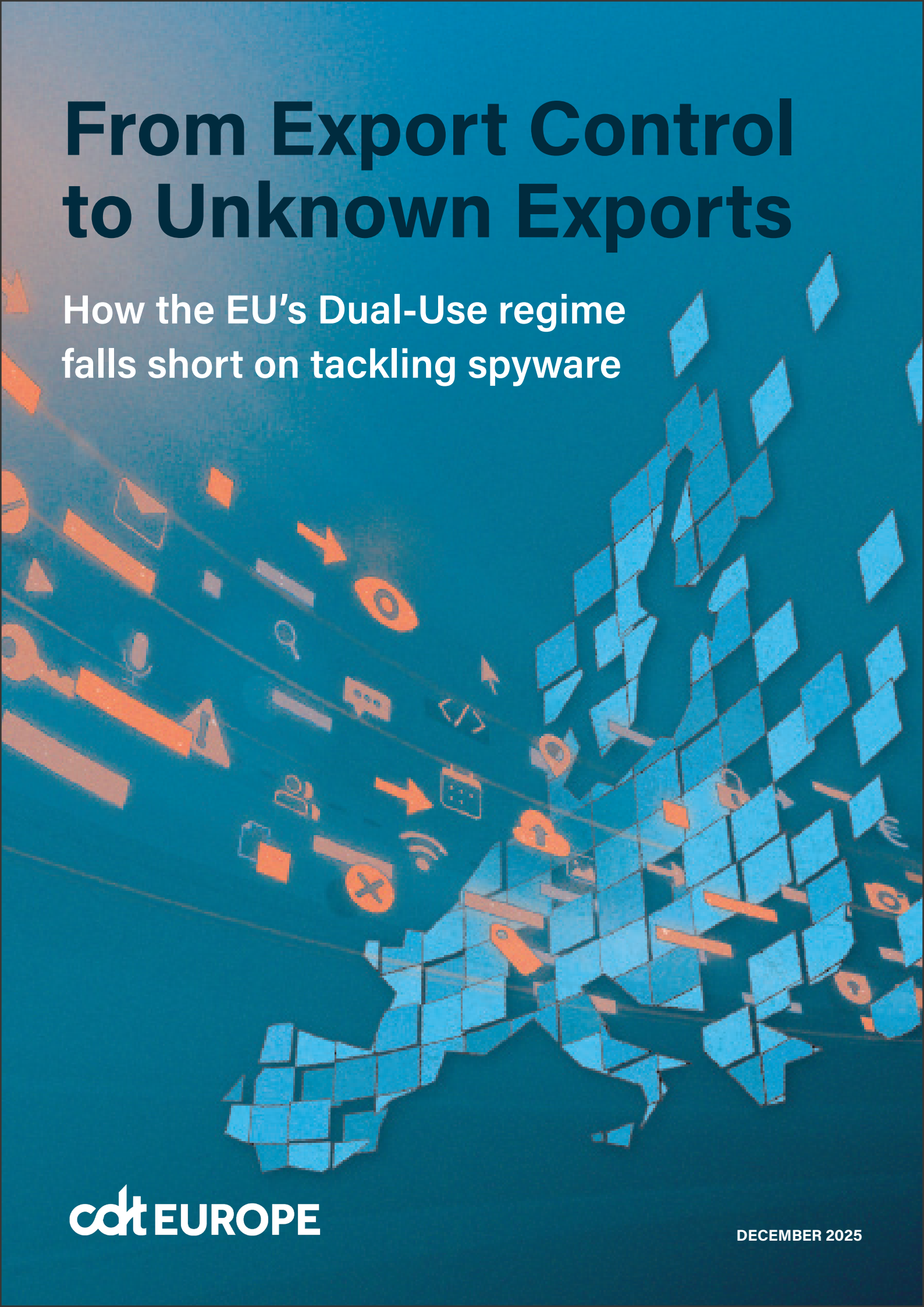
From Export Control to Unknown Exports

How the EU's Dual-Use regime falls short on tackling spyware



cdt EUROPE

DECEMBER 2025

DECEMBER 2025

From Export Control to Unknown Exports

How the EU's Dual-Use regime falls short on tackling spyware

AUTHOR

Joanna Tricoli

WITH CONTRIBUTIONS FROM

Silvia Lorenzo Perez, Asha Allen, Aimée Duprat-Macabies, Sarah Graham, Tom Bowman, Dhanaraj Thakur

Illustration and layout by Jaś Lewicki

ACKNOWLEDGEMENTS

We thank internal reviewers at the Center for Democracy & Technology Global for their valuable feedback and guidance throughout this project. We are also deeply grateful to Professor Fionnuala Ní Aoláin KC and Dr. Mark Bromley (Stockholm International Peace Research Institute, SIPRI) for their insightful external reviews and expert comments, which significantly strengthened the analysis.

Special thanks to the experts and officials who participated in interviews and consultations across EU Member States for generously sharing their time and experience.

cdt EUROPE

Executive Summary

The proliferation of commercial spyware and cyber-surveillance technologies poses serious challenges to the protection of human rights and the resilience of democratic institutions. Investigations and parliamentary inquiries have documented repeated instances in which these technologies have been used to target journalists, human rights defenders and political opponents, contributing to systematic violations of fundamental rights. In the absence of substantive regulatory action to address these patterns of abuse, commercial spyware continues to be marketed and deployed with limited oversight. Export controls, while not sufficient on their own to address the entire lifecycle of spyware, remain one of the few binding instruments available to constrain this trade by imposing licensing requirements, recording transactions, and introducing a measure of transparency and accountability into a sector that otherwise operates with little scrutiny.

This report examines how the EU Dual-Use Regulation (DUR), the only binding EU framework currently governing the export of spyware, is being implemented in practice. It analyses national licensing systems in four Member States, France, Germany, Italy and the Netherlands, to assess how export controls function on the ground. The research highlights both common shortcomings and divergences in procedures, resources and institutional capacity that fragment implementation across the Union.

The findings show that the spyware trade raises distinct challenges that existing export control frameworks are not fully equipped to address. Vendors often rely on complex corporate structures that obscure accountability while maintaining close ties with state actors, and they benefit from the absence of controls on intra-EU transfers. At the same time, the market is shifting toward modular components and service-based delivery models that are poorly captured by frameworks designed for tangible goods. These dynamics complicate oversight and increase the risk that surveillance capabilities escape effective control. Across all four Member States examined, the research identified the following challenges that limit the effectiveness of the DUR in preventing spyware misuse:

- **Lack of transparency:** licensing decisions remain largely shielded from public scrutiny. National reports, where they exist, are highly aggregated, delayed, or incomplete. Denials are rarely published with reasons, and confidentiality is particularly acute for decisions under Article 5 of the Regulation. Persistent transparency gaps also extend to exporters, who report uncertainty about how decisions are reached and how human rights risks are weighed.

- **Weak due diligence obligations:** exporters face significant uncertainty in implementing export controls. Guidance is fragmented and often insufficiently detailed, with major divergences between Member States in the availability of practical tools. Companies lack clarity on what constitutes an adequate human rights risk assessment, and many stressed that better feedback from regulators, especially on licence refusals, would help them refine compliance practices.

- **Absence of systematic end-use monitoring:** once a licence is granted, there are generally no binding obligations to monitor the actual deployment of exported spyware. Exporters and authorities alike indicated that once exports leave EU borders, visibility over their final use is extremely limited.

- **Uneven national procedures:** Member States' administration of export controls varies in both procedure and capacity, which may create uncertainty for industry and the risk of forum shopping toward jurisdictions perceived as less stringent.

- **Internal market asymmetries:** the lack of controls on intra-EU transfers of spyware creates a loophole that companies can exploit to bypass external trade rules. Persistent opacity also makes it difficult to map the industry within Europe, and regulators themselves often lack clarity on which vendors operate in the Union and what technologies they provide.

The forthcoming evaluation of the Dual-Use Regulation provides a critical opportunity to strengthen the framework and ensure it addresses the unique risks associated with spyware. Against this backdrop, the report sets out the following policy recommendations:

1. **Closing the intra-EU gap:** establish a regulatory framework governing the internal movement of spyware and related cyber-surveillance tools, either by including them in Annex IV of the Dual-Use Regulation or through new internal market legislation, to ensure consistent scrutiny and prevent circumvention of external trade controls.

2. **Enhancing transparency:** introduce clear and harmonised transparency standards for the licensing of spyware exports. Member States should be required to publish disaggregated and timely information on applications and decisions, including the nature of the technology, destinations, and reasons for approval or denial, while ensuring that confidentiality exceptions remain narrowly defined.

3. **Strengthening due diligence obligations:** clarify and reinforce exporters' duties requiring documented human rights risk assessments in line with international standards. Due diligence obligations should extend beyond pre-licensing to cover the full lifecycle of the technology with clear consequences for inadequate due diligence or non-compliance.

4. **Developing systematic end-use monitoring:** create binding and harmonised requirements for exporters to monitor the actual use of licensed spyware, including

contractual safeguards and reporting duties, making use of technical features such as update dependencies to ensure compliance.

5. **Building capacity within national authorities:** provide sustained support to strengthen the technical and human rights expertise of licensing authorities through common training, dedicated staff, and structured knowledge-sharing mechanisms, ensuring that all Member States can effectively assess spyware exports.

6. **Reinforcing external oversight:** ensure that licensing decisions are subject to regular parliamentary scrutiny and that independent human rights expertise is systematically integrated into the assessment process, mitigating conflicts of interest and enhancing accountability.

7. **Improving information-sharing among Member States:** strengthen the use of existing coordination mechanisms, including the Dual-Use Coordination Group, to facilitate systematic exchanges on approvals, denials, and the application of catch-all controls to spyware.

8. **Harmonising procedures and documentation:** promote convergence of national licensing practices by establishing a common template for end-user statements and aligning procedural requirements, thereby reducing opportunities for forum shopping and enhancing legal certainty for exporters.

9. **Strengthening international coordination:** the EU should lead efforts to coordinate spyware controls, set common standards, and embed human-rights safeguards in export licensing, while continuing to press for progress in multilateral export control regimes.

Contents

Introduction

The regulation of the trade in commercial spyware[1] has emerged as a critical policy challenge for the European Union (EU) and the international community, given its growing misuse against journalists, political opponents, human rights defenders, and civil society actors (OHCHR, 2021; Tech Global Institute, 2025). Concerns about the role of spyware in enabling human rights violations first gained prominence after the 2011 Arab Spring, when it was revealed that European and other Western companies had supplied surveillance tools to governments accused of human rights abuses (Mildebrath, 2024). Although these concerns had long been raised in relation to contexts outside Europe, their urgency became particularly evident within the EU in 2021, when disclosures revealed that spyware had been used by EU and non-EU governments against members of the European Parliament, journalists, diplomats, political opponents, and civil society organisations. The European Parliament's Committee of Inquiry on Pegasus and equivalent surveillance spyware (PEGA Committee), concluded that spyware had been misused within the Union for political purposes. In some Member States it became embedded into governance structures in ways that facilitated authoritarian practices (PEGA Committee, 2023). The impacts of such deployment are far-reaching, undermining electoral integrity by disrupting opposition campaigns, emptying press freedom of its substance by exposing journalists and their sources to covert surveillance, and generating a climate of fear and self-censorship that weakens civic space and erodes public trust in institutions (Asher-Schapiro, 2018; CDT Europe, 2025).

1 For the purposes of this report, "spyware" refers exclusively to commercial spyware, i.e. surveillance software developed by private companies and offered as a product on the global surveillance market, often purchased by government agencies. By contrast, state-developed spyware is designed in-house by states, usually those with significant signals intelligence capacity. Studies note that in countries permitting the use of spyware, it is often unclear whether authorities rely on commercial products or domestically developed tools (European Commission for Democracy through Law, 2024). In both cases, spyware typically infiltrates personal devices covertly, often through zero-day or even zero-click exploits, to intercept communications, track movements, and extract sensitive data while remaining undetected. Certain spyware models also allow the active manipulation of the contents of an infected device, including the alteration, deletion, or addition of files (see also Kaye, 2021; United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 2023; Kaye & McKune, 2023; United Nations High Commissioner for Human Rights, 2018). In international policy discussions, spyware is also addressed within the broader category of "commercial cyber intrusion capabilities," as defined by the Pall Mall Process Declaration, although observers have noted that this broader focus, rather than a specific emphasis on spyware, despite its central role in prompting the initiative, may dilute the Process's ability to respond effectively to spyware-related threats (UK Government, 2024; Herpig & Paulus, 2024).

Despite this, the proliferation of spyware remains widespread, sustained by a global commercial market that is both lucrative and opaque. While a few vendors have gained notoriety, most operate with little transparency or public scrutiny, enabling continued circulation of these technologies across jurisdictions (Roberts et al., 2024). This opacity underscores the need for structural regulatory measures and as the Venice Commission has observed, effective export controls are thus a necessary component of any credible governance framework (European Commission for Democracy through Law, 2024). Export controls, long established as instruments to manage the trade in sensitive goods and technologies for reasons of non-proliferation and national security, have increasingly been mobilised to address the risks posed by commercial spyware (van Daalen, van Hoboken, & Rucz, 2023). While these mechanisms were not designed with cyber-surveillance in mind, they have become one of the few legally binding tools available to governments to scrutinise and restrict the transfer of such technologies. By requiring prior authorisation and licensing, export controls provide a means, albeit insufficient alone, of injecting oversight and transparency into a market that is otherwise obscure and largely driven by private actors (Anstis, Leonard, & Penney, 2023).

Within the EU, export controls represent the only binding instruments that explicitly regulate the trade in spyware and other cyber-surveillance items.[2] The 2021 recast of the Regulation (EU) 2021/821 (Dual-Use Regulation) sought to reflect the technological evolution of surveillance tools by introducing new provisions for their control, expressly recognising the human rights risks they pose and the potential for their abuse. Yet, the scope of this express recognition in operative provisions remains more limited than the breadth of risks acknowledged, a tension that has been particularly evident in the spyware domain and will be examined in further detail below. Because the responsibility for assessing export licence applications and overseeing compliance lies primarily with national authorities, it is crucial to examine how these obligations are implemented in practice. Understanding how national licensing authorities evaluate risks, how exporters apply due diligence, and where challenges or divergences arise sheds light on how companies established in the EU participate in the spyware trade with third countries. Examining national implementation is therefore key to assessing whether the Regulation delivers on its objectives of preventing misuse and ensuring accountability.

In light of the above, CDT Europe conducted a comparative study of how four Member States, France, Germany, Italy, and the Netherlands, have implemented the Dual-Use Regulation with regard to spyware. These countries were selected as some are

2 For the purposes of this report, "cyber-surveillance items" follows the definition set out in the EU Dual-Use Regulation, which describes them as items "specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems." In this context, the term covers hardware and software used by intelligence agencies and law enforcement authorities or by network operators acting under their direction to covertly access and collect communications data processed through ICTs (see Bromley & Maletta, 2025).

leading actors in international initiatives such as the Pall Mall Process, others are major exporters within the EU, and, in some instances, the national landscape includes a substantial number of companies active in the cybersecurity and surveillance sectors. By analysing their legal frameworks, licensing procedures, risk assessments, and transparency practices, this report provides evidence-based policy recommendations with the aim to strengthen oversight and transparency in the trade of spyware and surveillance technologies, and ensure that EU export controls effectively safeguard human rights and security.

The report is structured as follows: Chapter 1 provides an overview of the role of export controls with regard to spyware in current multilateral regimes and international fora. Chapter 2 turns to the EU export control framework, outlining the recast process and the relevant provisions of the Dual-Use Regulation concerning surveillance technologies. Chapter 3 presents the core of the study, with an analysis of four Member States (France, Germany, Italy and the Netherlands), focusing on their legal frameworks, licensing procedures, risk assessment processes, and transparency practices. Chapter 4 offers a comparative discussion of these findings. Lastly, Chapter 5 concludes with policy recommendations to strengthen the effectiveness of the EU's export control regime in addressing the challenges posed by spyware.

Methodology

This report is based on a mixed-methods approach that combines in-depth desk research with semi-structured interviews with experts.[3] The desk research consisted of a comprehensive review of academic literature, EU and Member State laws, policy documents, institutional reports, and publicly accessible online resources. This helped to establish a foundational understanding of the legal and institutional context of the EU dual-use export control regime in relation to spyware and cyber-surveillance technologies.

To complement the desk research and gain a practical understanding of how the Dual-Use Regulation is being implemented at national level, CDT Europe conducted a series of 16 confidential, semi-structured interviews. All interviews were carried out with the informed consent of the participants. The interviewees were selected to reflect a broad range of perspectives and included representatives from EU institutions, national licensing authorities in the four Member States under review, civil society organisations, journalists, legal practitioners, researchers, industry actors, and academic experts in export controls and surveillance technologies.

3 All interviews were conducted remotely, primarily in English, with field notes taken during each session. Where consent was provided, interviews were also recorded to ensure accuracy. Interviewees were informed in advance that their contributions would be anonymised and would not be attributed to them or their organisations, in order to enable candid reflections on sensitive policy and institutional practices. All data gathered through interviews was analysed to identify patterns, divergences, and emerging themes, and has been used to inform the findings and recommendations presented in this report.

01

Regulating the trade of spyware through export controls

Spyware and related cyber-surveillance tools, including markets for software vulnerabilities, so-called "cyber-mercenaries" or hacker-for-hire firms, developers of "cyber-weapons," and access-as-a-service providers, fall within what is often referred to as the offensive cyber capabilities sector (Anstis, Leonard, & Penney, 2023). Although spyware and related surveillance tools have been recognised as dual use by some international frameworks, such as the Wassenaar Arrangement (see more below) they are better described as single-use technologies because they are designed solely for deployment by law-enforcement and intelligence agencies (Riecke, 2023; Bromley & Maletta, 2024). They are thus subject to export controls through their listing, rather than because they correspond to the traditional definition of dual-use items in the arms-control context, a term traditionally used to describe goods that can serve both civilian and military purposes (Council of the European Union, 2021, Art. 2(20)). This listing however, brought spyware and related surveillance tools under the scope of export control frameworks, which are designed to monitor and restrict the transfer of goods and technologies in order to limit their proliferation and preserve international security and stability (Anthony, Bauer, and Wetter, 2007; Rosen Zvi, 2023).

However, the trade in spyware presents distinct challenges that existing dual-use regulatory frameworks are not fully equipped to address. These challenges manifest mainly in two ways. Firstly, interviewees noted that while the listing of spyware within the dual-use export control system provides a basis for control, it does not adequately capture the specific human rights risks or the highly secretive nature of the spyware industry. These concerns were echoed in the PEGA Committee report which highlighted that spyware vendors often deliberately maintain complex corporate structures that conceal problematic activities and affiliations (PEGA Committee, 2023). The Committee found that many spyware vendors were based in or operated from EU Member States, benefitting from the EU internal market, and exported surveillance technologies to third countries. It further observed that spyware functions not only as a commercial

product but also as a form of "political currency" in international relations, serving as an instrument that states can deploy to secure leverage, consolidate alliances, or exchange concessions, which significantly complicates regulatory oversight. The Committee ultimately found that the close ties between vendors and state actors, together with the opacity of commercial arrangements, the lack of transparency in licensing, and the challenges in verifying end-users, result in structural gaps that undermine the effectiveness of the existing EU export control framework. Such gaps allow vendors to exploit opaque corporate structures or shift operations to jurisdictions with weaker rules, limiting the reach of EU export controls.

Secondly, the spyware trade has, over time, undergone a profound transformation (Fidler, 2024). The contemporary landscape of offensive cyber capabilities has moved beyond traditional, integrated surveillance platforms toward fragmented offerings of discrete technical components, modular exploitation frameworks, and cloud-based infrastructures (Sheniak, 2023). This shift has enabled surveillance-as-a-service models, where offensive capabilities, such as data extraction tools, zero-day exploits, or command-and-control infrastructures, are accessed remotely through distributed architectures (Sheniak, 2023). Such developments complicate regulatory oversight and challenge export control frameworks designed for the transfer of complete, tangible systems, particularly when surveillance tools are delivered via cloud infrastructures without physical transfer or local installation, a context in which the applicability of export controls becomes unclear, creating a risk that such technologies may elude such controls (Brockmann & Héau, 2025). These structural shifts underscore the inadequacy of existing oversight mechanisms and the need to reconceptualise regulation so that it addresses not only end products but the entire lifecycle of offensive cyber capabilities and services that constitute the modern spyware ecosystem (Sheniak, 2023).

Multilateral export control regimes and international frameworks

Despite their limitations, export controls are one of the main policy instruments available to regulate the trade in commercial spyware (Bromley, 2024). Historically conceived as mechanisms to prevent the proliferation of goods and technologies liable to threaten international peace and security, export control frameworks can play a significant role when applied to spyware (Bromley & Brockmann, 2021). They provide a legal and institutional basis for oversight and establish procedures through which licensing authorities can scrutinise transfers of highly sensitive technologies (Anstis, Leonard, and Penney, 2023). When effectively designed and implemented, export controls can operate as a safeguard against abuse, introduce a measure of accountability for both vendors and end-users, and reinforce commitments to the protection of human rights, the rule of law and institutional integrity (Bromley & Maletta, 2025).

At the same time, the distinct risks associated with spyware, its intrinsic connection to the exercise of state power, its heightened potential for rights-abusive deployment, and the hidden nature of the commercial surveillance industry, render existing dual-use frameworks insufficient in isolation (Access Now, 2019). The growing availability of spyware also raises the prospect of acquisition and deployment by non-state actors, creating state security risks: criminal groups and terrorist organisations could use commercial surveillance tools to monitor officials, compromise law-enforcement operations, or target informants and witnesses (Vitale, 2025). Without substantive regulation, the risk of such access can only proliferate. Therefore, ongoing policy discussions need to focus on how export controls can be strengthened and adapted to address the human rights and international security risks posed by spyware and related surveillance technologies, particularly modern spyware-as-a-service models. To overcome their inherent limitations, export controls must also be situated within a wider ecosystem of legal, institutional, and political measures, so that regulation is not confined to formal enactment but translated into meaningful and enforceable practice.

Experiences with international export control regimes illustrate both the potential and the limitations of this approach. Long-standing multilateral and regional arrangements such as the Treaty on the Non-Proliferation of Nuclear Weapons, alongside influential but non-binding regimes like the Australia Group, the Nuclear Suppliers Group, and the Wassenaar Arrangement — originally conceived to mitigate military risks — remain important coordination platforms and have gradually broadened to address emerging technologies. However, these frameworks have been criticised for their limited capacity to address the human rights implications of such technologies (Kanetake, 2021). More recently, new international fora such as the Pall Mall process have begun to emerge and adopt a more multi-faceted approach, situating export controls alongside other policy levers such as cybersecurity and civil liability mechanisms for vendors and intermediaries, sanctions, procurement rules, and human rights due diligence. Together, these developments reflect a growing recognition that while export controls remain an important element of the global response to spyware proliferation, they are not sufficient on their own (Bromley & Maletta, 2025).

The following information boxes provide an overview of the main multilateral arrangements and international fora relevant to these efforts.

The Wassenaar Arrangement

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a voluntary multilateral agreement of 42 participating states that seeks to enhance transparency and responsibility in the transfer of both military items and sensitive dual-use goods and technologies that could contribute to regional or international instability. While the Arrangement does not explicitly focus on human rights, it has increasingly become a reference point in global efforts to prevent the misuse of surveillance capabilities, including commercial spyware (Maurer, 2016).

The Wassenaar Arrangement operates by requiring states to maintain national export controls over a common list of items and by providing a forum for information exchange and regular consultation among participating states (Open Technology Institute, 2013). Although all licensing decisions remain at the discretion of individual governments, the Arrangement aims to build a shared understanding of risks and promote coordinated responses to emerging threats (Lubin, 2024).

In the aftermath of the Arab Spring, and in response to documented abuses of surveillance technologies by authoritarian regimes, Wassenaar Arrangement members initiated negotiations to bring certain cyber-surveillance tools under multilateral control (Benson & Mouradian, 2023). Despite these additions, the Wassenaar Arrangement faces sustained criticism from academics and policymakers for its limited effectiveness in addressing the proliferation of commercial spyware (Fidler, 2015). As a voluntary and non-binding mechanism, it lacks enforcement tools and provides no direct guidance on human rights safeguards (Kaye, 2019). Divergent national implementation further undermines consistency, while the absence of several major spyware-producing states, such as China, Israel, and the United Arab Emirates, creates significant loopholes (Arms Control Association, 2022). More recently, the geopolitical tensions deepened by Russia's invasion of Ukraine have made consensus on new control list categories or emerging technologies increasingly difficult to achieve and raises doubts about the Arrangement's ability to function as an effective framework for spyware governance.

Joint Statement on efforts to counter the proliferation and misuse of commercial spyware

In March 2023, the United States spearheaded another multilateral effort and issued the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, endorsed by 23 states as of September 2024, including 10 EU Member States. The statement:

- commits governments to take collective steps to mitigate misuse, such as establishing safeguards to ensure any deployment of spyware is consistent with international human rights standards and the rule of law, and preventing exports to end-users likely to engage in malicious cyber activity (US Department of State, 2024).

- underscores the role of export controls, calling on states to align their domestic frameworks and apply existing regimes to restrict transfers of spyware technologies to high-risk destinations.

- commits governments to improve information-sharing, cooperate with industry and civil society to raise awareness and develop standards, and broaden international participation to strengthen policy coherence.

While non-binding, the Joint Statement reflects a growing consensus that export controls and coordinated regulatory action are necessary to curb spyware proliferation and its associated human rights risks. This sentiment can similarly be applied to the Export Controls and Human Rights Initiative, which create a shared framework for preventing the proliferation of surveillance technologies that enable human rights abuses. Through the Summit for Democracy series, 25 states endorsed a voluntary Code of Conduct, committing to use export controls as a tool to prevent misuse and reiterated that export controls must serve not only security interests but also function as safeguards against the misuse of spyware and related surveillance tools.

Pall Mall Process

The Pall Mall Process, launched in 2024 by France and the U.K., represents one of the most notable recent developments in international efforts to curb spyware proliferation. Conceived as a multi-stakeholder initiative, it brings together governments, industry, and civil society around the goal of addressing "the proliferation and irresponsible use of cyber intrusion capabilities" (UK Government, 2023). Its creation reflects a growing recognition among states globally that inaction is no longer tenable and that the costs of spyware misuse for the rule of law, democratic institutions, and national security are too high to ignore (Ní Aoláin & Edmeades Jones, 2024).

At its core, the Process is structured around a non-binding Code of Practice for States, endorsed by 26 states as of September 2025, including 18 EU Member States.[4] The Code is organised around four pillars: accountability, precision, oversight, and transparency. Each pillar outlines commitments designed to prevent misuse of commercial cyber intrusion capabilities. Notably, under the accountability pillar, states recognise export controls as one of the primary levers available to control the trade of cyber intrusion capabilities. States therefore pledge to ensure that licensing decisions explicitly weigh the risk of internal repression or serious human rights abuses, to restrict exports to specific lawful end-users and defined purposes, and to strengthen published guidance so that exporters have clarity on their obligations. In addition, signatories commit to reviewing their domestic regulatory frameworks, updating multilateral arrangements where necessary, and investing in capacity-building to address the technical complexities of implementation.

At the time of writing, the Pall Mall Process is also initiating discussions on a prospective Code of Practice for Industry, which could provide an opportunity to engage industry on strengthened due diligence obligations linked to export controls and to encourage greater transparency in human rights risk assessments.

4 Austria, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Luxembourg, the Netherlands, Poland, Ireland, Romania, Slovakia, Slovenia, and Sweden.

02

The EU export control legislative framework: the Dual-Use Regulation

In the EU, prior to 2021, dual-use exports were originally governed by Regulation (EC) 428/2009, which established a common legal basis for controls on export, re-export, brokering, and transit of dual-use items. Consistent with the traditional purpose of export controls, EU dual-use rules were historically justified in terms of non-proliferation and international security, particularly the prevention of illicit transfers to weapons of mass destruction programmes (Kanetake, 2020). Over time, however, this rationale was increasingly supplemented by concerns about emerging technologies, such as surveillance items, artificial intelligence systems, and cyber-intrusion tools, whose misuse raised security, human rights and accountability concerns (European Commission, 2016).

This evolution therefore laid the groundwork for momentum to strengthen EU oversight of cyber-surveillance exports in the aftermath of the Arab Spring. These cases raised questions about the adequacy of existing controls and the consistency of EU export practices with its broader foreign policy objectives, including the promotion of human rights (Kanetake, 2019).

Against this backdrop, in 2016 the European Commission proposed a recast of the Dual-Use Regulation to introduce, among other things, more stringent provisions on the export of cyber-surveillance technologies. By explicitly linking export controls to human rights considerations for the first time, and thereby moving beyond the framework's traditional emphasis on non-proliferation and security risks (European Commission, 2016), the proposal triggered political debate over the implications of integrating human rights into an instrument historically centred on security and trade. Member States diverged on whether the EU should move beyond the parameters set by multilateral export control regimes, with Germany, France and nine other states making clear in a 2018 working paper that the definition of dual-use items should remain based on the traditional civil-military dichotomy (Kanetake, 2019). Industry stakeholders warned of

legal uncertainty and administrative burdens (Assonime, 2021; DigitalEurope, 2017), whereas civil society organisations called for stronger safeguards to ensure that EU export policy reflects its broader normative commitments (Amnesty International, 2021; Access Now, 2017; Steering Committee of the Coalition Against Unlawful Surveillance Exports, 2018). After several years of debate, the European Parliament adopted the revised Dual-Use Regulation in May 2021, which entered into force on 9 September 2021.

The Recast Dual-Use Regulation

Building on the reform process launched in 2016, the recast Dual-Use Regulation constitutes the primary EU legal instrument governing the export, re-export, brokering, and transit of dual-use goods, including spyware and other cyber-surveillance technologies. As a regulation, it is directly applicable across all Member States, while implementation and enforcement responsibilities rest with national authorities. Export licensing applications are thus examined and decided by designated ministries or agencies, which also bear responsibility for monitoring compliance and investigating potential violations.

The core architecture of the framework was maintained, therefore the recast Regulation continues to form part of the EU's Common Commercial Policy and pursues both commercial and security objectives. To ensure coordination and information sharing, Member States meet in the Working Party on Dual-Use Goods, chaired by the rotating Presidency of the Council of the EU, and the Dual-Use Coordination Group, chaired by the Commission, which serves as the main venue for exchanging information on implementation practices, licensing decisions, and enforcement challenges. Technical discussions are further supported by the Surveillance Technology Expert Group, which brings together Member States' experts to address the complexities of cyber-surveillance technologies.

The Regulation combines controls on listed items, set out in Annex I, and catch-all provisions that extend oversight to non-listed technologies where there is a risk of misuse. Annex I is updated annually to reflect changes in the main multilateral regimes.[5] Since 2012, five categories of spyware and other cyber-surveillance tools, including intrusion software and IP network surveillance systems, have been incorporated into the Wassenaar lists and thereby brought within EU controls.

Article 5 establishes a catch-all control for non-listed cyber-surveillance items. Under this mechanism, authorisation may be required where there are reasonable grounds to believe that an item could be misused for repression or serious human rights

5 Such as the Wassenaar Arrangement, the Australia Group, the Missile Technology Control Regime, and the Nuclear Suppliers Group.

abuses. The obligation can be triggered either by the licensing authority or by the exporter. A central innovation of Article 5(2) is the explicit requirement that exporters themselves assess whether their products could contribute to internal repression or violations of human rights and international humanitarian law. These assessments are to be embedded in transaction-screening measures within Internal Compliance Programmes (ICPs), calibrated to the size and structure of each operator.[6] Article 5(3) further enables Member States to impose national authorisation requirements on non-listed cyber-surveillance items, while Article 5(6) provides a procedure for collective EU-level adoption of new controls. Based on information collected through interviews with licensing officials, however, the use of the catch-all control appears to have been limited, with no reported cases of Member States notifying exporters of the requirement to obtain a licence.

To support implementation, the European Commission issued guidelines in October 2024. These clarify the definition of cyber-surveillance items as tools designed primarily to enable covert monitoring of individuals by extracting, collecting, or analysing data from ICT systems. Furthermore, the guidelines provide "red flags" to help exporters identify risky transactions and note that technologies such as certain types of facial recognition software, location-tracking systems, and social media analytics tools may fall within the scope of Article 5 even if not covered by multilateral lists. They further stress that due diligence is an ongoing process requiring assessment of both technical features and intended end-uses, and that exporters should adopt internal compliance measures to mitigate risks of contributing to repression or serious violations of international law.

In parallel Article 15 sets out the criteria that licensing authorities must apply when deciding on export authorisations. Article 15 requires Member States to take into account a range of considerations, including international obligations, sanctions, foreign and security policy considerations, and the criteria set out in the EU Common Position on arms exports (2008/944/CFSP). The Common Position establishes eight criteria, including the risk of internal repression and the risk of serious violations of international humanitarian law. Its User's Guide clarifies that "internal repression" includes torture and other major violations of human rights and fundamental freedoms,[7] and that the current and past human rights record of the end-user and recipient country should be considered. For serious violations, the User's Guide calls for assessing the recipient's attitude towards IHL by looking at its record, its formal commitments, and its capacity to uphold relevant provisions. In April 2025, Criterion 2 of the Common Position was amended to require denial of an export licence not only where there is a clear risk that items might be used to commit internal repression or serious IHL violations, but also

6 Internal Compliance Programmes (ICPs) are company-level policies and procedures designed to ensure compliance with export control obligations, as defined in Article 2(21) of Regulation (EU) 2021/821 and further elaborated in the European Commission's 2019 Guidance on ICPs (European Commission, 2019).

7 In addition to other cruel, inhuman and degrading treatment or punishment, summary or arbitrary executions, disappearances, arbitrary detentions.

where they might facilitate such acts. While detailed, the Common Position and its User's Guide focus on transfers of military equipment and do not explicitly consider 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 misuse. However, how Member States operationalise human rights assessments in this context remains unclear, as licensing practices are subject to very limited transparency. At the same time, civil society organisations continue to document cases where states failed to conduct adequate human rights risk assessments when providing surveillance capabilities to third countries in the context of law enforcement capacity-building activities (Amnesty International, 2025; Bromley & Maletta, 2025).

Intra-EU transfers

The EU's export control regime is designed primarily to regulate movements of dual-use items from the Union to third countries. As clarified in recital 27 of the Dual-Use Regulation, the existence of a common control system is the prerequisite for the free circulation of dual-use items within the EU customs territory (European Union, 2021). In practice, this means that export authorisations are required when items are destined for a third country, but not when the same goods are transferred between Member States.

The Regulation therefore reflects the underlying principle of the internal market. Licensing requirements for intra-EU transfers are limited to a very small subset of particularly sensitive goods listed in Annex IV of the Regulation, such as cryptanalytic tools, most nuclear-related items, stealth-related technology and items related to missiles and chemical warfare. Spyware and other cyber-surveillance tools for which catch-all controls apply, are not included. As a result, these items are subject to export licensing when leaving the EU but may circulate freely once inside it.

This results in a regulatory asymmetry with implications for fundamental rights and while the EU has developed strict export controls to prevent spyware from reaching third countries with poor human rights records, no equivalent safeguards apply to its circulation within the Union. In particular, intrusion software and communication surveillance systems require prior authorisation when exported abroad, yet face no comparable oversight internally. This gap means that once a spyware vendor is established in one jurisdiction, its products can circulate freely across the internal market without further licensing or scrutiny, even when destined for domestic law enforcement, security, or intelligence services.

The European Parliament has already highlighted this regulatory gap and warned that existing controls protect non-EU citizens against surveillance abuses more effectively than persons residing in the EU (European Parliament, 2023). This discrepancy is particularly troubling given that the risks to privacy, freedom of expression, and democratic participation are also present inside the Union.

The European Parliament's PEGA Committee has already documented cases in which spyware was deployed inside EU Member States for political purposes, in clear violation of democratic safeguards (European Parliament, 2023). Yet little meaningful follow-up has taken place since the Committee issued its key recommendations in 2023. More recent cases, such as the reported deployment of Paragon's Graphite spyware against journalists and human rights defenders in several EU Member States, demonstrate that the risks remain acute. In response, the Spyware Coordination Group, a coalition of civil society organisations led by CDT Europe, has urged EU institutions to adopt concrete and coordinated measures to counter these threats, strengthen the resilience of Europe's digital infrastructure, and address the unchecked proliferation of surveillance technologies within the internal market (Spyware Coordination Group, 2025).

Beyond the risks of abuse for fundamental rights, this regulatory asymmetry also undermines the effective implementation of the Dual-Use Regulation. Divergent national practices in licensing and enforcement create uneven levels of scrutiny, leaving open loopholes that can be exploited by spyware vendors. In fact, companies denied an authorisation in one Member State may be able to route the same transaction through another jurisdiction with lighter procedures, or establish themselves where oversight is weaker. The broader implications of these dynamics, and how divergences in Member State practice exacerbate them, are examined in Chapter 4.

03

National implementation of the EU Dual-Use Regulation

Case studies from France, Germany, Italy and the Netherlands

The Dual-Use Regulation expressly provides that responsibility for deciding on individual, global, or national general export authorisations, as well as for brokering services, technical assistance, transits of non-Union dual-use items, and intra-EU transfers of items listed in Annex IV, lies with the competent national authorities. In practice, this means that Member States exercise primary authority over licensing and enforcement, with decisions shaped by their national legal frameworks and administrative structures, and are responsible for establishing the mechanisms through which EU export control obligations are enforced. As a result, the institutional architecture of export control systems varies across the EU. In some countries, responsibility is vested in the ministry of the economy, while in others it lies with the ministry of foreign affairs or trade, or it is managed within a broader institutional framework that also oversees military equipment. The competent national authority may either function as an internal unit within a ministry or operate as a separate, semi-autonomous agency.

In general, the common model consists of a dedicated licensing authority and the Dual-Use Regulation sets common minimum standards on the information to be provided in such applications. Exporters are generally expected to supply details on the exporter and the consignee, a description of the items, their destination and intended end-use, together with supporting documentation. This documentation includes end-use statements which are declarations signed by the recipient certifying the intended use of the goods and committing not to re-transfer them. In parallel, exporters are expected to conduct due diligence and integrate risk assessments into ICPs, to enhance traceability and ensure that exports are not diverted or misused. For particularly sensitive or high-risk cases, decisions may be escalated to an interministerial body tasked with assessing

such exports in accordance with both the technical criteria and broader foreign policy or security considerations established under EU and national law. When assessing licence applications, national authorities must take into account the criteria set out in Article 15 of the Regulation, which include those drawn from the EU Common Position on arms exports. How these criteria are applied in practice, however, remains difficult to ascertain, as the internal standards, methodologies, and guidance used by licensing authorities are not systematically made public.

In practice, this means that while the Regulation establishes common obligations at EU level, licensing remains embedded in national systems, shaped by each state's administrative traditions, resources that governments allocate to export control, such as staffing levels, technical expertise, institutional infrastructure, and the nature of relationships with industry (Kanetake, 2024). **This decentralised approach makes the functioning of EU export controls inseparable from the legal and political contexts of individual Member States.**

These structural and contextual differences provide important background for the comparative case studies that follow. The analysis of France, Germany, Italy, and the Netherlands illustrates how divergent institutional arrangements and levels of resourcing shape the practical implementation of the Regulation, and in turn affect transparency, due diligence obligations, and human rights safeguards in place.

France

National legal framework and competent national licensing authority

In France, the national legal framework governing the control of dual-use goods and technologies is primarily grounded in three key legislative instruments[8] and the export control system for dual-use goods is managed through a centralised interministerial structure involving two primary bodies. The first is the Dual-Use Goods Service (Service des biens à double usage, SBDU), which operates under the Directorate-General for Enterprises within the Ministry of the Economy, Finance and Industrial and Digital Sovereignty. The SBDU acts as the national authority for the classification of

8 Decree No. 2001-1192 of 13 December 2001, as amended, which regulates the export, import, and transfer of dual-use items; Decree No. 2020-74 of 31 January 2020, which outlines the competencies and organisational structure of the national competent authority for dual-use goods; and Decree No. 2010-294 of 18 March 2010.

goods and is responsible for issuing export licences for dual-use, certain restricted items and evaluates authorisation requests and issues licences valid for two years, permitting multiple customs clearances within the specified limits of quantity and value (Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, n.d.). In addition to licensing, the SBDU handles requests related to classification and the feasibility of exports involving sensitive but non-listed goods. For complex or ambiguous cases, it may consult with members of the interministerial commission.

The second key institution is the Interministerial Commission on Dual-Use Goods (CIBDU). The CIBDU functions as the primary forum for interministerial coordination and expertise in dual-use export controls. Until June 2023, it operated under the authority of, and was chaired by, the Ministry for Europe and Foreign Affairs. Since 20 June 2023 however, chairmanship of the CIBDU has been transferred to the General Secretariat for Defence and National Security (Secrétariat général de la défense et de la sécurité nationale, SGDSN). The SGDSN is an interministerial body reporting directly to the Prime Minister and tasked with assisting in the exercise of his responsibilities for national defence and security. The commission's secretariat is managed by the SBDU. The French government has justified this institutional change by referencing the deteriorating international context, concerns over proliferation and sanctions circumvention, and intensifying technological competition (Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, 2024). At the same time, the reorganisation sought to enhance responsiveness to international security challenges, while also taking into account economic and competitiveness considerations for French companies. This shift signals a stronger securitisation of dual-use export controls in France, bringing them closer to the framework for military exports. Moreover, given the SGDSN's mandate as an interministerial body supporting the Prime Minister on defence and security matters, its chairmanship of the CIBDU may narrow the scope for transparency and external engagement, as national security institutions have traditionally operated with limited openness toward civil society and independent experts.

The CIBDU brings together representatives from a wide array of ministries and public bodies with relevant expertise.[9] This broad interministerial composition allows for comprehensive assessments of export licence applications, particularly those involving sensitive end-uses or destinations. While routine applications are processed by the SBDU, cases deemed particularly sensitive may be referred to the CIBDU for deliberation. In such cases, the SBDU is bound to follow the opinion issued by the commission. In cases involving goods and technologies related to cryptology, the SBDU is required to consult the National Cybersecurity Agency of France (Agence nationale de la sécurité des systèmes d'information, ANSSI) and must adhere to its technical assessment.

9 This includes the SGDSN, Ministry for Europe and Foreign Affairs, Ministry of the Armed Forces, Ministry of the Interior, Ministry of Energy Transition, Ministry of Research, Ministry of Health, Ministry of Agriculture, Ministry of Customs, Ministry of Foreign Trade, and the French Atomic and Alternative Energy Commission.

Licensing procedure

According to interview information, the review process for all export applications is conducted on a case-by-case basis and involves a risk-based approach that takes into account geopolitical, industrial, technical, and human rights considerations. Particular emphasis is placed on preventing exports that could contribute to serious violations of international and human rights law. While internal criteria are reportedly applied, their practical modalities are not reflected in public reporting, and interview sources indicated that these could not be shared for reasons of confidentiality. Exporters are expected to conduct an initial risk assessment concerning the potential end-use of their products. Given their proximity to the customer and knowledge of the technical capabilities of the product, companies and research institutions are considered best positioned to assess whether an export might be misused. Interview sources emphasised the responsibility of exporters to assess both the declared and potential end-uses of their goods, especially where there is a risk of diversion to unlawful or harmful applications.

Oversight of the export control system is further reinforced through formal accountability and appeal mechanisms. Exporters who are denied a licence may request a second assessment. If the Interministerial Commission confirms the initial decision, it can be appealed before an independent administrative court. Additionally, independent oversight is exercised through parliamentary review. As such, the French Parliament receives an annual report on dual-use exports, and a dedicated parliamentary commission has been established to examine the export of dual-use, military, and related items.

Compliance with the EU Dual-Use Regulation is enforced through the French Customs Code. Violations of export control obligations, including non-compliance with licensing conditions, are subject to administrative and criminal penalties under national law.

As for mechanisms aimed at detecting the misuse of exported cyber intrusion capabilities after the fact, or the existence of ex-post monitoring frameworks to assess end-use compliance, no publicly available information is currently available to allow a definitive assessment. French law does not stipulate specific post-export surveillance obligations on exporters or authorities in this area.

Due diligence and human rights assessments

According to interview information, France's approach to due diligence within its dual-use export control system combines interministerial coordination and exporter outreach. While several initiatives are in place, including an annual forum organised by the Ministry of Economy and the publication of general information and guidelines,

these mechanisms provide only limited public insight into how due diligence obligations are interpreted and applied in practice.

Both administrative bodies and exporters have the ability to request an official assessment of whether specific goods or technologies fall within the scope of the Dual-Use Regulation. Although this offers legal certainty regarding product classification, it does not extend to the broader question of human rights-related due diligence, which remains largely embedded in internal processes and discretionary assessments.

Official communication indicates that France systematically takes into account human rights considerations in its licensing decisions (Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, 2023). Notably, reference is made to allegations of violations reported by the UN, EU, the European Union, or the Council of Europe. France's accession to the U.S.-led voluntary Code of Conduct on the export of dual-use goods with potential for misuse also reflects an intention to align with international human rights standards.

In accordance with Article 15 of the Dual-Use Regulation, French licensing authorities apply the criteria set out in Council Common Position. However, the internal criteria used to assess human rights risks are not publicly available, and no supplementary due diligence obligations are imposed on exporters beyond basic regulatory compliance. Authorities may request additional information from exporters, but the process for determining whether mitigation measures are sufficient is not subject to external review or routine publication. As such, it is difficult to assess how consistently and effectively human rights risks are evaluated across different cases.

In its most recent annual report to Parliament, the French government reiterated the need for heightened vigilance in the export of dual-use items, emphasising the particular sensitivity of spyware and cyber-surveillance technologies given their potential impact on privacy and human rights.

Transparency

As of mid-2025, three reports have been submitted by the Ministry of the Economy, Finance and Industrial and Digital Sovereignty on the implementation of dual-use export controls, to the Parliament.

While the existence of these reports constitutes a formal gesture toward transparency, the level of detail they provide remains limited. The published data is largely confined to aggregate statistics for categories of dual-use goods, including the number of licence decisions issued, the average processing time for applications, the country of destination and the overall customs clearance rate. However, the reports do not provide granular information on the nature of the controlled items, the specific end-users of exports, the exporting company per transaction or the criteria used in assessing licence applications. In particular, they offer no systematic insight into how sensitive factors, such as the

potential for human rights violations, surveillance misuse, or end-use diversion, are evaluated during the decision-making process. This lack of detail makes it difficult to assess the consistency, rigour, or precautionary orientation of France's control system.

The legal basis for this reporting obligation charges the SBDU with maintaining statistical and documentary oversight of dual-use exports. Although this legal provision provides a clear mandate for monitoring and data collection, its operationalisation has not yet led to the establishment of a robust public reporting framework. As a result, opportunities for independent scrutiny, informed public debate, or comparative evaluation with other EU Member States remain constrained.

Germany

National legal framework and competent national licensing authority

In Germany, the administrative implementation of export controls on dual-use goods rests with the Federal Office for Economic Affairs and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle, BAFA),[10] which functions as the central licensing authority and is charged with operationalising the Federal Government's export control policy. The legal framework underpinning BAFA's mandate is anchored in the Foreign Trade and Payments Act (Außenwirtschaftsgesetz, AWG) and the Foreign Trade and Payments Ordinance (Außenwirtschaftsverordnung, AWV), which sets out national obligations, and is further complemented by directly applicable EU legislation.[11] Within this structure, BAFA's primary responsibility is to determine whether specific exports, services, or transit activities fall within the scope of licensing requirements and, if so, whether an authorisation can be granted in light of technical, legal, and policy considerations.

Licensing procedure

The licensing process is document-intensive and places considerable responsibility on exporters to provide comprehensive information. For exports of listed goods, including spyware, an end-use declaration prepared by the foreign customer on company letterhead, in German or English, specifying the intended use of the product, is required. Where exporters seek clarification on whether a licence is required for a given product,

10 According to interview information, BAFA is structured into two main departments, one administrative and one technical, and employs around 250 staff in total. In addition to its administrative personnel, the authority relies heavily on its technical expertise, with approximately 100 engineers specialising across the spectrum of items regulated under the EU Dual-Use Regulation.

11 Dual-Use Regulation, Regulation (EU) No. 258/2012 (the Firearms Regulation), Regulation (EU) 2019/125 (the Anti-Torture Regulation), and the corpus of EU embargo regulations.

commonly via a so-called "zero-licence", BAFA conducts a statutory review, ultimately issuing either a formal statement that a licence is not required or a notification that a licence is necessary. Export applications must additionally be accompanied by copies of the relevant contractual agreements, detailed technical descriptions of the goods, and corporate profiles of all actors involved in the transaction, including the buyer, recipient, and end user (Federal Office for Economic Affairs and Export Control, 2021).

Licensing files undergo an initial completeness check within the administrative department before being referred to the technical unit. There, engineers assess the goods in detail, reviewing technical documentation, classification issues, and product specifications to determine whether the items fall within the scope of the control lists and to assess the plausibility of the declared end-use. Their technical expertise ensures that the authority can accurately distinguish between legitimate commercial applications and items with potential for misuse.

Appeal mechanisms are formally available to exporters who wish to contest the denial of a licence, including before an administrative court if subsequently denied after internal review. However, the scope of judicial review is limited: courts assess whether procedural or legal errors occurred, for example, a failure to observe the principle of proportionality or to adequately consider relevant facts, but they do not substitute their own discretion for that of the licensing authority. Importantly, standing to initiate such proceedings is restricted under German law to exporters directly affected by licensing decisions, meaning that civil society organisations cannot challenge authorisations or denials unless they are able to demonstrate that their own individual rights have been directly infringed. According to information obtained during interviews, to date no appeals have been lodged in relation to cyber-surveillance export decisions.

Enforcement and monitoring are shared responsibilities between BAFA and German customs authorities. Customs may flag suspicious exports and, where necessary, require the exporter to seek a licence before goods can leave the country. However, once an export has been licensed and completed, no general reporting obligations exist for exporters to inform authorities about the subsequent use of their products. In practice, however, authorities may obtain indirect insights into end-use through subsequent applications, for instance when companies request authorisations to export updates or complementary goods to the same end user. In such cases, BAFA can assess whether the behaviour of the end user in the intervening period is consistent with the declared commitments. Exporters are also bound by non-re-export clauses: any planned transfer of the product to a third country requires a new authorisation, thereby allowing authorities to reassess potential human rights risks at each stage.

Due diligence and human rights assessments

Germany's approach to due diligence is primarily structured around existing EU frameworks. Licensing authorities apply the criteria established under Council Common Position on arms exports. BAFA also refers both to its own Leaflet on Article 5 of the

EU Dual-Use Regulation (published in 2021) and to the more recent guidance issued by the European Commission in October 2024.

In practice, according to interview information, BAFA applies a risk-based and forward-looking assessment of both the end-use and the end user. This means that the authority does not limit itself to verifying the declared purpose of an export, but actively considers whether the goods could reasonably be misused in the future. According to interview information, this predictive assessment is particularly relevant in the field of cyber-surveillance technologies, where misuse often materialises only after export. To inform its evaluations, BAFA draws on a broad range of sources such as public reports by international human rights organisations, open-source investigations, assessments by the Ministry of Foreign Affairs and German diplomatic missions in destination countries, as well as intelligence inputs. However, intelligence services tend to prioritise risks linked to weapons of mass destruction, which limits the extent to which their contributions systematically capture the misuse potential of cyber-surveillance tools.

Cases in which no credible risks, or significant risks are identified generally result in either the issuance or denial of a licence. According to interview information, borderline situations are more complex and are assessed against additional criteria, such as the technical sophistication of the item, the likelihood of diversion, and the availability of corroborating evidence regarding the end user's track record. Particularly sensitive or politically salient cases are escalated to the Federal Ministry for Economic Affairs and Climate Action or to the Federal Foreign Office, ensuring that politically accountable ministries are directly involved in difficult decisions.

According to interview sources, due diligence obligations are not treated as a central pillar of the German licensing system. Licences are hence issued unless a risk threshold is clearly met, which makes the process more reactive than preventive. The role of company-level due diligence becomes decisive primarily in cases where exporters fail to disclose material information that they could reasonably have been expected to know. In such instances, omissions may be interpreted as evidence of insufficient due diligence and can form an independent ground for licence denial.

Human rights risks are considered the most important substantive criterion in the decision-making process. Interviewees highlighted that licences would not be granted if there is credible information that exported technologies could be used to monitor political dissidents, enable their capture, or contribute to torture. Mass surveillance practices are regarded as an additional area of concern. However, interviewees reported that such clear-cut cases are relatively rare, partly because exporters themselves often avoid applying for licences in contexts where risks are manifest, for example in relation to countries already known for repressing political opposition.

More frequently, according to interview information, authorities encounter "grey-zone" scenarios, where the end users are law enforcement or intelligence agencies in countries with contested human rights records. In these cases, interviewees reported

that the declared purpose may be legitimate, such as criminal investigations or counter-terrorism, yet the possibility of abuse remains present. These situations are particularly difficult to assess according to interviewees, given divergent legal standards outside the EU and the absence of conclusive evidence. They therefore require detailed fact-finding, consultation with other ministries, and inter-agency coordination. Interviewees underlined that the quality of information gathering and sharing is decisive in such cases.

German authorities also participate actively in multilateral coordination. All denials are systematically shared with other EU Member States and with the European Commission, and authorities are required to consult if another state has previously issued a denial in a comparable case. Additional exchanges take place within the Dual-Use Coordination Group and the Subgroup on Export Controls, as well as bilaterally, to promote consistency and prevent exporters from "shopping" between jurisdictions.

Judicial practice adds a further dimension. German administrative courts, particularly in relation to Article 4 of the Dual-Use Regulation, have clarified that authorities cannot rely solely on broad or generalised concerns about a country's human rights record. Instead, they must establish a concrete factual basis to justify a denial. Combined with restrictive standing rules that prevent civil society organisations from challenging export authorisations, judicial review remains limited as an external check.

Lastly, outreach to industry constitutes an important component of Germany's due diligence framework. BAFA organises two major events each year: the Export Control Information Day and the Export Control Forum, the latter primarily aimed at practitioners and officials. It also disseminates explanatory materials and guidelines for exporters on their obligations under the Dual-Use Regulation, ICPs and the procedure. Customs authorities complement these efforts by applying risk profiles at the border. When red flags are identified, they may require exporters to obtain a zero-licence, providing an additional safeguard and reinforcing compliance (Federal Office for Economic Affairs and Export Control, 2024).

Transparency

In Germany, transparency on dual-use export controls is markedly limited. Unlike in the field of conventional arms, where the government publishes annual reports on authorised exports, there is no equivalent reporting practice for dual-use items. Interview information indicates that Germany generally provides no systematic public information on authorisations granted or denied under the Dual-Use Regulation, nor on the application of Article 5 to cyber-surveillance technologies.

The absence of a dedicated reporting framework means that data on licensing decisions, destination countries, categories of controlled items, or end-use considerations remain unavailable to the public. While Germany participates in EU-level information exchange and denial notification mechanisms among Member States, these processes are confidential and do not translate into public-facing transparency.

Italy

National legal framework and competent national licensing authority

Italy's regulatory framework for the export of dual-use goods is primarily established under Legislative Decree No. 221/2017, which transposed into national law the rules laid down in the Dual-Use Regulation. A significant institutional change took effect on 1 January 2020, when the responsibility for issuing export authorisations for dual-use items was transferred from the Ministry of Economic Development to the Ministry of Foreign Affairs and International Cooperation (MAECI). According to the explanatory memorandum of Legislative Decree No. 104/2019, this reform was justified as necessary to "confer a unified vision of the promotion of the national interest abroad" by centralising trade promotion, internationalisation, and export control within a single ministry. Within this new framework, the Unit for the Authorisation of Armament Materials (UAMA) within MAECI was designated as the national authority responsible for managing export controls.

Within this framework, UAMA is tasked with issuing authorisations for the transfer of dual-use materials, certifying companies, and ensuring compliance with related regulatory obligations. For exports or imports involving non-NATO/EU destinations, UAMA relies on the advice of an Advisory Committee. This Committee is composed of representatives from MAECI, which coordinates its work, as well as the Ministries of the Interior, Defence, Enterprise and Made in Italy, Economy and Finance, Customs and Monopolies Agency, and the Ministry of the Environment and Energy Security. In cases involving classified materials or sensitive information, UAMA is further required to obtain binding opinions from the Presidency of the Council and the Department of Security Information. Where appropriate, the process may also involve securing specific commitments from competent authorities in the destination state, often through the direct involvement of Italian diplomatic missions abroad.

Within the Italian Ministry of Foreign Affairs, the division responsible for dual-use items consists of approximately ten officials, a number that may rise to twelve in the future. According to interview information, this staffing level has proven insufficient given the increasing workload generated by additional responsibilities, particularly in relation to the implementation of sanctions regimes. Unlike in other export control domains, such as the Missile Technology Control Regime or the Nuclear Suppliers Group, where three dedicated experts are already employed, the division reportedly currently lacks equivalent in-house expertise for cyber-surveillance technologies. Recognising that these items evolve rapidly and demand a level of technical understanding that goes beyond ordinary administrative competence, UAMA has moved to strengthen its expertise. On 28 August 2025 it launched a public selection process for five external experts, including one specialising in cyber-surveillance (MAECI, 2025).

Licensing procedure

As of 1 July 2022, export licence applications are processed through an electronic licensing portal, where companies are required to submit supporting documentation, including contractual agreements, information on the transaction partners and end-users, relevant technical specifications, and an end-user statement. Unlike the arms sector — where registration in the National Register of Enterprises engaged in the production and movement of armament materials (SeRNI), is a mandatory precondition — companies exporting dual-use items are not subject to such registration requirements. Instead, access to the e-licensing portal and submission of the necessary documentation serve as the operative prerequisites for the authorisation process, ensuring that only duly identified entities may engage in the trade and export of controlled dual-use goods.

Where applications are refused, companies are first notified through an advance notice of refusal, which gives them ten days to submit comments or additional information. These submissions are taken into consideration and may, in certain cases, lead to a reconsideration of the initial decision. Where the concerns persist, a formal denial is issued, which applicants may challenge before the administrative courts. Importantly, if new information arises after a licence has been granted but before its validity has expired, UAMA has mechanisms to suspend or revoke the licence. According to interview information, authorities do take into account any new elements that may emerge during the licence's validity period and that could justify a reconsideration. However, once the export has already taken place, the margin for intervention is considerably limited. As reported during interviews, such decisions must be grounded in verifiable and reliable sources, and mere informal communications, such as an email, are insufficient. Revocation is possible, but only where concerns are substantiated by credible evidence.

Due diligence and human rights assessments

Italy does not publish national guidelines on due diligence in the field of dual-use export controls. Instead, according to interview information, reference is made to the guidelines issued by the European Commission in October 2024 concerning cyber-surveillance items. Interviewees indicated that, in the case of surveillance technologies, there is a reliance on company-led due diligence to demonstrate that items will not be used to commit human rights violations.

While the authorisation procedure is largely uniform across product categories, the export of cyber-surveillance tools is subject to additional scrutiny. In these cases, UAMA applies an explicit human rights criteria set out in the Council's Common Position on arms exports: licences must be denied if there is a risk that the technology could be used for harmful purposes or in connection with human rights violations. To that end, UAMA places emphasis on the due diligence carried out by exporting companies and maintains regular contacts, including on-site visits, with actors from the private sector in this field. Authorisation requests are reviewed in consultation with the relevant Directorate-General within MAECI and the Italian embassy in the recipient country,

which are asked to provide assurances regarding human rights protections and the likelihood of misuse. Where concerns persist, negative opinions lead to a refusal of the licence.

The process for assessing end-use and preventing misuse relies heavily on the human rights situation in the recipient country. In certain cases, private actors may collaborate with public authorities in providing relevant information. Where doubts remain, Italian embassies are tasked with conducting further assessments of the prospective end-users. Applications are also systematically reviewed by national intelligence services, which provide sensitive information not otherwise publicly available, and by the Advisory Committee, which allows multiple ministries to give input. The Committee's opinion is mandatory but, importantly, non-binding as the final decision rests with the Director of UAMA, who presides as chair.

Interviewees reported that UAMA maintains close and frequent contact with exporting companies, which includes not only routine communications but also on-site visits and interactions at international trade fairs and exhibitions. Interview sources highlighted that authorities know the main companies present on the territory well, including their internal compliance cultures and operational practices, and that this familiarity reinforces their confidence in company-led due diligence.

Authorities also have the ability to verify whether exporters are complying with their obligations through inspections. According to Article 17 of Legislative Decree No. 221/2017, export, import, transfer, brokering, transit, technical assistance and related activities may be subject to checks either before or after an operation. These may take the form of documentary reviews or on-site inspections at the premises of exporters, intermediaries, or technical service providers, with the stated purpose of confirming the declared end-use and final destination of items.

However, unlike in the arms sector, where UAMA is required to conduct regular inspections of companies listed in the National Register of Enterprises, inspections for dual-use and cyber-surveillance technologies are discretionary. In practice, this results in a dual system: while arms exports are subject to mandatory and systematic compliance checks, the oversight of cyber-surveillance and dual-use exports relies more heavily on the due diligence carried out by companies and the selective use of inspections by authorities. This discretionary framework provides a legal basis for compliance verification but falls short of ensuring consistent and systematic scrutiny, particularly in light of the human rights risks associated with surveillance tools.

Transparency

In Italy, transparency on dual-use exports of spyware and cyber-surveillance items is limited. Unlike for arms exports, there is no dedicated national reporting mechanism that provides systematic public data on dual-use authorisations. The only information

available is that which Italy transmits to the European Commission for inclusion in the EU's annual report under Article 26 of the Dual-Use Regulation.

The absence of a standalone national report means that Italian transparency is effectively restricted to aggregated EU-level statistics, which do not identify the Member State behind individual licensing decisions, the destinations concerned, or the reasoning applied.

This gap is significant. While Italy complies with the EU reporting obligation, the lack of national disclosure prevents external stakeholders from understanding how human rights criteria are weighed in the licensing process, or how Italian practice compares to that of other Member States. In practice, there is little insight into the scope of Italy's dual-use exports.

The Netherlands

National legal framework and competent national licensing authority

In the Netherlands, the regulatory framework for the export of dual-use and military goods is grounded in several national acts, orders, and measures. The General Customs Act (Algemene Douanewet, Staatsblad 2008, 111) provides the overarching legal basis for customs controls, defining the competences and responsibilities of Dutch Customs with regard to goods and their movement, including strategic goods. Complementary legislation includes the Strategic Goods Act (Wet strategische goederen), which governs services related to strategic exports, and the Chemical Weapons Convention Implementing Act, which sets specific controls for chemical weapons and related dual-use materials.

The Strategic Goods Order 2012 (Besluit strategische goederen 2012) operationalises these obligations by establishing rules for the export and transit of dual-use and military goods. It designates the Minister for Foreign Trade and Development Cooperation as the competent authority and specifies licensing or notification requirements for military goods, including criminalisation of certain violations. The Order is currently under review, in an effort to update export control legislation in line with evolving security and international obligations.

Within the Ministry of Foreign Affairs, responsibility for export controls lies with the Strategic Goods team, which, according to interview information, comprises 21 staff. Dutch Customs staff complement this work by carrying out enforcement at the border and supporting the implementation of licensing decisions.

Licensing procedure

In the Netherlands, companies or individuals wishing to export items listed in Annex I of the Dual-Use Regulation must apply to the Central Import and Export Office (Centraal Bureau voor de In- en Uitvoer, CDIU) for an export authorisation. The CDIU operates as a subdivision of the Dutch Customs Administration and is responsible for issuing licences under the policy supervision of the Ministry of Foreign Affairs. Certain applications, particularly those deemed sensitive or high-risk, are escalated to the Ministry of Foreign Affairs for a final decision (Ministry of Foreign Affairs, 2013). Export authorisations are formally issued on behalf of the Minister for Foreign Trade and Development Cooperation.

The licensing process requires exporters to provide comprehensive documentation, including technical specifications of the goods, contractual agreements, and information about end-users and end-use. While the CDIU handles the majority of routine applications, sensitive cases involving dual-use items with potential human rights or security implications are reviewed at ministerial level. Authorities may seek additional assurances from foreign counterparts where necessary. According to interview information, Dutch authorities also rely extensively on open-source materials and reports from civil society organisations when assessing risks. Reportedly, intelligence service information is used as well, but it tends to be focused more on exports connected to weapons of mass destruction, meaning that cyber-surveillance cases are primarily informed by non-governmental reporting and open-source intelligence.

Once an export licence is granted, companies are expected to comply with conditions attached to the authorisation, including non-re-export clauses. Any subsequent transfer of the goods to third countries requires a new authorisation, allowing Dutch authorities to reassess the associated risks at each stage. Enforcement and monitoring responsibilities are shared between the CDIU and Dutch Customs, which may inspect shipments and verify compliance with licensing requirements.

Due diligence and human rights assessments

The Dutch framework for dual-use export controls places particular attention on due diligence obligations for exporters Authorities have issued several official publications, such as brochures on cyber-surveillance provisions and the User Guide on Strategic Goods and Services, which are intended to provide companies with guidance on applicable requirements under national and EU law. These documents outline expectations for exporters, including the establishment of ICPs and procedures for assessing human rights-related risks.

The ICP is presented as a central element of company compliance. Guidance issued by the authorities specifies that such programmes should include procedures for product classification, customer and end-user due diligence, transaction monitoring, staff training, and record-keeping. Exporters are advised to review their ICPs on a regular

basis, and to supplement them with enhanced measures in cases involving sensitive items or destinations.

A key element of due diligence in the Dutch framework is systematic screening. Exporters are required to consult restricted party lists, sanctions regulations, and other relevant sources to ensure that goods are not supplied to entities associated with diversion risks or human rights abuses. The Dutch guidelines published a red flag checklist to help exporters identify suspicious circumstances. These include indicators such as opaque ownership structures, unverifiable addresses, unusual payment methods, or incomplete end-use statements.

With regard to cyber-surveillance items, Dutch guidelines foresee that ICPs include supplementary sections addressing potential human rights risks. The government maintains a dynamic list of countries excluded from global licences due to concerns about possible human rights violations, while other countries are subject to careful monitoring, for instance when goods are supplied to government authorities. Implementing human rights-related procedures focuses on raising awareness and acquiring knowledge about potential misuse of the goods and identifying regions requiring more vigilance. Companies are advised to assess factors such as the political situation of the country and the role of the end user, and to include additional declarations or conditions in end-use statements where relevant. ICPs should address at least the following: management's vision on human rights, potential uses of goods in violating or protecting human rights, awareness of regions requiring careful checks, special attention to supplies to government authorities and telecom or data storage providers, procedures to prevent misuse, mechanisms for staying informed on policy changes and communicating them to staff, and the point at which authorities would be consulted if doubts arise. In assessing authorisation applications for dual-use items, including software and technology, the Dutch authorities explicitly consider the risk of human rights violations and will deny applications where concerns regarding end use or end users exist.

The Netherlands aligns its framework with international standards on responsible business conduct, explicitly referencing the OECD Guidelines for Multinational Enterprises and the UN Guiding Principles on Business and Human Rights. Exporters are therefore expected to integrate human rights due diligence into their business practices more broadly, ensuring that risks of adverse impacts are identified, prevented, and mitigated. This alignment is particularly visible in the 2025 Dutch guidelines on cyber-surveillance exports, which underline that exporters must not only examine the technical risks of their goods but also critically assess the credibility of stated end-uses, the institutional context of end users, and the availability of mitigating measures. According to interview information, the brochure accompanying these guidelines is designed with a double function: on the one hand, to raise awareness among companies that they may fall within the scope of the Dual-Use Regulation; on the other, to allow the government to map and identify companies active in this sector. The interviewee further explained that a further objective of the brochure is to operationalise Articles 5 and 2 of the Regulation by making it easier for exporters to understand when their products may

be subject to control. Given the broad and open-ended wording of these provisions, interpretation can be challenging for companies, and the brochure therefore provides practical guidance, including a flowchart and a step-by-step guidance.

Transparency

In the Netherlands, transparency on dual-use exports is primarily exercised through monthly overviews published by the Ministry of Foreign Affairs. These overviews provide information on the permits issued for dual-use goods, specifying the type of goods involved, the intended end-use, the value of the items, and the destination country. The identities of exporters and end users, however, are not disclosed, and information on licence denials is likewise not made public.

The monthly statements are compiled in a file that has been maintained since 2004, allowing for a long-term view of Dutch dual-use exports. This reporting practice enables at least a partial mapping of which goods are exported from the Netherlands, and to which countries.

04

Comparative findings

Drawing from the evidence collected on the four Member States, our findings show that while the Regulation is directly applicable across the Union, its application varies across Member States. Most notably, with differences affecting transparency, the integration of human rights safeguards, the due diligence expected of companies, and the monitoring of end-uses. As outlined in Chapter 2, the absence of intra-EU transfer controls for spyware and cyber-surveillance tools already creates a structural asymmetry in the Regulation. This chapter examines how the divergences in national implementation and enforcement found further reinforce this asymmetry, producing uneven levels of scrutiny across the Union and leaving open channels through which these technologies may be traded with insufficient safeguards.

COUNTRY	COMPETENT AUTHORITY AND STRUCTURE	LICENSING PROCEDURE	HUMAN RIGHTS ASSESSMENTS	DUE DILIGENCE	TRANSPARENCY
France	Dual-Use Goods Service (SBDU), Ministry of the Economy, Finance and Industrial and Digital Sovereignty	Applications submitted to SBDU; routine cases handled directly, sensitive cases reviewed by the inter-ministerial CIBDU	Human rights assessments are carried out on a case-by-case basis	Due diligence obligations fall primarily on exporters, with authorities conducting outreach through annual forums and general guidance	Annual reports to Parliament providing aggregate statistics on licences and destinations
Germany	Federal Office for Economic Affairs and Export Control (BAFA), Federal Ministry for Economic Affairs and Climate Action	Applications submitted to BAFA; routine cases handled administratively, sensitive cases escalated to the Federal Ministry for Economic Affairs and the Federal Foreign Office	Human rights assessments on a case-by-case basis; decisions must rest on a concrete factual basis rather than general concerns about a country's record	Due diligence obligations fall primarily on exporters, with BAFA providing supplementary guidance through leaflets, explanatory materials, and outreach events	No dedicated reporting exists for dual-use exports
Italy	National Authority for Export Control of Armament and Dual-Use Materials (UAMA), Ministry of Foreign Affairs and International Cooperation	Since 2022, applications via an e-licensing portal managed by UAMA; sensitive cases reviewed by an Advisory Committee with multiple ministries and intelligence input	Human rights assessments on a case-by-case basis, rely on systematic consultations with embassies, intelligence services, and interministerial review	Due diligence relies heavily on exporters' internal checks, alongside regular exchanges and close engagement between UAMA and key companies	No dedicated reporting exists for dual-use exports
The Netherlands	Central Import and Export Office (CDIU), Dutch Customs (Ministry of Finance), under policy supervision of the Ministry of Foreign Affairs	Applications submitted to CDIU, routine cases handled by CDIU, sensitive exports escalated to the Ministry of Foreign Affairs	Human rights assessments for sensitive cases are reviewed at ministerial level, with authorities relying extensively on open-source materials and civil society reporting; intelligence inputs are used to a more limited extent, so cyber-surveillance cases are primarily informed by non-governmental sources	Due diligence obligations fall primarily on exporters, but authorities provide extensive and detailed guidance on what is expected, including brochures, checklists, and practical instructions on ICPs	Monthly overviews published by the Ministry of Foreign Affairs list permits by category, value, end use, and destination, though exporters and end users are not disclosed

Transparency

COUNTRY	TRANSPARENCY
France	Annual reports to Parliament providing aggregate statistics on licences and destinations.
Germany	No dedicated reporting exists for dual-use exports.
Italy	No dedicated reporting exists for dual-use exports.
The Netherlands	Monthly overviews published by the Ministry of Foreign Affairs list permits by category, value, end use, and destination, though exporters and end users are not disclosed.

One of the main challenges to ensuring effective oversight of spyware exports lies in the **persistent lack of transparency surrounding this trade** (Kanetake, 2020). Governments rarely publish information on whether export licences for spyware have been granted, to which destinations, or under what conditions. Vendors likewise decline to disclose their customer base, and transactions are often routed through intermediaries or proxies, making it difficult to trace the ultimate end-users. Freedom of information requests by journalists and civil society almost invariably yield little or no substantive data. Ultimately, the global trade in spyware and related cyber-surveillance tools remains largely hidden from public scrutiny, with significant implications for accountability and human rights oversight.

Interviewees noted that a distinctive feature of this market is the unusually close relationship between regulators and vendors, with the same governments that are responsible for exercising export control often also acting as clients of the same spyware companies. This creates structural conflicts of interest and reinforces the culture of secrecy. As Anstis, Leonard, and Penney (2023) note, governments and companies alike cultivate "opportunistic secrecy", invoking vague and contingent national security or commercial justifications to withhold information, while continuing to benefit from the opacity they sustain. Former UN Special Rapporteur David Kaye likewise observed that the surveillance market, from licensing to after-sales support, "is shrouded in secrecy," with most public knowledge coming from investigative reporting and whistleblowers rather than from official sources (Kaye, 2019).

Transparency has therefore become a central demand of reform initiatives. Amnesty International has called for disclosure of corporate structures, decision-making policies, and export records as a prerequisite for accountability (Amnesty International et al., 2021). The European Parliament's PEGA Committee recommended amending the Dual-Use Regulation to oblige Member States to publish specific details on licence approvals and denials, without relying on broad exceptions that allow withholding information (European Parliament, 2023).

Transparency is not an end in itself but the foundation for accountability and a prerequisite for ensuring that the Regulation fulfils its objective of preventing exports that could

contribute to human rights violations. Enhanced disclosure also benefits governments, by enabling a clearer understanding of the scope, scale, and destinations of surveillance exports and thereby strengthening oversight capacities. Information already collected by states during the licensing process has significant potential in this regard. If made public, such data could allow civil society, journalists, parliamentarians, and oversight bodies to monitor implementation and assess whether export controls are applied consistently and responsibly.

Our research reveals **uneven implementation of transparency measures across Member States.** While France established a reporting mechanism, the information released is highly aggregated and provides little insight into how sensitive criteria, such as human rights safeguards, are assessed. Italy and Germany publish no systematic information on dual-use exports, with transparency limited to confidential EU-level exchanges. By contrast, the Netherlands provides monthly reports specifying goods, values, destinations, and end uses, though exporters are not named and denials are not published.

These divergent practices underscore the absence of harmonised transparency standards and highlight areas where existing good practices could be expanded. Across all four Member States examined, however, public reporting does not extend to explaining how human rights assessments are integrated into licensing processes, nor to publishing detailed justifications for licence denials. Interviews suggest that authorities typically rely on a combination of intelligence assessments and open-source information when evaluating human rights risks. **Yet the precise scope of these assessments, and the relative weighting of different factors, are not publicly disclosed, reflecting both confidentiality concerns and the sensitivity of the information involved.** The cumulative picture is one of uneven and fragmented transparency, which constrains accountability and complicates efforts to develop a coherent EU-wide approach.

Interviews also highlighted challenges in information-sharing among authorities. The Dual Use Regulation requires Member States to notify the European Commission and their counterparts when they refuse a licence and must consult each other if a similar application arises. While this denial-notification mechanism plays an important role in preventing problematic exports, interviewees noted that the reasons underpinning denials are typically not disclosed. References such as "human rights concerns" may appear, but without elaboration, and detailed explanations are usually confined to bilateral exchanges upon request. Officials explained that this limited disclosure reflects the fact that assessments often rely on sensitive intelligence or diplomatic reporting, which constrains the scope of information that can be shared openly. **Confidentiality is even greater for decisions about cyber-surveillance items under the catch-all of Article 5 of the Dual-Use Regulation.** In practice, according to interviewees, Article 5 has been rarely applied, and where it has, sensitivity around such items has limited both intra-EU sharing and public disclosure. **Several authorities nonetheless acknowledged that an EU-wide mechanism for structured information exchange on spyware and related technologies would be valuable.**

At the EU level, the recast of the Dual-Use Regulation sought to strengthen transparency, particularly with respect to cyber-surveillance items. The Commission, in consultation with the Dual-Use Coordination Group, is to publish an annual report containing information on export applications, issuing Member States, destinations, and decisions. In practice, however, these provisions have only been partially implemented.

The Commission's first annual report, published in January 2025, covered only data from 2022. This two-year delay limits the relevance of the information for real-time oversight, making it difficult to assess current export practices or the evolving scope of the trade. The report recorded 288 applications for the export of cyber-surveillance items, primarily telecommunications interception systems (216 applications), followed by communication monitoring software (28) and intrusion software (20). Yet the figures were presented solely in aggregate form, with data shared by 14 Member States. As a result, the report offers only a partial and retrospective picture of the trade, reducing its utility for accountability or policymaking.

APPLICATIONS FOR THE EXPORT OF CYBER-SURVEILLANCE ITEMS BY TYPE

Type of item		Volume
CS1	Intrusion software	20
CS2	Telecommunication interception systems	216
CS3	Internet surveillance systems	16
CS4	Communication monitoring software	28
CS5	Forensic tool/investigative	1
CS6	Other listed items that can be used as cyber-surveillance items	7

The Commission's January 2024 guidelines on data gathering further illustrate this cautious approach. The guidelines specify that where information concerns only one or two Member States, publication will occur only with their explicit consent, in order to protect commercial, defence, or security interests. This restriction interacts with Article 26(3) of the Dual-Use Regulation, which allows Member States to withhold information altogether on the same grounds. **In combination, these provisions significantly constrain the scope of public reporting, reducing the transparency gains that the recast Regulation was intended to deliver and limiting the framework's effectiveness as a tool for external oversight.**

The implications of these transparency gaps are significant. It remains difficult to evaluate how human rights risk assessments are conducted, whether licensing practice is consistent across Member States, or the extent to which decisions reflect the Regulation's safeguards. For industry, the absence of accessible information creates uncertainty. Several exporters stressed that greater clarity, for example, through publication of reasons for licence refusals, would help guide future applications and strengthen corporate due diligence. Civil society organisations have similarly called

for the publication of reasons for both licence approvals and denials, as this would shed light on how assessments are conducted and thereby strengthen oversight and accountability. Authorities acknowledged this demand, but emphasised that refusals are typically based on sensitive case-specific information, which constrains disclosure.

Interviewees repeatedly observed that it is often easier to find information on arms exports than on dual-use goods. This imbalance is striking given the scale of risks associated with spyware and surveillance technologies, which are frequently destined for law-enforcement and intelligence services abroad. Without greater transparency, accountability is weakened and public trust in the export control system risks being undermined.

Human rights assessments

COUNTRY	HUMAN RIGHTS ASSESSMENT
France	Human rights assessments are carried out on a case-by-case basis
Germany	Human rights assessments on a case-by-case basis; decisions must rest on a concrete factual basis rather than general concerns about a country's record
Italy	Human rights assessments on a case-by-case basis, rely on systematic consultations with embassies, intelligence services, and interministerial review
The Netherlands	Human rights assessments for sensitive cases are reviewed at ministerial level, with authorities relying extensively on open-source materials and civil society reporting; intelligence inputs are used to a more limited extent, so cyber-surveillance cases are primarily informed by non-governmental sources

Transparency is closely linked to how human rights assessments are conducted. **Across the four Member States examined, human rights assessments remain only partially transparent.** Interviewees explained that licensing authorities generally rely on a combination of intelligence services, embassy reporting, and Ministry of Foreign Affairs advice when assessing potential misuse of surveillance exports. However, specialised human rights expertise is not embedded in licensing authorities, which likely affects both the consistency and the perceived credibility of these assessments. In some cases, interviewees noted that authorities limit access to this information on the grounds of confidentiality or national security, making it difficult for external stakeholders to understand how human rights considerations are weighed. A notable exception is the Netherlands, where, according to interviews, authorities reportedly draw more systematically on civil society reporting and open-source information when assessing risks linked to spyware and cyber-surveillance items (Minister of Foreign Affairs & Minister for Foreign Trade and Development Cooperation, 2021).

The opacity of human rights assessments raises significant concerns. In the absence of clear procedures or published criteria, it is not evident how risks are identified, what weight is assigned to different sources, or whether human rights concerns are applied consistently across Member States. Overreliance on intelligence and diplomatic reporting may help to identify risks that are not visible to the public, but it also sidelines input from civil society organisations, journalists, and academic researchers who often provide detailed evidence of patterns of abuse. Without integrating such external sources, assessments can remain narrow, reactive, or overly shaped by political and security considerations rather than by a comprehensive evaluation of human rights risks.

Due diligence

COUNTRY	DUE DILIGENCE
France	Due diligence obligations fall primarily on exporters, with authorities conducting outreach through annual forums and general guidance
Germany	Due diligence obligations fall primarily on exporters, with BAFA providing supplementary guidance through leaflets, explanatory materials, and outreach events
Italy	Due diligence relies heavily on exporters' internal checks, alongside regular exchanges and close engagement between UAMA and key companies
The Netherlands	Due diligence obligations fall primarily on exporters, but authorities provide extensive and detailed guidance on what is expected, including brochures, checklists, and practical instructions on ICPs

Transparency has furthermore direct implications for the due diligence obligations placed on exporting companies. Under the Dual-Use Regulation, due diligence is framed primarily as a risk-screening obligation (Stalenhoef, Kanetake, & van der Wende, 2022). Companies are required to identify actual and potential "adverse impacts" linked to the end-use of their exports and to take steps to mitigate them (Stalenhoef, Kanetake, & van der Wende, 2022). The Dual-Use Regulation requires exporters of cyber-surveillance items to carry out risk assessments as part of an ICP. Although narrower than the comprehensive concept of human rights due diligence under international soft law standards, this provision is significant because it imposes a legal duty on private actors to assess risks under both international human rights law and international humanitarian law (Kanetake, 2024).

The European Commission's 2024 guidelines aimed to clarify these requirements. However, according to companies interviewed for this study, the guidance remains insufficiently detailed and leaves gaps in practical implementation. Exporters reported difficulties in navigating the Regulation and stressed the need for more practical tools, such as checklists, red-flag indicators, and case examples that could be directly applied in compliance processes. They

also expressed frustration at the limited feedback they receive from regulators. In particular, industry representatives underlined that access to the reasoning behind licence denials would help them refine their due diligence practices, but such explanations are rarely provided in practice. The absence of feedback leaves exporters without clear reference points and limits the preventive effect that licensing decisions could otherwise have.

The research further found significant divergences in how Member States issue guidance materials and communicate with exporters. In some jurisdictions, step-by-step instructions, FAQs, and reference materials are easily retrievable on national authority websites, while in others such information is fragmented, limited, or absent altogether. For instance, the Netherlands provides accessible guidance online, including FAQs available also in English, whereas in France and Italy such materials are more limited. These discrepancies affect not only the ability of companies to comply consistently with the Regulation, but also the broader transparency and accountability of the licensing system.

These challenges are compounded by the absence of sector-specific guidance. While overarching instruments such as the UN Guiding Principles on Business and Human Rights (UNGPs) and the OECD Guidelines for Multinational Enterprises outline general expectations, they do not provide detailed benchmarks tailored to the risks posed by dual-use exports (Kanetake & Ryngaert, 2023). This leaves exporters uncertain about what constitutes best practice, whether newly developed corporate policies are adequate, and how far they must go in identifying and mitigating risks (Kanetake & Ryngaert, 2023). The resulting lack of clarity undermines both corporate compliance and the capacity of regulators to hold exporters accountable. This is particularly problematic for spyware and cyber-surveillance items, where technically complex products, sensitive law-enforcement and intelligence end-users, and heightened risks of human rights abuse demand clearer and more specific guidance.

From the perspective of regulators, licensing decisions often rely on sensitive, case-specific intelligence, which limits the scope of information that can be disclosed to exporters. Public communication is generally restricted to broad references to human rights concerns, and detailed explanations are typically shared only bilaterally among Member States and only upon request. This inevitably restricts the ability of companies to learn from past cases.

At the same time, state licensing decisions do not replace corporate due diligence. Governments may hold privileged intelligence or diplomatic information, but exporters often have unique insights into their products, clients, and end-use environments. Effective risk identification and mitigation should therefore be seen as a shared responsibility, in which companies and regulators complement each other's strengths. Under the UN Guiding Principles on Business and Human Rights, this means that while companies are expected to conduct due diligence, states also have a duty to ensure that licensing regimes themselves include meaningful human rights review (Rosen Zvi, 2023). Where such safeguards are lacking, states risk falling short of their obligations under the UNGPs.

ICPs can serve as a platform for dialogue between authorities and companies. When used proactively, ICP-based exchanges can encourage the development of additional safeguards, such as contractual conditions, enhanced end-use verification, or the integration of human rights standards into supply-chain management (Kanetake & Ryngaert, 2023). Yet, as this research shows, the use of ICPs varies significantly across Member States, and the level of human rights expertise within national authorities also differs. This uneven implementation means that companies receive highly variable support depending on their jurisdiction, reinforcing the case for more harmonised and practical, sector-specific guidance at the EU level.

Monitoring the end-use of exported spyware

There remains the crucial question of who bears responsibility for monitoring the actual end-use of the exported item, and to what extent are exporters or authorities under an obligation to verify that exports remain compliant and are not subsequently used in ways that give rise to violations of international human rights law or international humanitarian law. **Across the four Member States examined, there is little publicly available information and limited clarity regarding how the end-use of exported items is monitored once a licence has been granted.** Public sources do not clearly indicate whether, and in what manner, authorities conduct follow-up to verify compliance with declared end-uses. At the same time, industry representatives interviewed emphasised that they too have little visibility over how end-use monitoring operates in practice, noting that once an export has taken place, exporters generally retain limited insight into the final deployment of the product.

In practice, only limited ex post corrective measures appear to exist in this domain:

- According to interviews, **in Germany** there is generally no statutory obligation for authorities or exporters to monitor how an item is being used over a certain period of time once it has been exported. However, if an exporter becomes aware of credible information suggesting that the end-user has misused the item, the exporter is required to inform the competent authority, which may then take this information into account when reviewing any future licence applications. However, concerns remain as to whether such information is consistently acted upon. According to a report from Amnesty International, in the case of an export of interception technology from Germany to Pakistan, despite the disclosure of evidence regarding its misuse, the German authorities are reported not to have reviewed the export licence (Amnesty International, 2025). **Authorities in more than one Member State under analysis**

noted that while systematic post-export monitoring is absent, this is partially mitigated by the fact that the high-technology nature of the products such as spyware and cyber-surveillance items often necessitates regular updating and maintenance. As a result, long-standing business relationships between exporting companies and foreign customers are common, and these ongoing contacts may serve as an informal means of observing how the technology is being used.

- Similarly, according to interview information, **in the Netherlands**, exporters are bound by the broader principle of responsible business conduct, and require companies to take steps to ensure that their products are not misused. Reporting obligations also exist: when a licence has been approved, exporters may be required to report every three to six years on their specific exports. Moreover, Dutch Customs has the power to request, at any time, access to a company's internal administration concerning a licensed export. If evidence of a violation emerges, cases are referred to customs enforcement and may ultimately involve public prosecutors.

- **In Italy**, interviews indicate that once the authorisation process has been completed, there is generally no systematic follow-up by authorities unless specific monitoring obligations have been expressly included as a condition of the licence. In certain cases, particularly where concerns exist about the human rights record of the recipient country, such conditional obligations have indeed been imposed. These may require exporters to actively monitor for potential misuse of the technology, and in some instances exporters can rely on the technical features of the product itself. For example, software-based items require regular updates in order to remain fully functional, and this technical dependence often means that exporters and end-users remain in regular contact. Such ongoing relationships provide an occasion for exporters to observe how the technology is being used in practice, thereby creating a channel, albeit indirect, for monitoring final end-use. The legal basis for imposing such conditions is found in Article 10(7) of Legislative Decree No. 221/2017, which allows authorities to require additional obligations as part of the authorisation itself. These can include the production of formal declarations of receipt by the end-user, mandatory periodic inspections at the place of final destination to confirm that the items are being used consistently with their declared purpose, and the submission of written or photographic reporting to the competent authority.

Beyond the role of authorities and exporters themselves, questions also arise as to whether external actors can play a role in ensuring accountability for the end-use of exported technologies. An illustrative case is that of Italy, where in 2017 civil society organisations intervened by submitting a joint letter to the Ministry for Economic Development, leading to the revocation of an already granted licence for the export of surveillance items to Egypt (Coalizione Italiana Libertà e Diritti civili, 2017; Access Now 2017). The case is notable because, across the Member States analysed, the possibility of appealing licensing decisions is generally confined to exporting companies on narrow administrative grounds, leaving third parties such as civil society and journalists without formal standing to challenge such authorisations.

Viewed collectively, these findings underscore a broader challenge: while spyware and other surveillance tools are high-technology products that often require constant maintenance, which could enable closer oversight, there are few formal mechanisms in place across Member States to ensure systematic monitoring of their end-use. As several interviewees observed, for many dual-use items it is difficult for exporters to predict how the product will ultimately be used once it has arrived at its destination. Yet in the case of technologies such as spyware, which are almost always exported to law enforcement or intelligence agencies, or to actors closely connected to them, this argument is less persuasive. Precisely because of the high risks associated with such exports, higher standards of due diligence, ongoing monitoring obligations, and stronger transparency requirements should apply.

Implementation gaps and risks of divergences

Although the choice of a regulation rather than a directive was intended to bring uniformity, implementation in practice remains firmly embedded within national prioritisation as each Member State retains discretion over how licensing authorities are structured, how procedures are administered, and what resources are devoted to export controls (Kanetake, 2019). There is significant variation in administrative culture, legal frameworks, and government-industry relations, which weaken uniformity of a regulation and risk undermining the coherence of the EU's export control regime, producing uneven levels of scrutiny across the Union and, in turn, exposing gaps that can be exploited by spyware vendors seeking jurisdictions with more permissive oversight.

The risks of uneven implementation have already been highlighted by the European Parliament's PEGA Committee, which in the context of the internal market loophole detailed above has resulted in the industry becoming firmly established in the EU and benefitting from gaps in enforcement (PEGA Committee, 2022). The Committee stressed that such inconsistencies create opportunities for "forum shopping", whereby exporters denied a licence in one jurisdiction can reroute the same transaction through another with lighter oversight. Similarly in the context of intra-group transfers, the Dual-Use Regulation provides little clarity on how re-exports by non-EU subsidiaries should be treated, resulting in uneven national practices and opportunities for oversight to be bypassed (IrpiMedia, 2023). At the same time, threat analysis reports by Google (2024) and Meta (2024) have since confirmed a growing concentration of spyware vendors within the Union, underlining Europe's role as an increasingly attractive base of operations for such companies.

Persistent transparency gaps make it difficult to fully assess the scope of the problem. Nevertheless, a recent mapping has identified 188 companies in 31 states producing spyware and other cyber-surveillance tools, 65 per cent of which are concentrated in just seven countries, including Germany and Italy (Bromley & Maletta, 2025). Spyware producers are even more concentrated, with over half located in only three states, India, Israel and Italy. Beyond these figures, however, disaggregated data on exporting companies, exports volume, nature, value, and destination of the intended export is largely absent, limiting both public scrutiny and regulators' ability to build a comprehensive picture of the market. Interviews conducted for this study confirmed that even authorities themselves often lack visibility into which companies are established in Europe, what technologies they are offering, and to whom. Vendors frequently operate through intermediaries or complex corporate structures, further obscuring oversight. Industry representatives likewise highlighted the unevenness of national procedures. In certain Member States, exporters are required to comply with more extensive processes, whereas in others licensing processes are viewed as more streamlined and pragmatic.

Capacity constraints compound these problems. Expertise in highly technical fields such as spyware and intrusion software is not equally distributed across the Union. Interviews highlighted that Germany, for instance, was repeatedly identified as having comparatively stronger technical expertise and resources. By contrast, other Member States, such as Italy, were described as having more limited capacity to engage with complex cyber-surveillance licensing, despite Italy's recognised role as a key hub for spyware vendors and cybersecurity companies in the EU (The Record, 2024). Several authorities underlined that since Russia's invasion of Ukraine in 2022 and the resulting expansion of EU sanctions, export control units have faced surging workloads. Even administrations with relatively higher staffing have been overstretched, limiting their ability to conduct in-depth human rights assessments or technical evaluations.

In brief, consistent implementation of the Dual-Use Regulation represents a fundamental human rights concern. Divergent practices across Member States weaken the Regulation's preventive purpose and leave open channels through which spyware and surveillance technologies can reach high-risk destinations, where these tools risk being used to monitor journalists, intimidate civil society, and suppress democratic participation. Weak or uneven application also risks eroding public trust in the EU's export control regime, undermining the Union's credibility when it presents human rights as the cornerstone of its external action. To close these gaps, the EU must ensure that the Regulation is applied uniformly, effectively, and transparently across all Member States. Only then can export controls function as a credible safeguard against the misuse of surveillance technologies and demonstrate the EU's commitment to protecting fundamental rights in practice.

05

Conclusion and policy recommendations

This report has shown that while the Dual-Use Regulation provides a directly applicable framework for controlling the export of spyware and cyber-surveillance technologies, its current design and implementation reveal a number of shortcomings and areas where improvement is needed. Licensing processes reflect the administrative, legal, and political frameworks of each Member State which results in fragmented implementation across the EU. Assessments of transactions involving spyware and cyber-surveillance tools remain difficult to scrutinise and transparency in the licensing of spyware remains limited and uneven across Member States. Exporters continue to experience uncertainty regarding the scope of their obligations, while licensing authorities face challenges in terms of resources, expertise, and the availability of independent oversight mechanisms necessary for effective control. Addressing these challenges is essential to safeguarding accountability and to reducing the risk that spyware technologies may be misused in ways that threaten both fundamental rights and national security.

Export controls alone cannot provide a comprehensive solution. They intervene at a specific stage of the spyware lifecycle, and cannot, in isolation, address the broader risks linked to the development, marketing, and deployment of these technologies. A holistic response therefore requires the use of complementary legal and policy instruments, including privacy law, internal market regulation, cybersecurity frameworks, criminal procedure, and sanctions. At the same time, export controls, and in particular the EU Dual-Use Regulation, remain one of the few binding instruments in the EU that provides a legal basis to ensure that exported technologies are not used in ways that violate international law or fundamental rights.

Strengthening export controls, and adapting the EU framework to capture the specific challenges posed by spyware, is therefore essential to reduce opportunities for abuse, reinforce accountability, and enhance democratic oversight. It will be crucial to clarify how export controls apply to emerging models such as spyware- or surveillance-as-

a-service, and to engage systematically with exporters to ensure that due diligence obligations are properly understood, implemented, and enforced, so that controls are not circumvented. Importantly, a review of both the Regulation as a whole (between 2026 and 2028) and Article 5 specifically (after 2024) is already foreseen. In its 2024 White Paper, however, the Commission recommended that the evaluation be brought forward to 2025, explicitly acknowledging shortcomings in the Regulation's effectiveness and efficiency, and the urgency of addressing these challenges. This accelerated timeline provides a crucial opportunity to remedy the shortcomings identified and to strengthen the framework. The recommendations that follow identify concrete measures to reinforce the export control system under the Dual-Use Regulation. While they will not eliminate the risks inherent in the proliferation of spyware, they would establish a more coherent and accountable framework for regulating its trade and bring EU practice closer to the standards of transparency, restraint, and human rights protection that these technologies urgently demand.

1. Closing the regulatory gap on intra-EU trade of spyware

The absence of intra-EU controls on the trade of commercial spyware leaves a significant regulatory gap that companies can exploit to bypass external trade controls.

To close this gap, **the EU should establish a regulatory framework governing the internal movement of spyware and related cyber-surveillance tools.** This could be achieved, for instance, by including these technologies in Annex IV of the Dual-Use Regulation, thereby subjecting intra-EU transfers to licensing requirements. Alternatively, new legislative measures under the internal market legal basis could be considered. For instance, the Cyber Resilience Act, adopted on the basis of Article 114 TFEU, shows how this legal basis can be used to introduce harmonised rules for digital products across the Union, including mechanisms for oversight and enforcement. A similar approach could be considered to ensure that spyware and related surveillance tools do not circulate freely within the internal market without effective safeguards.

2. Enhancing transparency in export licences

Although the 2021 recast of the Dual-Use Regulation sought to strengthen transparency, practice shows that significant shortcomings remain as Member States' divergencies in reporting illustrate persistent disparities in both the quality and quantity of the information provided. This unevenness, combined with the limited granularity of the data published, undermines public scrutiny and restricts the ability of civil society, researchers, and policymakers to assess whether export controls are being applied effectively to prevent

misuse of spyware and related technologies. The absence of common guidelines on how to evaluate export applications further contributes to opacity, allowing divergent national practices to persist without meaningful oversight.

To address these gaps, the Commission and Member States should establish clear and harmonised transparency standards for the licensing of spyware and other dual-use cyber-surveillance items. National authorities should be required to publish detailed and disaggregated reports on applications and licensing decisions, including the nature of the technology, the number and value of licences sought, the identity of exporters and end-users, and the grounds for approval or denial. Reports should be made public on a regular and timely basis, at intervals that allow for meaningful oversight. They should contain information that is both sufficiently detailed and up to date, so that policymakers, civil society, and researchers are able to assess whether export controls are being implemented effectively. Data that is excessively aggregated, incomplete, or outdated does little to enhance accountability and risks reinforcing the opacity it is intended to counter.

In parallel, exceptions allowing Member States to withhold information on grounds of commercial sensitivity, defence, or foreign policy must be narrowly defined and strictly circumscribed. Where disclosure could create risks, information should be classified by the Commission rather than withheld entirely. Finally, parliamentary oversight should be reinforced through the creation of a dedicated standing committee with access to classified information, ensuring that licensing decisions are subject to independent and democratic scrutiny, as already recommended by the European Parliament in 2023.

3. Strengthening due diligence obligations for exporters

Export controls on spyware and surveillance technologies, carrying heightened risks of facilitating serious human rights violations, are currently heavily dependent on the due diligence undertaken by exporters and the robustness of their ICPs. At present, however, even where companies have adopted human rights due diligence or transparency policies, their substantive content is difficult to evaluate in the absence of reporting requirements. This results in information asymmetry, limiting the capacity of licensing authorities to exercise effective oversight and to prevent exports that may give rise to rights-abusive practices. **The framework should therefore be strengthened to require exporters to conduct, document, and disclose comprehensive human rights risk assessments covering the design, marketing, and transfer of their technologies, in line with the UN Guiding Principles on Business and Human Rights and OECD Due Diligence Guidance. These obligations should not be limited to the pre-licensing stage. Ex post monitoring requirements should also be foreseen, ensuring that exporters continue to identify, prevent, and mitigate risks once a licence has been granted and throughout the lifecycle of the technology.**

Furthermore, research conducted for this report shows that exporters face persistent uncertainty in applying the Dual-Use Regulation. Companies reported difficulties in determining whether their products or components fall within the scope of the Regulation, and in understanding what is expected of them when it comes to due diligence. This lack of clarity has a negative impact on compliance, particularly in carrying out human rights risk assessments, and results in uneven practices across Member States. Exporters would hence benefit from more concrete tools such as practical case studies, illustrative scenarios, and step-by-step approaches that help them operationalise their obligations in day-to-day business practice.

Governments also have a crucial role to play in supporting companies in this process. Exporters often know their products' technical capabilities and have direct access to their clients' operations, but they lack the diplomatic and security information needed to fully assess end-user risks. Risk identification and mitigation should therefore be seen as a shared responsibility, with governments and exporters each contributing their respective knowledge. Structured channels of dialogue, as highlighted by both industry and licensing authorities interviewed for this report, would facilitate the exchange of risk-related information, provide greater clarity, and support compliance with the export control legal framework. At the same time, the credible possibility of corporate liability should serve as a strong incentive for exporters to take human rights due diligence seriously and for governments to ensure that exporters receive effective guidance and oversight.

4. Strengthening the monitoring of end-use

At present, once an export licence is granted, there are generally no systematic follow-up obligations imposed on exporters, unless specific conditions are expressly included by the competent authority as part of the authorisation. This has resulted in significant divergences among Member States. In some jurisdictions, authorities have occasionally attached conditions requiring exporters to monitor signals of potential misuse, particularly where the destination raised concerns regarding possible human rights violations, even if not formally profiled as high-risk. In other Member States, no such practice exists, and exporters face no obligations once a licence is issued. As a result, end-use monitoring remains ad hoc, fragmented, and without a clear legal basis, leaving oversight inconsistent across the Union and undermining the effectiveness of the existing framework.

To ensure that export controls are effective in preventing human rights abuses, the EU should develop binding and harmonised requirements for the monitoring of end-use. Exporters should be obliged to put in place mechanisms capable of detecting signs of misuse, including contractual arrangements that allow for the suspension of services or support where violations are identified. Given the specificities of spyware, technical features such as the need for regular software updates can serve as a practical means for exporters to verify compliance: if updates are withheld due to contractual

breach, the technology ceases to function. Embedding such monitoring requirements into export control law would provide licensing authorities with enforceable tools, rather than discretionary conditions, and would help ensure that exported technologies are not diverted towards unlawful or rights-abusive purposes.

5. Building capacity for effective export control implementation

Divergences in resources and technical expertise among Member States have a direct impact on the effectiveness of export control implementation in the spyware and cyber-surveillance sector. Interviews conducted for this report highlighted that several authorities struggle to keep pace with rapid technological developments and emerging risks, which are often not fully captured by the current regulatory framework. The problem is compounded by the expansion of EU sanctions regimes, which places additional burdens on licensing authorities and disproportionately affects those with limited institutional capacity. At the same time, the EU has become an increasingly attractive base for cybersecurity and surveillance vendors, a trend that requires a parallel strengthening of knowledge and staff resources within national administrations. The absence of specialised expertise on both technical and human rights dimensions undermines the Union's ability to apply export controls in a manner that is consistent, effective, and aligned with its normative commitments.

To address these gaps, the EU should provide sustained support to national licensing authorities through targeted capacity-building initiatives. This should include common training programmes on the export control of spyware and other cyber-surveillance technologies, addressing both technical aspects of the products and their human rights implications. National authorities should be equipped with dedicated staff who possess expertise in evaluating due diligence obligations as well as in assessing the specific human rights risks associated with surveillance technologies. Capacity-building of this kind is indispensable to ensure that the normative shift of export controls, from a focus solely on military and security concerns to a framework that also addresses human rights risks, is meaningfully implemented in practice across all Member States.

6. Strengthening external oversight of licensing decisions

The current framework of the Dual-Use Regulation does not provide adequate guarantees of independent oversight in export licensing decisions concerning spyware and cyber-surveillance technologies. The lack of transparency in human rights assessments makes it difficult to evaluate whether licensing decisions are impartial, particularly given the structural conflicts of interest that arise when national authorities tasked with granting export licences are also themselves customers of the same surveillance vendors. In

practice, assessments often rely heavily on information provided by diplomatic or security services, which, while subject to parliamentary scrutiny in other contexts, are not open to external evaluation when used in the licensing process. This reliance further limits the possibility of independent review.

To address these shortcomings, **the Dual-Use Regulation should be amended to foresee explicit mechanisms of external oversight.** Licensing authorities should be required to report regularly to parliaments on their decisions, enabling democratic scrutiny of both the process and its outcomes. In addition, the Regulation should mandate the systematic inclusion of independent human rights expertise in the assessment of licence applications, ensuring that decisions are informed by rigorous rights-based analysis and not exclusively by security or diplomatic considerations. Embedding such external oversight within the Regulation would strengthen transparency, accountability and mitigate conflicts of interest.

7. Improving information-sharing between Member States

One of the main obstacles to effective oversight of spyware exports is the limited exchange of information among Member States on licensing decisions. Interviews with national authorities confirmed that mapping the trade in spyware and related cyber-surveillance tools is a major challenge, particularly in a sector characterised by secrecy and by a large number of small and less visible actors. While some major vendors are well known, many others remain outside the reach of consistent scrutiny, and the lack of systematic information-sharing enables companies to exploit differences in national practice or to seek licences in jurisdictions perceived as less restrictive.

To address this gap, **the Dual-Use Regulation should be strengthened to promote the use of existing coordination mechanisms, including the Dual-Use Coordination Group and the Surveillance Technology Expert Group, as well as electronic communication platforms, as channels for Member States to exchange information on approvals and denials of export licences.** Greater transparency on the application of catch-all controls would also allow Member States to identify emerging technologies and practices that fall outside Annex I but nevertheless present significant human rights risks. In addition, the systematic use of bilateral and multilateral channels to share information on licensing outcomes would contribute to more uniform controls across the Union and help to detect companies seeking to evade or circumvent regulatory coverage

8. Harmonising end-user documentation and licensing procedures

Greater consistency in licensing procedures, particularly with respect to the end-user statements, would improve the implementation of the Dual-Use Regulation. At present, procedural divergences across Member States risk being exploited through forum shopping, allowing companies to seek authorisations in jurisdictions where requirements are applied less rigorously. Such loopholes undermine the effectiveness of export controls and weaken the implementation of the Dual-Use Regulation.

To address this gap, **the EU should facilitate the harmonisation of end-user documentation and the streamlining of licensing procedures for spyware and other cyber-surveillance technologies.** Establishing a common template for end-user statements and aligning procedural requirements across Member States would promote consistency, reduce opportunities for jurisdiction shopping, and enhance legal certainty for exporters. In parallel, national transparency and reporting mechanisms should also be streamlined and standardised to ensure that the information available across Member States is comparable, accessible, and meaningful.

9. Strengthening international coordination on spyware controls

Given the global nature of the trade on spyware, international coordination in technical standards and regulatory approaches is indispensable. National measures alone are insufficient to address the transnational supply chains, vendors, and markets that characterise the spyware industry. At present, however, progress within multilateral export control regimes has become increasingly difficult. Interviews conducted for this report underscored that geopolitical tensions, exacerbated since the Russian invasion of Ukraine in 2022, have made consensus within forums such as the Wassenaar Arrangement more elusive. This lack of alignment limits the ability of participating states to develop common controls for spyware and related cyber-surveillance technologies, leaving significant regulatory gaps at the international level.

To mitigate these shortcomings, **the EU should take the lead in further developing Member States' as well as international coordination.** By driving efforts to establish spyware-specific commitments, promote the development of common technical standards, and embed human rights criteria in export licensing practices, the EU can set a benchmark for like-minded states.

References

Access Now. (2017, July 3). *Italy revokes export license to Egypt after civil society pressure*. https://www.accessnow.org/press-release/italy-revoke-export-license-cyber-surveillance-company

Amnesty International. (2021, March 25). *New EU dual-use regulation agreement a missed opportunity to stop exports of surveillance tools to repressive regimes*. https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes

Amnesty International. (2025, August 29). *A web of surveillance: Unravelling Pakistan's digital censorship and spyware industry (ASA33/0206/2025)*. Amnesty International. https://www.amnesty.org/en/documents/asa33/0206/2025/en

Anstis, S., Leonard, N., & Penney, J. W. (2023). Moving from secrecy to transparency in the offensive cyber capabilities sector: The case of dual-use technologies exports. *Computer Law & Security Review, 48*, 105787. https://doi.org/10.1016/j.clsr.2022.105787

Anthony, I., Bauer, S., & Wetter, A. (2007). *Controls on security-related international transfers. In SIPRI Yearbook 2007: Armaments, disarmament and international security*. Oxford University Press.

Arms Control Association. (2022, February). *The Wassenaar Arrangement at a glance*. https://www.armscontrol.org/factsheets/wassenaar

Asher-Schapiro, A. (2018, October 2). Spyware hijacks smartphones, threatens journalists around the world. *Columbia Journalism Review.* https://www.cjr.org/watchdog/pegasus-israeli-spyware.php

Assonime. (2021). *Dogane e commercio internazionale: Il contributo di Assonime alle consultazioni promosse dalla DG Trade in tema di programmi interni di conformità (ICP)* (Note e studi n. 6/2021). Assonime. https://www.assonime.it/attivita-editoriale/note-e-studi/2021/note-e-studi-62021

Benson, E., & Mouradian, C. (2023, November 29). *Export controls and human rights: An emerging technology agenda*. Center for Strategic and International Studies. https://www.csis.org/analysis/export-controls-and-human-rights-emerging-technology-agenda

Brockmann, K., & Héau, L. (2025, February 17). *Spyware-as-a-service: Challenges in applying export controls to cloud-based cyber-surveillance software*. Stockholm International Peace Research Institute. https://www.sipri.org/commentary/topical-backgrounder/2025/spyware-service-challenges-applying-export-controls-cloud-based-cyber-surveillance-software

Bromley, M. (2017). *Export controls, human security and cyber-surveillance technology: Examining the proposed changes to the EU dual-use regulation*. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2018-01/sipri1712_bromley.pdf

Bromley, M., Maltais, A., & Wezeman, S. T. (2016). ICT surveillance systems: Trade policy and the application of human security concerns. *Strategic Trade Review, 2*(3), 37–59.

Bromley, M., & Maletta, G. (2025, September). *Export controls and spyware: Enhancing oversight, transparency and restraint*. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2025-09/0925_export_controls_and_spyware.pdf

Bundesamt für Wirtschaft und Ausfuhrkontrolle. (2024). *Optimierte Antragstellung: Praxishilfe*. BAFA.

Centre for Democracy and Technology Europe. (2025, June 20). *Response to the European Commission public consultation on the European Democracy Shield* [PDF]. Centre for Democracy and Technology. https://cdt.org/wp-content/uploads/2025/06/CDT-Europe_-Response-to-the-European-Commission-Public-Consultation-on-the-European-Democracy-Shield.pdf

Coalizione Italiana Libertà e Diritti Civili. (2017, June 30). *Vittoria: Il MISE revoca la licenza ad Area verso l'Egitto*. CILD. https://cild.eu/blog/2017/06/30/vittoria-il-mise-revoca-licenza-ad-area-verso-legitto

Council of the European Union. (2009). *Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. Official Journal of the European Union*, L 134, 1–269. https://eur-lex.europa.eu/eli/reg/2009/428/oj/eng

Council of the European Union. (2015, January 20). *Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council preparatory bodies*. Council of the European Union.

DIGITALEUROPE. (2017, February 24). *Proposed recast of the European export control regime: Making the rules fit for the digital world*. https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2019/01/FINAL%20-%20DIGITALEUROPE%20paper%20on%20recast%20regs%20dual%20use%5B1%5D.pdf

European Commission. (2014). *Communication from the Commission to the Council and the European Parliament: The review of export control policy: Ensuring security and competitiveness in a changing world (COM/2014/0244 final)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0244

European Commission. (2024, October 11). *Public consultation: Guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) No 2021/821.* https://policy.trade.ec.europa.eu/news/commission-publishes-guidelines-cyber-surveillance-exporters-2024-10-16_en

European Parliament. (2015, December 17). *European Parliament resolution of 17 December 2015 on the annual report on human rights and democracy in the world 2014 and the European Union policy on the matter (2015/2229(INI))* [Resolution TA-8-2015-0470]. https://www.europarl.europa.eu/doceo/document/TA-8-2015-0470_EN.html

European Parliament. (2023). *Recommendation of the European Parliament to the Council and the Commission (2023/2500(RSP))*.

European Union. (2021). R*egulation (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). Official Journal of the European Union*, L 206, 1–461. https://eur-lex.europa.eu/eli/reg/2021/821/oj

Federal Office for Economic Affairs and Export Control (BAFA). (2021). *Manual: Export control and academia*. https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_manual_export_control_and_academia.pdf

Federal Office for Economic Affairs and Export Control (BAFA). (2021, October). *Leaflet on Article 5 of the EU Dual-Use Regulation (Regulation (EU) 2021/821)*. https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_leaflet_art-5_eu-dual-use-regulation.html

Fidler, M. (2023). Zero progress on zero-days: How the last ten years created the modern spyware market. *Nebraska Law Review, 102*(4), 713–759. https://digitalcommons.unl.edu/nlr/vol102/iss4/2

Google Threat Analysis Group. (2024, February). *Buying spying: Insights into commercial surveillance vendors*.

Herpig, S., & Paulus, A. (2024, March 19). The Pall Mall Process on cyber intrusion capabilities. *Lawfare*. https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities

IrpiMedia. (2023, March 20). Surveillance tech and export licenses: A match made in Europe. *IrpiMedia*. https://irpimedia.irpi.eu/en-eternal-struggle-between-good-and-evilware

Kanetake, M. (2019). The EU's dual-use export control and human rights risks: The case of cyber surveillance technology. *Europe and the World: A Law Review, 3*(1), 1–30.

Kanetake, M. (2019). The EU's export control of cyber surveillance technology: Human rights approaches. *Business and Human Rights Journal, 4*(1), 155–177.

Kanetake, M. (2025). *Governing the global proliferation of digital surveillance technologies: Lessons from the EU*. In J. van Dijck, K. van Es, A. Helmond, & F. van der Vlist (Eds.), *Governing the digital society: Platforms, artificial intelligence, and public values*. Amsterdam University Press.

Kanetake, M., & Ryngaert, C. (2023, May 10). *Due diligence and corporate liability of the defence industry: Arms exports, end use and corporate responsibility*. Flemish Peace Institute. https://vlaamsvredesinstituut.eu/wp-content/uploads/2023/05/VVI-Rapport-Due-Dilligence-WEB-new.pdf

Kaye, D. (2021). The spyware state and the prospects for accountability. *Global Governance, 27*(4), 483–504. https://brill.com/view/journals/gg/27/4/article-p483_1.xml

Kaye, D., & McKune, S. (2023, August 25). The scourge of commercial spyware – and how to stop it. *Lawfare*.. https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it

Marczak, B., & Scott-Railton, J. (2025, June 18). *First forensic confirmation of Paragon's iOS mercenary spyware finds journalists targeted*. The Citizen Lab. https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted

Meta. (2024, February). *Adversarial threat report: Countering the surveillance-for-hire industry & influence operations (Fourth quarter)*.

Mildebrath, H. (2024, November). *Setting spyware standards after the Pegasus scandal (PE 766.262)*. European Parliamentary Research Service.

Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique. (n.d.). *Service des biens à double usage (SBDU)*. Retrieved August 28, 2025, from https://www.entreprises.gouv.fr/service-des-biens-double-usage-sbdu

Ministero degli Affari Esteri e della Cooperazione Internazionale. (2025, August 28). *Avviso pubblico di selezione per 5 esperti di collaborazione UAMA*. https://www.esteri.it/wp-content/uploads/2025/08/Avviso_5esperti_collaboraz_Uama_Firmato.pdf

Ministry of Foreign Affairs. (2013). *User guide on strategic goods and services*. Ministry of Foreign Affairs. https://www.government.nl/documents/directives/2012/04/12/user-guide-on-strategic-goods-and-services

Ministry of Foreign Affairs. (2019). *Internal compliance programme guidelines for compiling an internal compliance programme for strategic goods, torture goods, technology and sanctions*. Ministry of Foreign Affairs.

Ní Aoláin, F., & Edmeades Jones, A. (2024, October 29). Spyware and the Pall Mall Process: Opportunities and risks for regulation. *Just Security*. https://www.justsecurity.org/104363/spyware-pall-mall-opportunities/

OHCHR. (2021, August 12). *Spyware scandal: UN experts call for moratorium on sale of "life-threatening" surveillance tech*. https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening

Open Technology Institute. (2013, December 9). *A guide to the Wassenaar Arrangement*. New America. https://www.newamerica.org/insights/a-guide-to-the-wassenaar-arrangement/

Organisation for Economic Co-operation and Development. (n.d.). *OECD guidelines for multinational enterprises*. Retrieved August 28, 2025, from https://www.oecdguidelines.nl

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), *OJ L 206*, 1. (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821

Riecke, L. (2023). Unmasking the term "dual use" in EU spyware export control. *European Journal of International Law, 34*(3), 697–720. https://doi.org/10.1093/ejil/chad039

Roberts, J., Herr, T., Bansal, N., & Messieh, N. (2024, September 4). *Mythical beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights

Rosen Zvi, R. (2023, January 30). Managing risky business – The international regulatory framework of spyware companies: Where it is lacking and where it is heading. *Georgetown Law: Center on Transnational Business and the Law*. https://www.law.georgetown.edu/ctbl/blog/managing-risky-business-the-international-regulatory-framework-of-spyware-companies-where-it-is-lacking-and-where-it-is-heading

Sevini, F. (2014). *Strengthening strategic export controls by internal compliance programmes* (Joint Research Centre Report). Joint Research Centre. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC92964/sevini%20-%20online.pdf

Sheniak, A. (2023). *Bringing technology back into spyware regulations*. Shasha Center for Strategic Studies. https://en-shashacenter.huji.ac.il/sites/default/files/en-shashacenter/files/amit_shenieak_maamar_01.pdf

Smalley, S. (2024, November 12). How Italy became an unexpected spyware hub. *The Record by Recorded Future*. https://therecord.media/how-italy-became-an-unexpected-spyware-hub

Steering Committee of the Coalition Against Unlawful Surveillance Exports. (2018, February). *The causes and consequences of communications surveillance* (CAUSE Report No. 8). https://privacyinternational.org/sites/default/files/2018-02/CAUSE_8.pdf

Tech Global Institute. (2025, August). *Cyber surveillance practices in Bangladesh*. Tech Global Institute. https://techglobalinstitute.com/wp-content/uploads/2025/08/TGI-Cyber-Surveillance-Practices-in-Bangladesh-F.pdf

UK Government. (2024, February 6). *The Pall Mall Process declaration: Tackling proliferation and irresponsible use of commercial cyber intrusion capabilities*. https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities

United Nations, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. (2023, April). *Global regulation of the counter-terrorism spyware technology trade: Scoping proposals for a human-rights compliant approach*. United Nations. https://repository.graduateinstitute.ch/record/301602?v=pdf

United Nations High Commissioner for Human Rights. (2018). *The right to privacy in the digital age (A/HRC/39/29)*. United Nations. https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high

United Nations Human Rights Office of the High Commissioner. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework*. United Nations. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

US Department of State. (2024, September 24). *Joint statement on efforts to counter the proliferation and misuse of commercial spyware*. https://2021-2025.state.gov/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/

van Daalen, O. L., van Hoboken, J., van Eijk, N., & Hins, W. (2021, June). *The new rules for export control of cyber-surveillance items in the EU*. Institute for Information Law (IViR), University of Amsterdam. https://www.ivir.nl/publicaties/download/Report-on-cybersurveillance-items.pdf

van Daalen, O. L., van Hoboken, J. V. J., & Rucz, M. (2023). Export control of cybersurveillance items in the new dual-use regulation: The challenges of applying human rights logic to export control. *Computer Law & Security Review, 48*, 105789. https://doi.org/10.1016/j.clsr.2022.105789

Vitale, E. (2025, July 18). *Spyware in the wrong hands: What can governments do?* American University. https://www.american.edu/sis/news/20250718-spyware-in-the-wrong-hands-what-can-governments-do.cfm

Wassenaar Arrangement. (n.d.). *Best practice guidelines on internal compliance programmes for dual-use goods and technologies*.

cdt.org/eu

eu@cdt.org

Centre for Democracy & Technology Europe
Avenue des Arts 11,
1210 Brussels
Belgium

The **Centre for Democracy and Technology Europe** (CDT Europe) is a non-for-profit organisation that works to increase equality, amplify voices, and promote human rights in European level tech law and policy debates. We champion policies, laws, and technical designs that protect against invasive, discriminatory, and exploitative uses of new technologies. CDT Europe works with our partner organisation, Center for Democracy & Technology which was established in 1994 and is headquartered in Washington, D.C.

cdt EUROPE