation (EU) 2019/125 of the European Parliament and of the Council of 16 January 2019 concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment (codification), *Official Journal of the European Union*, L30, 31 Jan. 2019.

[62] Council of the European Union, 'Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)', 11 June 2021.

[63] Stupp, C., 'Commission plans export controls on surveillance technology', EurActiv, 22 July 2016.

states about the potential impact on EU-based companies and the term was excluded from the final version of the regulation.[64]

Exports of FRTs could be captured by the EU's cybersurveillance catch-all. However, the dual-use regulation defines cybersurveillance items as 'dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems'. Relevant guidelines published by the EU clarify that 'covert surveillance'—when a person 'cannot objectively expect to be under surveillance'—in this context must be the 'main purpose' of the item's development and design.[65] The EU guidelines also explicitly exclude surveillance cameras and similar tools from the definition of cybersurveillance items. If an FRT is capturing data through systems of overt surveillance, such as closed-circuit television cameras, the catch-all controls do not apply.[66] However, the guidelines leave open the possibility that FRTs that operate on 'data extracted from information and telecommunications systems' would be captured.[67]

The role of soft law mechanisms

In addition to their obligation to comply with export controls, companies must also ensure that they do not violate human rights and IHL in the conduct of their activities.[68] Related obligations are outlined, for instance, in guidelines on responsible business conduct developed by the UN and the Organisation for Economic Co-operation and Development (OECD). The 2011 UN Guiding Principles on Business and Human Rights (UNGPs) state that businesses should have in place a 'human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights'.[69] The OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (the OECD Guidelines) build on the UNGPs and include recommendations to encourage positive contributions by businesses in different areas that minimize their adverse impact.[70] Both the UNGPs and the OECD Guidelines stress that businesses should respect IHL standards when operating in conflict-affected contexts.

The UNGPs and the OECD Guidelines are non-binding instruments but their content is rooted in established obligations under international law. Their recommendations have been incorporated into states' national legislation, creating obligations on companies to develop and apply their

[64] Stupp, C., 'Tech industry, privacy advocates pressure Commission on export control bill', EurActiv, 3 Aug. 2016; and Stupp, C., 'Juncker postpones controversial export control bill on surveillance technology', EuroActiv, 20 Sep. 2016.

[65] Council of the European Union (note 62); and Council of the European Union, 'Guidelines on the Export of Cyber-Surveillance Items under Article 5 of Regulation (EU) No. 2021/821', 15 Oct. 2024.

[66] Bromley, M. and Maletta, G., 'Making the most of the EU Catch-All Control on Cyber-Surveillance Exports', SIPRI Topical Backgrounder, 18 Oct. 2024.

[67] Council of the European Union, 'Guidelines on the Export of Cyber-Surveillance Items under Article 5 of Regulation (EU) No. 2021/821' (note 65).

[68] See Office of the United Nations High Commissioner for Human Rights, 'OHCHR and business and human rights', [n.d.]; and Pollard, M. et al., 'What private businesses need to know about international humanitarian law', *Humanitarian Law & Policy*, 26 Nov. 2024.

[69] UN Human Rights Council, 'Guiding Principles on Business and Human Rights', June 2011.

[70] Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct* (OECD: Paris, 2023).

provisions.[71] At the EU level, the Directive on Corporate Sustainability Due Diligence (CSDDD) builds on the UNGPs and the OECD Guidelines to establish a legally binding 'corporate due diligence duty'. Under the CSDDD, EU-based companies are legally required to identify and address 'potential and actual adverse human rights and environmental impacts in the company's own operations, their subsidiaries and, where related to their value chain(s), those of their business partners'.[72]

There have been discussions within the UN Human Rights Council and the Arms Trade Treaty Conference of States Parties about the extent to which the obligations outlined in the UNGPs and the OECD Guidelines are applicable when companies are exporting military and dual-use items.[73] Several arms manufacturers have human rights due diligence policies in place.[74] However, arms manufacturers have also argued that their primary obligation when transferring military equipment and dual-use items is to apply for an export licence, and that the state that issues the licence is ultimately responsible for assessing any human rights and IHL risks that might arise.[75] Following considerable debate, the CSDDD specifically excluded 'the distribution, transport and storage of a product that is subject to export controls under Regulation (EU) 2021/821 or to the export controls relating to weapons, munitions or war materials, once the export of the product is authorised'.[76] Some states have highlighted that the obligations outlined in the UNGPs apply to companies, regardless of whether they have received a licence to export military equipment or dual-use items.[77] This suggests that companies exporting military equipment or dual-use items have an obligation to conduct continuous due-diligence that runs in parallel with the process of applying for an export licence.

While there is debate about whether human rights due diligence obligations apply when companies are exporting items that are subject to export controls, these instruments are clearly applicable to transfers of items that fall outside the scope of such controls. The OECD Guidelines clarify that

[71] See German Bundestag, 'Act on Corporate Due Diligence Obligations in Supply Chains of July 16 2021'; and Official Bulletin of France, 'LOI no. 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre' [Law no. 2017-399 of 27 Mar. 2017 relating to the duty of vigilance of parent companies and contracting companies].

[72] European Commission, 'Corporate sustainability due diligence', 26 Feb. 2025.

[73] See Resolution adopted by the Human Rights Council on 13 July 2023, 'Impact of arms transfers on human rights', A/HRC/RES/53/15, 21 July 2023; and Austria, Ireland, Mexico, 'Joint Working Paper: Responsible Business Conduct and the Arms Trade Treaty', ATT/CSP9/2023/AUT-IRL-MEX/774/Conf.WP, 10 Aug. 2023.

[74] BAE Systems, 'Pursuit of export opportunities: Policy summary', 20 May 2025; Leonardo, 'Leonardo Group Trade Compliance Programme: Trade controls, import/export, international sanctions, monitoring of transactions with sensitive countries and respect of human rights', [n.d.]; and Rheinmetall, 'Export controls: Global, complex rules for import and export of goods and services', [n.d.].

[75] See United Nations, Human Rights, *Responsible Business Conduct in the Arms Sector: Ensuring Business Practice in Line with the UN Guiding Principles on Business and Human Rights*, Information Note by the UN Working Group on Business and Human rights, Aug. 2022; and Alwishewa, H., 'Human rights due diligence for arms companies: Lessons from supply chain regulations', *European Journal of Risk Regulation*, vol. 16, no. 2 (2025), pp. 704–20.

[76] European Union, 'Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859Text with EEA relevance', 5 July 2024, para. g (ii).

[77] Arms Trade Treaty, Joint Working Paper, 'Responsible Business Conduct and the Arms Trade Treaty', Submitted by Austria, Ireland and Mexico, 10 Aug. 2023.

their recommendations should also be observed by companies engaged in the 'development, financing, sale, licensing, trade and use of technology' and in 'scientific research and innovation'.[78] Companies are required to carry out risk-based due diligence to assess the 'actual and potential adverse impacts related to science, technology and innovation' and to ensure safe and secure transfers of technology by adopting all the necessary safeguards to prevent adverse impacts, such as complying with export controls regulations.[79] This could potentially cover technologies and systems, such as FRTs, that are being incorporated into the production of military and security equipment or used for military and security purposes.

Efforts have been made to clarify the content of these obligations and to specify how they should be applied, including in cases where FRTs or other surveillance tools are being exported. In 2019, the US State Department published a guidance document aimed at assisting 'US businesses that work with or design and manufacture products or services that have surveillance capabilities with implementation of the . . . UN Guiding Principles [and the] OECD Guidelines'.[80] The guidance is specifically focused on technologies that are beyond the scope of US export controls but that might be used for surveillance purposes in ways that would lead to violations of human rights. The document highlights the risks associated with 'Biometric identification (e.g., facial recognition software, automated biometric systems, rapid DNA testing, gait analysis software)' and lists a number of red flags that companies should seek to address.

The International Committee of the Red Cross has published a report that explains why IHL is relevant to private companies and clarifies the implications this has for the conduct of their businesses. The report argues that 'businesses should consider the wider IHL implications of developing and supplying technologies'. It also notes that these obligations apply to both military or weapons-related technologies and 'civilian products and services' that could be used by warring parties in violation of IHL, and that these 'could include . . . surveillance and telecommunications equipment or cybersecurity software'.[81]

IV. Conclusions and recommendations

NGOs and advocacy groups have raised concerns about the possible use of military and security equipment that incorporates FRTs in connection with violations of human rights and IHL. They have also documented cases in which such violations could occur or may have already occurred.[82] Export controls require companies and academic and research institutes to apply for licences when they are exporting items that are captured by their scope. Certain exports of FRTs are captured by states' export controls. However, many FRTs are likely to fall beyond the scope of states' export controls, even in cases

[78] Organisation for Economic Co-operation and Development (note 70), p. 46.
[79] Organisation for Economic Co-operation and Development (note 70), p. 46.
[80] US Department of State, *Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities*, [n.d.].
[81] Pollard, M., *Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law* (International Committee of the Red Cross: Geneva, Nov. 2024), pp. 25–26.
[82] Privacy International (note 1).

where they are to be incorporated into military and security equipment or where risks of diversion or misuse might be present. States should consider clarifying and expanding the scope of their export controls to capture certain transfers of FRTs. This could involve expanding the scope of their catch-all controls to cover cases in which non-listed items might be incorporated into military and security equipment or have military and security-related uses.

However, there are likely to be limits to what export controls can achieve in the field of FRTs. The processes for agreeing on additional multilateral export controls on systems and technologies within the Wassenaar Arrangement, which are already particularly complex and lengthy, are being further challenged by the current geopolitical context. In addition, FRTs have a wide range of civilian and commercial applications, which can make states reluctant to make them subject to export controls. The fact that these systems and technologies are mostly provided through intangible means, such as cloud computing, adds to the complexity of defining controls that are effective and feasible to implement and enforce. These gaps and challenges highlight the need for states, companies and academic and research institutes to apply or make use of alternative regulatory instruments, particularly human rights due diligence standards, to ensure that the human rights and IHL risks associated with all transfers of FRTs are assessed and addressed.

The militarization of technology—in particular the incorporation of civilian technologies into military and security equipment and the development of items and systems that are dual use by design—is only likely to expand and accelerate as governments engage in rearmament processes. These trends indicate that the developments outlined above in the field of FRTs, and the risks and regulatory challenges that they generate are likely to be replicated, or are already being replicated, in other areas of technology. States will need to consider whether or how export controls can be applied to the new categories of dual-use items that might be created, and to ensure that the companies and academic and research institutes involved are aware of their regulatory obligations. Where the limits of what export controls can achieve are reached, all actors involved will need to ensure that human rights due diligence standards are being applied so that the risks of misuse and diversion connected with exports that fall beyond the scope of export controls are still assessed and addressed.

The following recommendations are directed at states, companies and academic and research institutes involved in the development and production of and the trade in systems and technologies that could be incorporated into the production of military and security equipment or that may be used for military and security purposes, including FRTs. They identify steps that these actors could take to mitigate the risk of the misuse and diversion of these systems.

Recommendations for states

Clarify and consider expanding the scope of export controls on FRTs

States should seek to determine and then clarify to exporters whether their existing list-based and catch-all controls apply to FRTs. States could also consider expanding the scope of either list-based or catch-all controls to include FRTs, especially in cases where the use of these technologies is

combined with AI or machine learning techniques that increase the risk of misuse at scale.

Condition the allocation of funding for research and development of items that are dual use 'by design' on specific compliance requirements

States should request that companies and other potential beneficiaries of funding for military-related R&D adhere to specific requirements. These should include a requirement to have an Internal Compliance Programme (ICP) in place to ensure that export controls are implemented. States should also require companies and other beneficiaries to adopt additional due diligence processes to ensure that their activities and businesses do not have an adverse impact on human rights and do not lead to violations of human rights or IHL.

Conduct export control-related awareness raising for new actors

An increasing number of actors in the private sector could be affected by export controls because of efforts to incorporate civilian technologies into military and security equipment or develop items and systems that are dual use by design. States should seek to map these new actors and involve them in outreach and awareness-raising activities in the field of export controls. These activities could include outlining obligations and practices in the field of human rights due diligence and be complemented by the development of sector- or actor-specific guidance.

Recommendations for companies and academic and research institutes

Adopt internal compliance programmes

Companies and academic and research institutes that might be affected by export controls should adopt an ICP to ensure compliance with these controls and their own internal policies. These efforts should build on the existing guidance available at the national and EU levels, developed by industry associations or publicly shared by other companies.

Ensure compliance with obligations in the field of human rights due diligence

Companies and academic and research institutes involved in the development and production of systems and technologies that could be militarized, but that might not be covered by the scope of export controls, should ensure that they comply with their human rights and IHL-related obligations as outlined in the UNGPs, the OECD Guidelines and other relevant instruments. An important step would be to establish related due diligence processes to mitigate and address relevant risks, as well as building or ensuring the presence of in-house expertise in the fields of IHL and human rights.

Connect internal compliance programmes with other relevant mechanisms

In establishing ICPs, companies and academic and research institutes should consider connecting these programmes with other internal due diligence frameworks. One advantage of establishing such connections would be strengthened risk assessment procedures built on the frameworks' respective approaches, especially in cases where export control obligations are not clear or well-defined.

Abbreviations

AI	Artificial Intelligence
CCL	Commerce Control List
CSDDD	Directive on Corporate Sustainability Due Diligence
DARPA	Defense Advanced Research Projects Agency
DOD	US Department of Defense
EDF	European Defence Fund
EU	European Union
EUDIS	EU Defence Innovation Scheme
FRTs	Facial recognition technologies
ICP	Internal Compliance Programme
IDF	Israel Defence Forces
IHL	International humanitarian law
IHRL	International human rights law
NGOs	Non-governmental organizations
OECD	Organisation for Economic Co-operation and Development
OECD Guidelines	OECD Guidelines for Multinational Enterprises on Responsible Business Conduct
R&D	Research and development
SaaS	Software as a Service
UAVs	Uncrewed aerial vehicles
UNGPs	UN Guiding Principles on Business and Human Rights

RECENT RELATED SIPRI AND EUNDPC PUBLICATIONS

Addressing the Risks that Civilian AI Poses to International Peace and Security: The Role of Responsible Innovation

Dr Vincent Boulanin, Jules Palayer and Charles Ovink
November 2025

Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint

Dr Mark Bromley and Giovanna Maletta
September 2025

Bias in Military Artificial Intelligence and Compliance with International Humanitarian Law

Laura Bruun and Dr Marta Bo
August 2025

Military and Security Dimensions of Quantum Technologies: A Primer

Dr Michal Krelina
July 2025

Autonomous Weapon Systems and AI-enabled Decision Support Systems in Military Targeting: A Comparison and Recommended Policy Responses

Dr Alexander Blanchard and Laura Bruun
June 2025

The Australia Group at 40: Making the AG Fit for an Era of Geopolitical Competition

Kolja Brockmann
June 2025

Cloud Labs and Other New Actors in the Biotechnology Ecosystem: Export Control Challenges and Good Practices in Outreach

Kolja Brockmann, Lauriane Héau and Giovanna Maletta
May 2025

Non-proliferation, Nuclear Technology and Peaceful Uses: Examining the Role and Impact of Export Controls

Giovanna Maletta, Dr Mark Bromley and Kolja Brockmann
April 2025

Trends in World Military Expenditure, 2024

Xiao Liang, Dr Nan Tian, Dr Diego Lopes da Silva, Lorenzo Scarazzato, Zubaida A. Karim and Jade Guiberteau Ricard
April 2025

An Introduction to Military Quantum Technology for Policymakers

Dr Michal Krelina
March 2025

SIPRI RESEARCH POLICY PAPER

THE MILITARIZATION OF TECHNOLOGY: PREVENTING DIVERSION AND MISUSE THROUGH EXPORT CONTROLS

MARK BROMLEY AND GIOVANNA MALETTA

CONTENTS

ABOUT THE AUTHORS

Dr Mark Bromley is the Director of the SIPRI Dual-Use and Arms Trade Control Programme. His research focuses on national, regional and international efforts to regulate the trade in conventional arms and dual-use items.

Giovanna Maletta is a Senior Researcher in the SIPRI Dual-Use and Arms Trade Control Programme. Her research work at SIPRI includes issues related to the implementation of national, multilateral and international export control instruments, with a particular focus on the European Union regulatory framework and the Arms Trade Treaty.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

DOI: https://doi.org/10.55163/VDOD7802