LUISS

Master's degree in Law, Digital Innovation & Sustainability

Chair of Law and Ethics of Innovation & Sustainability

"BALANCING INNOVATION WITH SECURITY: EXPORT CONTROLS ON DUAL-USE ITEMS. THE CASE OF EMERGING TECHNOLOGIES (AI, CYBER-SURVEILLANCE TOOLS) IN THE EU AND THE US"

Prof. Filiberto Brozzetti

SUPERVISOR

Prof. Mariavittoria Catanzariti

CO-SUPERVISOR

CANDIDATE

Silvia Carrara – 631633

Academic Year 2024/2025

Abstract

The fast-growing development of technology in recent years has fundamentally changed the world of international trade, research and security. Many current technologies have a dual nature: while they can be useful for civilian purposes, they also have the potential of being abused for military or repressive purposes.

In an era that is not only characterized by technological progress but also by geopolitical uncertainty, the regulation of dual use goods is an essential and critical aspect that policymakers, researchers and industry players must face.

This thesis explores the dilemmas that arise with dual use export controls, focusing on the tension between scientific freedom, ethical responsibility, national security, and human rights.

The dual use dilemma is not a new concept, it emerged when the first concerns over nuclear technology and its potential misuse came to the surface; it now extends to modern fields such as artificial intelligence, cybersecurity and surveillance technologies.

This study explores the legal framework of dual use export controls, the ethical and human rights concerns it presents, the different approaches to the governance of dual use items, in particular the differences between the European Union and the United States of America and analyses the limitations of the current framework in light of the Russian invasion of Ukraine.

To provide a stronger basis for my recommendations on a recast of the dual use legislation, qualitative findings from expert interviews and stakeholder recommendations were used. A framework that better incorporates ethical and human rights considerations and is based on member states harmonization is proposed as a solution.

Table of contents

Introduction

Dual-use goods and technology have long been integral to modern life, serving a variety of civilian needs, however, their potential for military or defense applications has created a significant regulatory challenge.

These technologies, which could have both positive and negative end-uses, are essential to discussions about international trade and security policy. Dual-use technologies, whether they are software, semiconductors, artificial intelligence systems, or surveillance tools, raise important issues on how to control innovation without sacrificing security.

To address these challenges and set up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, Regulation (EU) 2021/821 was introduced. It offers a thorough system to strengthen the prior export control framework and address changing security threats and new technological advancements.

A critical feature of the regulation is Annex I, which presents a list of the items that require export authorization, the list of dual-use items, that is updated periodically to guarantee that emerging technologies and the dangers they might pose are consistently addressed within the legislative framework.

The dual-use regulation must also address ethical and human rights concerns, given the potential repercussions of misuse. These issues are becoming increasingly urgent as cutting-edge technologies, like artificial intelligence, and advanced surveillance systems develop at a much faster rate than expected. The regulation's attempt to create a flexible and cohesive regulation mechanism for these rapidly changing sectors is crucial to the European Union's ability to remain resilient in the face of both geopolitical tensions and the technological outburst.

Indeed, in light of the current geopolitical instability, the current framework provides a strong basis to deal with the growing complexity of the trade of dual-use technology on a global scale. It strikes a compromise between the urgent need to stop the spread of sensitive technology that could be abused, whether for military purposes or human rights abuses, and the necessity to support lawful trade and innovation.

The regulation increases collaboration between the Commission and Member States, imposes particular duties on exporters, and implements safeguards against human rights abuses by cybersurveillance technologies.

The necessity for continuous reform and improved collaboration between the Member States and foreign actors, such as other regimes, but also industry stakeholders and researchers, is underlined by recent crises, for instance the Russian invasion of Ukraine, which have shown

weaknesses and difficulties in the enforcement, coordination, and adaptation of controls.

Methodology

This thesis aims to answer the following research question: How can the European Union's dual-use export control framework effectively balance the competing demands of technological innovation, national security, and human rights protection, particularly in light of emerging technologies and recent geopolitical challenges?

The analysis will focus on four key thematic areas:

1. Ethical dilemmas in dual-use research and innovation, examining how ethical considerations are integrated into regulatory frameworks and research practices.
2. Human rights concerns related to cyber-surveillance technologies, assessing the impact of export controls on privacy and freedom of expression.
3. A comparison of the regulatory philosophies and practices of the European Union and the United States, exploring how the two different approaches affect innovation and security.
4. The effectiveness of export controls and sanctions in the context of the Russia-Ukraine conflict, evaluating lessons learned and implications for future policy reform.

To explore these themes and gain better insight and a comprehensive understanding of the regulatory, ethical, and geopolitical challenges surrounding dual-use export controls, this thesis adopts a qualitative research approach, utilizing semi-structured interviews with experts drawn from public institutions, industry, and consultancy, contacted via professional platforms such as LinkedIn, as well as through referrals and recommendations within professional and academic networks.

Additionally, stakeholder consultation responses, including industry and civil society input to the European Commission’s White Paper on Export Controls, were included to offer a broader spectrum of perspectives and contribute to the final considerations.

The expert interviews and stakeholder consultation provided insights into the practical challenges and strategic considerations shaping dual-use export control policy and served as a basis for my considerations and recommendations for the next recast of the dual-use regulation.

Structure

This thesis is structured into three main chapters, each addressing key aspects of the dual-use export control regime:

- *Chapter 1: What is Dual Use?*

This chapter introduces the concept of dual-use goods and technologies and explains the historical context and the international regulatory frameworks governing their export, from the beginning up until Regulation (EU) 2021/821.

- *Chapter 2: Innovation vs. Security*

This chapter explores the ethical dilemmas inherent in dual-use research and the human rights implications of cyber-surveillance technologies. It examines how these topics intersect with innovation and security, drawing on the differences between the EU and the US approaches to innovation, and the effectiveness on the sanctions imposed on Russia after its invasion of Ukraine.

- *Chapter 3: Expert insights ahead of the review of the dual use regulation*

Building on the theoretical foundations, this chapter presents qualitative data collected through expert interviews and stakeholder consultations (Annex A and B). The findings are analyzed thematically, and personal recommendations for the next review of the dual use regulation are presented.

1. Dual Use in Context: Definitions, Origins and Implications

1.1 What is dual use?

The European Commission defines dual-use items as *"goods, software and technology that can be used for both civilian and military applications".*[1]

A dual-use item is generally recognized as an item that serves a dual purpose, a civilian and a military one. A number of products, materials and technologies that are so essential to our life we couldn't imagine living without them could potentially be used as a destruction tool by the armed forces of governments as well as non-state actors and terrorists.[2]

The academic literature and policy research on dual-use regulation focus on the risks associated with these technologies and the challenges in controlling their export while promoting innovation and trade.

Export control is a trade tool used to support global security goals within the framework of non-proliferation of weapons of mass destruction, or WMD. The export control of dual-use items falls under the domain of national, international and EU law. It is especially relevant in view of the current historical situation, where threats to security and safety are at their highest, and effective controls are more needed than ever.[3]

Scholars such as Bauer & Bromley (2016) emphasize that dual-use products are integral to modern economies; indeed, a large number of industry sectors are involved in the production of such items, including energy, security, chemical and electronics. Therefore, their development and commercialization is vital to the economic well-being of several state and non-state actors, and, since it would be impossible to block their production due to their dual nature, it is essential to control their end-use. Failure to effectively regulate their export could result in significant risks.[4]

Similarly to their production, export controls apply to a wide range of actors, from manufacturers to academics, institutions, and researchers, as Stalenhoef, Kanetake and van der Wende (2022) underline.[5]

---

[1] Exporting dual-use items. (2025). European Commission. Trade and Economic Security.

[2] Kanetake, M. (2018). Balancing innovation, development, and security: dual-use concepts in export control laws. Global Environmental Change and Innovation in International Law (Cambridge University Press, 2018 Forthcoming).

[3] Alavi, H., & Khamichonak, T. (2017). EU and US export control regimes for dual use goods: An overview of existing frameworks. Romanian J. Eur. Aff., 17, 59.

[4] Bauer, S., & Bromely, M. (2016). The dual-use export control policy review: balancing security, trade and academic freedom in a changing world.

[5] Stalenhoef, C., Kanetake, M., & van der Wende, M. (2022). The implications of the EU's dual-use export control regulation 2021/821 for universities and academics. Utrecht University School of Law Research Paper Forthcoming.

1.2 History of dual-use and importance for technological development and innovation

Indeed, many things that have now become part of our everyday life have a dual nature, and many originate from military inventions and were later adapted to civilian needs. For instance, something that we reach for a thousand times a day and that is now so embedded into our routine that we could not live without it, the smartphone, has a number of features that were originally designed for something else entirely.

Smartphones, while designed and catered for everyday personal communication, possess characteristics that spring from military and intelligence developments.

For instance, the GPS (or Global Positioning System), which is already installed in our mobile devices through apps like Google Maps or Apple Maps, and used daily to reach any kind of destination, was originally developed for military purposes. Indeed, in the early 1960s the United States Department of Defense developed TRANSIT, the first satellite-based navigation system, with the aim of improving military operations; and later it would go on to develop Navstar GPS, the system that is still used today.[6]

Touchscreen technology was also developed for military purposes. The idea is attributed to Eric A. Johnson, who developed a touch interface to control computers used by the U.K. National Air Defense in 1965, to aid air traffic control. [7]

Voice or virtual assistants such as Siri, also already integrated into a phone at purchase, operate according to speech recognition technology, developed by The Defense Advanced Research Projects Agency (DARPA) to create intelligent software assistants for military officers. Two of their most relevant programs are the "Harpy" a system able to understand 1,011 words developed by DARPA SUR (Speech Understanding Research) program[8] and "PAL" (Personalized Assistant that Learns), with CALO (Cognitive Assistant that Learns and Organizes) as one of the components, an artificial intelligence project which will be the precursor of one major spin-off: Apple iOS's Siri intelligent software assistant.[9]

Bluetooth, originally invented by Dr. Jaap Haartsen in the 1990s, follows in the footsteps of short-range radio communication, widely used by U.S. military for secure battlefield

---

[6] Mak, H. (2023). When was the GPS invented? The fascinating evolution of GPS technology. Global GPS Systems.

[7] OpenSystems Media. (n.d.). The Royal Air Force and the invention of the modern touchscreen - embedded computing design. Embedded Computing Design.

[8] Kikel, C. (2022). History of Voice Recognition Technology - Total Voice Technologies. Total Voice Technologies.

[9] Barnig, M. (2013). PAL : personalized assistant that learns | Internet with a Brain.

communication and encrypted signals, granted for by frequency-hopping spread spectrum (FHSS) transmission, a repeated switch of the carrier frequency during radio transmission to prevent interception and interference[10]. FHSS transmission is a fundamental feature of Bluetooth, thanks to its ability to avoid interference and resist jamming. Bluetooth is a commercial and moder application of short-range wireless technology.

Something else that we use daily, multiple times a day, is the internet. The U.S. Advanced Research Projects Agency Network (ARPANET) developed by DARPA is the precursor of the internet as we know it today. During the cold war, the US government wanted a secure and decentralized communication network, essential in case of any attacks, including nuclear ones. The initial concept was comprised of a dispersed communications network that would send messages via a system of switching nodes through computers until they arrived at their final destination. It was the first wide-area packet-switched network, connecting users over previously inconceivable distances, originally designed to ensure military bases and research institutions could stay connected.[11] ARPANET was later splint into MILNET, for military use, and a civilian network to avoid civilians getting access to the military line. This concept of message block switching served as the foundation for the architecture of the networks that would eventually make up the Internet[12].

Finally, cloud computing. Communication between networks outside and inside the US was made possible by the Transmission Control Protocol/Internet Protocol (TCP/IP) model, a standardized communication protocol developed by the Department of Defense in the 1970s, alongside the creation of ARPANET. Its main mission is to transfer the data of a computer from one device to another, originally developed for military purposes[13]. The TCP/IP protocol is now an indispensable part of daily life, powering everything from cloud computing to smartphones. It goes without saying that, without their military origins, most things that today we take for granted and are integral to our lives would not otherwise have existed.

However, this also means that we must regulate those technologies that have a dual nature to avoid their misuse.

1.3 Evolution of the (EU) regulatory framework

To ensure that dual-use technologies are not misused and avoid human rights violations, the European Union developed export control laws and regulations.

---

[10] Hanna, K. T., & Burke, J. (2021). Frequency-hopping spread spectrum (FHSS). Search Networking.
[11] Cloud computing history part 1: the origins of the cloud. (2022). Ascend Cloud Solutions.
[12] A brief history of the internet. (n.d.). Stanford Edu.
[13] GeeksforGeeks. (2025). TCP/IP model. GeeksforGeeks.

Export control finds its roots in the Wassenaar Arrangement, an international forum which addresses export restrictions for both conventional weapons and dual-use products and technologies, essential to global regulatory harmonization. The Wassenaar Arrangement's primary output is the extensive so-called "control lists," which act as a catalog of dual-use and military goods. Even though it is ultimately up to each participating state to determine at the national level whether to permit the transfer of controlled items in particular situations, the Arrangement has served as a basis for establishing guidelines for export control procedures, sharing information, and closing regulatory gaps among participating states.[14]

Starting from the 1990s, the EU started to develop controls on dual-use goods when they are subject to exports from the Community through a legislative framework regarding dual use exports and transit develop effective controls on dual-use goods. It first introduced the Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a community regime for the control of exports of dual-use goods[15].

Regulation 3381/94 is the foundation of all modern EU dual-use export controls, an important and needed first step towards the establishment of a common export control system. Before 1994, Member States had separate national export control systems for dual-use goods. The regulation introduced a requirement for export authorizations for certain dual-use items through an EU-wide export license for dual-use goods and established a common list of controlled goods in order to prevent the spread of weapons of mass destruction and limit the risk of dual-use items being used for military or terrorist purposes.

The 1994 regulation introduced a “catch-all mechanism” to control the export of unlisted dual-use items when there was reason to believe that they could be used as weapons of mass destruction or for military use. This control mechanism was established as an extra-security measure so that items not in the control list but of possible harmful end-use are considered dual use.[16]

However necessary, this first attempt at controlling the export of dual-use items presented loopholes, such as the lack of integrated regulation of some goods and relative enforcement, which is why a first update was introduced some years later, Council Regulation (EC) No 1334/2000, to strengthen the supranational power over the member states in relation to dual-use export controls. Other updates, in 2009, 2011 and 2016 followed, until the 2021 Recast was

[14] Kanetake, M. (2021). Dual-use export control: security and human rights challenges to multilateralism. In European Yearbook of International Economic Law 2020 (pp. 265-290). Cham: Springer International Publishing.
[15] Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods
[16] Control list, catch-all and technical assistance. (2023). Erhvervsstyrelsen Eksportkontrol.

introduced.[17]

The current key legislation governing export control of dual-use goods in the Union, Regulation (EU) 2021/821, sets up "a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items"[18].

The 2021 regulation or recast, an update of the original framework and its reviews, was developed to better adapt to the new technological and geopolitical needs we are currently facing and better comply with the demands made by Member States, which reflected a need to better harmonize national controls and respond to advances in technologies and cybersurveillance tools.[19]

The new framework enables the EU to take several significant and necessary steps, particularly in the areas of cyber-surveillance and emerging dual-use technologies. By enhancing the amount of reporting and consultation between Member States and the Commission, the regulation increases transparency and effectiveness[20]

In particular, the most important updates include: creating a mechanism for the exchange of information between member states' licensing authorities and enforcement agencies, cutting down on the time needed to process licensing applications, and enabling exporters to use cloud computing for the reduction of exporters' regulatory burdens and for the harmonization of national controls; and the introduction of a process for developing an EU list of controlled cybersurveillance goods, the introduction of further language in the preamble regarding human rights concerns, and the expansion of the catch-all mechanism for what regards cybersurveillance items control[21].

Indeed, the catch-all control mechanism, which was first introduced in 1994 and refined over the years and only applied to weapons of mass destruction and military end-uses, now includes cyber-surveillance technologies, emerging technologies and artificial intelligence, and enhanced due diligence for exporters.

It can be argued that the most important update of the recast, and the most relevant to today's concerns, is the strengthened control of emerging technologies such as AI and cloud computing to prevent them from being used for military or repressive purposes. The EU's dual-use export

[17] Walsh, E. P. (2004). Security shifts and power plays: the case of European Union dual-use export control regime development (Doctoral dissertation, University of Georgia).

[18] 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)

[19] Bromley, M., & Brockmann, K. (2021). Implementing the 2021 recast of the EU dual-use regulation: Challenges and opportunities.

[20] European Commission. (2021). Strengthened EU export control rules kick in.

[21] Bromley, M., & Brockmann, K. (2021). Implementing the 2021 recast of the EU dual-use regulation: Challenges and opportunities.

control list now includes artificial intelligence related technologies, however, even if an AI-related technology is not explicitly listed in the EU Dual-Use Control List, according to the updated catch-all mechanism it can still be subject to export controls if there is evidence that it could be destined for military use, human rights violations, or weapons of mass destruction related applications.

Due diligence is extremely important in this case, and its relevance is underlined heavily in the recast. Article 4 states "where an exporter is aware that dual-use items which he proposes to export, not listed in Annex I, are intended, in their entirety or in part, for any of the uses referred to in paragraph 1 of this Article, the exporter shall notify the competent authority. That competent authority shall decide whether or not to make the export concerned subject to authorization" and article 5 states: "an authorization shall be required for the export of cyber-surveillance items not listed in Annex I if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law".[22]

1.4 Latest developments

Since its entry into force, the implementation of Regulation (EU) 2021/821 has focused on harmonizing export controls across Member States, improving transparency and effectiveness and strengthening enforcement mechanisms. The 2025 Report from the European Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 provides a detailed assessment of the application and impact of the EU's dual-use export control regime. It is the first annual report prepared under the terms of the Regulation, prepared by the Commission with input gathered from Member States in the Dual-Use Coordination Group (DUCG)[23].

The report highlights the increase in transparency in export controls, with new data collection guidelines and enhanced reporting mechanisms for Member States, and; in light of the current shift in the geopolitical landscape, namely Russia's war of aggression against Ukraine and the conflict in the Middle East, which increased the need for stricter export controls on sensitive technologies, the strengthening of control over AI and surveillance exports due to human rights

[22] 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)

[23] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items

concerns[24].

The report provides an overview of developments relating to dual-use items in 2023 and 2024, including key data, updates to Annex I to the Regulation, export restrictions against Russia, and its international outreach, including partnerships with powers outside of the EU, such as the US, who is working with the Union trade facilitation and offered a strong basis for cooperation on Russia-related sanctions on the fourth meeting of the EU-US Trade and Technology Council.

Over the past years the EU has been discussing export controls in the context of the EU-US Trade and Technology Council (TTC). The TTC was created in 2021 to serve as a platform for the United States and the European Union to coordinate their approaches on tackling important global trade, economic, and technological issues. Their three main objectives are "advancing transatlantic cooperation on AI, 6G, critical and emerging technologies, promoting easier, more sustainable and more secure trade on the transatlantic market and defending human rights and values in a changing geopolitical digital environment" (EC).[25]

At their latest ministerial meeting, held in April 2024 in Leuven, Belgium, both parties reaffirmed a risk-based approach to AI, emphasizing the need of safe and trustworthy AI technologies. They are considering new due diligence obligations for cloud-based AI exports, a sign that the current dual-use export control framework may need to evolve, and that they could be a major part of it. As mentioned above, they recognize the geopolitical risks related to the export of AI surveillance technology and intend on expand the restrictions on cyber-surveillance tools to include emerging ai-powered tools.

Working Group 7, one of the ten working groups created by the TTC, primarily focuses on issues related to export controls, including that of dual-use items. It is part of the EU-US Trade and Technology Council Community on Futurium, a space where many actors, ranging from businesses to policymakers, can take part in the TTC discussions. In addition to exchanging information on risk assessments, licensing best practices, compliance and enforcement strategies, and convergent control approaches on sensitive dual-use technologies, the WG7 plans to conduct technical consultations on legislative and regulatory developments and conduct joint industry outreach on dual-use export controls.[26]

In their document "Input to EU-US Trade and Technology Council for Working Group 7 - Export Controls", the group highlight the need to strengthen risk assessment for dual-use technologies; expanding controls to early-stage R&D, engaging a broader set of stakeholders,

[24] Ibidem.
[25] EU-US Trade and Technology Council. (n.d.). European Commission.
[26] European Commission. (n.d.). Working Group 7 – Export control cooperation. Futurium.

like project leaders and researchers; develop human rights due diligence controls at the international level, integrating human rights risk assessments into export licensing; and engage with multilateral regimes, mostly the Wassenaar Arrangement, to strengthen AI and cloud computing controls internationally.[27]

Moreover, it is also worth mentioning the White Paper on Export Controls (COM(2024) 25 final), published by the European Commission in January of 2024 to address the need for more agile and effective EU export controls in light of growing geopolitical tensions and technological advancements.

Indeed, since the entry into force of the Dual-Use Regulation (Regulation (EU) 2021/821), the worldwide context for export controls has undergone a significant transformation, and unprecedented sanctions have been applied to Russia's war of aggression on Ukraine, including the prompt implementation of export controls on sensitive and dual-use goods. Moreover, there has been a surge of emerging technologies and thus, further national controls by some countries. Therefore, a Communication on a European Economic Security Strategy was adopted by the Commission and the High Representative (HRVP) on June 20, 2023, urging the EU to take swifter and more coordinated action to implement dual-use export controls and fully utilize the opportunities provided by the Dual-Use Regulation. The White Paper responds to that call.[28]

The document examines the current state of affairs and offers several recommendations to tackle the issues at hand. These include promoting consistent and efficient controls throughout the EU and initiating a dialogue with Member States, the European Parliament, and other stakeholders, including the business community, regarding the assessment of the Dual-Use Regulation's operation and the current framework's capacity to adequately address the EU's current and future security requirements.

The White Paper suggests a number of solutions to reduce the risks associated with Member States' national restrictions and to accomplish more swift and coordinated export control action at the EU level, including: ensuring the EU's uniform controls are maintained and strengthened broadening the EU list of dual-use items with items that have not been adopted by the multilateral export control regimes because of blockade by certain members (specifically Russia); creating a forum for export policy, given the geopolitical challenges, the Commission recommends creating a forum for political coordination between the Commission and Member States in order to promote shared EU ideas and plan and coordinate international action;

[27] Burkhard, S., Charatsis, C., Kanetake, M., Klein, R., Kolliarakis, G., Ladikas, M., & Whang, C. (2022). Input to EU-US Trade and Technology Council for Working Group 7-Export Controls. Multi-disciplinary Network of Experts.

[28] European Commission. (2024). White Paper on export controls (COM(2024) 25 final).

improved coordination of new national control lists, recommending that Member States must notify the Commission and each other of any new National Control Lists prior to their adoption and give them the opportunity to comment on the proposed list and voice concerns based on national security issues; and finally, moving the EU Dual-Use regulation evaluation forward: from the initial 2026–2028 timeframe to the first quarter of 2025 and doing so through the support of a study as well as engagements with member states and stakeholders.[29]

Following the publication of the 2024 White Paper on Export Controls, the European Commission has proposed several steps to enhance the effectiveness of the EU's export control system, including harmonizing export controls across Member States, establishing a political coordination forum, and advancing the review of the Dual-Use Regulation to address emerging technological and geopolitical challenges.[30] While these measures have not yet been formally adopted, they indicate a clear direction for future regulatory developments, particularly in the control of AI and cloud computing technologies.

The White Paper's primary goal is to assist in ensuring that EU member states adopt new export controls, especially those pertaining to emerging technologies, in a coordinated manner. If the proposed recommendations are followed through, the export of sensitive technologies could be effectively and safely managed.

In light of the Member States apprehension to restrict their control over their matters such as the control of exports, the proposed EU-level policy forum might be effective in achieving a middle ground between a safer Europe without compromising national sovereignty. The forum could promote consensus on delicate topics and link the various components of the EU's system for strategic trade controls, guaranteeing that EU-made weapons and technologies do not fall into the wrong hands, all-while strengthening the EU's capacity to accomplish its strategic goals and expand its influence globally.[31]

Following the 2024 White Paper on Export Controls, the European Commission published a second White Paper focused on enhancing support for research and development involving technologies with dual-use potential (COM(2024) 27 final). It calls for more options to improve the integration and cross-fertilization of dual use technologies in Europe, to better support innovation with dual-use applications, identifying opportunities under current or future EU

[29] Commission publishes White paper on Export Controls - ACQUIS. (2025, February 3).

[30] European Commission. (2024). Report on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (COM(2024) 22 final).

[31] A new political forum could help make the EU's strategic trade controls more strategic - if it is allowed to. (2024). SIPRI.

funding programs as well as important parameters that need more research. The paper argues for more funding to advance research and development of technologies with dual-use potential that can contribute to the creation of cutting-edge defense capabilities in the EU and proposes three different options to achieve such goal. The first one is building on the already existent legal framework but enhances coordination between civil and defense R&D by introducing improvements, including better communication, additional obligations and mechanisms. The second option goes beyond instruments and aims to create new EU-level funding mechanisms for dual-use tech including specific programs for startups, SMEs, and joint civil-defense projects. The last one is to create a dedicated instrument with a specific focus on R&D with dual-use potential, including an instrument dedicated to research with its own budget and rules, cross-program alignment with new flagship projects and overall a new legal or institutional set up. This is the most ambitious option, resulting in complexity for both the applicants and the Commission.[32]

1.5 Future challenges and opportunities

The regulation of dual-use exports is critical, many factors, such as security concerns, economic and national interests, and the fast development of technologies come into play, and the current geopolitical situation has not made things any easier. As this chapter has explored, many of the things we use daily, such as the internet, artificial intelligence and the cloud originated from military applications and were later adapted to civilian use applications. This ever-present dual nature brings into light the challenges in regulating the export of such items to avoid them being used for harmful and repressive purposes.

Over the past decades, the European Union has strengthened its export control framework, evolving from Council Regulation (EC) No 3381/94 to the current Regulation (EU) 2021/821 of the European Parliament and of the Council. The changes made in the recasts up until the latest developments have reflected the need of the Union to address any concerns that might arise from the export of AI and cloud computing technologies, especially in times of uncertainty such as the period we are living in today.

The European Union's concerns regarding dual-use technologies and need to effectively coordinate across member states and with international actors are also highlighted by the White Paper on Export Controls of 2024 and the creation of the EU-US Trade and Technology

[32] European Commission. (2024). White Paper on options for enhancing support for research and development involving technologies with dual-use potential (COM(2024) 27 final).

Council. However, many challenges still remain, and, as we will explore in later chapters, striking the right balance between security, trade, and innovation is not at all an easy task. As new dual-use technologies are consistently emerging, updating their export control is an ever-growing necessity, especially with regard to cybersurveillance technologies, AI regulation, and competitiveness and national control concerns. The future of export controls will be largely determined by how well the EU can coordinate this trade-off.

2. Innovation vs. security

2.1 Balancing scientific freedom and security

The "dual-use dilemma" is a popular concept in the scientific field to describe the duality of scientific research, born from the knowledge that discoveries regarding nuclear power could have both beneficial and harmful applications. The dual-use dilemma arises when a technology that benefits society can also be misused for harmful or military purposes. The ethical challenge is deciding where to draw the line between scientific freedom, innovation, and security risks.

When the same scientific work can be misused or used for good, the dilemma occurs, and it's not always clear how to stop such misuse without sacrificing useful applications. For instance, it happened when scientists recognized that atomic power could revolutionize the energy sector, but, at the same time, it could also lead to the production of weapons of mass destruction. New technologies led to the development of new weaponry and, subsequently, have allowed for the creation and development of weapons of mass destruction, including nuclear, chemical, and biological weapons; atomic bombs being one of the most notable.

The application of such dilemma is not limited to nuclear power; life science researchers today find themselves in the same predicament nuclear scientists did. Recent developments in biotechnology have plenty of benefits for an endless number of disciplines, including the medical one, however, they could also be used for repressive or terroristic purposes.[33]

The dual-use dilemma is an ethical one, and as such, it affects both the researcher and those who have the ability to support or obstruct the researcher's work. It is a moral matter since, when publishing someone's findings, there is the possibility of them being used to cause harm. It doesn't necessarily mean the researcher intends harm, but it turns into a dilemma because of the potential misuse of his findings by others. For instance, some notable examples of governments developing weapons of mass destructions include the use of mustard gas by the German and British armies during World War I (WW1) and the dropping of atomic bombs on Hiroshima and Nagasaki by the US Air Force during World War II (WW2). Governments are not the only agents employing scientific discoveries for harmful purposes, bioterrorism is a big threat, especially after the 11th of September 2001 attacks in the US.[34]

Recent discoveries have made the situation worse. Let's analyze the example of vaccine development, where genetic engineering techniques are employed to create recombinant viruses

[33] Atlas, R. M., & Dando, M. (2006). The dual-use dilemma for the life sciences: perspectives, conundrums, and global solutions. *Biosecurity and bioterrorism: biodefense strategy, practice, and science*, *4*(3), 276-286.

[34] Miller, S., & Selgelid, M. J. (2007). Ethical and philosophical consideration of the dual-use dilemma in the biological sciences. *Science and engineering ethics*, *13*, 523-580.

and infectious clones. There are two main methods for creating and molecularly cloning a viral genome: synthetic biology and traditional recombinant DNA techniques. Synthetic genomics, a rapidly evolving branch of synthetic biology, enables the rapid design and synthesis of both individual genes and entire viral genomes. While it has already shown promise in aiding in the development of the next generation of vaccinations, it also presents significant risks, particularly due to the lack of regulation stemming from limited understanding and oversight in the field.[35]

The above-mentioned risks could result in bioterrorism attacks. The genomics revolution has the potential to drive a new wave of biological program development, however, it could also enable the recreation of dangerous pathogens, enhance their virulence and transmissibility, and make them resistant to existing treatments. The accessibility of such tools raises concerns over the exploitation of this technology, highlighting the urgent need to strengthen biosecurity measures and ethical oversight.[36]

The ethical aspects of dual-use research, where scientific findings can be applied for both beneficial and harmful purposes, poses a significant dilemma between scientific freedom and security.

Scientific freedom is the freedom to conduct scientific research, acquire and use information, and communicate freely. Scientific research has long advocated for academic freedom, to serve the civil society with their findings and, in exchange, be awarded funding and institutional support. However, those focused on scientific freedom did not discuss the role of ethics and moral restriction in research. Indeed, the belief that conducting fundamental research absolved one of societal responsibility persisted even into the 1970s, when worries over the exploitation of human subjects in research, the creation of chemical agents for use in combat, and discussions regarding the usage of recombinant DNA surged. It was as if there was an unwritten rule where scientists conducting basic research were not responsible for considering the influence of their work on society. This idea was supported by the mid-20th century social contract for science, which rejects societal accountability for scientists under the idea of scientific freedom for basic research.[37]

The scientist is the ultimate master of force, the only one capable to learn from nature itself how to master it. Scientists are also servants, as in they serve science. As servants of science,

---

[35] Venter, J. C., Glass, J. I., Hutchison, C. A., & Vashee, S. (2022). Synthetic chromosomes, genomes, viruses, and cells. *Cell*, *185*(15), 2708-2724.

[36] Baric, R. (2007). Synthetic viral genomics: Risks and benefits for science and society.

[37] Douglas, H., & Branch, T. Y. (2024). The social contract for science and the value-free ideal. Synthese, 203(2), 40.

they realize that research must go on independently of its consequences: science allows for the evolvement of mankind and the consequent improvement of his quality of life, and inventors cannot put a stop to it. Therefore, as an innovator he has a responsibility towards progress, however, as a man, he also ought to protect nature.

When scientific discoveries have the potential to cause harm, whether through cyberwarfare, bioterrorism, or mass surveillance, the traditional social contract is challenged, raising fundamental ethical and policy questions. This calls for a consideration on where to draw the line between scientific freedom and security risks. There are two schools that debate on the topic: one advocates for innovation while the other for more stringent regulations.

Scientists, as mentioned, have a responsibility towards progress. They cannot hinder development, especially in respect to the duty they have towards future generations, since their actions and choices may have long-term effects on society. They have the duty of promoting societal advancement and tackling numerous international issues. This is because scientific knowledge, research and innovation can lead to significant and beneficial developments in a variety of fields, including technology, healthcare, and the environment. The demands and needs of society are an integral part of the scientific community's existence, and in turn it should contribute to its progress.[38]

Innovation is the process of creating, developing, and implementing new ideas, methods, products, or technologies that improve efficiency, effectiveness, or overall quality of life, often associated with scientific breakthroughs and technological advancements. Open science accelerates innovation by sharing knowledge, increasing collaboration, and reducing duplication of efforts.

Open Science is a movement that promotes transparency, accessibility, and collaboration in scientific research, it is an umbrella term that encompasses the concepts of Open Access, Open Data and Open Peer Review, based on the idea that open procedures and data exchange will promote scientific integrity, expedite scientific advancement, prevent the duplication of scientific work and resources, and increase openness. In short, it seeks to make scientific research freely available for everyone, including potentially harmful discoveries.

On the other hand, there is responsibility. The concept of responsibility is not new in science, scientific accountability lies in the correct application of scientific methods, the accurate report of results and the transparent dissemination of findings. But it is also commonly acknowledged that scientific responsibility goes beyond this and calls for taking the results and possible

[38] Rhodes, C. & Sulston, J. (2010) Scientific Responsibility and Development. The European Journal of Development Research. 22. 3-9.

ramifications of research into account. Moral considerations are often the basis for interpreting and determining such responsibilities. The research community has responsibilities to the public and decision-makers who shape the course and applications of science and technology. This is due to the fact that the scientific community is in a unique position to share the knowledge and information about the issues humanity is facing and their possible solutions, however, this information also faces the risk of being misused.[39]

Scientific freedom and security are heavily intricated and interconnected topics that can overlap at times. The freedom to share information that might result in breakthrough innovation, particularly the development of military technologies and mass destruction weapons, has strong ethical dilemmas that scientists and researchers must face when contributing to its creation. Morality and responsibility are dual-natured concepts that might be difficult to separate. This duality will most likely always be there, as it is difficult to define what is good and what is bad and impossible to do so when there are so many factors that come into play, however, there are ways to limit the spread of potential harmful products and research.

The very core principles of open science, while essential to progress, clash with export control regimes that seek to restrict the diffusion of sensitive knowledge. Governments are currently facing the difficult task of deciding what should be openly shared and what should be protected in the name of national and global security.

Over the past forty years, export restrictions have extended their authority to include knowledge and information, after initially limiting the movement of solely physical goods. This is especially relevant today as new technologies are emerging, and ideas and code can cross borders as easily as other products.

2.2 Human rights concerns

In the current digital age, the essential human right to privacy has faced serious obstacles, as well as freedom of expression, revolutionized by social media, blogs, forums, and other online spaces, The digital age has drastically changed the human rights landscape by providing previously unheard-of chances for democratic involvement, information access, and expression. Nevertheless, there are serious drawbacks to these developments, such as concerns about mass spying, the spread of misleading information, and the erosion of privacy.[40]

[39] Rhodes, C. & Sulston, J. (2010) Scientific Responsibility and Development. The European Journal of Development Research. 22. 3-9.

[40] Siddiqui, S. Y., Farooqi, S., & Zulfiqar, L. (2024). Human Rights for the Digital Age. arXiv preprint arXiv:2408.17302.

Indeed, the dual-use dilemma is not limited to biotechnology and synthetic biology, its scope goes way beyond that. We cannot talk about recent developments without mentioning artificial intelligence, one of the most powerful and transformative dual-use technologies. While it has revolutionized medicine, industry, and cybersecurity, AI also presents serious and harmful consequences if misused.

2.2.1 Artificial Intelligence

Artificial intelligence is amongst the most important and talked about dual-use technologies being innovated right now, and, as such, it is as much a tool as it is a threat. Apart from the fact it can be misleading by providing inaccurate information and could replace the workforce in many industries, it presents several security and human right concerns. The employment of AI weaponry without human intervention; problems with AI vulnerabilities in cyber security; intellectual property issues; privacy and data protection issues and the targeting of political messaging on social media are just some of the examples of the risks it brings upon, not including racial and gender bias.[41] Indeed, AI systems can perpetuate existing biases, leading to discriminatory outcomes in areas like hiring and criminal justice.

Significant socio-ethical issues brought up by AI systems in recent years, including discrimination, unwarranted action, and the impact of automation on the labor market, have demonstrated that this technology directly affects people's basic human rights.[42]

Basic human rights such as freedom of expression and freedom of opinion are at risk when employing such technologies. Algorithms for content moderation, AI programs that examine social media posts and identify which publications have to be removed, may mistakenly remove some types of legitimate and lawful expression more frequently than human content moderators might, meaning they are likely to have a negative effect on freedom of expression. Moreover, the majority of the time AI systems have trouble recognizing and comprehending irony and comedy, which makes their detrimental effects on free speech in terms of employment practices and content regulation much worse. Freedom of association is at risk as well, since people nowadays worry about posting or being posted attending a protest, for example.[43]

Artificial Intelligence also presents several transparency and accountability concerns, AI

[41] Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology, 4, 100005.

[42] Aizenberg, E., & Van Den Hoven, J. (2020). Designing for human rights in AI. Big Data & Society, 7(2), 2053951720949566.

[43] Gaumond, E., & Régis, C. (2023). Assessing Impacts of AI on Human Rights: It's Not Solely About Privacy and Nondiscrimination. Lawfare Media. Friday, January, 27, 8.

systems are in fact often compared to "black boxes" with mysterious internal workings that humans cannot understand, sometimes even the creators of such technologies. This means that accountability is severely hampered by AI systems' lack of explainability and transparency.[44]
The widespread use of AI-powered monitoring techniques, including cybersurveillance, discourages civil society participation in online debates, activism, and protests. This atmosphere of dread undermines democratic participation and freedom of assembly by disproportionately affecting vulnerable groups, including political dissidents, refugees, and ethnic minorities.

2.2.2 Cybersurveillance

Cybersurveillance items, as defined in article 2(20) of Regulation (EU) 2021/821 are "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analyzing data from information and telecommunication systems."[45]
They have a dual nature because they can be used for both legitimate and harmful purposes. While they can be utilized for cybersecurity, including lawful investigations and anti-fraud tools, they can equally be weaponized for illegitimate monitoring and repression, including for suppressing political opposition and mass data interference. This raises significant human rights concerns, particularly regarding privacy, freedom of expression, and protection from unlawful surveillance.
Such surveillance can deter individuals from freely expressing themselves, especially when they fear monitoring by authorities, and violation of their privacy when there is lack of consent to be monitored. Indeed, the deployment of surveillance technologies often occurs without public oversight, raising concerns about misuse; for instance, surveillance technologies that have been employed to monitor and suppress minority populations, such as the case of China.
The Xinjiang Uyghur Autonomous Region in the territory of East Turkistan, where approximately 11 million Uighurs and other Muslim minorities live, is an autonomous region in China's northwest that has been under Chinese control since 1949, with the establishment of the People's Republic of China. The region has been under strong scrutiny since the inhabitant protested their treatment by the government, People's Republic of China (PRC) in 2009 with riots. China uses technology extensively and strategically, subjecting Uyghurs to harsh monitoring and repression methods, through information and communication technologies

[44] Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. Frontiers in Human Dynamics, 6, 1421273.
[45] 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)

(ICTs), they are continuously subjected to China's gaze, even if they flee the region. East Turkestan's social and cultural life was reduced because of this high-tech repression: the pervasive placement of cameras on the streets, police searches at residences, mandatory GPS installation on cameras, and ongoing phone checks on the streets all significantly discourage people from congregating and engaging in political and religious discourse. While Uyghurs who flee to Turkey experience a greater degree of freedom, that China uses ICTs to carry out widespread repression against them by preventing them from communicating with their family members back home and exposing them to ongoing harassment and intimidation by the Chinese police, mostly through social media.[46]

Digital transnational repression is a growing trend which occurs when governments use digital technologies to carry out practices of repression against targeted individuals who have left their home country, willingly or by seeking safety and protection elsewhere, but continue to have strong critical opinions about its administration and show such dissent. Due to the flexibility, adaptability, and closeness of digital technologies, which include spyware, online harassment, and disinformation operations on social media, targeted individuals no longer feel safe expressing their views. Such self-censorship has severe impacts, including social isolation, withdrawal from advocacy work and ability to be resettled in the host state.[47]

Recently, the United States has added two Chinese companies to a trade restriction list for enabling abuses of human rights, such as sophisticated surveillance directed at Uyghurs and members of other ethnic and religious minorities, making the targeted companies' American suppliers seek a license that is very difficult to obtain before exporting to them, making such export nearly impossible.[48]

The EU–US Privacy Shield is a key example of how data protection, human rights, and international technology governance intersect. It is a framework for transatlantic data flows established by the European Commission and the United States, created to allow companies to legally transfer personal data from the EU to the US, in compliance with the EU's General Data Protection Regulation (GDPR). It is also known as Schrems II, replacing the earlier Safe Harbor Agreement, which was invalidated by the Schrems I case. In July of 2020, the CJEU invalidated the EU-US Privacy Shield in the Schrems II judgment, the Court ruled that the U.S. surveillance regime, specifically Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, did not offer guarantees equivalent to those required by EU law,

[46] Oztig, L. I., & Karluk, A. C. (n.d.). China's High-Tech Repression Against Uyghurs: Novel Theoretical Insights.
[47] Anstis, S. & Deibert, R.J. (2025) Silenced by Surveillance: The Impacts of Digital Transnational Repression on Journalists, Human Rights Defenders, and Dissidents in Exile, 25-05 Knight First Amend. Inst.
[48] Alper, A. (2024). U.S. imposes trade restrictions on two Chinese firms over human rights. Reuters.

particularly in relation to the protection of personal data and the absence of effective remedies for EU citizens.[49]

As a result, in 2023, the Commission adopted the new EU–US Data Privacy Framework (DPF) to support transatlantic trade by giving American businesses trustworthy ways to move personal information to the US from the EU/EEA, but also the UK (including Gibraltar), and Switzerland, abiding EU, UK, and Swiss law.[50]

The EU-U.S. Data Privacy Framework introduces new legally binding safeguards, including the establishment of a Data Protection Review Court (DPRC), to which EU citizens will have access, and restricting access to EU data by US intelligence services to that which is necessary and proportionate. This is a big improvement from the previous Privacy Shield. For instance, the DPRC will have the authority to order the destruction of data if it discovers that it was gathered in contravention of the new protections. Moreover, US companies importing data from the EU will be subject to additional obligations in addition to the new safeguards on government access to data.[51]

We cannot talk about data protection and human rights issues without mentioning one of the most emblematic cases of surveillance misuse, the Pegasus spyware, developed by the Israeli company NSO Group. A spyware is a malicious software that infiltrates a user's computer, collects information about the user, and then transfers it to outside parties without its permission.[52] Pegasus is a modular malware that can perform complete surveillance on the device it targets. It installs the modules it needs to read the user's mail and messages, listen to calls, transmit back the browsing history, and more, even accessing encrypted text and audio files on your smartphone. Promoted as a legitimate interception tool for criminal investigations and counterterrorism, it has been revealed by investigative reports that multiple nations, including European governments, were abusing it to target political dissidents, journalists, human rights advocates, lawyers, and even EU officials.[53]

In response to such claims, the European Parliament has set up a Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA) in 2022. In 2023, the European Parliament adopted its final report; its recommendations include: forming a

[49] Court of Justice of the European Union. (2020). Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Schrems II), Case C-311/18.
[50] U.S. Department of Commerce. (n.d.). EU-U.S. Data Privacy Framework: Program overview. Data Privacy Framework.
[51] European Commission. (2023). Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.
[52] Fortinet. (n.d.). Spyware. Fortinet CyberGlossary.
[53] Chawla, A. (2021). Pegasus spyware–'A privacy killer'.

special taskforce comprising national electoral commissions to safeguard the 2024 European elections throughout the Union; looking into and documenting any inadequacies in the application and enforcement of pertinent Union laws and present a plan to address them by no later than August 1, 2023; establishing an EU Tech Lab, establishing an autonomous European interdisciplinary research institute, and focus on research and development at the intersection of information and communication technology, basic rights, and security; ensuring that its rule of law toolbox is implemented effectively, including information about spyware use in its Annual Rule of Law Report; carry out a thorough investigation into the export licenses granted for spyware use, share the findings with the Parliament; and swiftly present legislative proposals based on this recommendation.[54]

Implementation is still scarce even after these suggestions were adopted. The PEGA report has not yet resulted in any binding legislation being proposed by the European Commission, and a number of Member States have been hesitant to act, frequently claiming national security concerns. To guarantee accountability and defend fundamental rights within the EU, civil society organizations and human rights campaigners maintain their pressure for more forceful action. [55]

Cybersurveillance, in light of the fast development of emerging technologies and the discourse around dual use, is one of the most pressing issues we are facing today, especially for policymakers. A formal recommendation on internal compliance programs (ICPs) for businesses exporting cyber-surveillance technologies was released by the European Commission in October 2024 (EU C(2024)7035 final). The recommendations are intended to further assist exporters in putting Regulation (EU) 2021/821's human rights protections into practice, especially Article 5, which introduces human rights as a ground for export restrictions, specifically in the case of cybersurveillance technologies. Article 5 is especially important because it recognizes human rights concerns as a separate basis for approving or prohibiting the export of cyber-surveillance equipment and extends to non-listed technology as well, giving Member States the authority to step in where there is a significant risk of internal repression through misuse. The report on recommendations advises exporters to evaluate end-use and end-users, perform human rights due diligence, and include red flag indicators in their risk

[54] European Parliament. (2024). The Pegasus spyware scandal and its implications for the EU (Briefing No. 761472). Directorate-General for Internal Policies.

[55] Digital Frontlines. (2025). Spyware regulation: European Commission slow to act on Parliament's call for reform.

assessment.[56]

This document, and all of the other steps mentioned above, reflect the EU's growing understanding that ethical responsibility and technical control are equally important in the administration of dual use technologies.

2.3 Differences between EU and US approaches to export controls

The US and Western European countries founded the North Atlantic Treaty Organization (NATO) following World War II, and established trade restrictions to support their national security objectives. This led to the establishment of the current domestic export control systems. Both military-use and dual-use products and technologies were included in such export controls, but in order to be more specific and fulfill security concerns without hindering economic development, the controls have been aimed at goods and technologies that have more of military than commercial application.[57]

The United States' export controls are currently under the regime of the Export Control Reform Act of 2018, or ECRA, a federal law that provides the statutory authority for regulating the export, re-export, and transfer of dual-use items, emerging technologies, and foundational technologies that are critical to U.S. national security and foreign policy interests.

The United States regulates the export of dual-use items through the Export Administration Regulations (EAR), which derive their legal authority from the ECRA. The EAR, administered by the Bureau of Industry and Security (BIS), governs the licensing and control of dual-use goods and less sensitive military items listed on the Commerce Control List (CCL). The CCL categorizes items based on their nature and the reasons for control, such as national security, anti-terrorism, and non-proliferation.

Emerging or foundational technologies chosen for control will thus be governed by the same regulations as other items now on the CCL, since ECRA serves as an addition to the EAR. Accordingly, ECRA applies to US-based businesses as well as any company anywhere that is re-exporting American goods or technology; incorporating technology previously exported from the US; and by persons subject to the jurisdiction of the United States for a given regulated technology. Consequently, if a product's use of controlled technology or USA-sourced components surpasses a specific level (%), even non-US-made goods may be subject to

[56] European Commission. (2024). Commission Recommendation (EU) C(2024)7035 final of 24 October 2024 on internal compliance programmes for the export of cyber-surveillance items under Regulation (EU) 2021/821.

[57] Whang, C. (2021). Trade and emerging technologies: A comparative analysis of the United States and the European Union dual-use export control regulations. Security and Human Rights, 31(1-4), 11-34.

ECRA.[58]

ECRA did not, however, explicitly outline the criteria and components for identifying emerging and foundational technologies, and the national security need's context differed somewhat from the conventional military-focused national security issues. When discussing the necessity for the US to continue to lead the world in manufacturing and science in order to remain competitive in global markets, ECRA's focus on national security has broadened to include economic issues.[59] This underlines the nations prevailing economic interests.

There is another legal framework for regulating US exports, the International Traffic in Arms Regulations (ITAR), however, while both ITAR and ECRA regulate exports from the United States, ITAR targets strictly military technologies, whereas ECRA and the EAR regulate dual-use and commercial items that may still pose national security risks.

Since the goals of the dual-use export control system have broadened to encompass factors other than national security, ECRA and Regulation (EU) 2021/821 on export controls represented this change in policy. As the policy objectives of dual-use export controls evolve, the US and EU are diverging in their approaches to control lists, enforcement priorities, and regulatory scope. Moreover, control of new emerging technologies is becoming more difficult to define as military and civilian technologies grow less distinct from one another. This will allow for observable distinctions between the two distinct export control regimes.[60]

The US and EU export controls on dual-use items differ in many ways. Firstly, structural differences: while the US operates a unified export control system, the EU's system is multi-level, while its legislation is formulated at Union level, it is implemented by individual member states. Secondly, policy objectives: both systems aim to prevent the proliferation of dual-use technologies that could threaten international security, however, it has been greatly debated that the US' controls are heavily influenced by economic factors and foreign policy interests, while EU export controls are focused mostly on non-proliferation and the harmonization of internal market principles. Third, control lists: the US utilizes the Commerce Control List (CCL), which is updated annually and categorizes items based on their nature and the reasons for control, which is more extensive than the European list because it includes items beyond those listed in multilateral regimes, while the EU utilizes a dual-use list, also updated annually, and based on the regimes' control lists. Fourth, enforcement mechanisms: the US employs a centralized enforcement mechanism using legal measures such as fines and prison sentences for violations,

[58] Lazarou, E. (2019). United States: Export Control Reform Act (ECRA).

[59] Whang, C. (2021). Trade and emerging technologies: A comparative analysis of the United States and the European Union dual-use export control regulations. Security and Human Rights, 31(1-4), 11-34.

[60] Ibidem

while in the EU enforcement fall exclusively on member states, who employ different enforcement practices, which results in a weaker system. Lastly, transatlantic cooperation: the Trade and Technology Council (TTC) is the platform for US-EU cooperation on export controls, which enabled consistent collaboration between them, however, there are still many challenges, including trade restrictions on countries like Russia and addressing technology transfers to China.[61]

The historical, political, and economic history of the EU and the US has resulted in the development of their export control regimes. The only similarity between the two is that they both utilize balancing exercises to coordinate the economic and security interests of a state and its internal market, as well as those of other governments against whom controlled goods may be deployed. Exporters worldwide must become familiar with the compliance requirements, relevant export control legislation in the client state, and the establishment of efficient compliance procedures for both. This complexity is reciprocal: while European exporters must keep up with the ongoing restructuring of the US export control system, US exporters should find and adhere to the applicable European regulations and the laws of the Member States.[62]

Although limiting the exploitation of dual-use technologies is the shared goal of the US and the EU, their regulatory measures reflect their differences in political priorities, governance models, and economic ideologies. Closing these gaps will be necessary for efficient worldwide coordination as new technologies like artificial intelligence and cloud computing make it harder to distinguish between military and civilian applications. Apart from being strong and risk-based, future export control regimes must be adaptable enough to keep up with technological advancements and uniform enough to prevent legal fragmentation that can jeopardize competitiveness or security.

The approaches they employ are different: each model represents a different vision of how to secure innovation, either through openness or through control. The European Union adopts a more research-friendly and ethics-based approach, allowing innovation to flourish under a regulated but open model, while the United States takes a more strategic and security-driven stance, seeking to safeguard its technological leadership.

Indeed, the goal of the US is security: to establish itself in a leading position rather than just maintain a competitive advantage in important technology domains. The imposition of too broad export controls might give competitors such as Chinese companies market dominance so

[61] Bromley, M., & Brockmann, K. (2024). A Tale of Two Systems: Alignment, Divergence and Coordination in EU and US Dual-use Export Controls. Istituto Affari Internazionali (IAI).

[62] Alavi, H., & Khamichonak, T. (2017). EU and US export control regimes for dual use goods: An overview of existing frameworks. Romanian J. Eur. Aff., 17, 59.

they can lower prices and take over the market. In order to guarantee that export controls are both efficient and do not jeopardize important economic policy goals, the US must work closely with its international allies.[63]

So, it can be argued that the United States is innovation driven, but in a national security way, in the sense that it wants to lead the development of foundational technologies and protect its innovation base from being leveraged by strategic rivals, adopting a protectionism approach. Its goal is to secure technological dominance, not through openness, but through controlled access, especially in dual-use and emerging technologies, so it uses strict, targeted export controls as a tool to preserve or gain leadership in key technological domains. This is not the same as fostering a globally open, collaborative, or science-first model of innovation, which in turn the EU leans toward.

For the European Union, innovation is the goal, and security is the condition. It fosters innovation by prioritizing regulatory transparency, scientific openness, and an ethical-based approach and its goal is to stop dual-use technology abuse without restricting commercial or scientific activities by enabling innovation to flourish within a regulated yet open environment. Even though this might result in slower implementation, it guarantees that export regulations are consistent with democratic norms and risks.

Indeed, the EU's dual-use export control framework reflects a more research-friendly and ethics-oriented regulatory approach by recognizing the particular difficulties faced by academic institutions and highlighting the significance of maintaining academic freedom and the free flow of knowledge.[64]

Each model reflects a distinct vision of how to secure innovation, either through openness or through control: the US places security at the center and fosters innovation as a tool of strategic dominance, while the EU promotes innovation as a value in itself and seeks to facilitate it through transparency, multilateralism, and ethical safeguards. Thus, it can be argued that both models are innovation-oriented, but only one treats innovation as the end rather than the means. In the end, the differences between these two regimes highlight a more profound philosophical dilemma: how to regulate innovation at a time of geopolitical uncertainty. In addition to balancing these two paradigms, the future of dual-use regulation may depend on the development of a common transatlantic strategy that balances transparency, ethical oversight,

[63] Bauer, M., & Pandya, D. (2024). Time to rethink export controls for strengthened US-EU cooperation and global trade rules (No. 07/2024). ECIPE Policy Brief.

[64] Stalenhoef, C., Kanetake, M., & van der Wende, M. (2022). The implications of the EU's dual-use export control regulation 2021/821 for universities and academics. Utrecht University School of Law Research Paper Forthcoming.

and technological sovereignty.

2.4 The conflict between Russia and Ukraine

Following the Russian invasion of Ukraine in 2022, the differences between the export control systems of the US and the EU became even more apparent. Both countries quickly increased their export control and sanctions in reaction to the crisis, focusing on a variety of military and dual-use technologies, such as semiconductors, drones, artificial intelligence components, and cybersecurity tools. The United States sanctioned hundreds of Russian companies and strictly prohibited the sale of sensitive technologies bound for Russia, while the European Union slowly but effectively adopted punishment packages that included dual-use bans and incorporated clauses addressing the use of surveillance technologies in human rights abuses.

Exporting goods to Russia and complying with export control regulations have become extremely difficult for EU exporters in the current political climate. In addition to dual-use items, other items included on prohibition lists are also prohibited from being exported from the EU to Russia, for instance goods that may contribute to expanding the industrial potential of the country. One of the powerful instruments that has severely undermined Russia's economic and military potential is this EU's restriction on exporting commodities to the country. Despite being put in place to restrict Russia's capacity to fund the conflict and to impose actual political and economic costs on the country's invading individuals, it also became a significant obstacle to EU business ventures, resulting in a decline in their revenue and, in certain situations, their bankruptcy.[65]

The Yermak-McFaul Expert Group, or International Working Group on Russian Sanctions, is an independent advisory body composed of a group of experts that provide experience and guidance on how to increase the effectiveness of sanctions imposed on Russia following its full invasion of Ukraine. Their findings show that Russia has not been able to find substitutes for many items it used to import from coalition countries, including electronics, indicating that export constraints still have the fundamental potential to drastically reduce Russia's capacity to carry out its aggressive campaign against Ukraine. However, it is still able to import significant quantities of materials required for military production. This means that, to increase their effectiveness, significant adjustments must be made to the current enforcement strategy, including strengthening corporate responsibility, filling the gaps in export control policies,

[65] Gwardzińska, E., & Chackiewicz, M. (2023). A Ban on the Export of EU Goods to Russia. Humanities and Social Sciences, 30(2), 27-35.

focusing on third-country evasion, and fostering international collaboration.[66]

Indeed, despite a shared commitment to weakening Russia's military-industrial base, transatlantic coordination has suffered from legal systems and enforcement capabilities. This lack of harmonization creates loopholes that can be used as an advantage by Russia through third-party intermediaries.

By enacting 16 rounds of restrictive measures aimed at increasing pressure on Russia's leadership and economy, the European Union has reiterated its sanctions policy toward the country, the latest of which was adopted in February 2025. These measures broaden the scope of trade restrictions against Russia. The Commission has also revised its non-binding guidelines, including updates on the so-called "no-Russia clause", a provision introduced by the EU which requires EU exporters to include contractual obligations in their trade agreements with non-EU third parties stating that the goods or technologies they are delivering must not be re-exported to Russia or used in Russia. These sanctions packages, particularly its 16th package, demonstrate the EU's ongoing commitment to applying pressure on Russia at a time when the overall future of the international sanctions regime targeting Russia is uncertain.[67]

This represents the EU's efforts to close the backdoors and loopholes that Russia uses to obtain sensitive and dual-use commodities through middlemen, give EU businesses more accountability for the products' further uses and improve enforcement.

In response to Russia's invasion of Ukraine, the United States imposed an unprecedented set of sanctions and export bans on the attacker. It has expanded its use of targeted financial and trade restrictions through the SDN, the Specially Designated Nationals list maintained by the US Department of the Treasury's Office of Foreign Assets Control (OFAC) and Entity List maintained by the Department of Commerce's Bureau of Industry and Security (BIS), which restrict access to capital and technology to individuals and organizations deemed a threat to national security or foreign policy interests. Additionally, two new Foreign Direct Product (FDP) regulations, US export control tools under the EAR, were developed to regulate multi-step manufacturing and expand the scope of US export prohibitions, immediately targeting a wide range of luxury and dual-use goods, allowing the States to extend their export control jurisdiction extraterritorially if they are produced using the States' technology or software.[68]

---

[66] Bilousova, O., Hilgenstock, B., Ribakova, E., Shapoval, N., Vlasyuk, A., & Vlasiuk, V. (2024). Challenges of export controls enforcement: how Russia continues to import components for its military production.

[67] Latest EU sanctions extend asset freezes, restrict oil industry dealings and target 'Shadow fleet.' (2025). Insights | Skadden, Arps, Slate, Meagher & Flom LLP.

[68] Red flags in real cases: enforcement and evasion of Russia sanctions. (2023). Wisconsin Project on Nuclear Arms Control.

Depriving Russia of electronics, materials, and sub-components required by the Russian defense, aerospace, and maritime industries and crucial to its war strategy and effectiveness was the main goal behind the efforts mentioned above. But a secondary aim was to target the ways of life of the Russian elite who backed and benefited from the conflict.[69]

This showcases the US is closely aligned with the EU on export controls. However, there is growing uncertainty about the future direction of US foreign policy in general and toward Russia, especially in light of recent political changes in the United States.

The Trump administration's recent actions suggest that the US export control system may become more stringent. Proposed regulations would target cloud-based access and AI model weights, which are inputs essential to algorithmic success, in addition to tightening limitations on chips. These actions would usher in a new era of innovation securitization, further obfuscating the distinction between national defense and economic policy. Although the stringent regulations are intended to slow China's technological advancement, U.S. tech companies are also concerned about losing market share globally and compromising the innovation ecosystem that the controls are meant to safeguard.[70]

For what regards Russia, the Trump administration has considered the possibility of easing certain sanctions on Russia as part of broader diplomatic negotiations, however, it has not yet imposed any new export restrictions or penalties on Russia, but it has upheld the current sanctions system against the country. Because of the already restricted trade brought about by these sanctions, the emphasis has been on using existing restrictions in diplomatic efforts and keeping Russia out of larger tariff measures.

What is believed to be the main problem why the sanctions on Russia are not working as well as they should is the re-export of goods through third countries or shell companies. This indicates the urgent necessity to extend monitoring and compliance outside the alliance borders. The G7's Export Enforcement Coordination Mechanism (EECM) has issued a document to help industries identify and mitigate risks associated with the evasion of export controls and sanctions by Russia. It provides a list of items, the Common High Priority List, that are crucial to Russia's military efforts are more likely to be illegally diverted to Russia, red flags indicators regarding possible evasion of sanctions and export control to watch out for, best practices, measures that businesses might take to resolve the red flags that have been discovered, like putting in place strong compliance systems, carrying out exhaustive due diligence on partners and clients, and making sure that products are properly verified at the end of use, and finally

[69] Ibidem.

[70] Hawkins, A. & Mui, C. (2025, March 20). Commerce weighs crackdown on export controls. Politico Pro.

additional resources to help businesses.[71]

The US Departments of Justice, Commerce, and the Treasury have jointly published a similar document that describes how Russian companies use third-party middlemen to get around export restrictions and sanctions, frequently hiding the real identities of end consumers, and also offers a list of typical warning signs that could point to attempts to get around export restrictions or sanctions, include using shell corporations, being reluctant to disclose end-use information, and sending shipments through unusual jurisdictions. The paper highlights the importance of strong compliance systems, including management commitment, risk assessment, internal controls, testing, auditing, and training and provides sources for voluntary self-disclosure.[72]

An investigation has found that since the invasion 450 parts of Russian weapon systems were manufactured by international companies. The researchers from the Royal United Services Institute who carried out the analysis found that US corporations produced an high number of these: 318. The fact that 18% of these goods are governed by export restrictions is even more startling.[73]

If the above-mentioned illicit action by Russia continues, it will continue to be extremely challenging to enforce provisions to stop exports. Another problem is posed by the rapid evolvement of AI systems, and the concern export controls on such items brings on, especially in light of the innovation vs. security debate.

Since the development of emerging technologies is so new and is moving at such rapid pace, loopholes can be found in the current legal framework. For instance, physical copies of the chips are not necessary to make them perform their tasks, the location of computer hardware is abstracted away by cloud computing, use cloud-based servers can be used train an AI model. This is to say that when technologies can be used remotely, regulations that try to stop a nation from physically obtaining those chips are ineffective and, sometimes, useless.[74]

It is necessary to strengthen export control measures to balance security concerns with the promotion of innovation and legitimate trade.

In conclusion, the difficulties brought to light by the Russian invasion highlight the need for a

---

[71] European Commission. (2024). Preventing Russian export control and sanctions evasion: Updated guidance for industry.

[72] U.S. Department of Justice, U.S. Department of Commerce, & U.S. Department of the Treasury. (2023). Tri-seal compliance note: Cracking down on third-party intermediaries used to evade Russia-related sanctions and export controls.

[73] Woods, C. (2024). Maximizing Defense Innovation While Holding the Line on Export Controls: What the Defense Sector Can Learn from Global Banks.

[74] Villasenor, J. (2024). The tension between AI export control and U.S. AI innovation.

more careful design of export controls to prevent hindering innovation or interfering with lawful commercial activity. This calls for a sophisticated strategy that balances security with international collaboration without blocking technological advancement.

3. Expert Insights ahead of the review of the dual use regulation

The primary ethical and regulatory conflicts that exist within the current dual-use export control regime were examined in the second chapter, with special attention to new technologies like artificial intelligence and cybersurveillance techniques. There was a clear disparity between the US and EU approaches, as well as a conflict between advancing innovation and safeguarding human rights and national security. The geopolitical ramifications of recent crises, such the Russian Ukrainian conflict, which have forced control regimes to upgrade more quickly, also reflect these problems.

After having reviewed the relevant legislation and ethical concerns the export of dual use technology presents, to gain further insights on the topic and on the possibility of finding a solution to the problems mentioned above, I decided to ask experts in different types of fields, both public and private their opinion on the topics proposed.

Such interviews, which investigated the strategic, ethical, and regulatory aspects of dual-use technology in light of new issues including artificial intelligence, cyber-surveillance, and geopolitical instability, were essential in deepening the theoretical and legal analysis established in earlier chapters and brought to light further points of discussion.

Moreover, they provided realistic, experience-based viewpoints on the challenges and opportunities of a new recast of the legislation, which were essential in understanding the real necessities of further regulatory interventions. The insights from the interviews are complemented by the info gathered in the stakeholder consultation on the White paper and other institutional documents published by dual use expert or international actors.

3.1 Methodology

To get in-depth knowledge from professionals working in pertinent fields, such as international law, export compliance, human rights, cybersecurity, and EU policies, a qualitative, semi-structured interviewing technique was used. Interviewees were able to articulate complex opinions and critically consider changing geopolitical and regulatory dynamics thanks to the use of open-ended questions. Furthermore, they were offered the possibility of anonymity if they preferred.

3.1.1 Participant selection

Participants were selected through a combination of expert identification and recommendations by other interviewees. Academic publications, institutional connections, and professional

expertise in dual use items, technology regulation, and international trade compliance were taken into consideration. Four experts participated in the study:

Riccardo Cima, Senior Consultant in Deloitte's Global Trade Advisory team, specializing in international trade policy, sanctions, and export compliance.

Marcello Irlando, Senior Technical Officer at the Italian Ministry of Foreign Affairs (Ministero degli Affari Esteri e della Cooperazione Internazionale – MAECI), involved in technical diplomacy and export regulation.

Carlo Fronduti, Integrated Management Systems Compliance and Risk Management Engineer at ENAV, with experience in corporate compliance frameworks and risk mitigation strategies.

Davide Lagni, trainee in the International Sanctions & Export Controls division at Airbus, with hands-on legal experience in managing compliance with EU and global trade restrictions.

These experts provide a fair and practical perspective on the ethical and regulatory issues pertaining to dual-use technology by contributing personal, institutional, corporate, and global views to the study.

3.1.2 Interview themes

Four main issues served as the framework for the interviews:

- Dual-use innovation and the ethical issues it presents.
- Human rights in cyber-surveillance technology regulation.
- Differences in export control systems across the Atlantic.
- The conflict between Russia and Ukraine and the efficiency of export regulations.

3.1.3 Data collection and result of interviews

All interviewees were informed of the purpose of the research and their rights regarding anonymity and data protection. Interviews were conducted between March and May of 2025, either in person or via video conferencing platforms, and notes were taken regarding their answers to the questions with the consent of the participants.

The result of the interviews can be found at the Annex below. In line with the results of the interviews, at the EU-level there have been demands for a recast of the dual use regulation that is better able to respond to the technological transition and the current geopolitical climate, its most relevant stakeholder insights can also be found in the Annex in section B.

3.2 Dual-use innovation and the ethical issues it presents

The ethical issues brought about by dual-use goods is one of the most pressing themes of our time. The interviews and stakeholder consultations underline how difficult it is to navigate this topic, and how making ethical decisions in dual-use research involves several actors and duties. Personally, I believe ethics is the foundation of the dual-use doctrine, and, more generally, of how we function as human beings: without ethics, we would live in chaos. I agree with Irlando that decisions should be taken according to one's moral conscience, however, when we are talking about sensitive information, there is a need for external guidance.

Ethical responsibility is a shared one, between the innovator and the regulator. While researchers cannot be held accountable for the application by third parties of their discoveries, they also must account for the potential misuse of their findings, and the dangers it might entail, especially given today's political climate. Seeing how technologies are developing more quickly than legal frameworks, I agree with Lagni (Airbus) that governments must step in and establish the parameters of appropriate behavior, and act quickly. But regulation isn't enough on its own: we saw in earlier chapters how Russia found loopholes to acquire restricted goods, in the same way, the law isn't always infallible and can sometimes present controversies in itself.

To navigate these gray areas, a more organized and frequent communication between the private and research sectors and regulatory agencies is essential. Moreover, it was stated (Cima) there is already a guideline on the topic, however, it needs to change from a voluntary guideline to a more comprehensive governance structure that not only increases awareness but also offers useful, flexible instruments for resolving any issues the researcher comes across.

Ethics in dual-use research shouldn't be neglected or left up to individual judgment, it is an essential part of the doctrine and must be treated as such. To do so, it needs to be ingrained in governance, supported by stakeholder communication, especially research centers and universities, as the interviewees point out, and guided by technological development. We can only maintain scientific freedom in dual use by using this integrated approach and view ethics as an aid rather than an obstacle to innovation, as the guiding principle rather than something that is up to the specific person moral compass and otherwise doesn't matter.

3.3 Human rights in cyber-surveillance technology regulation

Cybersecurity is another very pressing issue in today's day and age, engrained in ethics and the human rights doctrine. Personally, I believe that it is almost useless to still talk about privacy

in a world that is so interconnected that every single aspect of our life is under consistent monitoring.

I recognize and share the concerns expressed by Cima and Irlando, security is not a substitute for rights, rather, it is a prerequisite for them. A society threatened by cyberattacks, terrorism and external surveillance is unable to adequately defend the liberties of its people if not by using those same tools that can be a threat to them. To defend a person's fundamental right to live, sometimes one must violate another fundamental right, that of privacy. The duality of such sentence does not go unnoticed: it is the very core of this thesis, everything in life has a dual purpose.

I also find Lagni's point on the responsibility of external actors like private companies in surveillance, apart from governments, very critical. This raises another important question: how can we defend the human right to privacy if we don't even know, and consequently cannot control, who is usurping that right?

In the end, I think we must abandon, for now, the idea that privacy is absolute and that we, as people, have a complete right to it, when in the current geopolitical climate, security is of utmost importance. It goes without saying that privacy is still very important and remains a fundamental human right, however, in the special circumstances we are living in, where there is a threat at every corner, the fact that states have control over our activities and, for example, our internet searches, is the price we must pay for our wellbeing. What is not essential is that private companies have that same freedom, their surveillance methods are motivated by business logic rather than the welfare of people. Because of this, I think regulations need to be strict in limiting what businesses can do with personal data, particularly when it comes to dual-use technology like artificial intelligence.

Future EU export control regimes, as well as more general frameworks for digital governance, should, in my opinion, take this reality into account and acknowledge that safeguarding basic rights in the modern world also means limiting the power of private monitoring. The issue in most cases is, like the interviews have pointed out, that legislation is undoubtedly slower than innovation.

3.4 Differences in export control systems across the Atlantic

By stating earlier that ethics is essential in my view, I have practically already answered to the question of whether I find the EU or the US approach better in tackling dual use export controls. The United States follows a security-first approach, in which export restrictions are mainly

presented as tools of geopolitical and national defense (Irlando), exporting for them is a privilege rather than a right. In my opinion, the US model is perfect for dominance, and not so perfect for fostering openness and innovation.

On the other hand, the EU follows a more ethics-oriented logic, surely slower and less fruitful than the one of the US, it is more closely aligned to my values. I agree with Fronduti that the value of research does not only lie in its profit, but in the moral path taken to get there, and I think that the Union's approach follows this line of thinking, although I agree with Lagni that it leaves us behind in an optic of strategic dominance. The EU runs the risk of lagging behind without a more robust industrial foundation, a more unified foreign policy, or quicker regulatory processes.

I can also recognize the merit of the US system in achieving its goal: securing innovation by controlling it. While I do not think it is the ultimate way to go, I believe both approaches have merit, and they could learn from one another what they are lacking.

In the end, if one were to propose a better alternative, the best course of action would be a transatlantic framework where technological leadership is guided by ethics without being at its expense, and invention is preserved and controlled but up to a certain point. This way, the two views can learn from one another and set a precedence for dual use governance that is surely to be admired and followed.

3.5 The conflict between Russia and Ukraine and the efficiency of export regulations

In my opinion, the war in Ukraine exposed the fragility of export control systems when there is a lack of harmonization between the different actors. Although the US and the EU quicky implemented extensive measures to stop the Russian military capabilities, with tools such as prohibitions on dual-use technologies, the dispute exposed a more fundamental problem: export controls are only effective when they are coordinated, swift, and enforceable. And all three are lacking at the moment.

I agree with Cima that unilateral sanctions are ineffective, and sanctions are more symbolic than everything else in the absence of worldwide alignment. They convey a message, however, their effect is lessened when other nations keep up their open commerce with Russia. We live in a world where wester policies are losing their authority and effectiveness due to third-party intermediaries. This raises the topic that we already touched on: are we regulating too slowly in a world that is changing too quickly?

Another crucial point that was made (Fronduti) is that Europe depends too heavily on others.

The conflict in Ukraine has made it painfully clear that the EU cannot claim to be a superpower if it lacks the very thing superpowers have, and that is strategic autonomy. To pave the way for the EU to reach technological sovereignty and be completely autonomous, export controls can be used as a tool, like the US is doing.

I also share Lagni's concerns on the issue of regulatory disparities and the fact that national control list fragmentation leads to easily exploitable gaps, especially in cases on uncertainty like an armed conflict is. Thus, from my perspective, what is needed is a more coherent and internationally coordinated framework of export controls based on communication and mutual help from both governments and private actors. Only then can export control tools become instruments of ethical and security governance.

3.6 Next steps: towards a recast of the EU Dual Use Regulation

Based on the insights collected from expert interviews (Annex A) and recommendations from various stakeholders (Annex B), as well as my own critical reflections, I believe that a future recast of the dual use regulation must pursue ethics, human rights and harmonization.

In particular, civil society demanded more moral responsibility in the export of sensitive technologies, industry players emphasized the need for uniformity and clarity to reduce compliance requirements, while academic institutions underlined the importance of a clear knowledge transmission. These answers all support the necessity of a dual-use governance framework that strikes a balance between innovation, legal clarity, and human rights protection.

The absence of harmonization within the EU's dual-use export control regime is one of the most urgent issues this research has found. Member States are free to develop and enforce their own national control lists, grant individual licenses, and applies export restrictions in their own ways, even though Regulation (EU) 2021/821 is directly applicable. This undermines regulatory consistency and legal clarity, creating contradictions and loopholes that weaken the EU's credibility and enforceability.

Indeed, several experts underlined in the interviews that, when businesses look for the least restrictive national regimes for the same technology, forum shopping becomes a serious issue. This is especially problematic when it comes to sensitive or new dual-use products like AI systems, where delays or loopholes in one country could compromise the EU's whole security system.

In my opinion, the primary goal of the next recast should be harmonization, which could be achieved through a single control list at the EU level that is legally binding on all of its member

states and where additions and exceptions should be made at the Union level. To ensure the absence of loopholes and legal uncertainty, especially for emerging technologies, centralized risk assessment mechanisms should be put in place, for instance EU-level authoritative bodies or systems that standardize how dual-use risks are evaluated. Moreover, digital licensing platforms should be put in place to enable real-time export authorization monitoring, lowering the administrative load, boosting transparency, but most importantly, keeping up with technological progress, something the current regulation urgently needs to work on.

A harmonized regime not only fills in enforcement loopholes, but also sends a powerful message of unity, consequently improving the Union's position, helping it become a superpower.

Furthermore, I believe we must go beyond technical compliance and focus on incorporating ethical principles and human rights safeguards into the next recast. In particular, it should provide clearer guidelines on ethics in dual-use research, for instance by requiring institutions to adopt internal compliance programs that address ethical issues, or by introducing a dedicated oversight body to control and review exports that might pose human rights risks and provide binding or non-binding solutions to national authorities.

Another ethical addition could be that of including an "end-use ethics clause" in the regulation that requires export restrictions, even if the item isn't on a control list, if there is a reasonable suspicion that it will be used for discrimination, censorship, or repression purposes. Following the same principle, before allowing the export of high-risk goods, human rights assessments should be done, especially when we are dealing with artificial intelligence or cyber-surveillance technologies, effectively extending accountability to exporters like technology companies.

Ethics and human rights are as much of a priority as harmonization is. I believe that by adopting these recommendations in the next recast of the dual-use regulation, the EU could not only enhance its democratic commitment but also position itself as a strategic player in the global scene. More importantly, by fostering collaboration and consistent and frequent communication between all stakeholders, both public and private, especially in these uncertain times, and in light of the technological advancement, it could also catch up with the demands of today's society, securing a safer, more innovative and just future for us all.

Annex – Data collected to draft Chapter 3

Annex A – Interviews

Questions:

1. How should researchers and institutions navigate the ethical dilemmas that arise when their work has potential dual-use applications? Do you believe current regulatory frameworks provide sufficient guidance for ethical decision-making in this context or are there other steps that need to be taken?
2. Do you think cybersecurity and surveillance technologies are safeguarding fundamental human rights such as privacy and freedom of expression or endangering them in the name of security? Do you believe it is more important to safeguard safety or the freedom to privacy in this day and age?
3. The U.S. and EU both regulate dual-use technologies but follow different philosophies: one more security-driven, the other more ethics and innovation-oriented. Which approach do you think is best? How do the two different approaches affect research and innovation?
4. What lessons can be drawn from the Russia-Ukraine conflict regarding the effectiveness and limits of export controls? Do you think that the measures put in place have been effective to limit Russia's military capabilities? What could be done better to limit the problem of third parties intermediaries and shell companies put in place by Russia?
5. In light of the next review of the dual use regulation, what do you think should be added or modified? Do you think more regulatory interventions are necessary?

1. *How should researchers and institutions navigate the ethical dilemmas that arise when their work has potential dual-use applications? Do you believe current regulatory frameworks provide sufficient guidance for ethical decision-making in this context or are there other steps that need to be taken?*

In the first interview, Carlo Fronduti (ENAV) highlighted the complexity of balancing technological innovation with ethical principles, particularly within a corporate context. He emphasized that companies have specific guidelines, and they often operate in a regulatory grey area, where even information itself can become subject to compliance frameworks. Although cross-border cooperation and innovation are beneficial, they frequently clash with legal requirements. Due diligence and EU export control laws are essential tools, but they can sometimes be restrictive, particularly given the current geopolitical unpredictability due to the conflict in Ukraine. One of the biggest obstacles businesses encounter when trying to behave

ethically and competitively, according to Fronduti, is regulatory ambiguity. More clarification and interaction between industry and authorities are therefore needed to bridge this gap.

Riccardo Cima (Deloitte) highlighted the growing interest of dual use in research and the recent awareness specifically in universities, where there is specific concern on who is the recipient of information that could have a dual nature. He also specified that, from a legal point of view, dual use items in research are regulated by Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programs for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use item. Ethically, it is more difficult to find a line to set, however, he believes that where there is innovation at the base, it's worth it to pursue. This does not come without limitations, indeed, since companies see the business and monetary value in participating in military projects, there should be a clear due diligence system on who can participate, since if one understands who he is dealing with, it's easier to control any misdemeanors.

Marcello Irlando (MAECI) believes that the ethical problem of dual use research is a dilemma that remains such, it is up to the specific individual and his moral conscience on whether to publish his work or not. He, as well as Cima, highlighted that in many institutions, especially universities, awareness has been growing on the topic, and it can be seen in the growing number of panels in their ethics committees. What remains imperative is compliance with the regulations, which universities must follow by activating internal procedures. That is, it means that the regulatory framework must be clear enough to activate the measures so that they can operate accordingly. Raising awareness through pathways is also fundamental for a more informed ethical choice.

Davide Lagni (Airbus) argues that the current legal frameworks in the US and the EU enforce national ethical standards through compliance requirements rather than imposing ethical obligations per se. He stresses that lawmakers, not scientists, are in charge of ethical monitoring and governments should enact precautions where needed and that scientific research shouldn't be preemptively restricted unless it is motivated by personal conviction of the scientist. According to him, ethics is becoming increasingly important in the world of export controls, but dual-use export control law is still largely concerned with deterrence and national security, the ratio he gives is 60% deterrent to 40% ethical concern, with the possibility of ethics becoming even more important and impactful.

2. *Do you think cybersecurity and surveillance technologies are safeguarding fundamental*

human rights such as privacy and freedom of expression or endangering them in the name of security? Do you believe it is more important to safeguard safety or the freedom to privacy in this day and age?

Regarding the topic of cyber-surveillance and fundamental rights, Fronduti (ENAV) recognized the inherent conflict between the preservation of civil liberties and the requirements of maintain a high level of national security. He stated that neither freedom nor security should take precedence over the other. On the one hand, the need for safety is undeniable; on the other hand, a person must be free to express himself or herself without running the risk of repercussions, and that is why there is a need to balance the two values. Inclusive and participatory decision-making involving a variety of stakeholders, including the civil society, is the necessary tool to achieve such balance.

Cima (Deloitte) highlighted how in his view, security is the most important thing, and a greater emphasis should be put on it. He also recognized the EU's efforts in maintaining control over cybersecurity and cybersurveillance tools, essential in making sure that no third party could access that technology and abuse it.

Irlando (MAECI) also recognizes the EU's efforts in maintaining a proper control over cybersurveillance tools, and even though there is not currently a common licensing policy that regulates it, there is an acknowledgement and in-depth study on destination countries of those technologies. In his view, security prevails over the individuals' needs, not in a way that is unrestricted or that targets specific people, but in the way that countries need to prevent attacks, for instance cyber-attacks or terroristic ones, and in doing so they must have control over what people are doing.

Lagni (Airbus) compares the rationale of nuclear deterrence with the employment of cyber-surveillance tools. He contends that the widespread gathering and sharing of data by both public and private actors makes it more challenging to protect privacy in a hyperconnected environment, but states no longer have exclusive authority over surveillance since private organizations, especially those in the fields of artificial intelligence, telecommunications, and social media, are already gathering enormous amounts of data, making it more difficult to define or defend privacy as a stable right. Instead of trying to completely restrict or outlaw monitoring capabilities, states act to avoid misuse by maintaining superior knowledge and technological control and using it at their own advantage, for instance to detect terrorism attempts. In this situation, deterrence becomes the default logic.

3. *The U.S. and EU both regulate dual-use technologies but follow different philosophies:*

one more security-driven, the other more ethics and innovation-oriented. Which approach do you think is best? How do the two different approaches affect research and innovation?

Fronduti (ENAV) believes that it is not always black and white, while ethics cannot stop research, at the same time, research can also be done in different ways without having to necessarily become abuse. Also, man does not live by prestige alone, important values do not necessarily include having invented the most profitable thing but sometimes having followed one's personal values. This is why he believes the Union's approach is the better one and the one that best fits this description.

Cima (Deloitte) recognizes the US's position as a superpower, and as such, it has more autonomy; moreover, being a superpower on the topic, it can put in place secondary sanctions, that the EU does not have, and moreover, does not have the power to exercise its power on it. The EU tries to be democratic with everyone and does not have the upper hand that the US has.

Irlando (MAECI) underlined how the EU and the US have different philosophies as well as different systems: the US starts from the assumption that exports are a privilege and not a right, and therefore gives out license exceptions, while the EU believes it is a right, however, with its limitations, and everything that is regulated must be listed. The US uses export controls as a tool of trade policy disguised as national security, to gain technological and commercial supremacy; while the EU is the better approach in his opinion, however, he also sees the potential they are missing on, they could employ better instruments to secure themselves as pioneers in the market, strengthening their economic and trade resilience. Therefore, they could expand their export control policies, however, what is missing is the premise of a common foreign policy.

Lagni (Airbus) voiced doubts about the notion that EU export restrictions actively foster innovation. He contends that true innovation results from domestic industrial policy rather than export restriction, even though the EU presents its strategy as ethics oriented. Faster and more frequent changes to control lists provide the U.S. approach a strategic edge, while being more aggressive and motivated by national interest. The EU process, on the other hand, is more disjointed and slower, and it lacks the capital investment required to maintain innovation as well as a cohesive strategic goal. The EU's ethical leadership is sector-specific rather than structural, he adds, noting that EU legislation on ESG, anti-corruption, and deforestation channel ethics more thoroughly than export controls do.

4. *What lessons can be drawn from the Russia-Ukraine conflict regarding the effectiveness and limits of export controls? Do you think that the measures put in place have been effective*

to limit Russia's military capabilities? What could be done better to limit the problem of third parties intermediaries and shell companies put in place by Russia?

Fronduti (ENAV) has skeptical view on the efficacy of export controls and penalties imposed on Russia, characterizing their influence as "partial at best." He did, however, highlight a more general strategic lesson: Europe is vulnerable to systemic issues when it depends too much on outside parties, whether for energy or vital technologies. According to this viewpoint, the Ukrainian conflict emphasizes the lack of and need for strategic independence and a coordinated European response, especially in the areas of technological sovereignty and security.

Cima (Deloitte) also underlined how the measures imposed on Russia had partial capacity, since only EU goods were subject to such impositions. He stated that if everyone had decided to block certain technologies and goods from entering Russian soil, they would have been more efficient, however, we must keep in mind that countries have their own interests to safekeep, and in such a globalized world, where politics plays such a huge role, it's difficult to get a unanimous action from the biggest players in the game. He stated that, in general, sanctions are efficient, but more as a political tool than everything else, and they are not as outright as a military intervention could be.

Irlando (MAECI) also added that there is a high level of risk when confronting oneself with sanctions, the possibility of loopholes to be aware of, and the fact that the Russian market is important for many actors, even the EU, which depended on Russia for many goods and services, making it difficult to efficiently end all commercial exchanges with them. He hasn't yet given a definitive answer to whether the sanctions are effective or not because we still have to find it out, however, he stated that putting a barrier to avoid contributing to Russia's procurement of arms is critical, but it would be impossible to stop the whole export market to avoid that some goods legitimately traded in third countries might arrive to Russia. One solution he suggested was the introduction of new regulatory instruments that regulate the possibility of monitoring transactions on the basis of suspicions, without impacting legitimate trade.

According to Lagni (Airbus), the EU's most direct weapon against Russia has been financial measures, such as asset freezes. Although they are more difficult to implement, sectoral sanctions, such as those pertaining to luxury goods, dual-use products, and aviation, still severely limit Russia's access to vital technologies. Enforcement is still lacking, though, as third-country circumvention (particularly in the Global South) threatens complete control, and end-use tracking is almost impossible after commodities leave the EU. Restrictions on technical support and reactive enforcement, such as blacklisting businesses found to be providing Russia,

he finds as workable remedies. He also points out that a recurring flaw is the lack of international cooperation, as too many governments continue to maintain disparate national listings and regulations, permitting forum shopping for export and manufacture.

5. *In light of the next review of the dual use regulation, what do you think should be added or modified? Do you think more regulatory interventions are necessary?*

Fronduti (ENAV) believes the most important thing to do is to make a real connection between regulation and technology, the latter is growing at a much faster rate, making it difficult to obtain such balance, for instance, in five years, the items you wanted to control right now will be mainstream and regulation to stop its export will seem like an unnecessary burden. The necessity is finding a mechanism that evolves with time, to make sure that sensitive technologies are not for common use, but really sensitive. The feeling of companies is that more connection between regulator and companies is needed, especially on the cyber surveillance part. The structure of the regulation is already good, it has a list of controlled technologies that is updated every year. The list could be improved by being updated more often, or more in alignment with the concrete realities of companies: more contact with companies is needed, and at the same time, it also works the other way around for the regulator. Also, an element of confusion that could be improved is that each state can make its own list, so he believes that more synthesis is needed. The solution he believes is best and could be suggested as an alternative in the next recast is that of proposing one list for all that is based on a more dynamic conversation between companies and regulators.

Cima (Deloitte) also acknowledges how the regulation is struggling to keep up with technological progress, and he agrees that there needs to be better and more frequent dialogue with enterprises to further understand their needs, increased awareness from companies, and feedback from both the Union and enterprises on the details of the normative actions taken. Furthermore, there is an urgent need of harmonizing what member states have already done at the broader European level. In their lists, there are similar goods, but they might have different codes or small different parts that make them look like they are completely different technologies, thus he argues for a simplification of such details. He also believes there is a need for a more strategic approach to export controls, for instance, it's useless to try to stop Iphone chips from being exported, while the controls could focus on more strategic goods.

Irlando (MAECI) believes that currently the regulation is doing its job properly, and there is not an urgent need of changing the EU's already consolidated tools, however, he doesn't see the point in having national controls that are not shared by all member states, thus, an improvement

of the methods of control could be introduced, for instance one solution could be the introduction of EU-wide control measures where certain requirements are shared by the majority of member states, such as introducing additional controls, and provide a platform for the exchange of information between MS. Moreover, he advocates for the expansion of boundaries and to broaden the scope of Article 4, currently limited to small hubs.

Lagni (Airbus) believes that, in order to be more effective, regulations should place increased emphasis on end-use controls, like to those in the United States and offer more precise explanations of control arguments, particularly for cutting-edge technology like artificial intelligence, cryptography, semiconductors, and microchips. He also believes EU jurisdiction should expand to address gaps in extraterritorial enforcement and, as the other interviewees already stated, it's important to minimize fragmentation through an EU-wide harmonization of national lists and regulatory strategies. He concludes that businesses will keep taking advantage of national weaknesses unless the EU adopts a more assertive and unified strategy.

Annex B – Stakeholder views

AmCham, the American Chamber of Commerce to the EU, recognized the importance and relevance of Regulation 2021/821 in updating EU export control laws, however, it also pointed out the differences in the export control laws of Member States that are a result of several conceptual and procedural difficulties in the Dual-Use Regulation that must be addressed. They underlined the need of limiting export on dual-use goods to make sure they are not used for harmful purposes, however, they also recognize that these measures may unintentionally hinder lawful business, making it harder for EU exporters to compete internationally, weakening the EU's economic competitiveness and resilience by lowering the ability of EU exporters to invest in R&D, innovation, job creation, and talent acquisition. They underline the necessity of coordinated EU export control measures to safeguard industrial competitiveness and national and EU security interests. This calls for a better multilateral alignment, flexibility, proportionality, inclusive stakeholder participation and end-user focus.[75]

DigitalEurope believes the Commission should increase internal stakeholder participation and make use of industry and national authorities' inputs in order to develop a thorough understanding of the practical application of controls, for instance through public meetings might be planned on an as-needed basis. This would offer a forum for public consultation, insightful industry discussions, and useful input from government stakeholders. They propose, for the next revision, of introducing a new mechanism for a unified EU-wide list of excluded parties and/or countries of concern, consistency with other regulatory initiatives to lessen the burden of compliance on industries, and involvement of the private sector. They also underline the importance of ensuring Europe's competitiveness.[76]

Other than DigitalEurope, on the feedback to the White Paper, 23 actors have shared their opinions on the document and recommendations. The participants to the discussions are mainly business associations, worried for their interests and opertions. Industry associations empahsize the importance of balancing security concerns with the economic well being and competitiveness of European industries, Technology Industries of Finland advocate for the minimization of excessive government involvement and instead a focus on creating environments that support technological leadership and sustained global competitiveness, critical towards the hindering of competitiveness is also VDMA, the Mechanical Engineering Industry Association.

[75] AmCham EU. (2024). White paper on export controls. AmCham website.

[76] DigitalEurope. (2024, April 29). Contribution to the public consultation on the white paper on export controls. European Commission.

Two private citizens have also addedd to the discussion, one anonymous source has underlined the need to exclude consular software from export controls in general, especially cryptographic software, necessary for securely transmitting sensitive data like visa applications from foreign countries to the EU. Another person highlights the weakness of the EU in light of the current geopolitical scene, specifically the Russian offensive on Ukraine, and Europe's cutting of Russian hydrocarbons, which exposed its vulnerability. This vulnerability is not only tied to energy, but also to AI and semiconductor supply chains, thus the White Paper suggestion of strengthening EU-wide export controls on AI, quantum computing, and semiconductor technologies to reduce dependence on external powers.

Several organizations have expressed supportive stances towards the Paper, acknowledging its potential to enhance and harmonize export controls across the European Union. EECARO, the European Export Control Association for Research Organizations, values the Commission's initiative to gather industry and academic viewpoints on how export controls will develop in Europe and backs the plan to enhance the coordination of new export regulations among EU member states.[77]

Moreover, the Aerospace, Security and Defense Industries Association of Europe (ASD), a trade association for the aerospace, defense and security industries in Europe that represents over 3,000 companies including Airbus, Leonardo and Thales, has also provided a response to the Commission's White Paper, where they stated that, to foster innovation without creating needless complications, the goal should be to establish a balanced, integrated approach to funding and regulation, without jeopardizing the competitiveness and exportability of technologies developed through EU projects. To achieve such harmonization and to reach an increased collaboration, they emphasized the importance of simplifying processes and procedures, for instance, to enhance compliance among Member States, early consultation with regulatory authorities is crucial.[78]

The 2023 Factual Summary Report of a public consultation conducted by the European Commission under Article 26 of Regulation (EU) 2021/821, received 21 replies, mainly from NGOs, including Amnesty International and Human Rights Watch; research organizations, including European Export Control Association for Research Organizations and Universitá

[77] European Commission. (2024). Feedback and contributions to the public consultation on the White Paper on Export Controls. European Commission.

[78] Aerospace, Security and Defence Industries Association of Europe (ASD). (2024). ASD response to the EU White Paper on technologies with dual-use potential. Aerospace, Security and Defence Industries Association of Europe. ASD website.

degli Studi di Genova; and industry associations and companies, like Air France and ASSONIME demonstrated that the work being done by the Commission and Member States to create new standards for the gathering of information and creation of the EU annual report on dual-use export control is generally supported. Stakeholders in the industry point out that public reporting should assist businesses, particularly SMEs, in adhering to the Dual-Use Regulation, help in understanding the variations and uniformity of decisions across Member States' practices; and reduce complexities to avoid placing an additional administrative burden on exporters; NGOs, think tanks, and civil society all emphasize the need to preserve personal information, interpret exceptions to data sharing strictly, and encourage greater transparency with the annual report; while universities and research organizations push for public reporting which helps in clearly defining license management for their sector and in raising awareness and improving internal compliance programs.[79]

[79] European Commission. (2023). Factual summary report of the public consultation on dual-use export controls. CIRCABC.

Conclusion

With a focus on the European Union's regulatory framework in the face of conflicting needs for technological innovation, national security, and human rights protection, this thesis has explored the intricate and dynamic world of dual-use export controls. Several important findings were drawn from a combination of legal analysis, ethical contemplation, and qualitative information gathered from stakeholder inputs and expert interviews.

In particular, several important insights into the opportunities and difficulties related to dual-use export regulations were revealed by the qualitative analysis of the stakeholder consultations and interviews.

Experts have often emphasized how challenging it is to navigate moral dilemmas in dual-use research and innovation. Although the significance of ethics as the foundation of export controls is well acknowledged, its actual implementation is still a very difficult task. Due diligence and compliance procedures are viewed as both essential safeguards and possible barriers to innovation in regulatory grey areas, where researchers frequently find themselves. A recurring topic that emerged was the need for more proactive involvement from regulatory bodies and more precise advice and guidance to innovators.

Similarly, the interviews highlighted the underlying conflict between maintaining national security and defending fundamental human rights like freedom of expression and freedom to privacy. Experts had differing opinions on the extent to which surveillance technology could jeopardize civil liberties, but they all agreed on the fact that, in the current geopolitical climate, cybersecurity precautions are essential. In order to successfully balance these conflicting interests, many stressed the significance of inclusive, participatory decision-making and the importance of clear regulatory frameworks.

The analysis brought to light significant differences between the US and EU regulatory ideologies. The US policy, which uses export controls as instruments of geopolitical strategy, was described as being more dynamic and security driven. The EU strategy, on the other hand, was viewed as being more cautious and ethics-oriented, with human rights protection as their priority. For transatlantic collaboration and the creation of standardized export control regimes, this diversity offers an opportunity, and it was suggested that both systems could balance their viewpoints and learn valuable lessons from each other.

The conflict between Russia and Ukraine revealed serious flaws in the way export restrictions and sanctions are coordinated and enforced. Major risks identified by experts were the participation of third-party intermediaries, the difficulty of tracking end-use, and the fragmentation of national control lists. The most successful measures to date have been

determined to be asset freezes and financial sanctions; nonetheless, coordinated work and increased cooperation between all actors is still required to close such loopholes and prevent regulation evasion.

The regulation of dual-use technologies must strike a delicate balance between enabling innovation and preventing misuse, supporting the researcher while avoiding that his work could be exploited for harmful or unethical purposes.

Ethics and human rights are very important baselines for export control procedures. More transparency on exports of cyber-surveillance, enhanced compliance programs for research institutes, and the implementation of required human rights impact assessments can all help guarantee that advancements in technology do not come at the price of basic human liberties.

These problems highlight how urgent it is to advance a review of the dual use regulation, especially in light of the fast development of emerging technologies and the current geopolitical climate which comes with uncertainties and constant dangers.

To effectively address such concerns, it is important to retain a strong and flexible export control regime and to foster transatlantic cooperation with important allies. This kind of collaboration will not only improve the ability of mitigating the risks connected to dual-use technologies, but it will also create a safe atmosphere for innovation to flourish. By developing these strategic alliances and fostering innovation, the European Union may also establish itself as a global leader in technological governance.

Ultimately, to fight fragmentation and legal ambiguity, the proposed reform plan must prioritize enhancing harmonization among EU Member States. This entails enhancing collaboration between all involved actors, at governmental and industry level, harmonizing licensing procedures, and creating a single export control list.

Only by adopting this strategy and implementing these changes can export controls achieve their goal of fostering innovation while also protecting human rights and international security.

Bibliography

A brief history of the internet. (n.d.). Stanford Education.

A new political forum could help make the EU's strategic trade controls more strategic - if it is allowed to. (2024). SIPRI.

Aerospace, Security and Defence Industries Association of Europe (ASD). (2024). ASD response to the EU White Paper on technologies with dual-use potential. Aerospace, Security and Defence Industries Association of Europe. ASD website.

Aizenberg, E., & Van Den Hoven, J. (2020). Designing for human rights in AI. Big Data & Society, 7(2), 2053951720949566.

Alavi, H., & Khamichonak, T. (2017). EU and US export control regimes for dual use goods:

Alper, A. (2024). U.S. imposes trade restrictions on two Chinese firms over human rights. Reuters.

AmCham EU. (2024). White paper on export controls. AmCham website.

An overview of existing frameworks. Romanian J. Eur. Aff., 17, 59.

Anstis, S. & Deibert, R.J. (2025) Silenced by Surveillance: The Impacts of Digital Transnational Repression on Journalists, Human Rights Defenders, and Dissidents in Exile, 25-05 Knight First Amend. Inst.

Atlas, R. M., & Dando, M. (2006). The dual-use dilemma for the life sciences: perspectives, conundrums, and global solutions. Biosecurity and bioterrorism: biodefense strategy, practice, and science, 4(3), 276-286.

Baric, R. (2007). Synthetic viral genomics: Risks and benefits for science and society.

Barnig, M. (2013). PAL: personalized assistant that learns | Internet with a Brain.

Bauer, M., & Pandya, D. (2024). Time to rethink export controls for strengthened US-EU cooperation and global trade rules (No. 07/2024). ECIPE Policy Brief.

Bauer, S., & Bromely, M. (2016). The dual-use export control policy review: balancing security, trade and academic freedom in a changing world.

Bilousova, O., Hilgenstock, B., Ribakova, E., Shapoval, N., Vlasyuk, A., & Vlasiuk, V. (2024). Challenges of export controls enforcement: how Russia continues to import components for its military production.

Bromley, M., & Brockmann, K. (2021). Implementing the 2021 recast of the EU dual-use regulation: Challenges and opportunities.

Bromley, M., & Brockmann, K. (2024). A Tale of Two Systems: Alignment, Divergence and Coordination in EU and US Dual-use Export Controls. Istituto Affari Internazionali (IAI).

Burkhard, S., Charatsis, C., Kanetake, M., Klein, R., Kolliarakis, G., Ladikas, M., & Whang,

C. (2022). Input to EU-US Trade and Technology Council for Working Group 7-Export Controls. Multi-disciplinary Network of Experts.
Chawla, A. (2021). Pegasus spyware–'A privacy killer'.
Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. Frontiers in Human Dynamics, 6, 1421273.
Cloud computing history part 1: the origins of the cloud. (2022). Ascend Cloud Solutions.
Commission publishes White paper on Export Controls - ACQUIS. (2025, February 3).
Control list, catch-all and technical assistance. (2023). Erhvervsstyrelsen Eksportkontrol.
Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods
Court of Justice of the European Union. (2020). Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Schrems II), Case C-311/18.
Digital Frontlines. (2025). Spyware regulation: European Commission slow to act on Parliament's call for reform.
DigitalEurope. (2024, April 29). Contribution to the public consultation on the white paper on export controls. European Commission.
Douglas, H., & Branch, T. Y. (2024). The social contract for science and the value-free ideal. Synthese, 203(2), 40.
EU-US Trade and Technology Council. (n.d.). European Commission.
European Commission. (2021). Strengthened EU export control rules kick in.
European Commission. (2023). Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.
European Commission. (2023). Factual summary report of the public consultation on dual-use export controls. CIRCABC.
European Commission. (2024). Commission Recommendation (EU) C(2024)7035 final of 24
European Commission. (2024). Feedback and contributions to the public consultation on the White Paper on Export Controls. European Commission.
European Commission. (2024). Preventing Russian export control and sanctions evasion: Updated guidance for industry.
European Commission. (2024). Report on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (COM(2024) 22 final).
European Commission. (2024). White Paper on export controls (COM(2024) 25 final).
European Commission. (2024). White Paper on options for enhancing support for research and

development involving technologies with dual-use potential (COM(2024) 27 final).
European Commission. (n.d.). Working Group 7 – Export control cooperation. Futurium.
European Parliament. (2024). The Pegasus spyware scandal and its implications for the EU (Briefing No. 761472). Directorate-General for Internal Policies.
Exporting dual-use items. (2025). European Commission. Trade and Economic Security.
Fortinet. (n.d.). Spyware. Fortinet CyberGlossary.
Gaumond, E., & Régis, C. (2023). Assessing Impacts of AI on Human Rights: It's Not Solely About Privacy and Nondiscrimination. Lawfare Media. Friday, January, 27, 8.
GeeksforGeeks. (2025). TCP/IP model. GeeksforGeeks.
Gwardzińska, E., & Chackiewicz, M. (2023). A Ban on the Export of EU Goods to Russia. Humanities and Social Sciences, 30(2), 27-35.
Hanna, K. T., & Burke, J. (2021). Frequency-hopping spread spectrum (FHSS). Search Networking.
Hawkins, A. & Mui, C. (2025, March 20). Commerce weighs crackdown on export controls. Politico Pro.
Kanetake, M. (2018). Balancing innovation, development, and security: dual-use concepts in export control laws. Global Environmental Change and Innovation in International Law Cambridge University Press, 2018 Forthcoming.
Kanetake, M. (2021). Dual-use export control: security and human rights challenges to multilateralism. In European Yearbook of International Economic Law 2020 (pp. 265-290). Cham: Springer International Publishing.
Kikel, C. (2022). History of Voice Recognition Technology - Total Voice Technologies. Total Voice Technologies.
Latest EU sanctions extend asset freezes, restrict oil industry dealings and target 'Shadow fleet.' (2025). Insights | Skadden, Arps, Slate, Meagher & Flom LLP.
Lazarou, E. (2019). United States: Export Control Reform Act (ECRA).
Mak, H. (2023). When was the GPS invented? The fascinating evolution of GPS technology. Global GPS Systems.
Miller, S., & Selgelid, M. J. (2007). Ethical and philosophical consideration of the dual-use dilemma in the biological sciences. Science and engineering ethics, 13, 523-580.
October 2024 on internal compliance programmes for the export of cyber-surveillance items under Regulation (EU) 2021/821.
OpenSystems Media. (n.d.). The Royal Air Force and the invention of the modern touchscreen - embedded computing design. Embedded Computing Design.

Oztig, L. I., & Karluk, A. C. (n.d.). China's High-Tech Repression Against Uyghurs: Novel Theoretical Insights.

Red flags in real cases: enforcement and evasion of Russia sanctions. (2023). Wisconsin Project on Nuclear Arms Control.

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)

Report From the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items

Rhodes, C. & Sulston, J. (2010) Scientific Responsibility and Development. The European Journal of Development Research. 22. 3-9.

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology, 4, 100005.

Siddiqui, S. Y., Farooqi, S., & Zulfiqar, L. (2024). Human Rights for the Digital Age. arXiv preprint arXiv:2408.17302.

Stalenhoef, C., Kanetake, M., & van der Wende, M. (2022). The implications of the EU's dual-use export control regulation 2021/821 for universities and academics. Utrecht University School of Law Research Paper Forthcoming.

U.S. Department of Commerce. (n.d.). EU-U.S. Data Privacy Framework: Program overview. Data Privacy Framework.

U.S. Department of Justice, U.S. Department of Commerce, & U.S. Department of the Treasury. (2023). Tri-seal compliance note: Cracking down on third-party intermediaries used to evade Russia-related sanctions and export controls.

Venter, J. C., Glass, J. I., Hutchison, C. A., & Vashee, S. (2022). Synthetic chromosomes, genomes, viruses, and cells. Cell, 185(15), 2708-2724.

Villasenor, J. (2024). The tension between AI export control and U.S. AI innovation.

Walsh, E. P. (2004). Security shifts and power plays: the case of European Union dual-use export control regime development (Doctoral dissertation, University of Georgia).

Whang, C. (2021). Trade and emerging technologies: A comparative analysis of the United States and the European Union dual-use export control regulations. Security and Human Rights, 31(1-4), 11-34.

Woods, C. (2024). Maximizing Defense Innovation While Holding the Line on Export Controls: What the Defense Sector Can Learn from Global Banks.