sipri

EXPORT CONTROLS AND SPYWARE

Enhancing Oversight, Transparency and Restraint

MARK BROMLEY AND GIOVANNA MALETTA

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

The Governing Board is not responsible for the views expressed in the publications of the Institute.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Signalistgatan 9
SE-169 70 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

EXPORT CONTROLS AND SPYWARE

Enhancing Oversight, Transparency and Restraint

MARK BROMLEY AND GIOVANNA MALETTA

September 2025

sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

DOI: https://doi.org/10.55163/GVXO6716

Contents

Acknowledgements

This policy paper was produced with support from the Open Society Foundations, which is funding a project by the SIPRI Dual-Use and Ams Trade Control Programme on improving implementation of export controls related to surveillance technologies. SIPRI intern Monalisa Hazarika and SIPRI Researcher Lauriane Héau contributed to the data-collection effort presented in Section II. The authors are grateful to the SIPRI colleagues (Kolja Brockmann, Lauriane Héau, and Jingdong Yuan) and external experts (Jennifer Brody, Silvia Lorenzo Perez, Fionnuala Ní Aoláin, Jennifer Roberts, Greg Slovak, and Joanna Tricoli) who provided input on earlier drafts of this policy paper. The authors would also like to thank the experts who participated in an online webinar that SIPRI co-organized on 10 June 2025 on 'Export controls and spyware: Enhancing oversight, transparency and restraint', where a draft version of the policy paper was presented.

Executive summary

Cyber-surveillance tools are the hardware and software used by intelligence agencies and law enforcement agencies (LEAs)—or by network operators acting under their direction—to covertly monitor, extract or collect communications data that is stored, processed or transferred through information and communications technologies (ICTs). These tools can be broadly divided into those associated with processes of lawful interception (LI) and data retention and others, including spyware, that are associated with methods of device compromise. Many larger states can produce certain forms of spyware and other cyber-surveillance tools for use by their own intelligence agencies and LEAs. However, even well-resourced governments rely on the private sector for at least some of the tools used by LEAs and intelligence agencies, and for the acquisition of spyware and other cyber-surveillance tools.

Producers of spyware and other cyber-surveillance tools can also be broadly divided into those that produce tools associated with processes of LI and data retention and those that produce tools associated with methods of device compromise. These companies are diverse in terms of their size and their level of awareness of export controls and sanctions and the obligations these create. The production of spyware and other cyber-surveillance tools is highly concentrated. A mapping exercise conducted by SIPRI in connection with this policy paper identified 188 companies located in 31 states that manufacture different types of spyware and other cyber-surveillance tools. Of these companies, 51 per cent are located in 19 states in Europe, 22 per cent in three states in the Americas, 13 per cent in three states in the Middle East and 13 per cent in five states in Asia and Oceania.

The proliferation and misuse of spyware and other cyber-surveillance tools pose significant threats to human rights and national security. Multiple cases have been documented in which states have been accused of using spyware and other cyber-surveillance tools in connection with serious violations of international human rights law. NGOs have highlighted cases of spyware being used in connection with ongoing armed conflicts and the potential for them to be used in ways that violate international humanitarian law (IHL). Spyware has been used to target government officials and states have expressed concerns about its potential to facilitate attacks on critical infrastructure. States and parts of the private sector have developed a range of initiatives to tackle the proliferation and misuse of spyware and other cyber-surveillance tools. These aim to establish new norms and standards, encourage more effective implementation of international human rights law and seek financial compensation from the manufacturers of spyware.

Export controls and sanctions are a critical component of wider attempts to regulate the production, trade in and use of spyware and other cyber-surveillance tools. Since 2012, five categories of spyware and other cyber-surveillance tools have been added to the dual-use control lists maintained by the Wassenaar Arrangement and the European Union (EU). The EU adopted a new version of the EU dual-use regulation in 2021, which sought to strengthen controls on exports of spyware and other cyber-surveillance tools. EU sanctions have prohibited exports of these items to certain recipients and US sanctions have targeted spyware manufacturers. In addition, 43 states have committed to use export controls to prevent transfers of spyware and other cyber-surveillance tools that might be used to enable violations of human rights and IHL. These states are home to 68 per cent of the companies that manufacture spyware and other cyber-surveillance tools.

Export controls have allowed states to collectively identify the spyware and other cyber-surveillance tools that present the most significant risks to human rights and

national security, and to define their technical characteristics. Licence application procedures create records of where these tools are being exported and by whom. These procedures can increase government oversight of the trade in these tools and create the possibility of greater public transparency in this area. Export controls can be used to prevent exports of spyware and other cyber-surveillance tools and to impose constraints on how exported items are used. Sanctions have been used to prohibit certain exports of spyware and other cyber-surveillance tools to sensitive destinations and to swiftly target producers of spyware following cases of misuse. Finally, export controls and sanctions can enable the prosecution of companies that seek to transfer these items without the necessary approval.

Export controls and sanctions have yielded significant results in helping to tackle the proliferation and misuse of spyware and other cyber-surveillance tools. However, more could be done to improve their coverage and to strengthen and harmonize their implementation. Export controls are complex regulatory instruments that require the appropriate allocation of time, resources and expertise by a national government in order to function effectively. For instance, many of the items on the Wassenaar Arrangement and EU dual-use lists, including certain types of spyware and other cyber-surveillance tools, are not physical goods but 'intangible' products, such as software and technical data, that can be transferred electronically. Effective implementation and enforcement of controls on intangible transfers of technology require licensing authorities to have capabilities in certain areas, such as digital forensics, that may not be available in smaller states. Finally, available guidelines on how to assess the risks of exports do not explicitly consider the human rights- or IHL-related risks posed by exports of spyware and other cyber-surveillance tools.

The ability of the Wassenaar Agreement to play a leading role in developing new controls and norms is limited in the current international environment. Recent multilateral initiatives, such as the Export Controls and Human Rights Initiative, the White House Joint Statement on Spyware and the Pall Mall Process, have created alternative avenues through which states can draft guidelines, strengthen or expand existing controls and share confidential information. The USA has taken a leading role in demonstrating how export controls and sanctions can be used to tackle the proliferation and misuse of spyware and other cyber-surveillance tools. If US leadership in this area becomes less prominent, the EU has the potential to take on this role. The EU would be able to take steps to strengthen its own controls, connect relevant areas of EU policymaking and establish standards for other states to draw on.

Recommendations to all states

- States should examine the potential to adopt new list-based controls and catch-all controls to capture additional categories of cyber-surveillance tools.
- States should share more detailed information on the content and implementation of their export controls on spyware and other cyber-surveillance tools using established or newly created channels.
- States should agree on minimum standards for the publication of data on licences for exports of spyware and other cyber-surveillance tools, building on existing practices.
- States should develop guidelines on how to implement export controls on spyware and other cyber-surveillance tools, covering areas such as awareness raising and risk assessments.
- States should establish a global commitment to make spyware subject to export controls, potentially as part of the new UN Global Mechanism on Developments in the Field of ICTs.

Recommendations to the EU and EU member states

- The EU should move additional categories of cyber-surveillance tools from Annex I to Annex IV of the EU dual-use regulation to improve oversight of intra-EU transfers.
- The EU should connect discussions on export controls and misuse of spyware and other cyber-surveillance tools with broader EU-level debates on their misuse, particularly those in the European Parliament.
- The EU should examine whether spyware and other cyber-surveillance tools are being made available via Software-as-a-Service (SaaS) models and how these are regulated by EU member states.
- The EU and EU member states could develop training programmes for national officials on the implementation of controls on exports of spyware and other cyber-surveillance tools.
- The EU and EU member states should examine the role that EU sanctions could play in tackling the proliferation and misuse of spyware and other cyber-surveillance tools.

Abbreviations

ACE	Authorized Cybersecurity Exports
ASD	Aerospace, Security and Defence Industries Association of Europe
BIS	US Bureau of Industry and Security
CCICs	Commercially available cyber intrusion capabilities
CFSP	Common Foreign and Security Policy
CCL	US Commerce Control List
EAR	Export Administration Regulations
EEAS	European External Action Service
EU	European Union
FOI	Freedom of information
ICTs	Information and communications technologies
IHL	International humanitarian law
IMSI	International mobile subscriber identity
ITT	Intangible technology transfer
LEAs	Law enforcement agencies
LI	Lawful Interception
NGOs	Non-Governmental Organizations
OEWGs	UN Open-Ended Working Groups
OFAC	US Department of the Treasury's Office of Foreign Assets Control
OHCHR	United Nations Human Rights, Office of the High Commissioner
PSSA	Federal Act on Private Security Services Provided Abroad
SaaS	Software as a Service
STEG	Surveillance Technology Expert Group
UAE	United Arab Emirates

1. Introduction

The proliferation and misuse of 'spyware' and other 'cyber-surveillance tools' pose significant threats to human rights and national security. For the purposes of this paper, cyber-surveillance tools refers to the different types of software and hardware used by intelligence agencies and law enforcement agencies (LEAs)—or by telecommunications network operators acting under their direction—to covertly monitor, extract, collect or analyse communications data. Similarly, spyware refers to a specific category of cyber-surveillance tools that can be inserted into computers and mobile phones without detection and used to remotely monitor and, in certain cases, control them.

Following the 2011 Arab Spring, reports indicated that western companies had supplied spyware and other cyber-surveillance tools to states in the region that were accused of using them in connection with serious violations of international human rights law (human rights).[1] The debate about the use of these tools and their human rights implications accelerated in the early 2020s following reports of the use of spyware to target and intimidate journalists and political opponents, including in European democracies.[2] Non-governmental organizations (NGOs) have highlighted cases of spyware being used in connection with ongoing armed conflicts and the potential for them to be used in ways that violate international humanitarian law (IHL)—also known as 'the laws of armed conflict'.[3] States have also noted the national security risks posed by spyware, highlighting cases where it has been used to monitor government officials and the risk that it might be used to facilitate attacks on critical infrastructure.[4]

A number of initiatives have been launched to develop and apply stronger controls on the development, production, acquisition, transfer and use of different types of spyware and other cyber-surveillance tools. States have developed multilateral initiatives to tackle the proliferation and misuse of spyware by establishing new norms and standards and encouraging more effective implementation of international human rights law. These initiatives include the 2023 'Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware', launched by the United States, and the 2024 Pall Mall Process, launched by France and the United Kingdom. Tackling the security risks posed by spyware has also been one of the focuses of the UN Open-Ended Working Groups (OEWGs) on 'security of and in the use of information and communications technologies'. Concerns about the human rights risks posed by spyware and other cyber-surveillance tools have also generated responses from the private sector. Network operators have pushed for greater transparency and accountability in the way governments request and collect communications data using cyber-surveillance tools.[5] Communications service providers have sought financial compensation from the manufacturers of spyware that has targeted their products.[6]

States have also used export controls and sanctions to tackle the proliferation and misuse of spyware and other cyber-surveillance tools. Export controls are used by states to require companies to obtain licences before transferring military equipment and dual-use items identified in control lists. Their content can be established at the national, international or multilateral level, including through multilateral export

[1] Silver, V. and Elgin, B., 'Torture in Bahrain becomes routine with help of Nokia Siemens', Bloomberg, 23 Aug. 2011; Business and Human Rights Resource Centre, 'Amesys lawsuit (re Libya)', [n.d.]; and Silver, V., 'Italian firm exits Syrian monitoring project, Republica says', Bloomberg, 28 Nov. 2011.

[2] See 'About the Pegasus Project', Forbidden stories, 18 July 2021; and European Parliament, 'Spyware: MEPs sound alarm on threat to democracy and demand reforms', Press release, 5 Aug. 2023.

[3] Krapiva, N., Coppi, G. and Hammoud, R., 'Armenia spyware victims: Pegasus hacking in war', Access Now, 25 May 2023.

[4] See US Department of State, 'United States International Cyberspace & Digital Policy Strategy', July 2024.

[5] See Global Network Initiative (GNI).

[6] Smalley, S., 'Judge rules NSO Group is liable for spyware hacks targeting 1,400 whatsapp user devices', The Record, 21 Dec. 2024.

control regimes such as the Wassenaar Arrangement and European Union (EU) legal instruments. Since 2012, five categories of spyware and other cyber-surveillance tools have been added to the dual-use control lists maintained by the Wassenaar Arrangement and the EU. Sanctions are a separate type of regulatory tool. They can comprise banking restrictions, travel bans, asset freezes or prohibitions on transfers of military equipment, dual-use items or other commodities and can be imposed on states, companies or individuals. Their content can be established at the national, international or multilateral level, including through UN Security Council resolutions and EU legal instruments. While there is no prospect of UN sanctions being applied to the trade in spyware and other cyber-surveillance tools, EU sanctions have prohibited certain exports and US sanctions have targeted spyware manufacturers.

Many states seek to maintain a clear distinction between export controls and sanctions and are resistant to policy discussions that merge the two. Sanctions are more politically sensitive than export controls and are subject to greater levels of inter-state disagreement and contestation. Nonetheless, a joint analysis of the use of export controls and sanctions to tackle the proliferation and misuse of spyware and other cyber-surveillance tools is justified. Maintaining a clear distinction between the content and focus of export controls and of sanctions presents various challenges. For example, some aspects of US export controls, particularly the prohibitions they can establish on transfers to specific end-users, would be described as sanctions in other jurisdictions. In addition, the coverage of export controls and sanctions can overlap, and they are often implemented at the national level by the same government authorities.[7]

Export controls and sanctions have yielded significant results in tackling the proliferation and misuse of spyware and other cyber-surveillance tools. However, more could be done to improve their coverage and to strengthen and harmonize their implementation. The expanded use of export controls and sanctions has been encouraged by the multilateral initiatives that states have launched to tackle the proliferation and misuse of spyware. However, to deploy these tools effectively, states require a deeper understanding of how they work and what they can and cannot achieve. Effectively addressing the proliferation and misuse of spyware and other cyber-surveillance tools requires the use of a range of hard and soft law instruments, such as industry standards, legal action and the full implementation of international human rights law. Export controls and sanctions are an essential piece of this puzzle that if framed and deployed effectively, can limit the proliferation and misuse of spyware and other cyber-surveillance tools and support other relevant regulatory instruments.

This policy paper reviews the content of the export controls and sanctions that have been applied to the trade in spyware and other cyber-surveillance tools and outlines recommendations on how they could be strengthened, expanded and harmonized. Section II outlines the different types of software and hardware that are included under the concept of spyware and other cyber-surveillance tools employed by this paper and maps the location of manufacturing companies. Section III outlines the content of the export controls and sanctions that have been applied to the trade in spyware and other cyber-surveillance tools. Section IV examines the wider set of international and multilateral initiatives that include a focus on using export controls and sanctions to tackle the proliferation or misuse of spyware and other cyber-surveillance tools. Section V presents recommendations aimed at helping to improve the consistency and effectiveness of efforts to use export controls and sanctions to tackle the proliferation and misuse of cyber-surveillance tools, highlighting steps that can be taken at the national, multinational and EU levels.

[7] See UK Government, 'Export Controls: Dual-Use Items, Software and Technology, Goods for Torture and Radioactive Sources', 7 July 2025; and Swedish Inspectorate for Strategic Products (ISP), 'Assignments'.

2. Mapping the trade in spyware and other cyber-surveillance tools

Categories of cyber-surveillance tools

The concept of cyber-surveillance tools used in this paper covers the hardware and software used by intelligence agencies and LEAs—or by network operators acting under their direction—to covertly monitor, extract and collect communications data that is stored, processed or transferred through information and communications technologies (ICTs). These tools can be broadly divided between those associated with processes of lawful interception (LI) and data retention and others, including spyware, associated with methods of device compromise. The concept used in this paper does not include tools associated with overt surveillance and offensive forms of malware, mainly because these have not been the focus of export controls that have been adopted in this area.

Tools associated with processes of lawful interception and data retention

Governments have long sought to put in place regulatory and technical tools that allow them to access communications data for law enforcement and intelligence-gathering purposes. The most established and standardized are processes of LI, through which telecommunications network operators can be required to provide communications data on one or more of its users; and data retention, through which telecommunications network operators are required to store certain types of communications data for potential later handover.[8] 'LI systems' are used by network operators to assist with compliance with LI requests.[9] 'Data retention systems' are used by network operators to assist with meeting their obligations to store certain types of communications data for potential later use.[10] States can also employ 'network surveillance systems' that conduct mass surveillance by collecting data as it passes through the networks that carry internet communications.[11] 'Monitoring centres' are used by intelligence agencies or LEAs to collect, store and analyse communications data collected by these and other sources.[12]

International standards have been developed that specify how processes of LI and data retention should operate, and define the functions and technical parameters of the systems that provide these capabilities.[13] Some of these standards provide a certain level of protection against the use of these tools in connection with human rights violations.[14] Certain LI systems have in-built capabilities that can help to prevent human

[8] See Frost & Sullivan, 'Lawful interception: A mounting challenge for service providers and governments', Press release, 16 May 2011; and Vodafone, 'Law enforcement disclosure report', Feb. 2015.

[9] See Utimaco, 'What is lawful interception', [n.d.].

[10] Rojszczak, M., 'Surveillance law, data retention and human rights: A risk to democracy', *Journal of Law and Society*, vol. 52, no. 2 (2025).

[11] Anstiss, D., 'What is Target Intercept vs Bulk Intercept?', SS8, 27 Oct. 2020.

[12] Privacy International, 'Monitoring centres: Force multipliers from the surveillance industry', 29 Apr. 2014.

[13] These include international standards drawn up by the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP), as well as national standards, such as the 'Technical Guideline for implementation of legal measures for monitoring telecommunications and to information requests for traffic data' (TR TKÜV) developed in Germany, the American National Standards Institute (ANSI) standards developed in the USA and the System of Operative Investigative Measures (SORM) standards developed in Russia.

[14] ETSI technical standards on LI state that 'Law Enforcement Network systems' should never be integrated 'directly into the public network architecture'. In contrast, SORM technical standards on LI do not contain these types of safeguards and are generally seen as being more prone to facilitating human rights abuses. ETSI, 'Lawful

rights abuses.[15] Nonetheless, surveillance frameworks that use LI systems and data retention systems have been used to enable processes of bulk surveillance that have been criticized for violating people's right to privacy.[16] In certain cases, states require a network operator to provide them with some form of 'direct access' to all communications data.[17] In such cases, international and national standards on how LI systems and data retention systems should operate are effectively bypassed.[18]

LI systems, data retention systems, network surveillance systems and monitoring centres have been captured by export controls and sanctions adopted since 2012 (see chapter 3).

Tools associated with methods of device compromise

Since the early 2000s, governments have argued that the growing use of 'over-the-top' messaging services, such as Skype, as well as default end-to-end encryption and the so-called dark web have made traditional processes of LI and data retention ineffective.[19] In response, governments have sometimes sought to require providers of over-the-top messaging services or device manufacturers to deploy 'back doors' that provide them with direct access to decrypted communications data.[20] However, the creation and use of back doors have been criticized for their potential to create cybersecurity flaws.[21] LEAs and intelligence agencies also use different methods of 'device compromise' that allow direct or remote access to a target individual's mobile phone or computer.[22] Governments remain strongly committed to retaining access to device compromise tools and view them as necessary for national security.[23]

'Mobile phone interception equipment' is used to remotely track, identify, intercept and record mobile phones.[24] The most widely cited example of this type of equipment is international mobile subscriber identity (IMSI) catchers, which mimic the functionality of a mobile phone tower in order extract data from mobile phones.[25] 'Digital forensics systems' are used by LEAs or intelligence agencies to retrieve and analyse data stored

interception (LI): Concepts of interception in a generic network architecture (ETSI TR 101 943 V2.2.1)', Nov. 2006; and 'Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America', Insikt Group, 7 Jan. 2025.

[15] E.g., Ericsson's 'Lawful Interception Solution' is designed to limit the number of people who can be intercepted simultaneously. Purdon, L., *Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems*, Case Study, Ericsson (IHRB: London, Nov. 2014).

[16] 'Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), Mass surveillance: ECtHR and CJEU Case-Law: Joint factsheet', 2 Apr. 2025.

[17] EU-based network operators have been criticized for allowing the states where they operate to have direct access to their communication networks. See Galperin, G., 'Swedish telecom giant Teliasonera caught helping authoritarian regimes spy on their citizens', Electronic Frontier Foundation, 18 May 2012.

[18] Privacy International, 'Submission to the UN Special Rapporteur on freedom of expression—Freedom of expression and the private sector in the digital age', Jan. 2016.

[19] See Hess, A., Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, 'Statement before the House Oversight and Government Reform Committee, Subcommittee on Information Technology', 29 Apr. 2015.

[20] See Acosta, L., *Government Access to Encrypted Communications: Comparative Summary* (US Library of Congress: Washington, DC, May 2016).

[21] Vagle, J., 'Cybersecurity and the risks of law enforcement back doors', *Regulatory Review*, 22 Dec. 2014; and Privacy International, 'Liberty and Privacy International complaint against Government's "backdoor" access to Apple data to be heard by Tribunal', 7 Apr. 2025.

[22] Anderson, D., *A Question of Trust: Report of the Investigatory Powers Review* (Her Majesty's Stationery Office: London, June 2015).

[23] See Niinistö, S., Strengthening Europe's Civilian and Military Preparedness and Readiness, European Commission, 2024, p. 115.

[24] Access Now, 'New paper recommends how to keep surveillance tech from human rights abusers', 13 Mar. 2015.

[25] Privacy International, 'IMSI Catchers', 6 Aug. 2018.

on networks, computers and mobile devices.[26] Spyware can be inserted into computers and mobile phones without detection and used to remotely monitor and, in certain cases, control them.[27] Different types of device compromise tools, and particularly spyware, use 'vulnerabilities' and 'exploits' to gain access to the device they are seeking to monitor.[28]

In contrast to the processes of LI and data retention, there is little in the way of detailed international standards regarding when or how tools associated with methods of device compromise can and should be deployed by LEAs and intelligence agencies. These tools, and particularly spyware, have been at the centre of some of the most well-documented cases in which cyber-surveillance tools have been used in connection with serious violations of human rights, including freedom from unlawful detention and freedom from torture.[29] In response, various groups and experts appointed by the UN Human Rights Council have argued for tighter controls on the sale and use of spyware.[30] There have been some efforts to develop clearer standards in this area. The European Commission for Democracy through Law has mapped states' legal frameworks for governing 'the use of spyware as a tool of targeted surveillance'.[31] Experts appointed by the UN Human Rights Council have called for legally binding standards that would make spyware compliant with human rights by design.[32] The Pall Mall Process has sought to outline agreed standards on the responsible production, acquisition and use of spyware (see chapter 4).

The use of tools associated with methods of device compromise also raises a range of national security concerns. The USA has highlighted the use of IMSI catchers in the theft of government and commercial secrets.[33] Digital forensics tools are viewed as tools that can support military operations, since they can be used to gain access to data stored on enemy combatants' electronic devices.[34] Spyware has been a particular source of concern in relation to national security risks. It has been used to target government officials and concerns have been raised about its potential to facilitate attacks on critical infrastructure.[35]

Mobile phone interception equipment, digital forensics systems and spyware have been captured by export controls and sanctions adopted since 2012 (see chapter 3).

Tools of overt surveillance

This paper focuses primarily on software and hardware that have been the focus of export controls adopted at the Wassenaar Arrangement, EU and national levels. For

[26] See 'Digital forensics', Interpol, [n.d].

[27] Council of the European Union, 'Guidelines on the export of cyber-surveillance items under Article 5 of the Regulation (EU) 2021/821 of the European Parliament and of the Council', 15 Oct. 2024, pp. 18–19.

[28] See 'We're All in this Together: A Year in Review of Zero-Days Exploited In-the-Wild in 2023', Google, Mar. 2024.

[29] Citizen Lab, 'Mapping hacking team's "untraceable" spyware', 17 Feb. 2014; and Marquis-Boire, M. et al., 'You only click twice: FinFisher's global proliferation', Citizen Lab, 13 Mar. 2013.

[30] United Nations Human Rights, Office of the High Commissioner (OHCHR), 'Spyware scandal: UN experts call for moratorium on sale of "life threatening" surveillance tech', Press release, 12 Aug. 2021.

[31] Venice Commission, 'Report on a rule of law and human rights compliant regulation of spyware, European Commission for Democracy through Law', [n.d], accessed 5 Sep. 2025.

[32] United Nations Human Rights (OHCHR), 'United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism', Apr. 2023.

[33] Clapper, J. R., Director of National Intelligence, Statement for the Record, 'Worldwide Threat Assessment of the US Intelligence Community', US Senate Select Committee on Intelligence, 23 Mar. 2013; and Stein, J., 'New eavesdropping equipment sucks all data off your phone', Newsweek, 22 June 2014.

[34] Braccini, C. et al., Battlefield Ditigal Forensics: Digital Intelligence and Evidence Collection in Special Operations (NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, 2016).

[35] US Department of State (note 4).

Box 2.1. Categories of cyber-surveillance tools

Tools associated with processes of lawful interception and data retention

Lawful Interception (LI) systems are used by network operators to enable them to comply with requests from LEAs and intelligence agencies to provide users' communications data

Data retention systems are used by network operators to comply with a legal requirement to store 'meta data' on their users for potential later use by LEAs or intelligence agencies

Network surveillance systems are used to intercept, collect and, in some cases, analyse data as it passes through an Internet Protocol network

Monitoring centres are used by LEAs and intelligence agencies to collect, store and analyse different forms of communications data from various surveillance sources

Tools associated with methods of device compromise

Mobile phone interception equipment, such as 'IMSI catchers', is used to remotely track, identify, intercept and record mobile phones

Digital forensics systems are used by LEAs or intelligence agencies to retrieve and analyse data stored on networks, computers and mobile devices

Spyware can be inserted into computers and mobile phones without detection and used to remotely monitor and, in certain cases, control them

Notes: A network operator is a company that manages a communications network. Communications data can be: (*a*) meta data, information about the use of a network or the calls that a network user has made; (*b*) content data, information about what is said in a network user's phone calls or the content of their text messages; or (*c*) location data, information about the movements of a network user.

this reason, the definition of cyber-surveillance tools used in this paper does not include the software and hardware that states use to conduct overt surveillance. These tools include 'social media analytics', 'facial recognition software' and other 'biometric tools'. Due to the risk that they might be used in connection with violations of human rights, the European Parliament and NGOs have called for some of these tools to be made subject to export controls.[36] In July 2024, the USA published a proposal to create licensing requirements for certain exports of 'facial recognition systems specially designed for mass-surveillance and crowd scanning'.[37] However, most states have been unwilling to apply export controls to tools of overt surveillance for fear of disrupting the trade in legitimate cybersecurity products.[38]

The global trade in spyware and other cyber-surveillance tools

States differ in terms of their ability to develop spyware and other cyber-surveillance tools internally and their reliance on the private sector. Many larger states can produce certain forms of spyware and other cyber-surveillance tools for use by their own intelligence agencies and LEAs. However, this model does not appear to be viable for most states, which remain exclusively reliant on the private sector for the procurement of spyware and other cyber-surveillance tools. Even well-resourced governments rely on the private sector for at least some of the tools used by LEAs and intelligence agencies and for the acquisition of spyware and other cyber-surveillance tools.

[36] Amnesty International, 'New EU Dual Use Regulation agreement "a missed opportunity"', 25 Mar. 2021.

[37] US Department of Commerce, 'Export Administration Regulations: Crime Controls and Expansion/Update of US Persons Controls', Federal Register, vol. 89, no. 145, 29 July 2024.

[38] During the review and recast of the EU dual-use regulation, the Commission had proposed extending dual-use export controls to include biometric tools but this was resisted by industry and some EU member states. Stupp, C., 'Commission plans export controls on surveillance technology', EurActiv, 22 July 2016.

Table 2.1 shows the location of companies that produce the seven categories of spyware and other cyber-surveillance tools listed in box 2.1 and that were active in August 2025. The information in table 2.1 is the result of a mapping exercise that SIPRI conducted as part of the drafting of this policy paper. The goal of this mapping was to assess the potential impact of export controls and sanctions on tackling the proliferation and misuse of spyware and other cyber-surveillance tools.

The exercise drew on two sets of sources. First, the mapping analysed previous studies conducted on the scope and content of the 'surveillance industry', the 'spyware market' or the ICT sector more broadly to identify companies that might be relevant.[39] Second, the mapping analysed open-source information produced by these companies, either on their websites or in brochures, to clarify which types of cyber-surveillance tools they produce and where they are located. The mapping sought only to include cases where there was a high level of certainty regarding what the company produced. The mapping only included cases where the company has indicated that it produces a technology that matches the descriptions provided in box 2.1 or where there are two independent sources that indicate that this is the case. When determining location, the mapping sought to list only one state and to indicate the state where a company's main production facilities are located and where export control-related obligations would be most likely to apply. The mapping avoided listing companies as being located in states where they only had sales offices or where their subsidiary companies are located.

The data presented in table 2.1 does not claim to be exhaustive and there are likely to be companies that could have been included if additional source material had been available. There are also likely to be biases in the data, since there are more sources available concerning companies operating in certain parts of the world, such as Europe and North America, than in others, such as China and Russia.

The mapping aims to provide a baseline overview of the proportion of companies that are producing the different types of spyware and other cyber-surveillance tools that have been the focus of export controls and sanctions adopted by the Wassenaar Arrangement, the EU and national governments. To avoid misperceptions about the companies' intentions and any misunderstandings created by the incorrect inclusion of companies, the study does not name the companies identified. The results of this baseline overview are presented in the conclusions of the policy paper. However, some initial findings concerning the range and location of companies that are producing different types of spyware and other cyber-surveillance tools are also presented here.

Producers of spyware and other cyber-surveillance tools can be broadly divided between those that produce tools associated with processes of lawful interception and data retention and those that produce tools associated with methods of device compromise. Among the former are: (*a*) telecommunication network manufacturers, such as Nokia and Ericsson, that produce telecommunications networks for network operators, and which are legally required to have either LI or data retention systems 'built in' to these systems or to enable an interface for their use; (*b*) specialist surveillance technology manufacturers, such as AQSACOM and Utimaco, that produce LI systems and data retention systems for integration into telecommunications networks; and (*c*) large military contractors, such as Thales and BAE Systems, that produce network surveillance systems and monitoring centres for use by intelligence agencies and LEAs. The latter include surveillance technology manufacturers, such as Gamma

[39] The main sources consulted were: Privacy International, 'The Global Surveillance Industry', July 2016; 'Mapping the Shadowy World of Spyware and Digital Forensics Sales', Carnegie Endowment for International Peace, 27 Feb. 2023; Roberts, J. et al., 'Mythical beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights', Atlantic Council, 4 Sep. 2024; 'Technology company dashboards', Business & Human Rights Resource Centre, [n.d], accessed 5 Sep. 2025; and 'Surveillance Watch', [n.d], accessed 5 Sep. 2025.

Table 2.1. Location of companies supplying spyware and other cyber-surveillance tools

	Tools associated with processes of lawful interception and data retention				Tools associated with methods of device compromise			
Technology/ State	Lawful Interception (LI) systems	Data Retention systems	Network surveillance systems	Monitoring centres	Mobile phone interception equipment	Digital forensics systems	Spyware	No. of companies
Australia	..	..	1	..	..	..	1	2
Austria	..	..	..	..	..	..	1	1
Canada	..	..	1	..	1	4	..	6
China	3	..	..	..	1	4	2	10
Croatia	1	1	1	..	..	..	..	1
Cyprus	..	..	..	..	1	1	1	3
Czechia	..	..	..	..	..	2	1	3
Denmark	..	..	..	..	2	1	..	3
Finland	1	..	..	..	1	..	..	2
France	2	2	3	2	1	4	..	8
Germany	4	2	4	5	2	3	2	15
India	1	..	2	3	2	2	5	8
Israel	1	..	1	4	7	3	11	21
Italy	3	1	1	7	4	3	9	13
Luxembourg	..	..	..	..	..	..	1	1
Mexico	..	..	..	..	1	..	..	1
Netherlands	1	1	..	1	1	..	..	2
New Zealand	..	..	1	..	1	..	..	2
North Macedonia	..	..	..	..	..	..	1	1
Russia	8	1	1	2	..	1	1	11
Serbia	..	..	..	..	2	..	..	2
Singapore	..	..	..	1	1	..	1	2
Slovenia	1	..	..	..	..	..	..	1
South Africa	..	..	1	..	..	..	..	1
Spain	..	..	..	1	..	..	1	2
Sweden	2	..	..	..	1	1	..	3
Switzerland	..	..	..	..	6	1	..	6
Türkiye	..	..	1	1	1	1	1	2
UAE	..	..	..	..	..	..	2	2
United Kingdom	4	1	1	3	5	6	1	18
USA	7	2	3	11	7	16	1	35
Total	**39**	**11**	**22**	**41**	**48**	**53**	**43**	**188**

.. = no data found.

Note: The table lists the number of companies located in each country and the types of spyware and other cyber-surveillance tools that they produce. Since many companies produce more than one type of technology, the number of companies located in each country is often lower than the number of technologies produced.

International and NSO Group, that produce certain types of device compromise tools, such as mobile phone interception equipment, digital forensics systems or spyware, for use by intelligence agencies and LEAs.

These companies are diverse in terms of their size, their level of familiarity with export controls and sanctions, and their awareness of the obligations these create. They do not form any kind of coherent 'sector' and there is no single industry association at either the national or the regional level to which they all belong. Larger military contractors might be members of defence and security associations, such as the Aerospace, Security and Defence Industries Association of Europe (ASD), while telecommunication network manufacturers might be members of ICT-focused associations, such as Digital Europe. However, very few companies are likely to be members of both types of association and specialist surveillance technology manufacturers might not be a member of either type or any association at all.

While these companies are located on all continents, this is a highly concentrated sector. The mapping identified 188 companies located in 31 states that are manufacturers of spyware and other cyber-surveillance tools: 65 per cent of these are in seven states (China, Germany, Israel, Italy, Russia, the United Kingdom and the USA). The industry is also geographically concentrated: 51 per cent of companies are located in 19 states in Europe, 22 per cent are in three states in the Americas (Canada, Mexico and the USA), 13 per cent are in three states in the Middle East (Israel, Türkiye and the United Arab Emirates (UAE)) and 13 per cent in five states in Asia and Oceania (Australia, China, India, New Zealand and Singapore). Only one company is located in Africa (South Africa). The mapping identified 43 companies located in 18 states that manufacture spyware, indicating that this sector is more concentrated than for cyber-surveillance tools more broadly. Over half of these companies (58 per cent) are located in three states (India, Israel and Italy); 44 per cent are located in 10 states in Europe, 33 per cent in three states in the Middle East (Israel, Türkiye and the UAE) and 21 per cent in four states in Asia and Oceania (Australia, China, India and Singapore).

3. Regulating the trade in spyware and other cyber-surveillance tools

States have developed instruments at the multilateral, regional and national levels to establish common standards on export controls for dual-use goods and technologies. These have been used to increase oversight and control over the trade in certain categories of spyware and other cybersurveillance tools. The Wassenaar Arrangement is the primary multilateral instrument in this field. The controls agreed at the Wassenaar Arrangement are integrated into other relevant regulatory frameworks, such as those developed within the EU, and implemented by states through their national export control systems. In addition to export controls, states have collectively or individually used sanctions to prohibit transfers of spyware and other cybersurveillance tools to specific destinations or to target certain spyware manufacturers.

The Wassenaar Arrangement

The Wassenaar Arrangement was established in 1996 to promote 'transparency and greater responsibility' regarding transfers of military and dual-use items. The Wassenaar Arrangement has 42 participating states and maintains detailed control lists of military and dual-use items.[40] Any Wassenaar Arrangement participating state can propose changes to the control lists, which must be adopted by consensus. At least 22 states that are not Wassenaar participants apply the Wassenaar dual-use list through their national export controls.[41]

Almost all EU member states are Wassenaar Arrangement participating states, alongside Russia, Ukraine and the USA. The work of the Wassenaar Arrangement has become increasingly challenging since Russia's full-scale invasion of Ukraine in February 2022. For instance, it has reportedly become more difficult to agree on the adoption of new control list categories for key emerging technologies.[42] The challenges that this forum currently faces might limit its potential to adopt new controls or to establish new norms or good practices in this area. However, the Wassenaar Arrangement continues to function and is due to hold its next annual plenary meeting towards the end of 2025.

Spyware and other cyber-surveillance tools captured by the Wassenaar Arrangement dual-use list

The Wassenaar Arrangement dual-use list is intended to capture items that have been developed for civilian purposes but are also 'major or key elements for the indigenous development, production, use or enhancement of military capabilities'.[43] Before 2012,

[40] These states are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, the United Kingdom and the United States. Wassenaar Arrangement, 'Introduction'.

[41] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Cyprus, Georgia, Jordan, Kazakhstan, Kosovo, Laos, Malaysia, Moldova, Montenegro, North Macedonia, Pakistan, Panama, Philippines, Serbia, Singapore, Thailand and the UAE have integrated the EU dual-use list, which incorporates the Wassenaar dual-use list, into their national control lists. See Michel, Q. and Paile, S., 'Countries having adopted the EU dual-use list as national control list: Working Document', University of Liege, [n.d]. In addition, Israel integrates the Wassenaar dual-use list into its national control list. See US Department of Commerce, 'Israel export control information'.

[42] Brockmann, K. and Héau, L., 'The multilateral export control regimes', *SIPRI Yearbook 2024: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2024).

[43] Wassenaar Arrangement, 'Criteria for the selection of dual-use items (Adopted in 1994 and amended by the Plenary in 2004 and 2005)', 2005.

systems that employ a certain standard of encryption, or that enable the decryption of encrypted data, were included in Category 5, Part 2 (Information Security).[44] Certain types of LI systems and data retention systems use a level of encryption that can make them subject to dual-use export controls on these grounds.[45] Since 2012, list-based controls have been adopted to capture five additional categories of spyware and other cyber-surveillance tools (see below). Although they have been added to the Wassenaar dual-use list, these are better described as 'single-use' technologies because they are designed solely for use by LEAs and intelligence agencies and are not intended for civilian applications.

Mobile telecommunications interception or jamming equipment

Controls on 'mobile telecommunications interception or jamming equipment' (5.A.1.f) were added to the Wassenaar Arrangement dual-use list in 2012. The controls capture IMSI catchers and equipment that creates fake Wi-Fi hotspots for surveillance purposes, as well as 'certain types of items specially designed to enable "deep packet inspection" into telecommunications systems'.[46] These controls capture certain types of mobile phone interception equipment (see box 2.1).

Internet Protocol network communications surveillance systems

Controls on 'IP [internet protocol] network communications surveillance systems' (5.A.1.j) were added to the Wassenaar Arrangement dual-use list in 2013. They capture tools that can monitor and analyse internet traffic and that are able to analyse, extract and index 'transmitted metadata content (voice, video, messages, attachments) based on "hard selectors", and map the relational network of people'.[47] These controls capture certain types of network surveillance systems (see box 2.1).

Systems for the generation, command and control or delivery of intrusion software

Controls on systems for the 'generation, command and control, or delivery' of 'intrusion software' (4.A.5) were added to the Wassenaar Arrangement dual-use list in 2013. The controls define intrusion software as software that is 'specially designed or modified to avoid detection by "monitoring tools", or to defeat "protective countermeasures", of a computer or network-capable device' in order to remotely extract or modify data and, in some cases, take control of the device. The controls capture certain types of spyware (see box 2.1). Following adoption of the controls, companies and researchers noted that the language used describes systems and processes that are essential to IT security. Particular concern was raised about the possibility that the controls might capture tools used for 'penetration testing', in which attacks on ICT systems are simulated to test their weaknesses, and processes of 'vulnerability disclosure', through which software vulnerabilities are identified and reported.[48] In 2017, explanatory

[44] See Saper, N., 'International cryptography regulation and the global information economy', *Northwestern Journal of Technology and Intellectual Property*, vol. 11, no. 7 (Fall 2013).

[45] See Utimaco, *Utimaco LIMS: Lawful Interception of Telecommunication Services* (Utimaco Safeware AG: Aachen, Germany: Feb. 2011).

[46] Council of the European Union (note 27)

[47] Council of the European Union (note 27), p. 18. 'Hard selectors' refers to data or a set of data that is 'related to an individual (e.g., family name, given name, e-mail, street address, phone number or group affiliations)'. Wassenaar Arrangement, 'List of Dual-use Goods and Technologies and Munitions List', 5 Dec. 2024, p. 222.

[48] Bratus, S. et al., 'Why Wassenaar Arrangement's definitions of intrusion software and controlled items put security research and defense at risk, and how to fix it', 9 Oct. 2014. 'Penetration testing tools' are used to test the

notes were added to the controls, specifying that they do not apply to 'vulnerability disclosure' and 'cyber incident response'.[49] The explanatory notes did not explicitly exclude penetration testing tools or software vulnerabilities and exploits from their coverage.[50] Certain penetration testing tools have the potential to be repurposed as offensive cyber tools and certain types of software exploits can be used to gain control of a target device.[51] There are indications that some governments are using the controls on intrusion software to regulate the trade in certain advanced types of penetration testing tools and software exploits.[52]

Communications monitoring software

Controls on software 'for monitoring or analysis for law enforcement purposes' (5.D.1.e) were added to the Wassenaar Arrangement dual-use list in 2019. The controls apply to software used by LEAs and intelligence agencies to analyse communications data or meta data that has been provided by a communications service provider. These controls capture certain types of monitoring centres (see box 2.1).

Digital forensics or investigative tools

Controls on digital forensics or investigative tools (5.A.4.b) were added to the Wassenaar Arrangement dual-use list in 2019. The controls apply to systems that can '"Extract raw data" from a computing or communications device' and 'Circumvent [the] "authentication" or authorisation controls of the device'.[53] These controls capture certain types of digital forensics systems (see box 2.1).

All these controls only apply if the exported item meets the technical standards described in the control list category. This means that tools that perform the functions described in box 2.1 might not be captured if they do not meet these technical standards. There have been reports of companies supplying digital forensics tools that do not meet the technical standards specified in the Wassenaar dual-list and that therefore do not require an export licence.[54] States can and do use 'catch-all controls' to capture exports of items that are not covered by their control lists but which could be supplied to prescribed end-users or for prescribed end-uses.[55]

The potential and limitations of the Wassenaar Arrangement controls

The controls that have been adopted by the Wassenaar Arrangement can play a key role in improving oversight, transparency and restraint in the trade in spyware and other cyber-surveillance tools. However, there are also limitations to what they can achieve. Some of these limitations mirror issues encountered in the application of export

security of a network by simulating attacks against it to locate vulnerabilities. 'Vulnerability disclosure' is the means through which software vulnerabilities are identified and reported.

[49] Wassenaar Arrangement (note 47).

[50] See Hinck, G., 'Wassenaar Export Controls on surveillance tools: New exemptions for vulnerability research', *Lawfare*, 18 Jan. 2023.

[51] See UK National Cyber Security Centre, 'The threat from commercial cyber proliferation', 19 Apr. 2023.

[52] See UK Export Control Organisation, 'Intrusion software tools and export control', 10 Aug. 2015.

[53] Wassenaar Arrangement (note 47), p. 99.

[54] Chandler, Z. C. and Caitlin L., 'Tools for repression in Myanmar expose gap between EU tech investment and regulation', The Intercept, 14 June 2021.

[55] Italian Ministry for Foreign Affairs and International Cooperation, UAMA National Authority, 'Applicazione clausola "catch all" per motori e componenti destinati al settore dell'aviazione [Application of the 'catch-all' clause to engines and components intended for the aviation sector]', 19 July 2023.

controls to other technologies and sectors but some are more specific to controls on spyware and other cyber-surveillance tools.

Export controls and 'oversight'

The Wassenaar Arrangement guidelines specify the information that states should require as part of an export licence application. This information comprises a description of the item, such as 'type, quantity, value, [and] weight', its 'specifications' and 'performance characteristics', the 'applicant', the 'purchaser', the 'end-user' (if different from purchaser) and the 'end-use'.[56] Similar language is used in other agreements and good practice guides in the field of export controls. This information can provide a detailed record of the activities of companies that are supplying spyware and other cyber-surveillance tools. Wassenaar Arrangement participating states share information with each other on denials of dual-use export licences for transfers to non-participants and discuss aspects of export control enforcement.

Export controls and 'transparency'

If it is made public, the information that states collect as part of the export licensing process can act as a source of transparency, in terms of assessing how states are implementing controls on exports of spyware and other cyber-surveillance tools and generating a more detailed picture of the global trade in these items. The Wassenaar Arrangement does not impose any requirements regarding public transparency. Many states publish detailed information on licences issued and denied for exports of military equipment.[57] However, very few states publish equivalent information on exports of dual-use items. Two key exceptions are the UK and Switzerland, which publish data on exports of dual-use items at a level of disaggregation that makes it possible to identify licences granted, and in the case of Switzerland denied, for spyware and other cyber-surveillance tools.[58] In several cases, journalists have been able to access additional data that states have not published by submitting freedom of information (FOI) requests.[59]

Export controls and 'restraint'

Export controls allow states to block transfers of controlled items due to national security concerns, threats to regional or international security or the potential risk of violations of human rights and IHL. All states have an obligation under Article 1 common to the Geneva Conventions of 1949 to 'respect and ensure respect' for IHL, which is widely viewed as a requirement to assess whether exported arms will be used in violation of IHL.[60] States can also use export controls to impose 'post-shipment controls' that seek to place limits on the ways an exported item can be used or who can

[56] Wassenaar Arrangement, 'Public documents, volume III: Compendium of best practice documents compiled by the Wassenaar Arrangement Secretariat', Dec. 2023.

[57] See SIPRI, 'National reports on arms exports', [n.d], accessed 5 Sep. 2025.

[58] See UK Department for International Trade, 'Reports and statistics home', 15 May 2025, '; and Switzerland State Secretariat for Economic Affairs (SECO), 'Permis d'exportation individuels établis pour les biens à double usage et de biens militaires spécifiques [Individual export permits issued for dual-use and specific military goods]', 1 Apr. 2025.

[59] See Tesic, A., 'Serbia imports wireless equipment capable of indiscriminate mass surveillance', Balkan Insight, 12 Dec. 2024; Cox, J., 'New data gives peek at European IMSI Catcher exports', VICE, 23 Mar. 2018; Gjerding, S. and Andersen, L. S., 'How European spy technology falls into the wrong hands', The Correspondent, 23 Feb. 2017; and WOZ, 'Der Rüstungsreport – ein Portal für die Transparenz [The Armaments Report – a portal for transparency]' [n/d]. accessed 5 Sep. 2025.

[60] ICRC, 'Arms transfers to parties to armed conflict: What the law says', 3 June 2024. Many of the obligations outlined in the Geneva Conventions, including those on the prevention of torture, are widely viewed as 'erga omnes',

use it.[61] The Wassenaar Arrangement has produced a range of good practice guides that specify standards that participating states should apply when assessing export licences. The guides recommend that states exporting conventional weapons consider whether there is 'a clearly identifiable risk that the weapons might be used to commit or facilitate the violation and suppression of human rights and fundamental freedoms' or 'the laws of armed conflict'.[62] However, there is no equivalent recommendation for exports of dual-use items. The Wassenaar Arrangement guidelines also state that 'decisions on export licensing remain under national control of each [Wassenaar Arrangement] Participating State'.[63] States that participate in the Wassenaar Arrangement have been criticized for approving licences for the transfer of cyber-surveillance tools to states accused of using them in ways that violate human rights.[64]

Export controls and 'intangible items'

Export controls are a complex regulatory instrument that require the appropriate allocation of time, resources and expertise by a national government in order for them to function effectively. Many of the items on the Wassenaar Arrangement dual-use list are not physical goods but 'intangible' products, such as software and technical data, that can be transferred electronically. Effective implementation and enforcement of controls on intangible transfers of technology (ITT) require licensing authorities to have capabilities in certain areas, such as digital forensics tools, that may not be available in smaller states.[65] The application of export controls to ITT presents compliance challenges for companies. One key point that has emerged in discussions about ITT controls is how export controls should apply when an end-user is given access to controlled software in a Software as a Service (SaaS) model.[66] SaaS models involve vendors making software applications available to users through cloud computing without having to download them. There appear to be cases in which companies make different forms of spyware and other cyber-surveillance tools available to end-users in a SaaS model.[67] The decisions that states make about how export controls are framed and applied in this area might affect their ability to require companies exporting spyware and other cyber-surveillance tools to apply for licences.

The EU dual-use regulation

Regulation (EU) 2021/821, the EU dual-use regulation, establishes common standards among EU member states for controls on the export, re-export, brokering and transit of dual-use goods, software and technology.[68] The regulation is directly applicable

meaning that all states are obliged to take steps to prevent violations by another state. See International Criminal Tribunal for the former Yugoslavia, 'Prosecutor V Anton Furundzija: Judgement', 10 Dec. 1988, para. 151.

[61] See Bromley, M., Héau, L. and Maletta, G., 'Post-shipment on-site inspections: Multilateral steps for debating and enabling their adoption and use', SIPRI, Oct. 2022.

[62] Wassenaar Arrangement, 'Elements for Objective Analysis and Advice Concerning Potentially Destabilising Accumulations of Conventional Weapons', adopted in 2004 and revised in 2011.

[63] Wassenaar Arrangement (note 56).

[64] Stamouli, N., 'Greece leaves spy services unchecked on Predator hacks', Politico, 7 Aug. 2024; and Business and Human Rights Resource Centre, 'Novalpina Capital claims NSO Group received export licences from Bulgaria & Cyprus, but both states deny claims', 13 Sep. 2019.

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

[66] Brockmann, K. and Héau, L., 'Spyware as a service: Challenges in applying export controls to cloud-based cyber-surveillance software', SIPRI, 27 Apr. 2025.

[67] Brockmann and Héau (note 66).

[68] 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),

law across the EU but is implemented and enforced by EU member states through their national control systems. This means that EU member states are responsible for assessing and issuing export licences.

The current version of the EU dual-use regulation entered into force in September 2021 after an extensive process of review and recast that, among other things, sought to strengthen controls on exports of spyware and other cyber-surveillance tools. During the process, members of the European Parliament and NGOs argued that the controls adopted by the Wassenaar Arrangement left gaps and were being applied inconsistently by EU member states.[69] They sought to use the review process to establish more comprehensive and better aligned export control measures at the EU level. The 2021 dual-use regulation outlines a number of measures aimed at creating stronger controls on exports of 'cyber-surveillance items', which are defined 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'.[70] The definition of cyber-surveillance items captures all the spyware and other cyber-surveillance tools listed in box 2.1.

Spyware and other cyber-surveillance tools captured by the EU dual-use regulation

Annex I of the regulation lists the dual-use items subject to control under the EU dual-use regulation, which integrates the control lists adopted by the four multilateral export control regimes, including the Wassenaar Arrangement. EU member states are also able to adopt national controls on items that are not captured by the EU dual-use list. Germany and Spain have each adopted national controls on data retention systems (see box 2.1).[71]

Certain dual-use items considered particularly sensitive are listed in Annex IV of the regulation. These require a licence for intra-EU transfers. Certain powerful encryption and decryption tools are listed in Annex IV and are subject to intra-EU transfer controls. However, the five categories of spyware and other cyber-surveillance tools added to the Wassenaar Arrangement since 2012 and the EU dual-use lists since 2013 are not included. This means that transfers of these items between EU member states are not subject to the same level of regulatory oversight as when they are exported outside the EU. A 2023 report by the European Parliament's Committee of Inquiry investigating the use of Pegasus and equivalent surveillance spyware (PEGA Committee) highlights several cases in which spyware had been deployed within the EU without appropriate checks or used by national governments 'for purely political purposes', such as to target 'critics and opponents of the parties in power'.[72] In response, the European Commission was reported to be working on a draft communication in mid-2024 to address the possible misuse of spyware at the national level.[73]

Official Journal of the European Union, L206, 11 June 2021.

[69] Bromley, M., *Export Controls, Human Security and Cyber-Surveillance Technology: Examining the Proposed Changes to the EU Dual-use Regulation* (SIPRI, Stockholm, 2017).

[70] Bromley, M. and Brockmann, K., 'Implementing the 2021 recast of the EU dual-use regulation: Challenges and opportunities', *EU Non-Proliferation and Disarmament Papers*, no. 77, EU Non-proliferation and Disarmament Consortium, Sep. 2021.

[71] 'Information on measures adopted by member states in conformity with Articles 4, 5, 6, 7, 8, 9, 11, 12, 22 and 23. 2023/C 208/06', *Official Journal of the European Union*, C 208, 15 June 2023.

[72] European Parliament, 'Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware', (2022/2077(INI)), 22 May 2023.

[73] Roussi, A., 'Curb your snooping, Commission tells EU governments', Politico, 22 July 2024.

Article 5 of the 2021 dual-use regulation introduced a new 'catch-all control' to regulate exports of cyber-surveillance items that are not covered by the EU dual-use list but which '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'.[74] The catch-all control can be triggered by the licensing authority notifying an exporter of the need to apply for a licence. It can also be triggered by an exporter notifying the licensing authority that, based on its due diligence findings, it has become aware that the exported items could be used for proscribed end-uses. Article 5(3) allows member states to impose an authorization requirement on non-listed cyber-surveillance items. Article 5(6) creates a procedure through which EU member states can collectively choose to adopt new controls on cyber-surveillance items. In October 2024, the European Commission published guidelines aimed at supporting the implementation of Article 5 by exporters.[75] The guidelines elaborate on the content of the provisions in Article 5 and the definition of cyber-surveillance items provided by the dual-use regulation. They also outline various 'red flags' that might signal a risk of potential misuse.

Article 5 could be used to control spyware and other cyber-surveillance tools that do not meet the thresholds outlined in the Wassenaar Arrangement control list or to adopt new control list categories that cannot be agreed within the Wassenaar Arrangement. However, use of the new catch-all control has been limited to date. There have been no reports of member states notifying an exporter of the need to apply for a licence or a company notifying a member state of the potential need to do so. As of October 2024, only five EU member states had adopted automatic licensing requirements under Article 5(3) and Article 5(6) had not been used.[76] The EU and EU member states are discussing how to overcome the challenges created by current difficulties with adding new items to the control lists of the multilateral export control regimes. In January 2024, the European Commission published a white paper that recommended the creation of uniform EU controls on 'those items that were not adopted by the multilateral export control regimes due to the blockage by certain members'.[77] In September 2025, the Commission published its annual update of the EU dual-use list and included, for the first time, items that had not been added to the control lists of the multilateral export control regimes.[78] The precedent set by this step establishes another potential avenue for agreeing EU controls on new categories of cyber-surveillance tools.

The potential and the limitations of the EU dual-use regulation

The framework established by the EU dual-use regulation has the potential to go significantly further than the Wassenaar Arrangement in terms of using export controls to promote oversight, transparency and restraint in the trade in spyware and other cyber-surveillance tools. However, there also limitations in what the EU framework has achieved to date and could achieve in future.

[74] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 (note 68).

[75] Council of the European Union (note 27).

[76] European Union, Information Note, 'Regulation (EU) 2021/821 of the European Parliament and of the Council Setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items: Information on measures adopted by member states in conformity with articles 4, 5, 6, 7, 8, 9, 11, 12, 22 and 23', 2 Oct. 2024.

[77] European Commission, 'White paper on export controls', COM(2024) 25 final, 24 Jan. 2024.

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

Export controls and 'oversight'

There are detailed structures for sharing information on approvals and denials of export licences at the EU level. Under the EU dual-use regulation, member states are required to share information on approvals and denials of export controls licences. EU member states also meet in the Dual-use Working Party (chaired by the European Council) and the Dual-use Coordination Group (chaired by the European Commission) to discuss implementation of the EU dual-use regulation. These are supported by various technical expert groups, including the Surveillance Technology Expert Group (STEG) which focuses on exports of spyware and other cyber-surveillance tools. The 2021 dual-use regulation also establishes an 'enforcement coordination mechanism' to bring together member states' licensing authorities and enforcement agencies to discuss 'the detection and prosecution of unauthorised exports of dual-use items'.[79]

Export controls and 'transparency'

The 2021 dual-use regulation commits the EU to release more detailed information on exports of dual-use items, and cyber-surveillance items in particular. Prior to 2021, the EU published aggregated data on members states' exports of dual-use items. The 2021 regulation creates an obligation on member states to provide this information and on the European Commission to publish an annual report. It also specifies a greater level of detail to be included in the report.[80] In January 2025, the EU published the first edition of this annual report, covering 2022.[81] Through these reports, the EU has provided aggregated data on member states' licence applications for the export of cyber-surveillance items broken down by category and destination, the overall number of authorizations granted and the overall number of licence applications denied for 2015 to 2022 (see table 3.1). There is still room to improve the quality and quantity of information provided through this aggregated report. Only 14 member states provided data on their exports of cyber-surveillance items for the 2022 reporting period.

Notably, only two licence applications for exports of digital forensics tools were reported in the period 2021–22, even though there appear to be at least 15 companies based in EU member states that supply these tools (see table 2.1). This could indicate that companies are supplying digital forensics tools that do not meet the technical thresholds specified in the Wassenaar Arrangement dual-use list. Since 2015, between 7 and 25 licences for exports of intrusion software have been approved or applied for in each year. However, the significance of this data is hard to determine without knowing more about the types of products that are being captured by these licences. As highlighted above, there are indications that exports of certain advanced types of penetration testing tools and software exploits may be captured by these controls.

Export controls and 'restraint'

EU member states are required to 'take into account' the considerations covered by the EU Common Position on arms exports (EU Common Position) when assessing exports of dual-use items to 'the armed forces or internal security forces or similar entities in [a] recipient country'.[82] The EU Common Position outlines a range of risk criteria, such

[79] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 (note 68), Article 25(2).

[80] European Commission, 'Statistical update on dual-use export control (2021)', Commission Staff Working Document, SWD(2023) 341 final, 19 Oct. 2023, p. 2.

[81] European Commission, 'Staff working document, comprehensive data sets related to export controls of dual-use items for the year 2022, accompanying the document report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items', 30 Jan. 2025, pp. 30–32.

[82] Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment, *Official Journal of the European Union*, L335, 8 Dec. 2008.

Table 3.1. Export licences and denials by EU member states for exports of spyware and other cyber-surveillance tools, 2015–22

	2015	2016	2017	2018	2019	2020	2021	2022
Mobile telecommunications interception or jamming equipment	98	111	168	127	31	24	96	216[a]
Internet Protocol network communications surveillance systems	10	3	8	20	5	3	1	16[a]
Systems for the 'generation, command and control, or delivery' of 'intrusion software'	7	25	16	13	8	10	11	20[a]
Communication monitoring software	..	..	..	..	..	..	6	28[a]
Digital forensics or investigative tools	..	..	..	..	..	..	1	1[a]
Other listed items that can be used as cyber-surveillance items	–	–	–	–	–	–	–	7[a]
Total number of denials	**–**	**17**	**34[b]**	**–**	**81**	**32**	**35**	**37**

[a] Figures refer to applications for export licences.

[b] 20 denials were issued in 2017 for 'mobile telecommunications interception or jamming equipment', 1 for 'Internet Protocol network communications surveillance systems' and 13 for systems for the 'generation, command and control, or delivery' of 'intrusion software'.

.. = The control list categories for these items were not in place.

– = Data either not available or not found

Source: European Commission, Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, COM(2017) 679 final, Brussels, 21 Nov. 2017; European Commission, Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, COM/2018/852 final, Brussels, 14 Dec. 2018; European Commission, Report from the Commission to the European Parliament and the Council, on the implementation of Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, including a report on the exercise of the power to adopt delegated acts conferred on the Commission pursuant to Regulation (EU) No 599/2014 of the European Parliament and the Council of 16 April 2014 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, COM(2019) 562 final, Brussels, 4 Nov. 2019; European Commission, Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, COM(2021) 716 final, Brussels, 23 Nov. 2021; European Commission, Commission Staff Working Document, Statistical update on dual-use export control (2021), Brussels, 19 Oct. 2023, p. 10; and European Commission, 'Staff working document, comprehensive data sets related to export controls of dual-use items for the year 2022, accompanying the document report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items', 30 Jan. 2025, p. 31.

as the likelihood that an item will be used for internal repression or in the commission of serious violations of IHL, and its accompanying User's Guide provides additional clarification on how to assess these risks.[83] The operative language on risk assessments was not substantially altered by the 2021 recast but additional text was added to the preamble, emphasizing that EU member states should pay particular attention to the risk that exported cyber-surveillance items might be misused to facilitate international repression and violate human rights and IHL. Amendments were also made to the text of the EU Common Position in April 2025.[84] According to amended criterion 2, EU member states should deny an export licence if there is a clear risk that the exported items might be used not only to 'commit' but also to 'facilitate' internal repression or serious violations of IHL.

The human rights violations that have been associated with the use of spyware and other cyber-surveillance tools range from infringements of the right to privacy, freedom of expression and freedom of association, to breaches of 'non-derogable' and 'inviolable' rights, such as freedom from torture and inhuman or degrading treatment.[85] Preventing these types of violations requires states to have effective technical and legal safeguards to ensure that spyware and other cyber-surveillance tools comply with human rights standards and are only deployed in ways that are in compliance with such standards.[86] Violations of IHL involving the use of spyware and other cyber-surveillance tools have not been as extensively documented but international organizations and NGOs have raised concerns about their potential to facilitate attacks on civilians during armed conflicts.[87]

While detailed, the EU Common Position and User's Guide focus on transfers of military equipment. They do not explicitly consider or elaborate on the human rights- or IHL-related risks posed by exports of spyware and other cyber-surveillance tools or how to identify and prevent potential cases of mis-use.[88] EU member states continue to be criticized by NGOs and parliamentarians for issuing licences for exports to third countries with problematic human rights records.[89] The EU has also been criticized for failing to conduct adequate risk assessments when providing surveillance capabilities to third countries in connection with law enforcement capacity-building activities.[90] Since 2021, the European Ombudsman has twice found deficiencies in the way the European Commission and the European External Action Service (EEAS) conduct human rights impact assessments in connection with these activities.[91]

[83] Council Common Position 2008/944/CFSP of 8 December 2008 (note 81); Council of the European Union, User's Guide to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment, 6881/25, Brussels, 14 Apr. 2025.

[84] Council Common Position 2008/944/CFSP of 8 December 2008 (note 82).

[85] OHCHR, 'Spyware and surveillance: Threats to privacy and human rights growing, UN report warns', Press release, 16 Sep. 2022.

[86] See Access Now et al., *Necessary and Proportionate: International Principles on Application of Human Rights to Communication Surveillance*, May 2014.

[87] Rizk, J. and Cordey, S., 'What we don't understand about digital risks in armed conflict and what to do about it'. ICRC, 27 July 2023.

[88] Bromley, M. and Maletta, G., 'Making the most of the EU catch-all control on cyber-surveillance exports', SIPRI Commentary, 18 Oct. 2024.

[89] Ekathimerini, 'NYT: Govt. admits giving Intellexa license to export Predator to Madagascar', 8 Dec. 2022.

[90] Privacy International, '"When spiders share webs": Unveiling privacy threats of EU-funded INTERPOL policing programme in West Africa', 26 Sep. 2024.

[91] European Ombudsman, 'How the European External Action Service (EEAS) assesses the potential human rights risk and general impact before providing assistance to non-EU countries to develop surveillance capabilities', 5 Oct. 2022; and European Ombudsman, 'Decision on how the European Commission assessed the human rights impact before providing support to African countries to develop surveillance capabilities (case 1904/2021/MHZ)', 28 Nov. 2022.

Export controls and 'intangible items'

The EU has a range of tools that could be used to increase the ability of member states to manage the complexities associated with implementing controls on exports of spyware and other cyber-surveillance tools. Under the 2021 dual-use regulation, the European Commission is tasked with supporting an EU 'licensing and enforcement capacity-building programme, including by developing, in consultation with the Dual-Use Coordination Group, common training programmes for officials of the Member States'.[92] The EU also publishes guidance material that aims to establish a more uniform application of the dual-use regulation among EU member states and to inform companies and research institutes of their compliance obligations.[93] The EU is currently working on common guidelines on the implementation of ITT controls among member states. The preamble to the EU dual-use regulation encourages member states to develop a harmonized approach with regard to the application of export controls to cloud computing and the common guidelines are expected to address this topic.[94]

US export controls

The export of dual-use items from the USA is governed by the Export Administration Regulations (EAR), which control the export of dual-use items on the US Commerce Control List (CCL). The EAR are administered by the US Bureau of Industry and Security (BIS) in the US Department of Commerce.[95] List-based controls under the EAR incorporate the control lists adopted by the four multilateral export control regimes, including the Wassenaar Arrangement. A licence exemption for Authorized Cybersecurity Exports (ACE) allows the export to most destinations of items necessary for legitimate cybersecurity work related to 'vulnerability disclosure' and 'cyber incident response', among other things.[96]

In addition to list-based controls, the EAR contain control instruments that in other regulatory frameworks, including the EU's, would typically fall outside the scope of export controls and be more closely aligned with sanctions. For example, the USA can use its Entity List as a form of end-user control to impose licence requirements on exports to specific individuals or addresses of persons that are believed to be involved in activities contrary to US national security or foreign policy interests. BIS has added several manufacturers of commercial spyware to the Entity List for engaging in malicious cyber activities. In November 2021, NSO Group and Candiru (based in Israel), Positive Technologies (based in Russia) and Computer Security Initiative Consultancy PTE. LTD (based in Singapore) were added to the list.[97] In July 2023, Intellexa SA

[92] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 (note 68), Article 24(4).

[93] See Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, *Official Journal of the European Union*, L 338/1, 15 Sep. 2021.

[94] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 (note 68); and European Commission, 'Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items', COM(2025)19, 30 Jan. 2025.

[95] Bromley, M. and Brockmann, K., *A Tale of Two Systems: Alignment, Divergence and Coordination in EU and US Dual-Use Export Controls*, IAI Papers no. 24/15, May 2024.

[96] Bureau of Industry and Security, § 740.22, Authorized Cybersecurity Exports (ACE), accessed 25 June 2025; and Wolf, K. J. et al., 'US Department of Commerce implements new export controls to combat malicious cyber activities', Akin, 17 Mar. 2022.

[97] US Department of Commerce, 'Commerce adds NSO Group and other foreign companies to Entity List for malicious cyber activities', 3 Nov. 2021.

(based in Greece), Intellexa Limited (based in Ireland), Cytrox AD (based in North Macedonia) and Cytrox Holdings (based in Hungary) were also added.[98] The listings specified that the companies had supplied 'spyware', 'cyber tools' or 'cyber exploits' that had been used to gain unauthorized access to information systems.

In 2020, amendments were made to the EAR to allow BIS to review licence applications for any items against human rights concerns.[99] Referred to as the 'Human Rights Crossover Rule', the amendments aimed to prevent US technologies being used for 'nefarious end uses', such as 'surveillance' and 'censorship'.[100]

The US government publishes information on exports of dual-use items in its 'Annual Country Licensing and Trade Analysis' reports, but these only provide details of the largest categories of exports, not at a level of disaggregation that allows for the identification of exports of spyware and other cyber-surveillance tools.[101] NGOs have called on the US government to publish more detailed information on exports of dual-use items, and particularly exports of spyware and other cyber-surveillance tools.[102] The 'Maintaining American Superiority by Improving Export Control Transparency Act' was signed into law in August 2025. This amends the 2018 Export Control Reform Act and requires BIS to submit an annual report to Congress on licence applications and enforcement actions.[103] However, the impact on public transparency will be quite limited since the report will not be publicly available, with the exception of aggregate statistics.[104]

Under the Biden administration, the USA focused on countering the proliferation and misuse of 'commercial spyware' because of the threats this poses to national security and human rights.[105] In Executive Order 14093 of March 2023, commercial spyware is defined as:

> Any end-to-end software suite that is furnished for commercial purposes, either directly or indirectly through a third party or subsidiary, that provides the user of the software suite the capability to gain remote access to a computer, without the consent of the user, administrator, or owner of the computer, in order to: (i) access, collect, exploit, extract, intercept, retrieve, or transmit content, including information stored on or transmitted through a computer connected to the Internet; (ii) record the computer's audio calls or video calls or use the computer to record audio or video; or (iii) track the location of the computer.[106]

This definition encompasses spyware but excludes the other categories of cyber-surveillance tools listed in box 2.1 The measures to address the risks linked to commercial spyware comprised the export controls instruments mentioned above and sanctions (see below). Beyond trade-related measures, the government also introduced limitations on procurement by seeking to ensure that US government agencies do not acquire commercial spyware that poses 'significant counterintelligence or security risks to the United States Government or significant risks of improper use by a

[98] US Department of State, 'The United States adds foreign companies to entity list for malicious cyber activities', 18 July 2023.

[99] US Department of Commerce, 'Commerce department broadens authority to review licenses for human rights concerns and adopts new controls on water cannons', Press release, 5 Oct. 2020.

[100] US Department of Commerce (note 99).

[101] See US Department of Commerce, 'Annual country licensing and trade analysis', [n.d.], accessed 5 Sep. 2025.

[102] Access Now et al., 'Proposed rules: End-Use and End-User Based Export Controls, Including US Persons Activities Controls', 15 Oct. 2024.

[103] US Congress, H.R.1316, 'Maintaining American Superiority by Improving Export Control Transparency Act', 19 Aug. 2025.

[104] US Congress, H.R.1316 (note 103).

[105] The White House, 'Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security', 27 Mar. 2023. and US Department of Commerce, 'Commerce adds NSO Group and other foreign companies to Entity List for malicious cyber activities', Press release, 3 Nov. 2021.

[106] The White House (note 105).

foreign government or foreign person'.[107] Additional measures included the screening of outbound US foreign investments in firms in 'countries of concern' that are using advanced technologies to develop surveillance tools and visa restrictions on individuals involved in the misuse of commercial spyware or that 'facilitate or derive financial benefit from the misuse of commercial spyware'.[108] The USA also sought to promote the wider adoption of some of these measures and standards by other countries (see chapter 4).

EU and US sanctions

Sanctions can comprise banking restrictions, travel bans, asset freezes or prohibitions on transfers of arms, dual-use items or other commodities. They can be imposed on states, companies or individuals. Their content can be agreed and determined at the national, regional, multilateral or international level, often through UN Security Council resolutions or EU legal instruments.

The EU established the ability to impose sanctions, which it refers to as 'restrictive measures', under its Common Foreign and Security Policy (CFSP) in 1993. These can be arms embargoes, travel bans, asset freezes or 'other economic measures such as restrictions on imports and exports'.[109] Proposals for new EU sanctions to be adopted by the European Council can be submitted by EU member states or the EEAS. EU member states retain powers of veto over their adoption and remain responsible for their implementation and enforcement.[110] EU member states' representatives meet regularly in the Foreign Relations Counsellors Working Party, a body within the European Council, to '[exchange] experience and [develop] best practice in the implementation and application of restrictive measures'.[111] The EU has sought to enhance the implementation and effectiveness of its restrictive measures in recent years. In 2024, the EU adopted a new Directive setting minimum penalties for criminal offences linked to violations of EU sanctions.[112]

Since 2011, the EU has used sanctions to impose bans on the transfer of 'equipment, technology or software which may be used for the monitoring or interception of internet or telephone communications' to Iran and Syria, and 'equipment, technology or software intended primarily' for these uses to Myanmar, Venezuela, Belarus and Russia.[113] An accompanying annex lists the 'equipment, technology and software' covered by these controls, which include, among other things, 'deep packet inspection equipment', 'network interception equipment' and 'interception and monitoring equipment'.[114] The list appears to capture all the spyware and other cyber-surveillance tools listed in box 2.1, as well as certain related parts and components. EU sanctions require

[107] The White House (note 105).

[108] Federal Registry, 'Provisions pertaining to US investments in certain national security technologies and products in countries of concern', 15 Nov. 2024; and US Department of State, 'Announcement of a visa restriction policy to promote accountability for the misuse of commercial spyware', 5 Feb. 2024.

[109] European Commission, 'Overview of sanctions and related resources', [n.d.].

[110] European Commission (note 109).

[111] Council of the European Union, 'Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy', 4 May 2018.

[112] European Union, 'Criminal offences and penalties for the violation of EU restrictive measures', 20 Sep. 2024.

[113] EU Sanctions Map, 'Restrictive measures against cyber-attacks threatening the Union or its Member States', [n.d.].

[114] See e.g. Consolidated text: Council Regulation (EU) No 401/2013 of 2 May 2013 concerning restrictive measures in view of the situation in Myanmar/Burma and repealing Regulation (EC) No 194/2008, Annex III; Consolidated text: Council Regulation (EU) 2017/2063 of 13 November 2017 concerning restrictive measures in view of the situation in Venezuela, Annex II; and Consolidated text: Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine, Annex III.

EU-based companies to apply for licences to export these items to these destinations and impose an obligation on EU member states to deny permission if they might be used for prohibited purposes or by certain designated entities.[115]

In 2019, the EU established a new sanctions regime that allows the imposition of measures targeted at individuals and entities involved in cyberattacks on the EU or its member states.[116] These measures can include an asset freeze and travel ban on persons or entities responsible for cyberattacks or attempted cyberattacks. The same restrictions can be applied to persons or entities providing technical or financial support for these attacks or otherwise assisting them.[117]

US sanctions are administered and enforced by the US State Department's Office of Economic Sanctions Policy and Implementation and the US Department of the Treasury's Office of Foreign Assets Control (OFAC). They can target 'foreign jurisdictions and regimes, as well as individuals and entities'.[118] Between March and September 2024, the OFAC imposed sanctions on various individuals and entities associated with the Intellexa Consortium for their roles in the development and use of commercial spyware technologies that have been used to target US citizens and officials, arguing that this posed 'a significant threat to the national security of the United States'.[119] Sanctions have also been used to target manufacturers of other categories of cyber-surveillance tools, such as Russian manufacturers of LI systems and monitoring centres.[120]

The broader limits and potential of export controls and sanctions

The use of export controls and sanctions can help mitigate the risks of proliferation and misuse of spyware and other cyber-surveillance tools. US export controls and sanctions are widely credited with having a significant impact on the activities of the companies targeted.[121] However, their impact was enhanced by their connection and coordination with the other policy tools described above. What approach the Trump administration will take to tackling the proliferation and misuse of spyware remains unclear, as does whether or how it will make use of export controls and sanctions in this space. In January 2025, President Trump announced a review of the US export control system as part of its 'America First Trade Policy'.[122] At the time of writing, the results of the review are pending. There are signs of US interest in remaining engaged with multilateral processes in this area, such as the Pall Mall Process (see below), and in maintaining some of the export controls and sanctions adopted at the national level. In May 2025, it was reported that the US government had chosen not to remove the

[115] The specific language used in the sanctions applied to different destinations differs on this point. For example, for exports to Iran it is prohibited to export equipment or software 'intended for use in the monitoring or interception by the Iranian regime of the Internet and of telephone communications in Iran'. For exports to Myanmar (Burma), it is prohibited to export equipment or software if these 'are or may be intended for military use, military end-user or the Border Guard Police'. EU Sanctions Map (note 113).

[116] EU Sanctions Map (note 113).

[117] EU Sanctions Map (note 113).

[118] US Department of State, 'Economic Sanctions Programs'; and US Department of Treasury, Office of Foreign Assets Control, 'OFAC consolidated frequently asked questions'.

[119] US Department of Treasury, 'Treasury sanctions members of the Intellexa Commercial Spyware Consortium', Press release, 5 Mar. 2024; and US Department of Treasury, 'Treasury sanctions enablers of the Intellexa Commercial Spyware Consortium', Press release, 16 Sep. 2024.

[120] US Department of State, 'The United States takes sweeping actions on the one year anniversary of Russia's war against Ukraine', 27 Feb. 2023.

[121] See Ronalds-Hannon, E. and Scigliuzzo, D., 'Israel's Pegasus spyware maker takes drastic measures to survive global scandal', Bloomberg.com, 4 Nov. 2022.

[122] The White House, 'America First Trade Policy', Jan. 2025.

NSO Group from the Entity List or to reverse the decision to place limits on government procurement of commercial spyware.[123]

One key limitation of the effectiveness of export controls and sanctions is that many of their provisions only apply in countries that have integrated them into their national laws and regulations. Companies that manufacture or provide spyware and other cyber-surveillance tools can therefore escape their coverage by moving to states where they do not apply. Following the introduction of controls on exports of intrusion software in 2012, FinFisher, which produces the FinSpy spyware, was reported to have moved its work in this area to offices in states that are not participating states in the Wassenaar Arrangement.[124] However, other companies in the same field have sought to abide by the new controls and have not moved. One EU-based producer of network surveillance systems has noted that being subject to export controls has certain advantages, which include the possibility of greater political and economic support from their national government.[125]

In many states, the decision to deny an export licence can be challenged in court and the government might need to demonstrate that it is in line with the criteria outlined in the national legislation.[126] This may involve having to demonstrate that there was a risk that the exported item would have been used in connection with a serious violation of human rights or IHL. This could be challenging in the case of spyware and other cyber-surveillance tools, since the connection between the use of the item and a human rights violation might not be as direct as it would be for other items covered by export controls, such as military equipment. Companies and individuals have also launched legal challenges to contest their inclusion in the scope of EU and national sanctions.[127]

In 2015, the Swiss government introduced a new ordinance to its export controls specifying that permits for the export and brokering of 'goods intended for the surveillance of the Internet and mobile communications' will be refused 'if there is reason to believe that the goods will be used by the final recipient for the purposes of repression'.[128] This language creates greater scope to deny licences for exports of spyware and other cyber-surveillance tools captured by the Wassenaar Arrangement dual-use list. The changes made to the criteria of the EU Common Position in April 2025 highlighted above also have the potential to strengthen controls over transfers of cyber-surveillance tools. By specifying that export licences should be denied if there is a clear risk that the items might be used to 'facilitate' serious human rights or IHL violations, the language suggests that a direct link between the item and a possible violation would not be the only necessary grounds for denial.

Export controls may also be less effective at controlling companies and individuals operating a 'hacker for hire' model, which involves gaining access to a target's emails and phone accounts for a state or corporate client.[129] If these activities involve the cross-border movement of controlled items, then they might be subject to export

[123] Nakashima, E. et al., 'Pegasus spyware maker rebuffed in efforts to get off trade blacklist', *Washington Post*, 20 May 2025.

[124] Omanovic, E., 'Surveillance companies ditch Switzerland, but further action needed', Privacy International, 5 Mar. 2014; and Habegger, H., 'Bund Verscheucht Hersteller von Spionagesoftware Aus Der Schweiz' [Federation chases manufacturer of spy software from Switzerland], Schweiz Am Sonntag, 1 Aug. 2015.

[125] Bromley (note 69).

[126] Wegner, T., 'Ausfuhrgenehmigung abgelehnt—Was tun? [Export license rejected—what to do?' O&W Rechtsanwaltsgesellschaft mbH, 5 May 2019.

[127] Wahl, T., 'CJEU: Recent rulings on EU's restrictive measures against Russia', Eucrim, Feb. 2024; and Lester, M. and O'Kane, M., 'De-listing', Global Sanctions, [n.d.].

[128] Government of Switzerland, 'Ordonnance du 25 novembre 2020 sur l'exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles (OSIC) [Ordinance on the export and brokering of goods intended for the surveillance of the Internet and mobile communications]', 22 Nov. 2020.

[129] See Roberts et al. (note 39).

controls. However, the picture is less clear in situations where there are no cross-border movements of controlled items. In 2015, Germany added controls on 'technical support' for previously exported cyber-surveillance tools to its national dual-use export controls.[130] These provisions, which have not been included in the scope of the EU dual-use regulation, could allow the provision of certain surveillance-related services to be regulated by export controls.

Licensing systems to regulate the actions of private security firms could also be a way of controlling the actions of companies or individuals that are providing these services. In Switzerland, the Federal Act on Private Security Services Provided Abroad (PSSA) requires companies and individuals that provide security services abroad to notify the competent authorities. It also prohibits the provision of such services where these could undermine Switzerland's internal or external security, its foreign policy objectives, its neutrality or its obligations under international law, including human rights and IHL.[131] Given its definition of 'security services', the PSSA could, under certain circumstances, also encompass cyber operations such as hacking-for-hire, particularly if provided to a state client.

[130] German Federal Ministry for Economic Affairs and Energy (BMWI), 'Stärkere Kontrollen beim Export von Überwachungstechnologie [BMWI: Stronger controls on the export of surveillance technology]', 15 July 2015.

[131] Federal Department of Foreign Affairs (FDFA), Federal Act on Private Security Services Provided Abroad (PSSA), [n.d.].

4. Multilateral initiatives focused in whole or in part on the use of export controls and sanctions

In addition to specific export controls and sanctions, states have also developed a range of multilateral initiatives that seek to address the proliferation and misuse of different categories of spyware and other cyber-surveillance tools. Some of these initiatives focus on the use of export controls and sanctions alongside additional tools to tackle the risks posed by these items.

The US Export Controls and Human Rights Initiative and the commercial spyware initiative

The Export Controls and Human Rights Initiative (ECHRI) was launched by the USA at the first Summit for Democracy in 2021. It provides a framework for the development of multilateral commitments to prevent states and non-state actors from using spyware and other cyber-surveillance tools to violate human rights.[132] The first step taken in this direction was a Code of Conduct—endorsed by 25 states at the second Summit for Democracy in March 2023—that contains voluntary commitments to use export controls to 'prevent the proliferation of goods, software, and technologies that enable serious human rights abuses'.[133]

States committed 'to develop common guidelines for assessing exports, share information on transfers and denials, and develop and promote best practices for industry'. The Code of Conduct refers to 'surveillance tools and other technologies', which means that it has the potential to cover all the categories of spyware and other cyber-surveillance tools listed in box 2.1, as well as other systems used to monitor, extract, collect or analyse personal data using overt measures.

In parallel, the USA has launched multilateral efforts more specifically focused on addressing the risks posed by commercial spyware. These include the White House 'Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware', which had been endorsed by 23 states as of September 2024.[134] The joint statement commits states to take steps to tackle the risks of misuse and proliferation of commercial spyware, such as 'preventing the export of software, technology, and equipment to end-users' that might use these tools 'for malicious cyber activity, including unauthorized intrusion into information systems', in line with states' regulatory frameworks and 'appropriate existing export control regimes'.[135]

The ECHRI and joint statement were strongly driven by the Biden administration. While none of these initiatives has been formally discontinued by President Trump, it is unclear whether the same level of leadership in driving multilateral initiatives will be maintained on these issues.

[132] US Department of State, 'Export Controls and Human Rights Initiative Code of Conduct released at the Summit for Democracy', 30 Mar. 2023.

[133] US Department of State, 'Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights', 3 Mar. 2023. The governments that have endorsed the voluntary Code of Conduct are Albania, Australia, Bulgaria, Canada, Costa Rica, Croatia, Czechia, Denmark, Ecuador, Estonia, Finland, France, Germany, Japan, Kosovo, Latvia, The Netherlands, New Zealand, North Macedonia, Norway, Republic of Korea, Slovakia, Spain, the United Kingdom and the United States.

[134] US Department of State, 'Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware', 22 Sep. 2024. The endorsing states are Australia, Austria, Canada, Costa Rica, Denmark, Estonia, Finland, France, Germany, Ireland, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, Republic of Korea, Slovenia, Sweden, Switzerland, the United Kingdom and the United States.

[135] US Department of State (note 134).

Box 4.1. UN process on responsible behaviour in cyberspace and use of ICTs

States have been discussing the issue of information security at the UN level since 1998, following submission by Russia of a draft resolution on the subject to the First Committee of the UN General Assembly. Since then, multiple processes have been launched to explore the use of information and communication technologies (ICTs) in the context of international security. These include six Groups of Governmental Experts (GGEs) between 2004 and 2021 on 'advancing responsible state behaviour in cyberspace in the context of international security' and two Open-Ended Working Groups (OEWGs) on 'security of and in the use of information and communications technologies'—one in 2019–2021 and one that began work in 2021 and concluded in 2025.[a]

The final report on the work of the second OEWG highlights the threats posed by 'the growing market for commercially available ICT intrusion capabilities as well as hardware and software vulnerabilities'.[b] The report notes states' concern regarding the increasing availability of these technologies, and the interest in taking 'steps to ensure that their development, facilitation, dissemination, purchase, transfer, export or use is consistent with international law'.[b] States have agreed to turn the OEWG into a 'Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour'. Within the framework of the UN General Assembly, states have discussed a proposal to establish a politically binding UN Programme of Action (POA) on responsible state behaviour in cyberspace. This was formally endorsed in resolutions adopted in 2022 and 2023.[c] The 'Global Mechanism' does not fulfil all of the objectives states had sought to achieve with a UN POA but does lay the groundwork for two thematic groups, an annual plenary meeting and review conferences every five years.[d] While not explicitly mandated by the final report, these mechanisms could provide a space to further explore the steps that could be taken to tackle the proliferation and misuse of ICT intrusion capabilities at the UN level.

[a] United Nations, Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', [n.d.], accessed 5 Sep. 2025.

[b] UN General Assembly, Open-ended working group on security of and in the use of information and communications technologies 2021-2025, 'Draft final report', A/AC.292/2025/CRP.1, 11 July 2025.

[c] UN General Assembly, 'Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security', A/RES/77/37, 7 Dec. 2022; and UN General Assembly, 'Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security', A/RES/78/16, 6 Dec. 2023.

[d] Pytlak, A., 'Discord and diplomacy: Reviewing outcomes from the UN's cyber working group', Stimson Centre, 14 Aug. 2025.

The Pall Mall Process

The Pall Mall Process was launched by France and the UK in 2024 to address the challenges posed by the 'proliferation and irresponsible use' of commercially available cyber intrusion capabilities (CCICs).[136] The Pall Mall process brought together states with representatives of the private sector, academia and NGOs to discuss possible policy options and the principles that should apply to the development, facilitation, purchase, transfer and use of CCICs to address the risk that these could be used to disrupt cyberspace or facilitate violations of human rights or IHL. The process has so far resulted in the adoption of a Code of Practice for States published in April 2025, which is to be followed up by an equivalent Code of Practice for Industry.[137]

[136] UK Foreign, Commonwealth & Development Office, 'The Pall Mall Process: Tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities, Declaration', 6 Feb. 2024.

[137] UK Foreign, Commonwealth & Development Office, 'The Pall Mall Process Code of Practice for states', 25 Apr. 2025; and Statements made by UK and French officials at the Pall Mall Process conference in Paris, 3–4 April 2025.

The code seeks to build on aspects of international law, including human rights treaties and standards, that are relevant to how states should act in relation to 'the development, transfer and use of CCICs'.[138] The code also recalls relevant commitments made by states at the UN level on responsible behaviour in cyberspace (see box 4.1).

The code commits endorsing states, among other things, to apply export controls 'to mitigate risks of potential irresponsible use' of CCICs. More broadly, export controls are identified as part of a set of measures that aims to ensure accountability across the market for CCICs. The code does not include a list of items that should be subject to export controls. However, officials associated with the Pall Mall Process have indicated that the main focus of attention will be spyware (see box 2.1), hackers-for-hire services and hacking as a service, as well as vulnerabilities and exploits that underpin cyber intrusion activity.[139]

According to the Code of Practice for States, export control decisions should 'take into account' the risk of exported CCICs being used for international repression and serious violations of human rights, and licences should only be granted to 'a specific end-user and for a defined lawful and legitimate purpose'. The code also outlines the steps that states can take to support the implementation and enforcement of applicable controls by exporters, such as the imposition of measures to deter or punish the irresponsible behaviour of individuals or entities across the market, the development of guidance and the provision of capacity building. In certain areas, the code reflects the approach the USA has taken to tackling the proliferation and misuse of spyware, in that it calls for governments to use financial and travel restrictions to hold individuals and relevant entities accountable for misuse.[140] As of September 2025, 26 states had endorsed the Code of Practice, including the USA.[141]

The frameworks created by the ECHRI, the Joint Statement on Spyware and the Pall Mall Process highlight the role that export controls can play in mitigating the risk of the misuse or proliferation of spyware. While these instruments do not completely overlap in participation and scope, at a time when other relevant processes are being challenged by the current geopolitical context, they have the potential to create alternative avenues through which like-minded states can draft guidelines, strengthen or expand existing controls and share confidential information. In addition, by focusing on various aspects related to the control of spyware and other cyber-surveillance tools, these frameworks engage with a more diverse range of stakeholders. These include representatives of companies that produce different categories of spyware and other cyber-surveillance tools. This provides an opportunity to develop a more comprehensive and effective lifecycle approach to tackling the risk that these technologies could be misused.

[138] UK Foreign, Commonwealth & Development Office, 'The Pall Mall Process Code of Practice for states' (note 137); and Ní Aoláin, F., 'One step forward? Agreement on spyware regulation in the Pall Mall Process', *Just Security*, 9 May 2025.

[139] UK Foreign, Commonwealth & Development Office, Statements made by UK and French officials at the Pall Mall Process conference in Paris, 3–4 April 2025 (note 137).

[140] Freedom House, 'How the Pall Mall Process can help combat commercial spyware abuse', 8 May 2025.

[141] UK Foreign, Commonwealth & Development Office, 'The Pall Mall Process Code of Practice for states' (note 137). The states that have endorsed the Code of Practice are Austria, Denmark, Estonia, Finland, France, Germany, Ghana, Greece, Hungary, Ireland, Italy, Japan, Kosovo, Latvia, Luxembourg, Moldova, the Netherlands, Poland, Republic of Korea, Romania, Slovakia, Slovenia, Sweden, Switzerland, the United Kingdom and the USA.

5. Conclusions and recommendations

As is the case for other technologies and tools, export controls and sanctions will not be able to address all of the risks and challenges posed by the proliferation and misuse of spyware and other cyber-surveillance tools. Export controls only apply to one point in the lifecycle of spyware and other cyber-surveillance tools: the moment of cross-border transfer. Sanctions can target the actions of specific states, companies and individuals. However, their adoption has distinct political implications, and their use, scope and impact are often the subject of contestation and disagreement among states. Export controls and sanctions do not aim to establish standards for or controls on the development, production or use of these tools. These measures must therefore be complemented by other hard and soft law instruments to regulate the full lifecycle of cyber-surveillance tools. The ECHRI, the Joint Statement on Spyware and the Pall Mall Code of Practice for States, the scope of which go beyond export controls, are examples of such soft law instruments. In addition, international law—especially international human rights law and IHL—remain applicable to and binding on states in this domain. The use of export controls to regulate the trade in spyware and other cyber-surveillance tools also risks legitimizing and normalizing their trade, which many NGOs and human rights experts believe should be prohibited. This is especially the case for spyware, which has been the subject of calls for bans or moratoriums.[142]

At the same time, export controls and sanctions are also a necessary and critical component of wider attempts to regulate the production, trade in and use of spyware and other cyber-surveillance tools. Export controls have allowed states to collectively identify the spyware and other cyber-surveillance tools that present the most significant risks to human rights and national security, and to define their technical characteristics. Licence application procedures create records of where these tools are being exported and by whom. They can increase government oversight of the trade in these items and create the possibility of greater public transparency in this area. Export controls can be used to prevent exports of spyware and other cyber-surveillance tools and to impose constraints on how exported items are used. Sanctions have been used to prohibit certain exports of spyware and other cyber-surveillance tools to sensitive destinations and to swiftly target producers of spyware following cases of misuse. Finally, export controls and sanctions can enable the prosecution of companies that seek to transfer these items without the necessary approval.

At least 64 states apply the Wassenaar Arrangement dual-use list through their national export controls. According to the data mapping conducted for this paper, these states are home to 95 per cent of the companies that manufacture spyware and other cyber-surveillance tools. In addition, 43 states have committed to use export controls to prevent transfers of spyware and other cyber-surveillance tools that might be used to enable violations of human rights and IHL by virtue of being EU member states or signatories to the ECHRI, the Joint Statement on Spyware or the Pall Mall Code of Practice for States. These states are home to 68 per cent of the companies that manufacture spyware and other cyber-surveillance tools.

The potential for export controls and sanctions to have a more significant impact is limited by both technical and political challenges. Export controls are a complex aspect of government legislation that require the appropriate allocation of time and resources. Many exports of spyware and other cyber-surveillance tools are examples of ITT that pose specific licensing and enforcement challenges. States differ in their application of ITT controls, which can create limitations on and loopholes in their implementation.

[142] United Nations Human Rights (note 30).

While more detailed information is being published, gaps in states' public reporting on exports of spyware and other cyber-surveillance tools means that the potential for these controls to create greater transparency is not being fulfilled. Furthermore, there is little in the way of agreed guidance on how to frame and apply controls on exports of spyware and other cyber-surveillance tools to ensure that exports that might be used to enable violations of human rights and IHL are prevented. Finally, the effectiveness of multilaterally agreed export controls on spyware and other cyber-surveillance tools relies on cooperation and information sharing among states.

The ability of the Wassenaar Agreement to play this role is limited in the current international environment. The EU and the frameworks created by the ECHRI, the Joint Statement on Spyware and the Pall Mall Process create alternative avenues through which states can draft guidelines, strengthen or expand existing controls and share confidential information. The USA took a leading role in showing how export controls and sanctions can be used to tackle the proliferation and misuse of spyware and other cyber-surveillance tools. If US leadership in this area becomes less prominent, the EU has the potential to take on this role. The EU would be able to take steps to strengthen its own controls, connect relevant areas of EU policymaking and establish standards for other states to draw on.

The recommendations below highlight the steps states could take individually or collectively—via the Wassenaar Arrangement, the ECHRI, the Joint Statement on Spyware or the Pall Mall Process—to strengthen the role of export controls in promoting transparency, oversight and restraint in the trade in spyware and other cyber-surveillance tools. They also focus on what the EU and EU member states can do to strengthen the use of both export controls and sanctions in this space.

Recommendations to all states

Address the remaining gaps in the scope of export controls

States should examine the potential to adopt new list-based controls and catch-all controls to capture additional categories of spyware and other cyber-surveillance tools. These could involve capturing covert surveillance tools, such as certain types of digital forensics tools, that might not meet the technical thresholds outlined in the control lists. They could also involve expanding the controls to capture overt surveillance tools, such as social media analytics, facial recognition software and other biometric tools. EU member states could also explore the use of Article 5 of the 2021 dual-use regulation and other mechanisms to make additional cyber-surveillance tools subject to export controls.

Exchange information on the implementation of export controls

States should share more detailed information on the content and implementation of their export controls on spyware and other cyber-surveillance tools. This would create more uniform controls, help to identify companies that are seeking to evade or bypass their coverage and enable a discussion of how export controls and other regulatory tools can capture the provision of surveillance-related services. This could be done using the established channels that exist under the Wassenaar Arrangement and the EU and by creating new ones through the ECHRI and Pall Mall Process.

Publish data on exports of spyware and other cyber-surveillance tools

States should agree on minimum standards for the publication of data on licences for exports of spyware and other cyber-surveillance tools, building on existing national and EU practices. Making this information available would create a better picture of the trade in spyware and other cyber-surveillance tools and improve public oversight of the application of controls.

Develop guidelines to inform the implementation of export controls on spyware and other cyber-surveillance tools

States should develop guidelines outlining how to implement export controls on exports of spyware and other cyber-surveillance tools. These guidelines should outline how to make exporters aware of their licensing obligations, apply the control list categories and assess licence applications. The process of developing these guidelines should build on engagement with companies that produce and export spyware and other cyber-surveillance tools to identify the way export controls are understood and applied. The process should also be informed by efforts to establish criteria on the procurement and use of spyware and other cyber-surveillance tools.

Establish a global commitment to regulate transfers of spyware

While it may not be possible for all types of cyber-surveillance tools, there is the potential to establish a global commitment to make spyware subject to export controls. This commitment could be a component of the newly established Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour.

Recommendations to the EU and EU member states

Include additional categories of spyware and other cyber-surveillance tools in Annex IV

Stronger controls on transfers of spyware and other cyber-surveillance tools could be achieved by moving some or all of the five categories of spyware and other cyber-surveillance tools that have been added to the Wassenaar Arrangement control list from Annex I to Annex IV of the EU dual-use regulation. Adding these items to Annex IV would make their intra-EU transfer subject to additional regulatory oversight.

Connect dual-use export controls to EU discussions on spyware regulation

The European Commission, which oversees implementation of the EU dual-use regulation, is reportedly working on measures to address misuse of spyware at the national level. The Commission is therefore well-placed to connect export control discussions on spyware and other cyber-surveillance tools with broader EU-level debates on their misuse, particularly those in the European Parliament. Linking these processes could help the EU to develop standards to regulate both internal use and the export of these tools to third countries.

Integrate discussions on spyware and other cyber-surveillance tools into standard-setting on ITT

The ongoing process of developing EU guidelines on controls on ITT could be used to examine whether spyware and other cyber-surveillance tools are being made avail-

able via SaaS models and how these transfers are regulated by EU member states. This would help to clarify the extent to which these tools are being provided via SaaS models and create greater clarity for companies that are seeking to comply with controls. The guidelines would create a common EU approach to these issues and establish standards that could be adopted by states outside the EU.

Provide capacity building for implementation of export controls

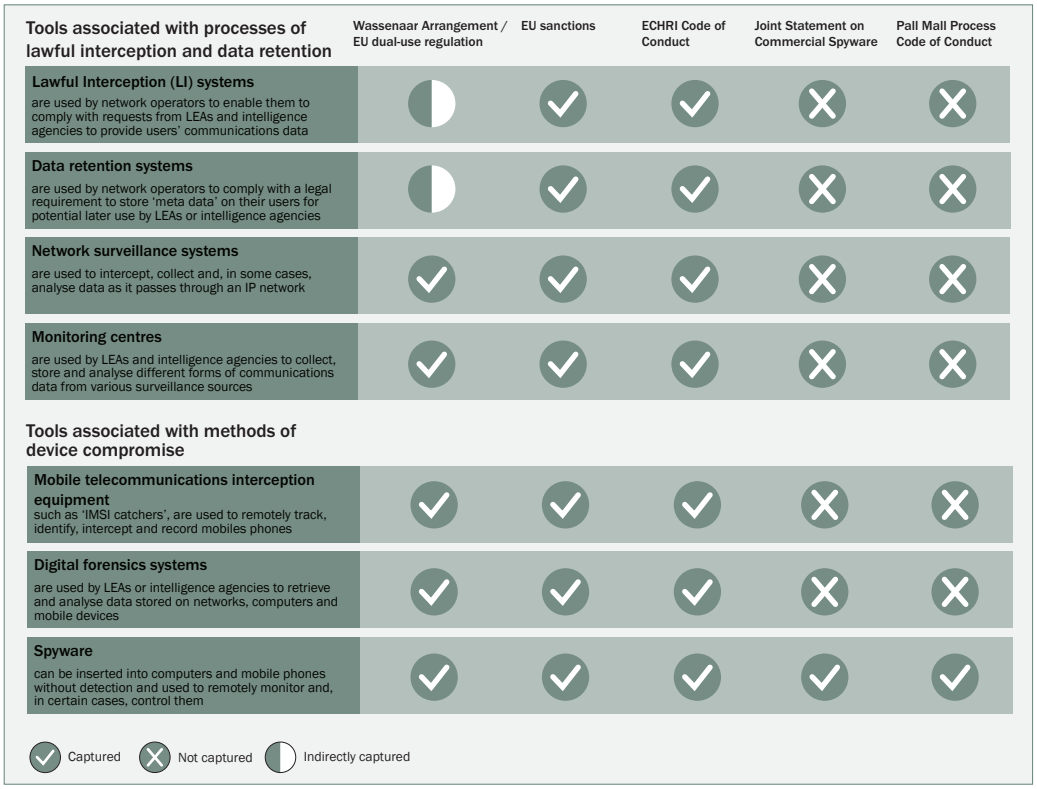
The 2021 EU dual-use regulation committed the EU to develop export control-related training programmes for officials in EU member states. The implementation of controls on the export of spyware and other cyber-surveillance technologies is one area where common training could be developed and provided by the European Commission in cooperation with national authorities.

Examine the potential to expand the use of sanctions

The EU and EU member states should examine the role that EU sanctions could play in tackling the proliferation and misuse of spyware and other cyber-surveillance tools. This should include a detailed assessment of the way sanctions imposed since 2011 have been implemented, their impact and their potential to be harmonized and expanded. As part of this process, the EU and EU member states could assess the potential use of EU sanctions to target the activities of spyware manufacturers whose actions pose a threat to human rights and national security.

Appendix A. Coverage of export control and other related instruments

Figure A.1. Categories of spyware and other cyber-surveillance tools captured by export control instruments, sanctions measures and multilateral initiatives



Appendix B. Participation in export control and other related instruments

Table B.1. Membership of or signatory to agreements aimed, in whole or in part, at using export controls to regulate spyware and other cyber-surveillance tools

	Wassenaar Arrangement	European Union[a]	ECHRI Code of Conduct	Joint statement on spyware	Pall Mall Code of Practice
Albania			✓		
Argentina	✓				
Australia	✓		✓	✓	
Austria	✓	✓		✓	✓
Belgium	✓	✓			
Bulgaria	✓	✓	✓		
Canada	✓		✓	✓	
Costa Rica			✓	✓	
Croatia	✓	✓	✓		
Cyprus		✓			
Czechia	✓	✓	✓		
Denmark	✓	✓	✓	✓	✓
Ecuador			✓		
Estonia	✓	✓	✓	✓	✓
Finland	✓	✓	✓	✓	✓
France	✓	✓	✓	✓	✓
Germany	✓	✓	✓	✓	✓
Ghana					✓
Greece	✓	✓			✓
Hungary	✓	✓			✓
India	✓				
Ireland	✓	✓		✓	✓
Italy	✓	✓			✓
Japan	✓		✓	✓	✓
Kosovo			✓		✓
Latvia	✓	✓	✓	✓	✓
Lithuania	✓	✓		✓	
Luxembourg	✓	✓			✓
Malta	✓	✓			
Mexico	✓				
Moldova					✓
Netherlands	✓	✓	✓	✓	✓
New Zealand	✓		✓	✓	
North Macedonia			✓		
Norway	✓		✓	✓	

	Wassenaar Arrangement	European Union[a]	ECHRI Code of Conduct	Joint statement on spyware	Pall Mall Code of Practice
Poland	✓	✓		✓	✓
Portugal	✓	✓			
Republic of Korea	✓		✓	✓	✓
Romania	✓	✓			✓
Russia	✓				
Slovakia	✓	✓	✓		✓
Slovenia	✓	✓		✓	✓
South Africa	✓				
Spain	✓	✓	✓		
Sweden	✓	✓		✓	✓
Switzerland	✓			✓	✓
Türkiye	✓				
Ukraine	✓				
United Kingdom	✓		✓	✓	✓
United States	✓		✓	✓	✓

Sources: Authors' compilation based on the following sources: Wassenaar Arrangement, 'Introduction'; European Union, 'EU Countries', accessed 5 Sep. 2025; US Department of State, 'Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights', 3 Mar. 2023; US Department of State, 'Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware', 22 Sep. 2024; and UK Foreign, Commonwealth & Development Office, 'The Pall Mall Process Code of Practice for States', 25 Apr. 2025.

[a] EU member states are required to implement the EU dual-use regulation through their national laws and regulations.

About the authors

Dr Mark Bromley is the Director of the SIPRI Dual-Use and Arms Trade Control Programme. His areas of research include international, regional and national standards in dual-use and arms export controls and efforts to combat the illicit trafficking of small arms and light weapons (SALW). Other areas of expertise include the arms and dual-use export policies of EU member states, the Arms Trade Treaty, and controls on the trade in cyber-surveillance tools. Prior to joining SIPRI, he was a Policy Analyst with the British American Security Information Council (BASIC).

Giovanna Maletta is a Senior Researcher in the SIPRI Dual-Use and Arms Trade Control Programme where she works on issues related to the implementation of national, multilateral and international export control standards and instruments. Her areas of research cover the EU framework for strategic trade controls, the implementation of the Arms Trade Treaty and cooperation and assistance activities in the field of arms transfer and SALW controls. Recently she has also conducted research on the UN discussion on technology transfers and 'peaceful uses' and their impact on multilateral cooperation in the field of export controls.

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