The European Journal of International Law Vol. 34 no. 3

Unmasking the Term 'Dual Use' in EU Spyware Export Control

Lena Riecke*

Abstract

Spyware has been heralded as an essential tool for law enforcement and intelligence operations. However, examples abound of states that use it in a manner that violates human rights as well as undermines democracy and the rule of law. Against this backdrop, the European Union (EU) Dual-use Regulation was recast in 2021. It now makes an effort to control the export of cyber surveillance technologies, including spyware, which it defines as dual use. What narrative is created by framing spyware as 'dual use'? This article illustrates how the term 'dual use' roots in a distinction between 'peaceful' and 'non-peaceful', or 'civil' and 'military' uses, and has gradually become associated with a broader dichotomy between 'legitimate' and 'illegitimate' purposes. Historically, this duality served not only to articulate the risks posed by certain technologies and indicate the rationale for their export control but also to justify their trade. Yet recourse by EU actors to dual use tilts the EU discourse on spyware export control towards state-centric security considerations and commercial interests over human rights. Unmasking how the term transposes a conceptually flawed, deceptive and empty duality to the spyware context, this article shows that the very concept of dual use may undermine human rights safeguards in spyware export control.

1 Introduction

Since 2021, the European Union's (EU) Dual-use Regulation (EUDUR) makes an effort to control the export of cyber surveillance technologies (CSTs), meaning 'items … specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems'.[1] CSTs

* PhD candidate, Institute of Security and Global Affairs, Leiden University, The Netherlands; European Cybersecurity Fellow, European Cyber Conflict Research Initiative. Email: l.riecke@fgga.leidenuniv.nl.

1 Council Regulation 2021/821 (EUDUR [recast]), OJ L 206/1, Art. 2(20) (which sets up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items). Given the article's focus on European Union (EU) spyware export control, it follows the recast EUDUR's definition of cyber surveillance technologies (CSTs). For criticism of its ambiguity see, e.g., van Daalen, van Hoboken and Ruz, 'Export Control of Cybersurveillance Items in the New Dual-Use Regulation: The Challenges of Applying Human Rights Logic to Export Control', 48 *Computer Law and Security Review (CLSR)* (2023) 1.

include spyware, which some view as a key tool for collecting intelligence and fighting organized crime and terrorism in the 21st century.[2] However, recent revelations underscore how spyware has long been used in violation of human rights and poses a fundamental threat to democracy and the rule of law.

A *The Booming Cyber Surveillance Industry*

In 2021, the media consortium Forbidden Stories spearheaded a series of investigations that revealed how – over the course of multiple years – the Israeli firm NSO Group sold the spyware Pegasus to states that used it to spy on politicians, government officials, journalists, activists, lawyers and other public figures across the world.[3] For persons targeted with spyware and their contacts, infection can have nefarious consequences beyond surveillance. The United Nation's investigation into the arbitrary detention, torture and murder of the journalist Jamal Khashoggi by Saudi agents warns of 'the extraordinary risk of abuse of surveillance technologies', citing allegations that Saudi Arabia spied on Khashoggi's communications in the months before his death by infiltrating the device of one of his close associates using Pegasus.[4]

Though arguably unparalleled in their scale, the Pegasus revelations are not the first of their kind. Examples abound of the export of spyware to states that have used it in violation of human rights.[5] A decade ago, the Bahraini government allegedly spied on human rights activists with FinSpy, which it purchased from Gamma International UK.[6] In 2015, the Italian firm Hacking Team made headlines for exporting spyware to governments with a track record of human rights violations.[7] Between 2011 and 2020, Steven Feldstein identified at least 65 countries as commercial spyware clients.[8] The updated 2023 dataset includes 74 states.[9] Meanwhile, a series of spyware scandals have swept through the EU in, *inter alia*, Poland, Hungary, Cyprus, Greece and

[2] Note that spyware firms sell not only intrusion and extraction tools but also related services.

[3] 'About the Pegasus Project', *Forbidden Stories* (2021), available at https://forbiddenstories.org/about-the-pegasus-project/.

[4] Human Rights Council, Annex to the Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Investigation into the Unlawful Death of Mr. Jamal Khashoggi, Doc. A/HRC/41/CRP.1, 19 June 2019, at 90–91, para. 449.

[5] See, e.g., 'Teach em' to Phish: State Sponsors of Surveillance', *Privacy International* (2018), at 4, available at https://privacyinternational.org/report/2159/teach-em-phish-state-sponsors-surveillance.

[6] 'Complaint: Privacy et. al. vs Gamma International', *OECD Watch* (2013), available at www.oecdwatch.org/complaint/privacy-international-et-al-vs-gamma-international/.

[7] A. Hern, 'Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim', *The Guardian* (6 July 2015), available at www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.

[8] S. Feldstein, 'Commercial Spyware Global Inventory', *Mendeley Data* (2020), available at https://data.mendeley.com/datasets/csvhpkt8tm/2.

[9] S. Feldstein and B. Kot, 'Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses', *Carnegie Endowment* (14 March 2023), available at https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

Spain.[10] Clearly, Pegasus is just the tip of the iceberg: the private cyber surveillance industry is booming both in democratic and authoritarian states.

B *Human Rights under Threat*

On the one hand, spyware threatens the right to privacy of targeted persons. While certain interferences with privacy are permissible, international human rights law dictates that any lawful limitation of the right must be prescribed by law, in pursuit of a legitimate aim and proportionate, meaning no more than necessary in a democratic society.[11] The European Court of Human Rights has elaborated on this proportionality test by providing minimum safeguards 'that should be set out in law in order to avoid abuses of power' during targeted surveillance operations.[12] In principle, spyware use for law enforcement and counterterrorism purposes could pursue a legitimate aim, such as the protection of national security or public order. From the viewpoint of the European Data Protection Supervisor (EDPS), this would only apply to 'situations of a very serious threat, such as an imminent terrorist attack'.[13] The EDPS warns that 'such cases would be of exceptional nature and cannot justify a wider or systematic deployment of highly intrusive technology'.[14]

Even if conducted for a legitimate aim, the proportionality of spyware-enabled surveillance is contentious, given its intrusiveness: infection with spyware may procure access to, *inter alia,* communications data, geolocation, camera and microphone on targeted devices.[15] It can enable not only real-time but also retroactive access to data of targeted persons as well as those in contact with them, turning phones into what the Office of the United Nations High Commissioner for Human Rights (OHCHR) calls '24-hour surveillance devices'.[16] For many spyware targets, a violation of the essence

[10] R. Bergman and M. Mazzetti, 'The Battle for the World's Most Powerful Cyberweapon', *New York Times*(31 January 2022), available at www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html; J. Scott-Railton *et al.*, 'CatalanGate: Extensive Mercenary Spyware Operation against Catalans using Pegasus and Candiru', *Citizen Lab* (18 April 2022), available at https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/; 'Pegasus Scandal: In Hungary, Journalists Sue State over Spyware', *Deutsche Welle* (29 January 2022), available at www.dw.com/en/pegasus-scandal-in-hungary-journalists-sue-state-over-spyware/a-60598885; R. Farrow, 'How Democracies Spy on Their Citizens', *The New Yorker* (18 April 2022), available at www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.

[11] See, e.g., European Convention of Human Rights 1950, 213 UNTS 221, Art. 8(2); EU Charter of Fundamental Rights, OJ 2007 C 303/01; International Covenant on Civil and Political Rights 1966, 999 UNTS 171, Art. 17.

[12] ECtHR, *Big Brother Watch and Others v. United Kingdom,* Appl. nos. 58170/13, 62322/14 and 24960/15, Judgment of 25 May 2021, para. 335. All ECtHR decisions are available at http://hudoc.echr.coe.int/.

[13] 'Preliminary Remarks on Modern Spyware', *European Data Protection Supervisor* (2022), at 8, available at https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

[14] *Ibid.*

[15] B. Gurijala, 'What Is Pegasus? How Surveillance Spyware Invades Phones', *Scientific American* (9 August 2021), available at www.scientificamerican.com/article/what-is-pegasus-how-surveillance-spyware-invades-phones/.

[16] Office of the United Nations High Commissioner for Human Rights (OHCHR), The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights, Doc. A/HRC/41/35, 28 May 2019, at 3, para. 7.

of their right to privacy seems apparent, meaning 'the interference … is so severe that the individual is … deprived of [the right]'.[17]

On the other hand, the Council of Europe's commissioner for human rights has warned that, beyond its implications for privacy, 'spyware has a chilling effect on other human rights and fundamental freedoms' and may 'creat[e] a climate of self-censorship and fear' that impedes individuals from exercising their freedom of expression and participating in public, political life.[18] As in the Khashoggi case, spyware may provide a gateway to the violation of other rights, including the right to liberty, the freedom from torture and even the right to life.[19] Fundamentally, spyware abuse poses an existential threat to democracy and the rule of law.

Despite these concerns, past efforts to curtail the transfer of spyware to actors with records of human rights abuse have had little success. For example, FinSpy was allegedly again sold by Gamma International through its German branch to Turkey in 2017 and deployed against the country's main opposition party.[20] Reportedly, in the year of Khashoggi's murder, the US Central Intelligence Agency brokered and paid for the acquisition of Pegasus by the government of Djibouti, despite human rights abuse allegations against the state. In 2019, David Kaye, then special rapporteur on the promotion and protection of the right to freedom of opinion and expression, considered global spyware export controls 'ill-suited to addressing the threats that targeted surveillance poses to human rights'.[21] According to the Coalition against Unlawful Surveillance Experts (CAUSE), there is a clear need for stronger human rights safeguards.[22]

C *Unmasking the Term Dual Use in the EU Discourse on Spyware Export Control*

Against this backdrop, the EU recast its EUDUR in 2021. The recast EUDUR makes multiple changes to dual-use export controls. Notably, it includes controls on CSTs and explicitly defines them as dual-use items.[23] The president of the Council of the European Union at the time, João Leão, celebrated the recast EUDUR for setting out 'rules … that give human rights the prominence they deserve'.[24] Meanwhile, CAUSE members, including Human

17 *Ibid.*

18 D. Mijatovic, 'Highly Intrusive Spyware Threatens the Essence of Human Rights', *Council of Europe* (27 January 2023), available at www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights.

19 OHCHR, *supra* note 16, at 4, paras 9, 12.

20 'Alert: FinFisher Changes Tactics to Hook Critics', *AccessNow* (2018), at 3, available at www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf.

21 Human Rights Council, Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/41/35, 28 May 2019, at 11, para. 34.

22 Coalition against Unlawful Surveillance Experts, A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation (2015), at 1, available at https://privacyinternational.org/sites/default/files/2018-02/CAUSE_8.pdf.

23 EUDUR (recast), *supra* note 1, Art. 2(20).

24 Council of the European Union, Trade of Dual-use Items: New EU Rules Adopted, press release, 10 May 2021, available at www.consilium.europa.eu/en/press/press-releases/2021/05/10/trade-of-dual-use-items-new-eu-rules-adopted/.

Rights Watch, Amnesty International and Reporters without Borders, have criticized it as 'a missed opportunity', condemning it for 'prioritis[ing] the narrow interests of industry over … obligations to protect human rights'.[25] This article examines the narrative created by situating spyware squarely within a dual-use export control framework and unmasks how the duality manufactured by the term undermines human rights safeguards in spyware export control. It first illustrates how dual use roots in a distinction between 'peaceful' and 'non-peaceful', or 'civil' and 'military' uses, and has gradually become associated with a broader dichotomy between 'legitimate' and 'illegitimate' purposes. Further, the article explains how the dual-use narrative historically served not only to articulate the risks posed by certain technologies and indicate the rationale for their export control but also to justify trade in them. Then, the article exposes how recourse by EU actors to dual use tilts the EU discourse on spyware export control towards commercial interests and state-centric security considerations over human rights.[26] Finally, it reveals why framing spyware as dual use creates a conceptually flawed, deceptive and empty duality that impedes efforts to restrict spyware exports on the basis of human rights risks.

2 The Dual-use Narrative: From Weapons of Mass Destruction to CSTs

A *Dual Use in Weapons-of-Mass-Destruction Regimes*

In the arms control context, the term dual use has long been used to describe technologies that are 'applicable both for military purposes and for … civilian ends'.[27] In relation to Weapons of Mass Destruction (WMDs), it initially introduced a duality between peaceful purposes and their opposite.[28] Although the Nuclear Non-proliferation Treaty, Biological Weapons Convention (BWC) and Chemical Weapons Convention (CWC) do not explicitly mention the term, these regimes nevertheless 'all establish the conditions states must fulfill to guarantee that certain items with a potential double application are only used for *peaceful* ends'.[29] Accordingly, the BWC commits state parties to 'never in any circumstances … develop, produce, stockpile or otherwise acquire or retain … microbial or other biological agents, or toxins … that have no justification for … other

[25] 'Human Rights Organizations' Statement in Response to the Adoption of the New EU Dual Use Export Control Rules', *Amnesty International* (2021) available at 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/.

[26] State-centric security is understood as the opposite of 'human security'. See section 3.B.

[27] United Nations, Economic and Social Consequences of the Arms Race and of Military Expenditures, UN Doc. A/32/88/Rev.1 (1978), at 68, para. 158.

[28] Q. Michel *et al.*, A Decade of Evolution of Dual-Use Trade Control Concepts: Strengthening or Weakening Non-Proliferation of WMD (2016), at 12, available at https://orbi.uliege.be/bitstream/2268/246711/1/full.pdf.

[29] *Ibid.*, at 13 (emphasis added); Treaty on the Non-Proliferation of Nuclear Weapons 1968, 729 UNTS 161; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction 1976, 1015 UNTS 163; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction 1993, 1974 UNTS 45.

peaceful purposes'.[30] Similarly, the CWC disclaims that '[p]urposes not [p]rohibited' by the convention refer to 'industrial … or other *peaceful* purposes'.[31] The Guidelines of the Nuclear Suppliers Group explicitly mention the term, clarifying that they 'gover[n] the export of nuclear related dual-use items and technologies' with the aim of 'ensur[ing] that nuclear trade for *peaceful* purposes does not contribute to the proliferation of nuclear weapons'.[32] This illustrates how dual use – that is, its introduction of a duality between the purposes for which export should be controlled versus the purposes for which trade should be permitted – is a 'key concept applied in the WMD context'.[33]

An alternative reading of dual use emerged during the Cold War era as the term began to 'appea[r] in discussions over technology transfers between "civil" and "military" applications'.[34] Dual use was thus associated with a duality between 'military' and 'civil', meaning civilian, uses. It 'became gradually perceived also as an industrial issue … constitut[ing] an opportunity to provide a wider exploitation of research and manufacturing beyond a given technology's initial objectives'.[35] Today, the multilateral export control regimes controlling spyware-related technologies – that is, the Wassenaar Arrangement (WA) and the recast EUDUR – conceptualize dual use through this 'military' versus 'civil' lens.[36]

B *The Wassenaar Arrangement*

The WA replaced the Coordination Committee for Multilateral Export Controls (COCOM), a Cold War-era forum to stem the proliferation of sensitive technologies to the Soviet Union and Eastern Bloc.[37] It emerged as the COCOM's successor to

[30] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) Toxin Weapons and Their Destruction 1972, 1015 UNTS 163, Art. 1 (emphasis added).

[31] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction 1997, 1974 UNTS 45, Art. 9(a) (emphasis added).

[32] 'Guidelines for Transfers of Nuclear-Related Dual-Use Equipment, Materials, Software, and Related Technology: Aim of the Guidelines', *Nuclear Suppliers Group* (1978), available at www.nuclearsuppliersgroup.org/en/guidelines#:~:text=The%20aim%20of%20the%20NSG,hindered%20unjustly%20in%20the%20process (emphasis added).

[33] Rath, Ischi and Perkins, 'Evolution of Different Dual-use Concepts in International and National Law and Its Implications on Research Ethics and Governance', 20 *Science and Engineering Ethics* (*SEE*) (2014) 769, at 782.

[34] *Ibid.*, at 770; see also Michel *et al.*, *supra* note 28, at 14; Molas-Gallart, 'Which Way to Go? Defence Technology and the Diversity of "Dual-Use" Technology Transfer', 26 *Research Policy* (1997), at 367; Alic, 'The Dual Use of Technology: Concepts and Policies', 16 *Technology in Society* (1994) 155, at 155.

[35] Martins and Ahmad, 'The Security Politics of Innovation: Dual-Use Technology in the EU's Security Research Programme', in A. Calcaro, E. Csernoti and C. Lavallée (eds), *Emerging Security Technologies and EU Governance: Actors, Practices, and Processes* (2020) 58, at 60.

[36] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies (WA), 11-12 July 1996, WA-DOC (19) PUB 007, available at https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf.

[37] WA Secretariat, Founding Documents: Final Declaration (1996), at 1, available at www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf; Ruohonen and Kimppa, 'Updating the Wassenaar Debate One Again: Surveillance, Intrusion Software and Ambiguity', 16 *Journal of Information Technology and Politics* (2019) 169, at 171; J. Henshaw, 'The Origins of COCOM: Lessons for Contemporary Proliferation Control Regimes', *Henry M. Stimson Center* (May 1993), at 2, available at www.files.ethz.ch/isn/105597/Report7.pdf.

control transfers of conventional weapons as well as dual-use goods and technologies.[38] To date, there are 42 participating states, including all EU member states, except the Republic of Cyprus.[39] The WA is a voluntary regime, under which states 'seek, through their national policies, to ensure that transfers of … [controlled] items do not contribute to the development or enhancement of military capabilities which undermine th[e] goals [of the WA]'.[40] It makes no mention of human rights. Fundamentally, the regime aims to 'complement and reinforce, without duplication, the existing control regimes for weapons of mass destruction' and thereby prevent 'destabilising accumulations' of goods and technologies that would undermine international security.[41] In practice, the WA's control list serves as a reference point for participating states, indicating which conventional arms and dual-use goods and technologies they should subject to domestic export control. It remains within each state's discretion to implement controls at the national level.[42] Moreover, the WA does not capture import by participating states from non-participating states.

As the reference to dual use in its title attests, the term is central to the WA.[43] However, the regime does not explicitly define dual use. The guidelines on the 'Criteria for the Selection of Dual-use Items' refer to 'dual-use goods and technologies' as those 'which are major or key elements for the indigenous development, production, use or enhancement of *military* capabilities'.[44] Simultaneously, the WA's founding documents disclaim that the regime 'will not impede bona fide civil transactions'.[45] By implication, the WA founds on a 'civil' versus 'military' duality. However, it seems to use 'civil' not only in its civilian sense but also to refer to commercial applications, thereby inviting a conflation of civilian with commercial uses. In fact, 'civil' and commercial applications are not necessarily synonymous. Both 'military' and 'civil' applications of dual-use items can be exploited for commercial purposes.

Since 2012 and 2013, the WA has regulated exports of certain CSTs. In the wake of revelations that EU-based companies exported spyware to states that used it in violation of human rights during the Arab Spring, the United Kingdom and France – which had been criticized for their failure to prevent such exports – submitted proposals to

38 Ruohonen and Kimppa, *supra* note 37, at 171; Henshaw, *supra* note 37.

39 'About Us', *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, last updated 23 December 2021, available at www.wassenaar.org/about-us/.

40 'Founding Documents: Initial Elements of the Wassenaar Arrangement', *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (1996), vol. 1(1), at 4, available at www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf; Korzak, 'Export Controls: The Wassenaar Experience and Its Lessons for International Regulation of Cyber Tools', in E. Tikk and M. Kerttunen (eds), *Routledge Handbook of International Cybersecurity* (2020) 297, at 299.

41 Initial Elements, *supra* note 40, vol. 1(1–2), at 4.

42 *Ibid.*, vol. 2(3), at 5.

43 'About Us', *supra* note 36.

44 'Criteria for the Selection of Dual-use Items', *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (adopted in 1994 and amended in 2004 and 2005), at 1, available at www.wassenaar.org/app/uploads/2019/consolidated/Criteria_for_selection_du_sl_vsl.pdf (emphasis added).

45 Initial Elements, *supra* note 40, vol. 1(4), at 5.

restrict trade in several technologies.[46] The proposals culminated in novel controls.[47] These Cyber Amendments do not create a separate control category for CSTs.[48] In fact, CSTs are not mentioned at all. Rather, the WA adopts an 'item-by-item approach' that restricts trade in certain surveillance goods and technologies – that is, telecommunications interception equipment (since 2012), intrusion software-related items and intellectual property network surveillance systems (both since 2013).[49]

The Cyber Amendments to the WA do not control the export of spyware *per se*. Rather, they apply to 'systems, equipment, and components … specially designed or modified for the generation, command and control, or delivery of "intrusion software"' and technology for its development.[50] Intrusion software is defined as software 'specially designed or modified to avoid detection by "monitoring tools", or to defeat "protective countermeasures" of a computer or network capable device' and performs 'extraction of data or information' or 'modification of the standard execution path of a program or process … to allow the execution of externally provided instructions'.[51] Overall, the Cyber Amendments thus control spyware-related items, which are added to the WA's Dual-use List rather than its Munitions List. By implication, the WA frames spyware as dual use.

C *The Recast EUDUR*

It is within the EU's exclusive competence to pursue supranational, Union-wide export controls.[52] The export of CSTs is primarily regulated by the recast EUDUR, which falls within the ambit of the EU's Common and Commercial Policy (CCP).[53] The EUDUR aims to 'implemen[t] internationally agreed dual-use controls, including … the Nuclear Suppliers Group (NSG), the WA and the Chemical Weapons Convention (CWC)'.[54] It integrates the WA's Cyber Amendments, controlling spyware-related technologies including 'systems, equipment, and components therefor, specially designed or modified for the generation, command and control, or delivery of "intrusion software"'.[55] Like all regulations, it is directly applicable – that is, legally binding

[46] T. Maurer, 'Internet Freedom and Export Controls', *Carnegie Endowment* (3 March 2016), available at https://carnegieendowment.org/2016/03/03/internet-freedom-and-export-controls-pub-62961.

[47] WA Secretariat, 'Public Statements: 2012 and 2013 Plenary Meetings', *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (December 2012 and 2013), at 45, available at www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-IV-Background-Docs-and-Plenary-related-and-other-Statements-Dec-2021.pdf.

[48] WA Secretariat, 'Summary of Changes: List of Dual-use Goods and Technologies and Munitions List' (4 December 2013), at 2, available at https://www.wassenaar.org/app/uploads/2019/consolidated/Summary%20of%20Changes%20to%20Control%20Lists%202013.pdf.

[49] Kim, 'Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue', 70 *International and Comparative Law Quarterly* (2021) 379, at 388.

[50] 'List of Dual-Use Goods and Munitions List', Categories 4(A)(5) and 4(E)(1)(c) WA-List (22) 1, at 80–81.

[51] 'List of Dual-Use Goods and Munitions List', Category 4, 5P2(a)-(b) WA-List (22) 1, at 226.

[52] Treaty on the Functioning of the European Union (TFEU), OJ 2016 C 202/47, Art. 207.

[53] *Ibid.*, Art. 207.

[54] EUDUR (recast), *supra* note 1, Annex I.

[55] Since 2014; now under *ibid.*, Annex I, at 265, para. 4(A)(005).

– in all member states, although its implementation hinges on national measures.[56] Namely, '[t]he responsibility for deciding on … export authorizations … lies with national authorities'.[57]

In 2021, the previous EUDUR[58] was recast as Regulation (EU) 2021/821. It was adopted in accordance with the EU's ordinary legislative procedure, which consists of trilogue negotiations between the European Commission, the European Parliament and the Council.[59] In 2016, the Commission formally recommended the recast EUDUR's amendment.[60] Two years later, the Parliament adopted an amended proposal.[61] The Council then agreed to a negotiating mandate in 2019, which culminated in a tripartite agreement and the adoption of the recast EUDUR in 2021.[62] The recast EUDUR defines dual-use goods and technologies as items that can be used for both 'military' and 'civil' purposes.[63] Neither the term 'military' nor 'civil' is elaborated. This ambiguity may invite a conflation of 'civil' with commercial applications, as seen in the WA, which it seeks to implement. The recast EUDUR goes further than the WA in one crucial regard: it explicitly categorizes CSTs as dual-use items.[64] What narrative does this create in the EU discourse on spyware export control?

D *The Dual-use Narrative*

The two readings of dual use that emerge from WMD literature, referring to a duality between 'peaceful' and 'non-peaceful' or 'civil' and 'military' uses, cannot necessarily be equated. The former, *prima facie*, appears broader than the latter, although commentators have concluded that it 'must be interpreted in connection with the wording of the [WMD] treaties', meaning that 'non-peaceful' should be understood as referring to 'any use intended to produce such a weapon'.[65] Nevertheless, both dualities fulfil a similar function. They illustrate how dual use

[56] TFEU, *supra* note 51, Art. 288; 'Exporting Dual-use Items', *European Commission*, available at https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en.

[57] EUDUR (recast), *supra* note 1, Recital 17.

[58] Council Regulation 428/2009, OJ 2009 L 134/1 (setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items). The title of the EUDUR (recast) remains the same.

[59] 'Ordinary Legislative Procedure: Interinstitutional Negotiations for the Adoption of EU Legislation', *European Parliament* (2017), available at www.europarl.europa.eu/olp/en/interinstitutional-negotiations.

[60] 'Proposal for a Regulation of the European Parliament and of the Council Setting Up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-use Items (recast)' ('Commission Proposal'), *European Commission* (2016), available at https://eur-lex.europa.eu/resource.html?uri=cellar:1b8f930e-8648-11e6-b076-01aa75ed71a1.0013.02/DOC_1&format=PDF.

[61] Think Tank European Parliament, Briefing: Review of Dual-Use Export Controls (2021), at 5, available at www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.

[62] General Secretariat of the Council, Proposal for a Regulation of the European Parliament and of the Council Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast), Doc. 9923/19 (2019), available at https://www.consilium.europa.eu/en/press/press-releases/2019/06/05/dual-use-goods-council-agrees-negotiating-mandate/; EUDUR (recast), *supra* note 1, Art. 31.

[63] EUDUR (recast), *supra* note 1, Art. 2(1).

[64] *Ibid.*, Art. 2(20).

[65] Michel *et al.*, *supra* note 28, at 13.

serves not only to articulate the risks posed by technologies and thereby indicate the rationale for controlling their export but also to justify trade in them. In other words, the term dual use in the recast EUDUR relates the rationale for regulating the transfer of technologies to their potential for military application and presumes that their trade for 'civil' uses need not be controlled. This assumption is anchored in the WA, which seems to conflate 'civil' and commercial applications of dual-use items. On this reading of dual use, the term pre-empts an assessment as to whether a technology should trigger export controls, beyond determining its potential for military deployment.

After the events of 9/11, which underlined how threats to international security increasingly straddle the divide between 'military' and 'civil' contexts, the term dual use underwent 'a conceptual transition'.[66] Attention in the literature shifted to the potential for dual-use goods to be used for 'malevolent' versus 'benevolent' objectives.[67] This understanding of dual use gained traction – for instance, in the life sciences – where dual use is commonly used to describe 'technology intended for beneficial purposes that can also be misused for harmful purposes'.[68] Thus, the duality manufactured by the term expanded beyond the 'military' versus 'civil' divide, prompting a broader inquiry into the legitimacy of a particular end-use by a particular actor.

However, neither the WA nor the recast EUDUR reflect this shift. Both regimes continue to frame dual-use technologies, including CSTs, in terms of a 'military' versus 'civil' duality. This links the rationale for spyware export control to the risk of its potential military application as well as presupposes that unrestricted spyware trade for 'civil' end-uses is justified. In the following sections, this article shows how this narrative undermines efforts to control spyware exports on the basis of human rights risks.

3 Dual Use as a Vehicle for Security and Commerce over Human Rights

Recourse to dual use by EU industry actors, the Commission, the Parliament and member states shows how the duality introduced by the term can steer the EU discourse on spyware export control towards commercial interests and state-centric security considerations over human rights.

A *EU Industry Actors*

Spyware firms have long employed the duality manufactured by dual use to lend legitimacy to their products by marketing them as essential crime prevention and

[66] *Ibid.*, at 15, 16.
[67] *Ibid.*
[68] See, e.g., National Research Council, Biotechnology Research in an Age of Terrorism (2004); Miller and Selgelid, 'Ethical and Philosophical Consideration of the Dual-Use Dilemma in the Biological Sciences', 13 *SEE* (2007) 523.

counterterrorism tools. For example, Hacking Team sold its technology as 'an 'offensive solution for cyber investigations' intended to make 'fighting crime … easy'.[69] The NSO Group advertises its products as tools to help 'prevent and investigate terrorism and crime to save thousands of lives around the globe'.[70] The spyware consortium Intellexa describes its mission as 'help[ing] LEAs [law-enforcement agencies] and Intelligence agencies across the world to close the digital gap with multiple and diverse solutions'.[71] This shows how spyware vendors instrumentalize the duality created by the term dual use, according to which dual-use items necessarily have a use for which trade is justified – to lend legitimacy to their business.

Recourse to the term dual use by DIGITALEUROPE further underlines how it may serve as a vehicle for commercial interests in the EU discourse on spyware export control. DIGITALEUROPE 'represent[s] digitally transforming industries in Europe', including multiple companies from the intelligence and cybersecurity sector.[72] Its 2017 commentary on the Commission's proposal for a recast EUDUR emphasized that '[d]ual-use items are often … leading-edge technologies that may be found across a wide range of key sectors of the EU economy'.[73] It argued that '[d]ual-use items are, and should be, identified by their technical characteristics and capabilities and not by their potential misuse'.[74] Thus, '[w]hether an application for an authorisation needs to be filed at all, should be based on objective, technical criteria alone'.[75]

This assumes that the inherent technical characteristics of dual-use technologies, including spyware, determine whether their export should be controlled. In fact, a key issue with controlling CSTs – that is, intrusion software – is that often 'technical attributes [are] common to both commercial surveillance and information security tools'.[76] In other words, the effects of the payload, meaning the 'code written to achieve some desired … end',[77] will 'remain unknown until the payload executes'.[78] Thus, the code underpinning penetration-testing software, which aims to detect software vulnerabilities for cyber-security purposes, and spyware, used for targeted surveillance, may 'up to a point, [be] largely indistinguishable'.[79] DIGITALEUROPE's position reflects the worry that the recast EUDUR could 'captur[e] … defensive security products and

[69] 'About Us', *Hacking Team*, available at https://web.archive.org/web/20140209024944/http:/hackingteam.it/index.php/about-us.

[70] *NSO Group*, available at https://www.nsogroup.com/.

[71] *Intellexa*, available at https://intellexa.com/.

[72] 'About Us', *DIGITALEUROPE*, available at https://www.digitaleurope.org/about-us/. A list of corporate members is available at www.digitaleurope.org/corporate/.

[73] 'European Commission Proposed Recast of the European Export Control Regime: Making the Rules Fit for the Digital World', *DIGITALEUROPE* (24 February 2017), at 2, available at www.digitaleurope.org/resources/european-commission-proposed-recast-of-the-european-export-control-regime.

[74] 'European Commission Proposed Recast', *supra* note 72, at 2, 4.

[75] *Ibid.*

[76] Bohnenberger, 'The Proliferation of Cyber-Surveillance Technologies: Challenges and Opportunities for Strengthened Export Controls', 3 *Strategic Trade Review* (2017) 81, at 86.

[77] Herr and Rosenzweig, 'Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model', 8 *Journal of National Security and Law and Policy* (2015) 301, at 303.

[78] Lin, 'Governance of Information Technology and Cyber Weapons', in E. Harris (ed.), *Governance of Dual-Use Technologies: Theory and Practice* (2016) 112, at 115.

[79] Herr and Rosenzweig, *supra* note 76, at 316.

services' and require its members to conduct, and carry the cost of, export risk assessments.[80] Its updated 2018 commentary thus claims that 'industry does not have sufficient information to … identify actors that violate or are likely to violate human rights' and supports 'the existing dual-use definition', based on the duality between 'civil' and 'military' uses'.[81] Ultimately, DIGITALEUROPE's recourse to dual use accommodates its members' commercial interests: it reaffirms the 'civil' versus 'military' duality, which does not entail a human rights risk assessment.

The impact of industry actors on the negotiations of the recast EUDUR should not be under-estimated. In 2018, Klaus Buchner – then rapporteur of the Parliament's Committee on International Trade – called for more transparency about the influence of private industry on the legislative process of the recast EUDUR.[82] The special rapporteur has observed that 'business interests were alleged to have influenced the decision to significantly curtail the inclusion of human rights safeguards [in the recast EUDUR]'.[83] Similarly, Maximiliano Seoane notes that 'firms … have been able to influence Member States at the Council towards a negotiating position against new regulations for cyber-surveillance technologies', revealing the 'preference of the European digital industry for preserving the usual military versus civilian distinction of understanding dual-use items'.[84]

B *European Commission and Parliament*

As Machiko Kanetake rightly notes, 'dual-use export control policies were not traditionally intertwined with respect for human rights'.[85] Rather, they 'developed to mitigate "military" risks' and pursued the state-centric security and foreign policy interest of preventing military and WMD end-uses of dual-use items.[86] Hence, '[b]y aligning itself with … multilateral export control regimes, the [EUDUR] inherits the[ir] military rationale'.[87] Moreover, it 'was adopted under the … CCP, making export control a corporate policy'.[88] Reiterating this in its 2011 green paper, the Commission formulates

[80] 'European Commission Proposed Recast', *supra* note 72, at 2. Note that there was similar opposition to the Wassenaar Agreement Cyber Amendments by industry stakeholders in the USA.

[81] 'Updated Comments on Proposal for Recast of Export Control Regulation', *DIGITALEUROPE* (30 January 2018), at 1–2, available at https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2019/01/Final_DualUse_Updated%20Position_30Jan.pdf.

[82] 'Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Debate)', *European Parliament* (16 January 2018), at 14, available at www.europarl.europa.eu/doceo/document/CRE-8-2018-01-16-ITM-014_EN.html (translated from German).

[83] Human Rights Council, *supra* note 21, para. 19.

[84] Seoane, 'Normative Market Europe? The Contested Governance of Cyber-Surveillance Technologies', in A. Calcara, R. Csernatoni and C. Lavallée (eds), *Emerging Security Technologies and EU Governance: Actors, Practices, and Processes* (2020) 88, at 93.

[85] Kanetake, 'Balancing Innovation, Development, and Security: Dual-use Concepts in Export Control Laws', in N. Craik *et al.* (eds), *Global Environmental Change and Innovation in International Law* (2018) 180, at 195.

[86] Kanetake, 'The EU's Dual-Use Export Control and Human Rights Risks: The Case of Cyber Surveillance Technology', 3(1) *Europe and the World: A Law Review* (2019) 1, at 2.

[87] *Ibid.*, at 9.

[88] Meissner and Urbanski, 'Feeble Rules: One Dual-Use Sanctions Regime, Multiple Ways of Implementation and Application?', 31 *European Security* (2022) 222, at 224.

the rationale for dual-use export control as 'bring[ing] together and try[ing] to balance security and non-proliferation efforts with the need to support the competitiveness of the EU industry'.[89] By design, the recast EUDUR thus pursues state-centric security and commercial considerations.

The term dual use serves as a vehicle for these interests. The green paper elaborates that, while 'trade will continue to be conducted in the vast majority of cases for legitimate purposes … [e]xport controls will … be driven in the future by the need to prevent sensitive items from being used for proliferation or military purposes'.[90] By emphasizing the military risks of dual-use items, while also depicting them as 'cutting edge high-tech and … a reflection of the EU's technological leadership in the world', the Commission employs the 'civil' versus 'military' duality manufactured by the term dual use to relate the rationale for export control under the EUDUR to state-centric security considerations – that is, potential for military application. Simultaneously, it endorses the commercial exploitation of dual-use technologies' 'civil' applications.[91]

In the aftermath of the Arab Spring, reports emerged that EU-based companies had exported spyware to authoritarian regimes that used it as a tool for political repression.[92] Seoane rightly observes that this 'exposed a highly problematic double-speak by the European Union',[93] which aimed to position itself as a 'global force for human rights'.[94] The EU had committed, *inter alia*, in its 2012 Strategic Framework and Action Plan on Human Rights and Democracy, to 'speak[ing] out against any attempt to undermine respect for universality of human rights'.[95] Moreover, in its 2013 Cybersecurity Strategy report, the Commission had warned that 'in countries outside the EU, governments may … misuse cyberspace for surveillance and control over their own citizens', claiming that it would focus on 'monitoring the export of products or services that might be used for censorship or mass surveillance online'.[96] Accordingly, the WA's Cyber Amendments

[89] European Commission, The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World, green paper, Doc. COM 393 final (2011), at 6, available at https://op.europa.eu/en/publication-detail/-/publication/e320e5f5-b204-47c6-9989-928a653a5e52/language-en.

[90] *Ibid.*, at 12.

[91] *Ibid.*, at 4.

[92] See, e.g., 'Surveillance Technologies "Made in Europe": Regulation Needed to Prevent Human Rights Abuses', *International Federation for Human Rights* (1 December 2014), available at www.fidh.org/en/issues/globalisation-human-rights/business-and-human-rights/16563-surveillance-technologies-made-in-europe-regulation-needed-to-prevent.

[93] Seoane, *supra* note 83, at 88.

[94] European Commission, Human Rights and Democracy at the Heart of EU External Action: Towards a More Effective Approach, Commission Joint Communication to the Parliament and Council, Doc. COM 886 final (2011), at 5, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0886:FIN:EN:PDF.

[95] Council of the European Union, EU Strategic Framework and Action Plan on Human Rights and Democracy, Doc. 11855/12 (2012), at 1–2, available at https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/foraff/131181.pdf.

[96] Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace, Commission Joint Communication to the EP, the Council, the European Economic and Social Committee and the Committee of the Regions, Doc. JOIN 1 final (2013), at 3, 16, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.

were integrated into the recast EUDUR, and the Commission, Council and Parliament released a joint statement 'acknowledg[ing] … [that] the export of certain information and communication technologies … can be used in connection with human rights violations'.[97] So too, in a 2014 communication, the Commission emphasized the 'new risks induced by … the emergence of specific "cybertools" for mass surveillance, monitoring, tracking and interception'.[98] The communication claimed that EU export controls 'need[ed] to integrate the security implications of … a broader range of dual-use items, in order to ensure their peaceful use'.[99]

Recognizing that '[t]he blurring of civilian and defense technology … make[s] it increasingly difficult to distinguish between purely civilian or dual-use transfers', the communication 'consider[ed] evolving towards a "human security" approach … addressing not only and strictly, items with possible military and WMD proliferation end-uses, but taking a wider security approach' that would 'recognis[e] the interlinkages between human rights, peace and security'.[100] Advocates of 'human security' celebrate the concept as a 'shift [away] from a focus on state security'[101] towards a 'focus on the individual as the … primary beneficiary'.[102] For Ronald Deibert, 'human security' introduces a human-centric perspective on security that 'places human beings … as the primary objects of security' and 'offers a better alternative to the traditional realist "national security-centric" approach … [that] places the sovereign state as the principal object of security'.[103] Accordingly, the communication appeared both to signal a recognition by the Commission of the shortcomings of the term dual use and to indicate a shift towards human rights.

The Commission's 2016 proposal for the recast EUDUR seemed to build on this intention by expressing its 'suppor[t] [for] … a revised definition of "dual-use items", reflecting the evolution beyond the traditional military and state-centric approach to security'.[104] Moreover, it suggested the '[i]ntroduc[tion] [of] an EU autonomous list of specific cyber-surveillance technologies of concern to be subject to controls … complemented by a targeted catch-all control, which allows controlling the export of non-listed cyber-surveillance technologies in certain situations where there is evidence that they may be misused … by the proposed end-user for directing or implementing serious violations of human rights or international humanitarian law'.[105] This posited

[97] Joint Statement by the EP, the Council, and the Commission on the Review of the Dual-use Export Control System of 4 April 2014, OJ 2014 C 100/11.

[98] European Commission, The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World, Communication from the Commission to the Council and the EP, Doc. COM 244 final (2014), at 3, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0244&from=EN.

[99] *Ibid.*, at 5.

[100] *Ibid.*, at 4 and 6.

[101] Glasius, 'Human Security from Paradigm Shift to Operationalization: Job Description for a Human Security Worker', 39 *Security Dialogue* (2008) 31, at 31.

[102] Newman, 'Critical Human Security Studies', 36 *Review of International Studies* (2010) 77, at 78.

[103] Deibert, 'Toward a Human-centric Approach to Cybersecurity', *32 Ethics and International Affairs* (2018) 411, at 411–412.

[104] 'Commission Proposal', *supra* note 59, at 11.

[105] *Ibid.*, at 9; General Secretariat of the Council, *supra* note 61.

human rights as 'a *normative justification* for imposing export control'.[106] It would have given the Commission the power to independently subject additional items to control where it deemed this 'necessary due to risks that the export of such items may pose as regards the commission of serious violations of human rights'.[107] However, the final text of the proposed amendments reiterated the 'military' versus 'civil' definition of dual-use items, choosing to include CSTs within its ambit.[108]

The Parliament's debate on the Commission's proposal for the recast EUDUR brought conceptual tensions resulting from the integration of spyware export controls into a dual-use framework to the fore. Notably, Dutch parliamentarian Marietje Schaake submitted several amendments to distinguish CSTs from dual-use items.[109] As Kanetake writes, this would have improved 'conceptual coherence by recognising … that the EU's export control is no longer constrained by the traditional dichotomy of civil and military purposes'.[110] Ultimately, the Parliament retained the 'civil' versus 'military' duality as a basis for controlling 'traditional dual-use items' but distinguished these from controls on 'cyber surveillance items … which can be used in connection with the violation of human rights'.[111]

C *EU Member States*

In a working paper leaked in 2018, multiple member states advocated for 'the development of effective EU cyber-surveillance controls for the protection of human rights'.[112] These states differentiated WMDs from CSTs, contending that '[c]yber-surveillance items usually cannot be misused … for conventional military uses … but … they can be misused for violations of certain human rights'.[113] They argued that 'the Council should address both but distinctively the internationally established dual-use controls … and the new items suggested to be specifically controlled by the EU for human rights reasons'.[114] In other words, they acknowledged the difficulty of situating spyware export controls within a dual-use framework. While maintaining '[t]he existing dual-use definition … as it is today', they supported the creation of an EU autonomous list for 'certain cyber-surveillance items which are not (yet) internationally listed dual-use items …[but] which raise concerns to be misused for serious violations of human rights'.[115]

[106] Kanetake, *supra* note 85, at 6 (emphasis in original).
[107] 'Commission Proposal', *supra* note 59, Art. 16(2b), at 35.
[108] *Ibid.*, Art. 2(1b), at 19.
[109] See, e.g., INTA Committee, Amendments: Draft Report on the Proposal for a [Recast], Doc. COM(2016)0616 – C8-0393/2016 – 2016/0295(COD) (2017), Amendments 58, 60, 65, 68, 116.
[110] Kanetake, *supra* note 85, at 9.
[111] Parliament, Amendments on the Proposal for a [Recast], Doc. COM(2016)0616 – C8-0393/2016 – 2016/0295(COD) (2018), Amendment 25.
[112] General Secretariat of the Council of the European Union, Working Paper: EU Export Control – Recast of Regulation 428/2009, Doc. WK 1019/2018 INIT, 29 January 2018, at 1, available at www.euractiv.com/wp-content/uploads/sites/2/2018/02/11_member_states_dual-use.pdf. Submitted by Croatia, the Czech Republic, France, Germany, Italy, Poland, Portal, Romania, Slovakia, Slovenia and Spain.
[113] *Ibid.*, at 2.
[114] *Ibid.*
[115] *Ibid.*, at 2–3.

Several other member states responded with a warning about '[t]he impacts of introducing an EU autonomous list … [which] relate[s] to foreign, security, and trade issues'.[116] They argued that 'an autonomous EU control list, could seriously undermine the competitiveness of EU-based industry' and 'in the worst case … develop into a broad-ranging list of any new technologies … thus portraying Europe as a technology-averse continent and an unlikely home for any global frontrunner on ICT [information and communications technology] or other technologies'.[117] While recognizing that 'cyber-surveillance technologies could be misused in connection with serious violations of human rights … in repressive states', they emphasized their 'entirely legitimate uses for law-enforcement purposes, countering radicalization and fighting terrorism'.[118] Ultimately, they argued, '[c]ontrols on EU exports without parallel measures in other major economies would … push the development … of relevant technologies outside of the EU'.[119] Hence, '[i]f the EU were to [unilaterally] … address new areas that go beyond what the Regulation was originally created for … there would be a risk of retaliatory actions … by important non-EU trading partners'.[120] Thus, they concluded, '[w]hile cyber surveillance items … can affect individual security and freedoms, they are equally militarily relevant … and therefore have their rightful place in the … Wassenaar Arrangement'.[121] The Council adopted this position in its negotiating mandate, which neither included an EU autonomous list nor defined CSTs as dual use.

In the end, the agreed recast EUDUR does go further than its predecessor in integrating human rights considerations. For example, it sets out novel 'catch-all' controls for unlisted CSTs, requiring an exporter to notify a national competent authority if 'aware, according to its due diligence findings, that [unlisted] cyber-surveillance items … are intended, in their entirety or in part, for [use in connection with internal repression and/or the commission of *serious* violations of human rights and international humanitarian law]'.[122] However, the adoption of such controls remains at the discretion of national authorities. Further, the recast EUDUR provides that member states may adopt national controls on unlisted CSTs 'if the exporter has grounds for suspecting that [the items] … are or may be intended … for any [of the aforementioned] uses'.[123] If a state chooses to do so, it must 'provide the other Member States and the Commission with relevant information' and all

[116] General Secretariat of the Council of the European Union, Working Paper: EU Export Control – Recast of Regulation 428/2009, Doc. WK 5755/2018 INIT, 15 May 2018, at 3, available at www.euractiv.com/wp-content/uploads/sites/2/2018/06/nine-countries-paper-on-dual-use.pdf. Submitted by the Czech Republic, Cyprus, Estonia, Finland, Ireland, Italy, Poland, Sweden and the United Kingdom.

[117] *Ibid.*, at 2, 4.

[118] *Ibid.*, at 1.

[119] *Ibid.*, at 4.

[120] *Ibid.*, at 3.

[121] *Ibid.*, at 5.

[122] EUDUR (recast), *supra* note 1, Art. 5(2) (emphasis added). 'Serious' is not defined. See the Commission's discussion of its meaning in their Article 5 Draft Guidelines, available at https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en.

[123] EUDUR (recast), *supra* note 1, Art. 5(3).

other Member States must give 'due consideration' to information received, within 30 days, to determine whether they will also subject it to export control.[124] Thus, member states retain wide national discretion in implementing these 'catch-all' controls. Moreover, the agreement of all member states is a prerequisite for controls on an item to apply harmoniously across the EU, meaning that each state seems to retain the power to veto Union-wide controls on unlisted CSTs.[125] Article 4 of the previous EUDUR, containing a similar catch-all provision for unlisted items with potential for WMD application or other military end-use, has been criticized as 'a source of potentially incoherent European dual-use governance' that facilitates 'license shopping' in member states with less stringent controls.[126] Notably, CSTs are excluded from the list of items for which intra-Union trade is controlled.[127]

Ultimately, the outcome of the trilogue negotiations signals an uncomfortable comprise that is conceptually unsound. Although the Commission publicly posits the recast EUDUR as a shift towards 'human security', neither an EU autonomous list for CSTs nor the term 'human security' feature in the regulation.[128] Rather, the perceived need for strengthening controls on CSTs is met by integrating them into a dual-use framework that is founded on a 'military' versus 'civil' use duality.[129] Recourse by EU actors to the term dual use illustrates how this duality may steer spyware export controls towards considerations of state-centric security and commercial interests over human rights.

4 Dual-use Unmasked

To explain why the very concept of dual use undermines efforts to restrict spyware exports on the basis of human rights risks, the article unmasks how the term introduces a conceptually flawed, deceptive and empty duality in relation to spyware.

A *Flawed Duality*

First, by framing spyware as dual use, the recast EUDUR creates a conceptually flawed duality. Namely, applying the duality between 'civil' versus 'military' uses to spyware at best oversimplifies, and at worst conceals, the risks posed by its export. Juxtaposing 'civil' and 'military' uses relates the rationale for regulating spyware to the risks stemming from its military application – that is, use during armed conflict. Recent revelations about the use of Pegasus in the Azerbaijan–Armenia conflict underscore the

[124] *Ibid.*, Art. 5(4–5).
[125] EUDUR (recast), *supra* note 1, Art. 5(6).
[126] Meissner and Urbanski, *supra* note 87, at 4.
[127] EUDUR (recast), *supra* note 1, Ar. 11(1), Annex IV. Intra-Union controls on CSTs would subject EU members to the same human rights standards that external states must meet. However, this falls outside of the EU's exclusive competence for EU-external export control.
[128] 'Strengthened EU Export Control Rules Kick In', press release, *European Commission* (9 September 2021), available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4601.
[129] EUDUR (recast), *supra* note 1, Art. 2(20).

risks posed by the military application of spyware.[130] However, an abundance of spyware abuse occurs during peacetime. The 'civil' versus 'military' duality thus masks the threat posed by spyware to fundamental human rights when not deployed for a military purpose. Hence, defining CSTs as dual use is a red herring. It introduces a conceptually flawed duality into the discourse on spyware export control that misleads about the legal criteria relevant for spyware export risk assessments. There are important differences between the law applicable during peacetime versus war. During peacetime, human rights law applies in full to regulate targeted surveillance. During armed conflict, international humanitarian law (IHL) and human rights co-apply.[131] The particularities of co-application – that is, how the operation of IHL affects human rights standards – remain disputed in legal scholarship.[132] Importantly, the existence of an armed conflict may open the door to derogations and emergency powers, as well as introduce different variables into the necessity and proportionality assessments required by human rights law. Accordingly, spyware deployment that would be disproportionate and violate human rights during peacetime might be lawful in the extreme circumstances of an armed conflict.

This illustrates why a conceptually coherent export control regime must recognize the legal distinction between wartime and peacetime spyware use. The recast EUDUR encourages national authorities to 'consider [both] … the risk of [CSTs] being used in connection with internal repression or the commission of serious violations of human rights and international humanitarian law'.[133] However, by framing CSTs as dual use, it relates the risks posed by spyware and the rationale for its regulation solely to its potential for military application. Thereby, it presumes that spyware's 'civil' use and trade are legitimate and need not be controlled. This not only masks the threat posed by spyware to human rights during peacetime but also infuses the recast EUDUR with conceptual confusion that undermines human rights risks as an independent basis for restricting spyware exports.

B *Deceptive Duality*

Second, dual use manufactures a deceptive duality in relation to spyware. It presupposes that the 'civil' applications of any dual-use technology, including spyware, are *ipso facto* legitimate, meaning that their trade need not be controlled. However, the legitimacy of spyware end-uses, whether for 'civil' or 'military' purposes, hinges on their respect for human rights. The 'military' versus 'civil' duality thus pre-empts an

[130] N. Krapiva and G. Coppi, 'Hacking in a War Zone: Pegasus in the Azerbaijan-Armenia Conflict', *Access Now* (25 May 2023), available at www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.

[131] Shany, 'Co-application and Harmonization of IHL and IHRL: Are Rumours About the Death of *Lex Specialis* Premature?', in R. Kolb, G. Gaggiolo and P. Kilibarda (eds), *Research Handbook on Human Rights and Humanitarian Law* (2022) 9, at 14; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004, ICJ Reports (2004) 136, para. 106.

[132] Lubell, 'Challenges in Applying Human Rights Law to Armed Conflict', 87 *International Review of the Red Cross* (2005) 737, at 738, 745.

[133] EUDUR (recast), *supra* note 1, Recital 17, Art. 5.

assessment as to which 'civil' uses of spyware, if any, and under what conditions, are 'legitimate' in that they are human rights compliant. Cognizant of the potential shortcomings of applying the 'military' versus 'civil' duality to spyware, several commentators have offered alternative interpretations of dual use in line with its evolution in the literature post 9/11. For James Shires, the traditional understanding of dual use refers to technologies with both 'security-relevant and non-security uses' and falls short in relation to spyware.[134] Instead, he recognizes 'a second, more complex, sense of dual-use' that entails a 'reinterpretation … between legitimate and illegitimate security technologies, rather than security-relevant and non-security technologies'.[135] Shires thus views the term as introducing a duality between technologies that can be used for legitimate, defensive security purposes to '*combat* security threats, such as … vulnerability disclosure and incident response' and those that can be used by 'threat actors' for illegitimate, offensive activities.[136]

A similar distinction is drawn by Herbert Lin, for whom dual-use technologies are not necessarily defined by the effects they produce but, rather, by the purposes for which they are used.[137] In his view, the use of CSTs to produce negative effects on another system – for example, by undermining the confidentiality of data – would be legitimate if used by the 'good guys' for a beneficial purpose, such as for law enforcement.[138] This reflects the expansive understanding of dual use that emerged in the literature post 9/11, as previously elaborated, which refers to a duality between 'malevolent' and 'benevolent' or 'legitimate' and 'illegitimate' uses. Yet conceptualizing spyware in terms of the legitimacy versus illegitimacy of the purpose of its use may replace one deceptive duality with another. In Lin's view, legitimacy of end-use depends on the actor: a technology may be susceptible to abuse when employed by 'the bad guys', but 'in the hands of the good guys (e.g., the police), its use is beneficial to society'.[139] As the recent Pegasus revelations demonstrate, however, it can be difficult to distinguish the 'good guys' from the 'bad guys' in the spyware context.

Spyware abuse allegations have been raised against several EU member states. This not only includes states facing a rule-of-law crisis, such as Poland and Hungary, but also nominally liberal democracies.[140] For example, at least 65 members of the Catalan civil society were targeted with Pegasus.[141] Circumstantial evidence points to

[134] J. Shires, *The Politics of Cybersecurity in the Middle East* (2021), at 126.
[135] *Ibid.*
[136] *Ibid* (emphasis in original).
[137] Lin, *supra* note 77, at 112–113.
[138] *Ibid.*, at 113.
[139] *Ibid.*
[140] M. Schaake, 'The EU Must Decide How to Limit the Use of Spyware by Member States', *Financial Times* (8 February 2022), available at www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e; P. Szabolcs and P. Andras, 'Hungarian Journalists and Critics of Orban Were Targeted with Pegasus, a Powerful Israeli Cyberweapon', *Direkt36* (19 July 2021), available at www.direkt36.hu/en/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele/.
[141] J. Scott-Railton *et al.*, 'Catalangate', *Citizen Lab* (18 April 2022), available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/#attribution-to-a-government.

the involvement of the Spanish authorities.[142] Moreover, Predator spyware was used to target Greek journalists and opposition politicians.[143] The Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee) considers it 'highly probable that Predator has been used by or on behalf of persons very close to the Prime Minister's office'.[144] As Deibert puts it, '[t]here is no jurisdiction that is immune to corruption and authoritarian practices – only greater or lesser degrees of protection against them'.[145] In his view, 'depending on *how* [spyware is] deployed, [it] may serve a legitimate … purpose … or a purpose that undermines human rights'.[146] In other words, deployment of spyware for a purpose that is legitimate in principle – such as for law enforcement, counterterrorism or intelligence – does not guarantee its lawfulness – that is, human rights compliance, in practice. Accordingly, the purpose of spyware deployment cannot determine whether its trade is justified *ex ante*. Rather, the compliance of the actual end-use with human rights matters.

Framing CSTs as dual use is thus deceptive because it treats the legitimacy of spyware's 'civil' use and trade for such purposes as a settled fact. This puts the cart before the horse in relation to spyware. The legitimacy of spyware trade hinges on the human rights compliance of its end-uses, which must be assessed rather than assumed. It remains an open question whether all goods and services currently marketed as 'spyware' can be used in a human rights-compliant manner. Although 'national security activities [such as spyware use] … can justify the restriction of fundamental rights' in principle, many publicly known instances of Pegasus deployment appear to fall short of the 'conditions of legitimacy, legality, necessity, balancing, and consistency with democracy'.[147] In fact, the EDPS has concluded that 'it is highly unlikely that spyware such as Pegasus, which de facto grants full unlimited access to personal data … could meet the requirements of proportionality … [unless] certain features of the tool might be switched off'.[148]

Common, public standards for human rights-compliant spyware use must be at the forefront of any spyware export control regime that takes human rights seriously. As Ben Wagner writes, 'human rights justifications for [dual-use] exports take place

[142] *Ibid.*

[143] 'Greece: Spy Chief Quits amid Predator Spyware Furor', *Deutsche Welle* (5 August 2022), available at www.dw.com/en/greece-spy-chief-quits-amid-predator-spyware-furor/a-62723640.

[144] PEGA Committee, *supra* note 2, at 7. Note that the committee's recommendations were adopted by the European Parliament. 'Spyware: MEPs Call for Full Investigation and Safeguards to Prevent Abuse', press release, *European Parliament* (15 June 2023), available at www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse.

[145] R. Deibert, *Reset: Reclaiming the Internet for Civil Society* (2020), at 199.

[146] R. Deibert, 'What to Do about "Dual-use" Digital Technologies', *Citizen Lab* (29 November 2016), available at https://deibert.citizenlab.ca/2016/11/dual-use/.

[147] Sartor and Loreggia, 'The Impact of Pegasus on Fundamental Rights and Democratic Processes', *European Parliament* (2022), at 54, available at www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740514.

[148] 'Preliminary Remarks', *supra* note 13, at 8.

behind closed doors'.[149] He rightly notes that '[a]ctors [who are] involved in performing human rights narratives … to justify the exports of technologies have little interest or incentive in an accurate portrayal of the actual human rights situation on the ground'.[150] Thus, clear standards against which to assess the risk of human rights violation by an intended spyware end-user are a necessary – though not individually sufficient – condition for a workable spyware export control regime. Currently, international guidance is lacking on what spyware uses, if any, and under which conditions, are 'legitimate' in that they are prescribed by law, pursue a legitimate aim and are proportionate as well as necessary in a democratic society. In recognition of this uncertainty, the PEGA Committee has called for 'the adoption of conditions for the legal use, sale, acquisition and transfer of spyware [and] insists that, for the continued use of spyware, Member States shall fulfil all of [these] conditions by 31 December 2023'.[151]

On the international plane, a number of states recently stated that they would 'work collectively … [to] develop and implement policies to discourage the misuse of commercial spyware'.[152] Denmark, France and Sweden were the only EU member states to join this statement. At the 2023 Summit for Democracy, 44 governments endorsed the Guiding Principles on Government Use of Surveillance Technologies.[153] However, the principles are limited to three areas of concern, which notably make no mention of spyware such as Pegasus. Establishing guidelines on spyware use is difficult because little is known about the spyware industry. Secrecy is perpetuated both by spyware firms and their clients: the very states tasked with regulating spyware exports.[154] For this reason, context can help flag human rights risks. Accordingly, the US executive order that prohibits government agencies from using commercial spyware with certain risks treats country reports on 'engag[ement] in systematic acts of political repression … or other gross violations of human rights' as sufficient evidence of a risk of 'improper use'.[155]

[149] Wagner, 'Whose Politics? Whose Rights? Transparency, Capture, and Dual-Use Export Controls', 31 *Security and Human Rights* (2020) 35, at 36.

[150] *Ibid.*

[151] PEGA Committee, *supra* note 2, at 18.

[152] White House, Joint Statement on Efforts to Counter the Proliferation and Misuses of Commercial Spyware, 30 March 2023, available at www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.

[153] 'Guiding Principles on Government Use of Surveillance Technologies', *Freedom Online Coalition* (30 March 2023), available at https://freedomonlinecoalition.com/publication-of-guiding-principles-on-government-use-of-surveillance-technologies/.

[154] On this point, see Anstis, Leonard and Penney, 'Moving from Secrecy to Transparency in the Offensive Cyber Capabilities Sector: The Case of Dual-Use Technologies Exports', 48 *CLSR* (2023) 2.

[155] White House, Executive Order on the Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, 27 March 2023, available at www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/. Though note that it only mentions risks of spyware abuse 'by a *foreign* government or *foreign* person (ibid, at Sec.2(a)) (emphasis added).

Even if clear guidelines are agreed, the adherence by national licensing authorities to them is not guaranteed. Serious doubts have been raised about the enforcement of the recast EUDUR at the member state level.[156] The risk of a spyware end-user violating human rights is context and case dependent. Hence, the details of individual licensing decisions matter. Reporting can help achieve greater transparency so that 'claims about human rights associated with the export of goods … would have to stand up to public scrutiny'.[157] The recast EUDUR contains new reporting obligations for CST licensing decisions, with the caveat that member states may give 'due consideration' to 'the protection of … commercially sensitive information or protected defence, foreign policy or national security information'.[158] It remains to be seen how these reporting obligations will be given effect. Clearly, much remains to be done to ensure the effective operation of EU spyware export controls. As a first step, 'an accurate human rights narrative … can help ensure a more effective dual-use governance regime'.[159] Accordingly, this article has highlighted conceptual issues within the recast EUDUR by unmasking how the dual-use narrative introduces a deceptive duality into the discourse on spyware export control that undermines human rights safeguards.

C *Empty Duality*

Third, the 'military' versus 'civil' understanding of dual use creates an empty duality that is without much practical utility when applied to spyware. As Bruno Martins and Neven Ahmad rightly note, 'a strict distinction between civilian and military technology has become increasingly difficult to draw' because 'the processes by which civilian technologies get military use … are becoming increasingly common'.[160] This holds true for spyware, the 'military' versus 'civil' use of which depends on little more than the context within which it is used. Moreover, the term dual use could today include such great 'variety of … technologies' that hardly any modern technology falls outside of its scope.[161] If nearly all technologies could potentially be dual use, then calling them such would be 'true' but 'not very helpful'.[162] Accordingly, framing spyware as dual use may do little other than introduce a conceptually flawed and deceptive duality into the discourse on its export control.

5 Conclusion

This article has demonstrated how dual use has served to articulate the risks posed by technologies and indicate the rationale for both their export control as well as their trade. It shows how the term became associated with a duality between 'peaceful' and

[156] See, e.g., Meissner and Urbanski, *supra* note 87.
[157] Wagner, *supra* note 147, at 39.
[158] EUDUR (recast), *supra* note 1, Art. 26(3).
[159] Wagner, *supra* note 147, at 37.
[160] Martins and Ahmad, *supra* note 35, at 58.
[161] Molas-Gallart, *supra* note 34, at 368.
[162] Alic, *supra* note 34, at 158.

'non-peaceful' or 'military' and 'civil' uses, which gradually expanded to 'legitimate' and 'illegitimate' purposes. Then, the article expounds how the recast EUDUR situates spyware squarely within this narrative by explicitly defining CSTs as dual use. Further, it exposes how recourse to dual use by EU actors can steer spyware export controls towards commercial interests and state-centric security considerations over human rights. Finally, it unmasks how the term dual use introduces a conceptually flawed, deceptive and empty duality in relation to spyware that undermines efforts to strengthen human rights safeguards in EU spyware export control.

Ultimately, export control is not a 'magic bullet' when it comes to regulating spyware.[163] Rather, it should form part of a broader toolkit. Nevertheless, how export control regimes frame spyware matters. By unpacking how the recast EUDUR conceptualizes spyware, this article has brought the tensions and competing interests that underpin the EU discourse on spyware regulation out into the open. It thereby exposes presumptions built into existing controls and illustrates how stakeholders can instrumentalize them for their own purposes. Ultimately, this shifts the debate to the question at the heart of the matter: what spyware end-uses, if any and under what conditions, are 'legitimate' in that they are human rights compliant? Multilateral efforts that set clear standards for spyware end-use can help provide the answer.

[163] W. DeSombre Bernsen, 'Export Control Is Not a Magic Bullet for Cyber Mercenaries', *Lawfare Blog* (24 March 2023), available at https://www.lawfaremedia.org/article/export-control-not-magic-bullet-cyber-mercenaries.