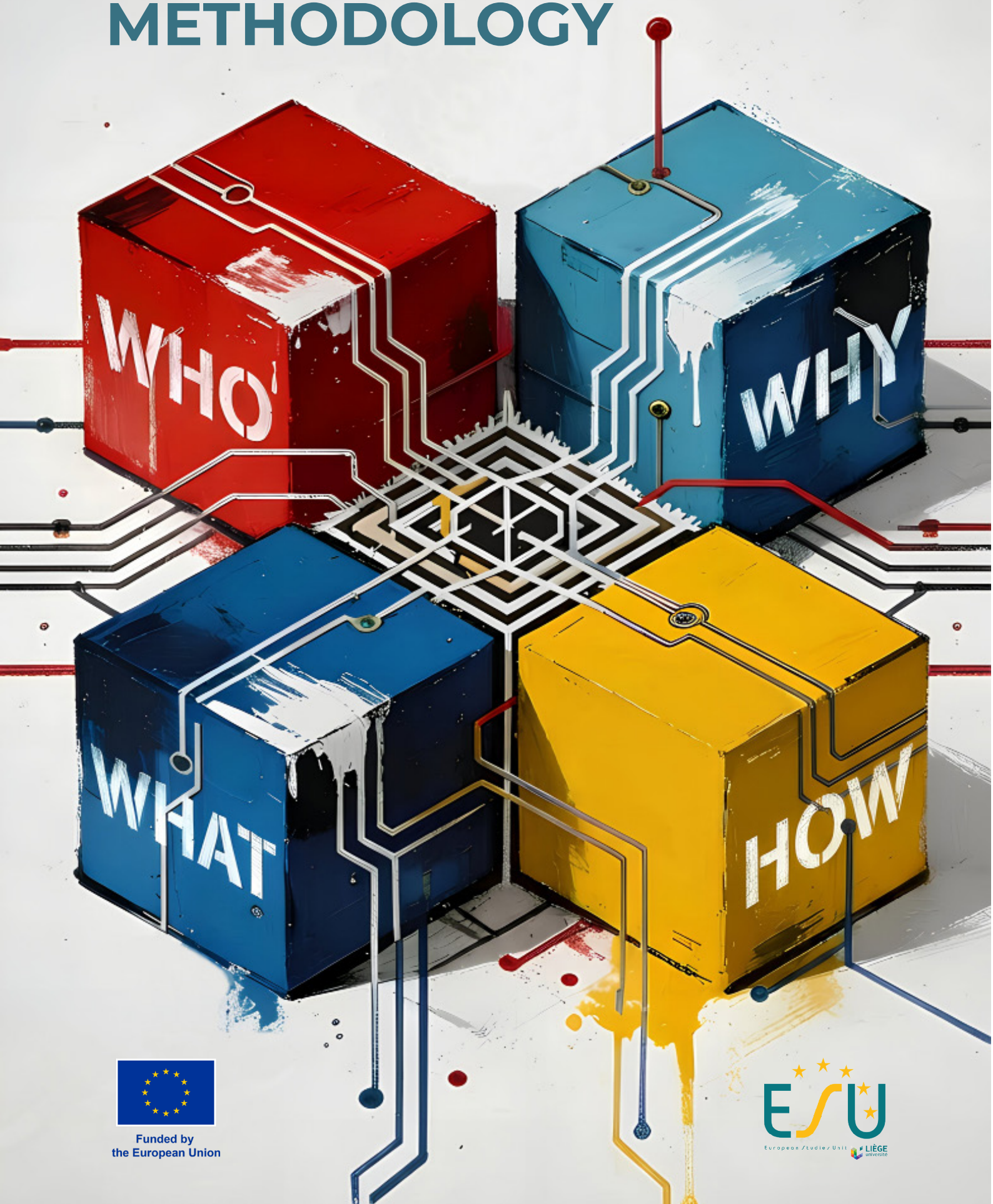
14th and 15th Chaudfontaine Group Meeting

A REVIEWED W3H METHODOLOGY



Funded by
the European Union

ESU
European Studies Unit
LIÈGE université

This collective work is the outcome of the 14th and 15th meetings of the Chaudfontaine Group, which were held in Spa and Wanze (Belgium) from 24 to 26 November 2024 and from 1 to 3 June 2025, and were funded by the European Commission.

The Chaudfontaine Group is a think tank gathering actors from academia, industry and (European, national, and regional) public authorities dealing with strategic trade control issues.

DISCLAIMER

The views and opinions expressed in this work do not represent those of the institutions the authors may be working for.

COPYRIGHT

European Studies Unit (ESU), University of Liege, January 2026

ISBN: 978-2-9601919-4-3
EAN: 9782960191943

CONTENTS

REPORT ON THE 14TH AND 15TH EDITIONS OF THE CHAUDFONTAINE GROUP MEETING

A REVIEWED W3H METHODOLOGY

INTRODUCTION

Dual-use items can be defined as goods and technologies that have both civilian and military applications and may pose significant risks if acquired by malicious actors. Conversely, these items can also contribute significantly to a country's economic competitiveness and innovation. This inherent duality necessitates the implementation of specific controls on the trade of such strategic items to strike an appropriate balance between security imperatives and economic interests.

The W3H methodology (formerly known as 3WH) was developed by the European Studies Unit of Liège University and the Joint Research Centre of the European Commission in 2017 to support state authorities and other relevant actors concerned with the transfer of dual-use items when drafting or amending a strategic trade control (STC) system.

The W3H methodology is divided into four parts:

- the **"why"**, which highlights motivations that might incentivise authorities;
- the **"who"**, which identifies the actors that draft and implement it;
- the **"what"**, which defines the scope of controls in terms of items and operations;
- the **"how"**, which frames the implementation (e.g., policymaking, licensing) and enforcement.

In the nearly a decade since its adoption, the Chaudfontaine Group[1] has dedicated two sessions to reviewing the W3H methodology in light of the lessons learned from its implementation and the evolution of the international geopolitical situation.

The group has conducted a systematic review of each element of the methodology. Based on the results of the discussion, a new version of the W3H methodology has been drafted.

This document presents this new version, and is intended to assist various stakeholders in drafting and reviewing the STC system.

1. The Chaudfontaine Group is a think tank gathering actors from academia, industry, and (European, national, and regional) public authorities dealing with strategic trade control issues.

REVIEW OF THE W3H METHODOLOGY

The idea and need for a methodology to develop and review an STC system emerged from the experiences gained by the European Union (EU) through the implementation of its projects supporting United Nations Security Council Resolution 1540 (2004) (UNSCR 1540).[2] While the matrices developed by the 1540 Committee serve as a useful reference tool for facilitating technical assistance and identifying the main elements of an STC system, they do not define the process for the actual development of such.[3] For example, the process to encourage various national authorities to allocate financial and human resources to a project whose direct benefits were not clearly identified was not outlined.

A decade later, most states involved in the European Union Partner-to-Partner (EU P2P) Export Control Programme for Dual-Use Goods had either developed, reviewed, or were in the process of establishing an STC system. While the methodology for creating an STC system remained relevant for some countries, there was a need to assess its relevance in terms of reviewing existing systems. Furthermore, the geopolitical landscape and international strategic trade policies had evolved, broadening the concept of security to include dimensions other than those traditionally considered, such as human security and the new concept of economic security, which has fostered protectionism and trade restrictions.

To address these changes, the Chaudfontaine Group committed to systematically reviewing the elements of the W3H methodology. Each participant was asked to analyse different components and present their views. The group dedicated a session to each element, engaging in in-depth discussions about its evolution. Following these debates, a new version of the methodology was collectively drafted and reviewed.

2. European Union, Chemical, Biological, Radiological and Nuclear Risk Mitigation, EU P2P Export Control Programme for Dual-use Goods. https://cbrn-risk-mitigation.network.europa.eu/eu-p2p-export-control-programme/dual-use-trade-control_en.

3. United Nations, 1540 Committee, 1540 Matrices. https://www.un.org/en/sc/1540/national-implementation/1540-matrices.shtml.

"FOR WHOM"

During the discussion, the question of the target audience for the W3H methodology was raised by some participants; specifically, they inquired whether the methodology is exclusively intended for state authorities responsible for drafting and implementing the national system or whether it might also be relevant to other stakeholders.

While it is clear that the primary audience should be state authorities involved in the process of establishing and implementing a trade control system, other interested parties should not be excluded. For instance, the arguments presented in the "why" section may also be valuable to operators seeking to persuade their senior management to set up an internal compliance programme (ICP). Furthermore, economic operators

and researchers may use the W3H methodology as a tool to better comprehend the functioning of an STC system and better understand their role(s) or contribution(s) to non-proliferation and (inter)national security objectives. This can be achieved through its incorporation into training sessions, as well as into undergraduate and graduate educational programmes, to elucidate the trade control system, thereby transforming it into a practical instrument for education and capacity-building purposes beyond government authorities.

A NEW TRANSVERSAL *CHAPEAU*: “WHEN” AND “WHERE”

Another element raised during the discussion was the universality of the W3H methodology. Although it has been designed to be used by any state considering implementing the commitments of UNSCR 1540, the W3H methodology’s intrinsic flexibility facilitates its adaptability to diverse national contexts, thereby promoting its universal applicability. This flexibility has two main transversal dimensions: WHEN and WHERE the methodology is applied. By way of example, the suitability of the diverse underlying justifications for establishing or amending STCs (WHY), the scope of their application (WHAT), and their operational mechanisms (HOW), may be influenced by:

- the country’s geographical context or institutional framework (WHERE), such as membership of a customs union, presence in a region facing specific security challenges, and the mandates and responsibilities of relevant ministries;

- the momentum (temporal context) of drafting or amending the STC system (WHEN), which can be shaped by economic, political, or other factors. For instance, this includes the country’s level of economic development, economic capacity—intended as the ability to oversee and regulate the export of sensitive goods, conduct risk assessments, and assist companies in implementing internal compliance programmes (ICPs)—, and consequent financial resources, the prevailing political agenda (which may be interrelated with the WHERE), and whether the country is already integrated into global supply chains or seeking access to high-tech trade.

Consequently, given that the relevance of each component of the W3H methodology is contingent upon a given country’s specific circumstances, it is essential to consider the temporal (WHEN) and geographical (WHERE) dimensions when applying the W3H methodology. This consideration is crucial for adapting the methodology to diverse national contexts.

WHY: RATIONALES BEHIND A STRATEGIC TRADE CONTROL SYSTEM

WHY: RATIONALES BEHIND A STRATEGIC TRADE CONTROL SYSTEM

The initial step in establishing or strengthening an STC system involves identifying the underlying reasons for undertaking this process. The motivations that drive governments and stakeholders (e.g., industry and research organisations) to implement STCs are multifaceted and can vary significantly from one case to another, notably depending on the temporal (WHEN) and geographical (WHERE) contexts in which STCs are to be applied. Nevertheless, these motivations can be broadly categorised into four primary rationales: security, economic, geopolitical, and other rationales.

In the following sections, each category is further elaborated upon and subdivided into more specific subcategories, thereby highlighting particular aspects of the security, economic, geopolitical, and other rationales.

1.1. SECURITY RATIONALES

The regulation of trade in dual-use items is a critical component of contemporary national and international security strategies. STCs play a pivotal role in managing the flow of such strategic items to prevent their misuse and to ensure they do not contribute to activities that might undermine global stability and security. This section describes the multifaceted reasons why STCs are essential to safeguarding national and international security.

WMD-PROLIFERATION

One of the primary rationales behind an STC system is to prevent the proliferation of Weapons of Mass Destruction (WMD). Dual-use items, including software and technology, can be used for the design, development, production, or use of nuclear, chemical, or biological weapons or their means of delivery. By regulating trade in dual-use items, countries can mitigate the risk of such sensitive goods and technologies falling into the hands of rogue states or non-state actors intent on developing WMDs.

The first concerns arose about non-civilian nuclear energy with the development of the nuclear bomb during WWII which then spread to the other WMDs, leading to more extensive STCs. The first binding international instrument was the Treaty on the Non-Proliferation of Nuclear Weapons (NPT, 1968-1970), followed by the Biological Weapons Convention (BWC, 1972-1975) and the Chemical Weapons Convention (CWC, 1993-1997). Each was aimed at prohibiting different types of WMD and were complemented

by multilateral export control regimes (MECRs). UNSCR 1540, adopted in 2004, was the first of these legal instruments to address non-state actors, extending the scope to terrorism-related concerns and covering the entire category of WMDs and their means of delivery for the first time.

A. Q. Khan's nuclear smuggling network is a well-known example of proliferation that contributed to the nuclear programmes of Pakistan, North Korea, Iran, Libya, and possibly others.[4] The discovery of these particular illicit procurement activities is among the reasons that led to the adoption of the United Nations Security Council 1540 Resolution, whose objective is, notably, to prevent non-state actors from developing, acquiring, manufacturing, possessing, transporting, transferring, or using any WMD and their means of delivery.[5]

Therefore, complying with the international obligation of implementing and enforcing STCs enhances national security and contributes to global stability by reducing the risk of catastrophic conflicts.

4. Stewart, I. J., & Salisbury, D. B. (2016). Non-State Actors as Proliferators: Preventing Their Involvement. Strategic Trade Review, 2(3), 5-26; Hastings, J. V. (2012). The Geography of Nuclear Proliferation Networks: The Case of A.Q. Khan. The Nonproliferation Review, 19(3), 429–450.

5. United Nations Security Council 1540, S/RES/1540, New York, April 2004.

PREVENTING THE ENHANCEMENT OF DESTABILISING FOREIGN MILITARY CAPABILITIES

Dual-use technologies, such as quantum computing, advanced semiconductors, and artificial intelligence, can play a critical role in enhancing military capabilities, particularly in the digital age, as well as threatening economic competitiveness and social welfare in the longer term.[6]

Controlling the transfer of these technologies and know-how is instrumental in preventing potential adversaries from strengthening their military powers. By controlling access to these technologies and know-how, countries can maintain a strategic advantage or balance and mitigate the escalation of military tensions, especially in regions characterised by ongoing geopolitical rivalries. Moreover, the transfer of these technologies may be used against the security interest of the European Union and its Member States, and as such the transfer may be undesirable.

Additionally, the significant role played by dual-use items in the enhancement of destabilising foreign military capabilities explains the inclusion of restrictions on exports of dual-use goods and technology when international sanctions are adopted in order to target countries that threaten the security of others, such as the restrictive measures adopted by the EU against Russia to undermine its ability to wage war against Ukraine.[7]

6. European Commission, Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy", JOIN(2023) 20 final, Brussels, 20.06.2023.

7. "19th package of EU sanctions: EU reaction to Russian invasion of Ukraine (regularly updated)". European Studies Unit (ESU), University of Liège (available at: https://www.esu.ulg.ac.be/wp-content/uploads/2025/11/Overview-of-EU-sanctions-against-Russia-Belarus-2014-2025_19th.pdf).

TERRORISM FROM AN INTERNAL SECURITY PERSPECTIVE

Terrorism, from an internal security perspective, is also a significant concern. Dual-use items can be exploited by terrorist organisations to carry out devastating attacks. For example, chemicals used in industrial processes can be repurposed for chemical

weapons, and advanced communication technologies can be used for coordinating terrorist activities. For instance, in May 2024, the UN Investigative Team to Promote Accountability for Crimes Committed by Da'esh/Islamic State in Iraq and the Levant (UNITAD, S/2024/408) certified that ISIS had occupied the University of Mosul and deliberately hijacked its infrastructure to establish a centre of operations for the production of chemical weapons, and used chemical weapons such as chlorine and sulphur mustard agents in Iraq and Syria since 2014.[8]

Although the case of Syria can be explained by its specific context of internal war, the possibility that terrorist groups may have access to sensitive goods, equipment, or technologies has led some states to adopt import controls on dual-use items. For instance, Morocco, Serbia, and the Philippines have decided to impose control on the import of dual-use goods for internal security reasons. Serbia has imposed import controls only on items from the CWC's lists, while the Philippines has even adopted controls on the "re-export" within the country of previously imported goods due to the challenges posed by the geographical shape of the archipelago in putting in place effective physical controls, as well as the presence of local terrorists.[9] By enforcing such controls, governments can help prevent terrorist organisations from acquiring such sensitive goods, equipment, and technologies, thereby enhancing internal security and protecting civilian populations from terrorist threats.

8. UN Investigative Team to Promote Accountability for Crimes Committed by Da'esh/Islamic State in Iraq and the Levant. UNITAD, S/2024/408.

9. Paile, S., Michel, Q., & Vella, V. (2024). Elaborating a Strategic Trade System of Dual-Use Items. Experiences from the European Union, Morocco, the Philippines, Serbia, Singapore and Ukraine. Publications Office of the European Union, pp. 26, 76, 78.

ECONOMIC SECURITY AND STRATEGIC AUTONOMY

Another important rationale behind STCs is the protection of a country's economic security.

Although still vague, the concept of "economic security" can be outlined in the EU context from the perspective of policy objectives, as a set of measures designed either to affect economic outcomes, such as protecting an economy against certain shocks through supply chain diversification or trade defence measures, or to affect non-economic outcomes, such as maintaining a technological lead in critical technologies with military applications.[10]

Intended as the latter, economic security encompasses measures taken in the economic sphere to ensure (national) security outcomes.[11] In particular, these economic policy tools include STC measures, such as export restrictions on high-tech products and controls on inbound and outbound investment, to prevent potential adversaries from gaining access to critical technologies with military applications or from controlling critical infrastructures.[12] Strategic autonomy is a key factor of an economic security strategy as it allows states to maintain independence in their strategic decisions.

Establishing an STC system is therefore an essential element of an economic security strategy to prevent or reduce various risks relating to critical technology security and technology leakage, the resilience of supply chains, the physical- and cybersecurity of critical infrastructure, and the weaponisation of economic dependencies.[13]

10. Chimits, F., McCaffrey, C., Lopez, J. M., Poitiers, N. F., Vicard, V., & Wibaux, P. (2024). European Economic Security: Current practices and further development, pp.4-5.

11. Ibid., p.5.

12. Council of the European Union, A Strategic Compass for Security and Defence, March 2022, pp. 47-48.

13. European Commission, Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy", JOIN(2023) 20 final, Brussels, 20.06.2023.

TECHNOLOGY LEAD AND SUPREMACY

Dual-use items often embody advanced technological capabilities that drive economic growth and military superiority. By controlling their export, states can protect their technological edge or dominant position, ensuring that they remain at the forefront of innovation and preventing the diffusion of critical technologies to competitors who could use them to their detriment. The export restrictions on semiconductors imposed on China by the United States are a particular and notorious example of the US attempting to maintain its hegemony on AI and advanced computing.[14]

HUMAN RIGHTS AND INTERNATIONAL HUMANITARIAN LAW VIOLATIONS

Respect for human rights has long been a concern of the international community as illustrated by the Universal Declaration of Human Rights proclaimed by the United Nations General Assembly in Paris on 10 December 1948.[15] In the context of strategic trade, the arms trade embargo imposed on China following the events at the Tiananmen Square protests of 1989 was one of the first examples where human rights considerations were noted as grounds for adopting such trade control measures.[16] Such human security considerations became more formally one of the criteria for assessing arms exports with the adoption of the European Union Code of Conduct on Arms Exports in 1998 (replaced by Council Common Position 2008/944[17]),[18] and one of the grounds for imposing a licensing requirement for exports of non-listed dual-use items with the adoption of Council Regulation (EC) No 1334/2000 (replaced by Regulation (EU) 2021/821[19]).[20]

Regarding the risk of human rights violations, cybersurveillance items deserve particular attention as their misuse can infringe a wide range of human rights such as the right to privacy, data protection, freedom of expression, association and assembly, freedom of thought, conscience, and religion, and the right to free, equal, and secret elections.[21] This explains why, in the recast of the EU Dual-Use Regulation, a specific provision has been devoted to the export of non-listed cyber-surveillance items.[22]

By restricting any export of dual-use items to countries known for human rights abuses, states can prevent these technologies from being used to suppress and harm civilian populations.

14. "Chip war ramps up with new US semiconductor restrictions on China". The Guardian, 3 December 2024. Available at: https://www.theguardian.com/us-news/2024/dec/03/joe-biden-china-microchip-export-restrictions-law-changes .

15. General Assembly resolution 217 A.

16. Presidency Conclusions, European Council of 26 and 27 June 1989 in Madrid, document SN 254/2/89. in relation to the events at the Tiananmen Square protests of 1989.

17. Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment, OJ L 335, 13.12.2008, p. 99–103.

18. Council of the European Union, European Union Code of Conduct on Arms Exports, document 8675/2/98 Rev 2, Brussels, 5 June 1998.

19. Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), OJ L 206, 11.6.2021, p. 1–461.

20. Article 5 of Council Regulation (EC) No 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology, OJ L 159, 30.6.2000, p. 1–215.

21. Commission Recommendation (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council, C/2024/7035, OJ L, 2024/2659, 16.10.2024, p. 15.

22. Article 5 of Regulation (EU) 2021/821.

INTERNATIONAL SECURITY INTERESTS

International security interests are paramount in the global arena. STCs help prevent the destabilisation of regions and the escalation of conflicts. Dual-use items can exacerbate regional tensions and arms races, leading to increased instability and the risk of conflict. This explains why the existence of an arms embargo is taken into account when deciding whether or not to export listed and not-listed dual-use items.[23] By regulating their export, states can promote regional stability and contribute to a more secure international environment.

23. See, for instance, article 4 of Regulation (EU) 2021/821.

PUBLIC HEALTH

Establishing an efficient trade control system can also have benefits for public security and public health. More specifically, controlling the transfer of dual-use items–such as biological pathogens dangerous for humans, animals or crops–can help prevent the spread of pandemics, catastrophic events for a country's food safety and security, or the misuse of chemical, biological, radiological, or nuclear (CBRN) materials, thereby safeguarding public health and public security. Moreover, export controls may also face significant tension during large-scale disease outbreaks, as critical items such as detection equipment and personal protective gear may become subject to regulatory restrictions. An illustration is the European Commission adoption of export restrictions on personal protective equipment in response to the COVID-19 pandemic.[24] Consequently, the governance of these items must strike a careful balance to reconcile both security imperatives and public health priorities.

24. Commission Implementing Regulation (EU) 2020/568 of 23 April 2020 making the exportation of certain products subject to the production of an export authorisation, OJ L 129, 24.4.2020, pp. 7–15.

RESEARCH SECURITY AND ETHICAL CONSIDERATIONS

As outlined in the Council Recommendation on enhancing research security, critical and dual-use technologies play a key role in the enhancement of economic and military capabilities.[25] In reason of its openness, academic freedom, institutional autonomy, and internationalisation, the research and innovation sector is particularly vulnerable to the risk of being misused for unethical purposes, such as surveillance or oppression, or in ways that enhance the military capabilities of EU competitors, such as countries pursuing civil-military fusion strategies.[26] An advanced STC system increases the capacity to control intangible transfers, notably, where necessary, sensitive scientific knowledge, and thus contributes to ensuring that sensitive research is not compromised by foreign entities.[27]

25. Council of the European Union, Council Recommendation of 23 May 2024 on enhancing research security, OJ C, C/2024/3510, 30.5.2024.

26. Ibid.

27. Council of the European Union, A Strategic Compass for Security and Defence, March 2022, p. 37.

COUNTERING PROLIFERATION FINANCE

Preventing persons and entities involved in WMD proliferation from raising, transferring, and using funds is a crucial component of non-proliferation efforts. The UN Security Council pursues these efforts at the global level through Resolution 1540–which prohibits financing proliferation-related activities by non-state actors–and at the

national level through country-specific measures.[28] This illustrates the extent to which the fight against proliferation financing is key to disrupting the networks that support the spread of WMDs and their means of delivery.

HYBRID THREATS

Hybrid threats combine military and non-military means (i.e., diplomatic, military, economic, technological) to achieve strategic objectives while remaining below the threshold of formal warfare.[29] STCs enhance resilience and the ability to counter hybrid threats by preventing dual-use items from being used in hybrid warfare tactics–such as cyberattacks, foreign information manipulation and interference[30]–that undermine national security and stability.

1.2 ECONOMIC RATIONALES

Beyond security-related motivations, STCs on dual-use items are instrumental in fostering economic resilience and potential growth, particularly within the context of a highly interconnected and increasingly competitive global economy. STCs address a variety of economic rationales, as outlined below, which are foundational to both national and international economic frameworks.

GEO-ECONOMIC AND SUPPLY CHAIN DE-RISKING

As previously explained in the "Economic security and strategic autonomy" section under "Security rationales", the protection of a country's economic security is an important rationale behind STCs.

Still from the perspective of policy objectives, the concept of "economic security" can be intended here as a set of measures designed to affect economic outcomes, such as protecting the economy against certain shocks through supply chain diversification or trade defence measures. The de-risking strategy then takes the form of various measures such as new economic partnerships aiming at reducing critical dependencies in strategic sectors, protecting critical infrastructures, and deploying tools to counter economic coercion, so strengthening economic security.[31]

OVERSIGHT OF INDUSTRY AT THE NATIONAL LEVEL

By implementing a sound trade control system, governments can more effectively monitor and regulate the flow of strategic goods. Such monitoring not only enhances their understanding of domestic industrial capabilities but also yields deeper insights

28. FATF (2018), Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, FATF, Paris, pp. 3-4.

29. European Commission, Hybrid threats (https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en).

30. See: Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I, 17.5.2019, p. 13–19 ; and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I, 17.5.2019, p. 1–12.

31. See: European Commission, Joint Communication to the European Parliament, The European Council and The Council On "European Economic Security Strategy", JOIN(2023) 20 final, Brussels, 20.06.2023 pp. 7-12.

into the sectors involved in their production and management— revealing both their strengths, such as critical roles in global supply chains, and their vulnerabilities, including economic dependencies. Ultimately, this informed approach enables the formulation of more targeted and effective policy measures.

BUSINESS RELIABILITY, DEVELOPMENT, AND ENHANCING COOPERATION

By establishing robust STC frameworks, governments impose certain obligations on operators (industry, research organisations, academia), taking the form of compliance measures, to control the flow of sensitive technologies and to prevent their misuse. Therefore, STCs can provide a framework for encouraging responsible trade and increase compliance amongst national operators. Through internal management systems, including for conducting due diligence on potential customers and business partners (notably, country of destination, end user, and end use), businesses can mitigate the risk of engaging in transactions with entities that may misuse dual-use items. In addition, trade control systems enhance the accountability and transparency of companies, which in turn can enhance their reputation and reliability, thereby promoting a stable and predictable business environment conducive to long-term economic growth.[32]

32. See: Sacedon-Dimayacyac, J. (2024). The Philippines. In Paile, S., Michel, Q., & Vella, V. (2024). Elaborating a Strategic Trade System of Dual-Use Items Experiences from the European Union, Morocco, the Philippines, Serbia, Singapore and Ukraine. Publications Office of the European Union, p. 80.

Cooperation between governments and businesses is essential for developing effective STCs and Internal Compliance Programmes (ICPs). The private sector contributes valuable trade data, practical approaches, and expertise, helping to build robust compliance systems. This collaboration aligns regulatory frameworks with industry needs, enhancing trade compliance and risk mitigation. As noted in the STM Office Annual Report 2024,[33] such partnerships are key to a secure and efficient trading environment.

33. Strategic Trade Management Office Annual Report 2024, the Philippines.

Finally, having some level of common established standards can create a level playing field that encourages fair competition and innovation between like-minded countries, thus facilitating business development and enhancing cooperation among international actors.[34] This can lead to increased investment in research and development, driving economic development and encouraging cooperation between industry and government, eventually developing new technologies and markets, thereby strengthening the overall economic ecosystem.

34. Paile, S., Michel, Q., & Vella, V. (2024). Op. cit., pp. 7, 62, 66.

FINANCIAL AND ECONOMIC REPUTATION, FOREIGN INVESTMENT ATTRACTION AND FACILITATION

The implementation of trade controls and the prevention of illicit trade activities, including financing proliferation, enhance a nation's credibility in the global financial system, as they demonstrate the country's commitment to stability, transparency, and the rule of law. This promotes the country an attractive destination for foreign investment, while leading to increased access to international capital markets, which boosts economic growth and development.

ACCESSING HIGH-TECHNOLOGY TRADE

Having a well-consolidated STC system is a guarantee of security standards that builds trust among countries. Alignment with MECRs, such as the Wassenaar Arrangement and the Missile Technology Control Regime, is generally a prerequisite for accessing high-technology markets and participating in global supply chains. By implementing robust trade controls, nations can demonstrate their commitment to international non-proliferation norms and gain access to cutting-edge technologies, enhancing their economic competitiveness and technological prowess.[35] The promotion of international cooperation on dual-use technologies for peaceful purposes is often presented, especially by emerging economies, as part of the non-proliferation bargain.[36]

35. Sánchez-Cobaleda, A., Paile, S., Michel, Q. (2024). An STC system: why?. In Paile, S., Michel, Q., & Vella, V. (2024). Op. cit., p. 26

36. Meier, O. (2013). Dual-use technology transfers and the legitimacy of non-proliferation regimes. In Technology Transfers and Non-Proliferation (pp. 3-21). Routledge, pp. 11-14.

FACILITATE LEGITIMATE TRADE

One of the main objectives of STCs is to strike a balance between security and economic interests by facilitating legitimate trade and preventing the proliferation of WMDs through a system of trade authorisations, including risk assessment procedures. Whilst strategic trade accounts for only a small portion of overall trade, it has a much greater impact on (international) security. By streamlining the trade control process, governments can achieve non-proliferation objectives without unduly impeding trade for peaceful purposes, minimising the administrative burden on businesses, reducing costs and enhancing efficiency. An additional example can be drawn from the sanctions imposed on Russia. Over successive packages, these restrictive measures have broadened beyond Russian entities to include actors outside Russia that provide direct or indirect support to its military-industrial complex or engage in sanction circumvention. This development underscores the role of STCs in facilitating legitimate activities. By clearly identifying and restricting high-risk entities, such controls help maintain the integrity of global supply chains and ensure that lawful trade can continue without inadvertently contributing to prohibited military capabilities.

MAINTAINING NATIONAL STOCKS AND SUPPLIES

Guaranteeing the security of national stocks and supplies is essential for economic resilience. STCs ensure that critical technologies are not depleted or diverted, maintaining adequate reserves for domestic use. This is particularly important in times of crisis, such as pandemics or natural disasters, where the availability of essential supplies, such as semiconductors, can be a matter of national security and economic stability.

TECHNOLOGICAL COMPETITIVENESS

STCs can safeguard technology development, as they protect sensitive technologies and intellectual property from being exploited by foreign competitors. By controlling the export of advanced technologies, countries can safeguard their innovative edge, ensuring that they remain at the forefront of technological progress. This, in turn, drives economic growth and enhances national competitiveness in the global market.

LEVEL-PLAYING FIELD

Adherence to international non-proliferation standards contributes to a level playing field by ensuring that all businesses operate within the same regulatory framework. This negates unfair competition and promotes a competitive and fairer trading environment.[37]

37. See : European Commission, White paper on export controls, Brussels, 24.1.2024, COM(2024) 25 final, pp. 12-13; Paile, S., Michel, Q., & Vella, V. (2024). Op. cit., pp. 7, 62, 66.

1.3 GEOPOLITICAL RATIONALES

STCs for dual-use items represent a valuable tool for navigating the complexities of the global geopolitical landscape, as they address various key geopolitical issues that underpin international relations, thereby enhancing a nation's ability to operate effectively on the global stage.

CIVIL/MILITARY SYNERGIES

Civil/military synergies may be enhanced through STCs, which ensures that dual-use technologies are developed and deployed in a manner that benefits both civilian and military sectors while preventing misuses.[38] For instance, advancements in artificial intelligence (AI) can be leveraged for both civilian, such as healthcare and transportation, and military applications, such as autonomous weapons systems and cyber defence. By controlling the export of these technologies, governments can prevent their proliferation to potential adversaries while stimulating innovation and technological advancements that have dual applications. This synergy strengthens defence capabilities and economic competitiveness.[39]

38. European Commission, White paper on options for enhancing support for research and development involving technologies with dual-use potential, Brussels, 24.1.2024, COM(2024) 27 final, p. 6.

39. Ibid., pp. 5, 18.

STRATEGIC AUTONOMY AND TRUSTWORTHY SUPPLY CHAINS

Trustworthy supply chains and, more generally, strategic autonomy are fundamental to making independent decisions in matters of national security and foreign policy. By implementing comprehensive STCs, including, inter alia, mechanisms to screen foreign direct investment, countries can protect their critical infrastructure–by preventing external actors from taking control of it–, mitigate the risk of supply chain disruption, or compromise–by reducing reliance on foreign and unstable suppliers. By effectively enforcing STCs, countries can maintain the trustworthiness of their supply chains and strengthen their geopolitical standing, notably by reducing their vulnerability to external threats such as the weaponisation of economic dependencies.[40]

40. European Commission, White paper on export controls, Brussels, 24.1.2024, COM(2024) 25 final, p. 11.

INTERNATIONAL REPUTATION AND PARTNERSHIP RELIABILITY

As for financial reputation, international reputation and partnerships' reliability are reinforced by the establishment of STCs, which demonstrate a country's commitment to international non-proliferation norms, security cooperation, and responsible trade practices.[41] This builds trust and credibility with allies and partners, encouraging stronger and more reliable international partnerships. This strengthens a country's geopolitical influence and contributes to a more stable and secure international environment.

41. Jesudevan, V., (2024). Singapore. In Paile, S., Michel, Q., & Vella, V. (2024). Op. cit., pp. 104-105.

REGIONAL REFERENCE AND LEADERSHIP

By demonstrating their commitment to regional security and stability, nations can emerge as leaders and points of reference in their respective regions.[42] This strengthens their geopolitical position and influence, enabling them to shape regional dynamics and promote their national interests more effectively.

42. See: Sánchez-Cobaleda, A., Paile, S., Michel, Q. (2024). An STC system: why?. In Paile, S., Michel, Q., & Vella, V. (2024). Op. cit., pp. 26, 29.

1.4 ALIGNMENT WITH THE INTERNATIONAL FRAMEWORK

STC systems must be grounded in and build upon existing international legally and politically binding obligations which have strengthened over time, forming the foundation of the global non-proliferation regime. Since the second half of the 20th century, international conventions have been established to address the non-proliferation of WMDs and related items, their use, and controls over their legitimate transfer. These consist of both soft and hard laws, depending on their legal and/or political nature. Collectively, they require states parties to establish and implement STCs for dual-use items. In this context, countries must implement the objectives of these international arrangements through their national trade control legislations.

LEGALLY BINDING OBLIGATIONS

The backbone of the international architecture of STCs consists of a few but foundational legally binding treaties negotiated and adopted at the international level. These include three key international treaties and one universal normative act, as outlined below:

- The 1968 **Treaty on Non-Proliferation of Nuclear Weapons** requires states that had not developed nuclear weapons prior to 1968 to commit to never developing or acquiring them.[43] In return, these states are granted facilitated access to the "peaceful uses" of nuclear technology, though under specific controls and safeguards. Meanwhile, nuclear weapon states are required to decommission their arsenals and facilitate the

43. "Treaty on the Non-Proliferation of Nuclear Weapons," opened for signature July 1, 1968, Treaty Series: Treaties and International Agreements Registered of Filed and Recorded with the Secretariat of the United Nations 729, no. 10485 (1974).

transfer of nuclear technology for peaceful uses to non-nuclear-weapon states. The treaty also mandates safeguards on the transfer of certain dual-use items (referred to as "source or special fissionable material in all peaceful nuclear activities") to ensure their exclusively peaceful use. Compliance with non-proliferation commitments is monitored by the International Atomic Energy Agency (IAEA).

- The 1972 **Biological Weapons Convention (BWC)** prohibits an entire category of WMDs by banning states parties from developing, producing, acquiring, transferring, stockpiling, and using biological and toxin-based weapons.[44] The treaty makes an (indirect) reference to dual-use items in its Article I(1), which allows exceptions for the peaceful use of microbial or other biological agents, as well as toxins, provided they are of a type and in quantities justifiable for legitimate purposes. However, the BWC relies solely on confidence-building measures and lacks a formal verification regime.

- The 1997 **Chemical Weapons Convention** seeks to eliminate the entire category of chemical weapons by prohibiting states parties from developing, producing, acquiring, stockpiling, retaining, transferring, or using such weapons.[45] States parties commit to enforcing this prohibition concerning natural or legal persons within their jurisdiction and to destroying all existing chemical weapons. However, the CWC allows for the development and transfer of certain chemicals and precursors for limited, legitimate purposes under a specific verification regime. The Organisation for the Prohibition of Chemical Weapons (OPCW) is responsible for monitoring compliance with CWC obligations.

- The 2004 **United Nations Security Council Resolution 1540**, adopted under Chapter VII of the UN Charter, requires all UN Member States to adopt and enforce national laws prohibiting non-state actors from acquiring, developing, and transferring WMDs and their delivery systems.[46] It also calls on states to implement controls on WMD-related items, including controls on export, transit, trans-shipment, re-export, and financing. Unlike other non-proliferation legal instruments, UNSCR 1540 addresses the full spectrum of WMDs, including their delivery systems and related items, and specifically focuses on non-state actors. The resolution encourages states to strengthen their commitment to multilateral cooperation, thus complementing and strengthening existing non-proliferation regimes.[47]

While these legally-binding conventions provide for the principles and general obligations surrounding the non-proliferation of WMDs and related items—most notably the obligation to establish and enforce STCs (UNSCR 1540)—, they do not specify the items to be controlled; nor do they provide control lists (with the exception of the CWC) for national implementation. The definition of these lists and the coordination of trade policies on dual-use items among countries proceeds through other forums and instruments. Unlike the legally binding conventions mentioned above, these forums and instruments are politically binding, as outlined below.

44. "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction", opened for signature April 10, 1972, United Nations Office of Disarmament Affairs, 1975.

45. "Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction", opened for signature January 13, 1993, United Nations, Treaty Series, vol. 1975.

46. United Nations Security Council Resolution 1540, S/RES/1540, New York, April 2004.

47. Johannes Rath, Monique Ischi, Dana Perkins, "Evolution of Different Dual-use Concepts in International and National Law and Its Implications on Research Ethics and Governance," Sci Eng Ethics (2014) 20, p 776.

POLITICALLY BINDING COMMITMENTS

To address the gap in the above-mentioned legal instruments, soft-law norms from the MECRs have been introduced to complement them. These are informal groups of supplying states that gather to consult multilaterally, define control lists, and establish the criteria for assessing transfers of sensitive items. MECRs focus on specific categories, including nuclear, chemical, biological, and conventional weapons and their means of delivery. Unlike legally binding treaties, the agreements reached within these regimes are politically binding and, therefore, not legally enforceable unless transposed into national legislation.

The most significant MECRs—four in total—form the basis for controlling sensitive items in the majority of countries.[48] Additionally, many states follow the principles and guidelines of these regimes even if they are not formal members. An overview of these MECRs is provided below.

48. The Zangger Committee, also known as "The Nuclear Exporters Committee" and initially formed to serve as the faithful interpreter of the NPT Article III.2, is also a relevant MECR, as it identified a list of key nuclear fuel cycle items to be controlled: the Trigger List. However, when referring to the MECRs, the literature generally refers to the four main ones, i.e. Nuclear Supplies Group, Australia Group, MTCR, and Wassenaar Arrangement.

- The 1995 **Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies** (hereinafter 'the WA') is an informal group of arms and sensitive item producers or exporters committed to non-proliferation policies and effective export controls. Its primary objective is to "contribute to regional and international security and stability" by promoting transparency and the responsible transfer of conventional arms and dual-use goods and technologies. The aim of the arrangement is to prevent civil technologies and materials from being used to enhance military capacities. At the operational level, the WA maintains two control lists: the list of dual-use goods and technologies, and the munitions list (covering conventional weapons and related items). Participating states ensure that the transfer of such items does not contribute to the development or enhancement of military capabilities or is diverted for such purposes, and will therefore prevent their unauthorised transfer or retransfer. While states retain the sovereign authority to approve or deny transfers, they nevertheless adhere to a set of 'guidelines, elements, and procedures' established through multilateral negotiation, and which should be applied within their national legislation and policies.[49] Additionally, a series of "best practices" documents are provided on various topics, such as implementing controls on intangible technology transfers, managing transit and transshipment, and ensuring effective enforcement.[50]

49. "About us", the Wassenaar Arrangement, accessed March 2025,https://www.wassenaar.org/about-us/

50. "Best practices and guidelines," the Wassenaar Arrangement, accessed March 2025.

- The 1974 **Nuclear Suppliers Group** (NSG) is a collective of nuclear supplier countries seeking to prevent the proliferation of nuclear weapons. It aims to control exports of nuclear materials and technologies which could be used for military nuclear programmes, while facilitating their transfer for peaceful nuclear activities under strict safeguards.[51] The NSG has developed guidelines that participating states follow when making national decisions about the kinds of exports to authorise.[52] Specifically, it implements two sets of guidelines that are adopted by consensus.[53] The Guidelines for nuclear transfers (INFCIRC/254, Part 1) are known as "the trigger list" as it activates export controls and IAEA safeguards for peaceful nuclear transfers to any non-nuclear-weapon state. It outlines conditions like physical protection, special controls on sensitive exports, safeguards, and controls on retransfers. The Guidelines for transfers of nuclear-

51. "About us", Nuclear Suppliers Group, accessed March 23, 2025, https://nuclearsuppliersgroup.org/index.php/en/about/about-the-nsg ; https://www.nti.org/education-center/treaties-and-regimes/nuclear-suppliers-group-nsg/

52. Ian Anthony, "Multilateral export controls," in SIPRI yearbook 2001: armaments, disarmament and international security, p. 752.

53. "Guidelines", Nuclear Suppliers Group, accessed March 23, 2025, https://nuclearsuppliersgroup.org/index.php/en/guidelines/nsg-guidelines

related dual-use equipment, materials, software, and related technology (INFCIRC/254, Part 2) outlines the principles, definitions, and export control list of equipment, materials, software, and related technology that could be used to contribute to nuclear proliferation, to acts of nuclear terrorisms, and to unsafeguarded nuclear activities.

• The 1984 **Australia Group** (AG) serves as an informal forum through which states harmonise export controls to prevent the development of chemical and biological weapons. This initiative responds to the legal obligations accepted under the BWC and the CWC—all AG participating states are parties to these treaties. To better coordinate national export control measures, the AG adopted a set of Guidelines for Transfers of Sensitive Chemical or Biological Items, explicitly aiming to control tangible and intangible transfers that could contribute to the development of chemical or biological weapons by states or non-state actors. Notably, the AG was a pioneer in recognising intangible transfers and acknowledging the potential role of non-state actors, including terrorist organisations, in WMD proliferation.[54] Similar to other MECRs, the AG encourages states to develop export licensing measures that effectively prevent the spread of chemical and biological weapons while remaining practical to implement. Importantly, these measures should not hinder the legitimate trade of items used for peaceful, lawful purposes.[55]

• The aim of the 1987 **Missile Technology Control Regime** (MTCR) is to prevent the proliferation of delivery systems for WMDs by establishing guidelines and principles to regulate their transfer. The regime does not seek to restrict access to technologies needed for peaceful end uses, such as civilian aerospace programmes or international scientific cooperation, but rather to prevent their diversion to WMD delivery system programmes. The MTCR guidelines help build confidence among suppliers by ensuring that the transfer of such technology is not misused for non-peaceful purposes.

As illustrated, each MECR defines a specific category of items subject to control. These controls are often integrated into comprehensive documents, as seen in the EU framework. The EU consolidates decisions from different regimes into a comprehensive control list of dual-use items—Annex I to EU Dual-Use Regulation—which is regularly updated based on changes made by MECRs. This list is also adopted by other (third) countries that may use the EU legal framework as a benchmark for regulating trade in dual-use items.

54. Ana Sánchez-Cobaleda, "Defining 'dual-use items': legal approximations to an ever-relevant notion", The Nonproliferation Review (2023), pp. 12-13.

55. "About us", Australia Group, accessed March 23, 2025, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/introduction.html

OTHER INTERNATIONAL PRINCIPLES AND INITIATIVES IN NON-PROLIFERATION

In the realm of STCs, other initiatives, international principles, and confidence-building mechanisms complement legally and politically binding measures. These serve as complementary instruments to further strengthen the framework of non-proliferation and export controls.

For example, the 2002 Hague Code of Conduct against Ballistic Missile Proliferation (HCOC) is a politically binding document aimed at curbing ballistic missile proliferation.[56] It is the only multilateral transparency and confidence-building instrument that specifically targets the spread of ballistic missiles. from the result of international efforts to regulate ballistic missiles capable of carrying WMDs, the HCOC complements the MTCR but has a broader membership, being open to all states. Participating states commit to voluntarily notifying launches of ballistic missiles and space launch vehicles, as well as test flights, in addition to submitting annual declarations on their ballistic missile and space launch vehicle policies. The HCOC fully acknowledges and supports the peaceful use of such systems, particularly for space exploration; however, it also calls on states to refrain from supporting ballistic missile programmes in countries that seek to illicitly develop or acquire WMDs.

Other notable international initiatives contributing to non-proliferation efforts include the Proliferation Security Initiative (PSI) and the Global Initiative to Combat Nuclear Terrorism (GICNT).

The PSI, launched in 2003, is an informal, voluntary partnership of states aimed at enhancing cooperation to interdict illicit transfers of WMDs, their delivery systems, and related materials and technologies;[57] in other words, it is designed to strengthen existing STC enforcement mechanisms. Participating states commit to the PSI Interdiction Principles,[58] which call for effective measures to interdict illicit transfers by states or non-state actors. The PSI is regarded as a key component of the global WMD non-proliferation framework,[59] aligning with national legal authorities and relevant international laws, such as UNSCR 1540, while complementing existing counter-proliferation efforts.

The Global Initiative to Combat Nuclear Terrorism (GICNT) is a voluntary partnership of countries and international observer organisations dedicated to enhancing the global capacity to prevent, detect, and respond to nuclear terrorism.[60] Beyond conducting field exercises, workshops, and similar training events, the GICNT has developed foundational documents and resources through collaboration among partner nations.[61] All members voluntarily commit to the GICNT Statement of Principles, which includes measures to improve the accounting for and control of nuclear materials, to detect and deter illicit trafficking, and to strengthen legal frameworks for prosecuting acts of nuclear terrorism.[62]

56. "What is HCoC?", the Hague Code of Conduct, accessed March 23, 2025, https://www.hcoc.at

57. "The Proliferation Security Initiative," Proliferation Security Initiative PSI, accessed March 23, 2025. https://www.psi-online.info/psi-info-en/2075520-2075520; "Proliferation Security Initiative (PSI)", NTI, accessed March 23, 2025, https://www.nti.org/education-center/treaties-and-regimes/proliferation-security-initiative-psi/.

58. As of March 25 2025, 116 countries have endorsed the PSI; "Proliferation Security Initiative," US Department of State, accessed March 23, 2025, https://www.state.gov/bureau-of-international-security-and-nonproliferation/proliferation-security-initiative; "Proliferation Security Initiative: Statement of Interdiction Principles," Proliferation Security Initiative PSI, May 14, 2018.

59. "Proliferation Security Initiative," US Department of State.

60. "The Global Initiative To Combat Nuclear Terrorism," US Department of State, accessed March 23, 2025, https://2017-2021.state.gov/the-global-initiative-to-combat-nuclear-terrorism/.

61. Luoto, J., "The GICNT Contribution to Nuclear Security," in International Cooperation for Enhancing Nuclear Safety, Security, Safeguards and Non-proliferation–60 Years of IAEA and EURATOM, eds. Maiani, L., Abousahl, S., Plastino, W, Springer Proceedings in Physics, vol 206. (Springer, Berlin, Heidelberg, 2018).

62. "The Global Initiative to Combat Nuclear Terrorism," Arms Control Association, accessed March 23, 2025, https://www.armscontrol.org/specialprojects/nnpm/GICNT.

1.5 OTHER CONSIDERATIONS BEYOND NON-PROLIFERATION

In addition to national security and international law considerations, STCs can also raise significant ethical questions. This is highlighted, for instance, in the UK House of Commons report "Developments in UK Strategic Export Controls", which states, "The export of, and trade in, defence and security goods raises major questions of ethics, national security, and international law".[63] Similarly, various research organisations mention human rights and ethical considerations among their guiding principles for export controls. These concerns are particularly relevant in cases where transfers may impact human rights, such as surveillance technologies used for repression or items supporting terrorism, corruption, or other illicit activities.[64]

However, explicit references to ethical issues are not frequently found in government declarations and policies on dual-use trade controls. Ethical concerns are more often associated with research contexts, where there is a potential risk of research outcomes being "misused." The EU Recommendations on research involving dual-use items, for example, warns that 'dual-use' in the context of research is often interpreted in its broad sense, encompassing both the desired civil and potential military applications of research, as well as its potential misuse for unethical purposes.[65] Importantly, the EU Recommendations emphasise that while all entities must comply with laws and regulations relevant to dual-use items, these legal obligations are distinct from—though they may overlap with—ethical motivations or self-restrictions aimed at preventing the misuse of research. The document underscores the importance of distinguishing the legal obligation to comply with dual-use regulations from the concept of the "misuse of research," which refers to research that could be exploited for unethical purposes. This includes research involving minority or vulnerable groups or developing social, behavioural, or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass, or intimidate individuals.[66] Although ethical considerations can guide decision making in certain transactions, they cannot replace the requirement to comply with STC laws.

Additionally, considerations related to environmental protection and public health can also arise in the context of STCs. However, similar to ethical concerns, these considerations are often framed according to the concept of the "misuse of research" with regard their potential applications that may violate human rights or compromise the safety of people, animals, or the environment. This interplay between legal and ethical obligations is complex, and while there is often overlap, they do not always fully align.[67]

In conclusion, STCs of dual-use items are necessary for a multitude of reasons, ranging from national security, economic stability, and technological development to ethical considerations and international peace. By effectively implementing and enforcing a comprehensive STC system, countries can protect their interests and

63. House of Commons Committees on Arms Export Controls, Developments in UK Strategic Export Controls, First Joint Report of Session 2022–23, October 28, 2022, https://committees.parliament.uk/publications/30529/documents/176077/default/.

64. South East Technology University (SETU), "Export control policy", January 21, 2025, https://www.setu.ie/Craft/assets/research/Export-Controls-Policy-V1.0-Approved-21-Jan-2025.pdf

65. Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, C/2021/6636, OJ L 338, 23 September 2021,p. 9.

66. "Guidelines for researchers on dual use and misuse of research", Flemish Interuniversity Council, 2022, https://vlir.be/wp-content/uploads/2022/10/VLIR-Dual-Use-2022-EN.pdf

67. Ibid., p. 5.

contribute to a more secure and stable global environment. For STCs to be truly effective, international cooperation is essential. The more countries adopt harmonised international standards and best practices, the more effective these controls will be, and the safer and fairer the global environment will be.

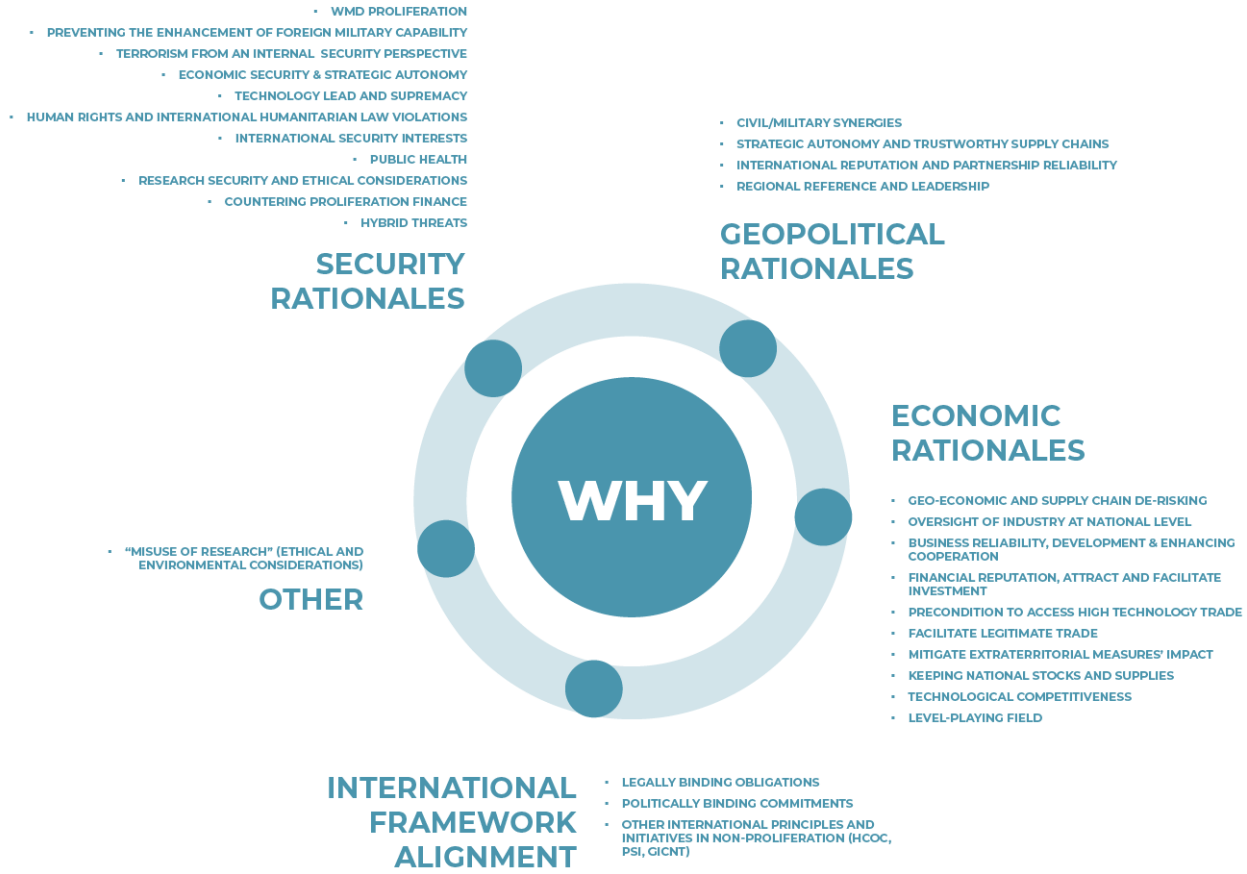


Figure 1 Overview of WHY

WHO: ACTORS INVOLVED IN A STRATEGIC TRADE CONTROL SYSTEM

WHO: ACTORS INVOLVED IN A STRATEGIC TRADE CONTROL SYSTEM

Numerous and varied actors are directly or indirectly involved in the establishment, maintenance, and implementation of STC systems and rules. These actors operate at international, regional, and national levels. They can be classified into three primary categories directly involved in the process, along with a fourth category for stakeholders involved in a more indirect manner. The main categories are: international/regional organisations and regimes; national authorities; operators; and other stakeholders.

2.1 INTERNATIONAL/REGIONAL ORGANISATIONS AND REGIMES

International/regional organisations and regimes play a crucial role in defining and issuing legal and political principles, obligations, and practices in STCs. These efforts aim to harmonise national practices, provide platforms for multilateral negotiations, and legitimise the standards and practices developed. Notable examples of international organisations include the United Nations and MECRs. Additionally, this category encompasses organisations that, instead of setting principles and obligations, actively support their implementation by conducting verification activities and providing technical assistance. For instance, the OPCW works to implement the CWC, focusing on eliminating chemical weapons and promoting peaceful chemistry. Similarly, the IAEA, an autonomous international organisation within the UN system, plays a critical verification role under the NPT.[68]

Regarding relevant regional organisations, notable examples include the European Union, which establishes and coordinates export control rules among its member states. Similarly, the African Union (AU) actively addresses regional security challenges, with a particular focus on non-proliferation initiatives. For example, the AU oversees the implementation of the Pelindaba Treaty, which establishes a nuclear-weapon-free zone in Africa.[69] In parallel, the Agency for the Prohibition of Nuclear Weapons inLatin America and the Caribbean (OPANAL) ensures compliance with the Tlatelolco Treaty, which creates a comparable nuclear weapon-free zone in Latin America and the Caribbean.[70]

68. IAEA factsheet, https://www.un.org/en/conf/npt/2015/pdf/IAEA%20factsheet.pdf

69. African Union website, https://au.int/en/treaties/african-nuclear-weapon-free-zone-treaty-pelindaba-treaty.

70. OPANL website, https://opanal.org/.

2.2 NATIONAL AUTHORITIES

National authorities are pivotal in STC systems, as they hold the competence and authority to transpose international principles and obligations into national legislation and regulations. Lawmakers and policymakers draft laws and define national and foreign policies related to STCs, including authorisation mechanisms and penalties for violations. Once the national framework is established, licensing or permitting authorities, along with enforcement agencies, implement the associated legislation and regulations. Licensing/permitting authorities may include ministries of foreign affairs, trade, commerce, industry, development, and defence, as well as technical agencies involved in energy or science.[71] Enforcement agencies, particularly customs, handle risk assessments, inspections, and audits, often cooperating with investigators and prosecutors. Additionally, some national authorities have dedicated units that conduct outreach and in-reach activities to raise awareness and provide technical training. These activities are essential for strengthening the understanding of STC regulations. Outreach efforts typically target third countries to enhance international cooperation, while in-reach initiatives focus on training national actors within government agencies or among operators.

71. **"Strategic Trade Control Enforcement (STCE) Implementation Guide 2023," World Customs Organisation, 2023, p. 16.**

2.3 OPERATORS

Operators are directly subject to the laws and policies that nations adopt and enforce. Their compliance is crucial for an effective STC system, as aimed at preventing the proliferation of WMDs and addressing conventional (e.g., airspace violations) and non-conventional (e.g., cyberthreats) risks. Operators are the 'eyes and ears' of the STC system in the sense that they have direct contact with research partners, suppliers, and customers in other countries. Some contacts are the results of longstanding relationships, while others are novel research or business partners. They are the first line of defence in detecting suspected end use of concern, or a risk of diversion. Rules target operators such as exporters, importers, brokers, providers of technical assistance, freight forwarders, and carriers (including shipping companies). While the term 'operators' traditionally referred primarily to industries, the evolving nature of STCs and changing geopolitical contexts necessitated the inclusion of researchers, research organisations, and academia within this category.

2.4 OTHER STAKEHOLDERS

Other stakeholders include entities indirectly involved in STC systems, such as financial institutions, donors, outreach providers, non-governmental organisations (NGOs), and sectoral associations. These actors may not be operators or competent authorities, but play significant roles in representing interests, lobbying for specific operator categories, and providing outreach activities that influence a country's STC system and its application by operators.

Financial institutions and funding bodies can also be crucial as they can establish criteria for financing strategic activities, define their boundaries, and ensure compliance with STC rules to avoid funding violations.

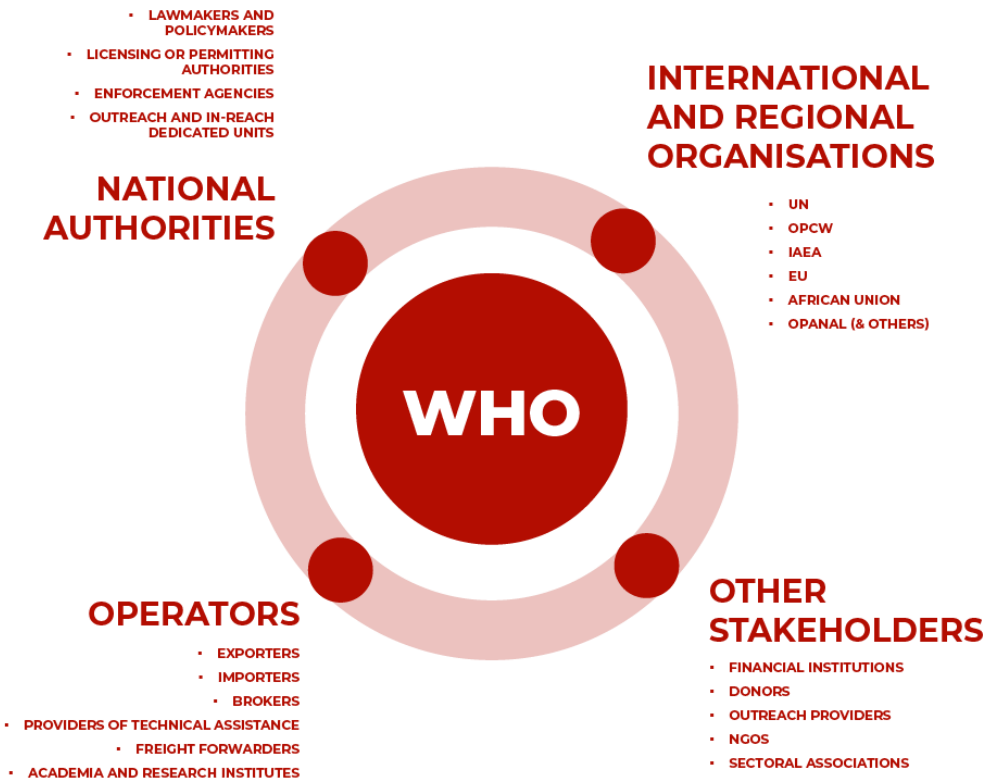


Figure 2 Actors involved in STC systems

WHAT: ITEMS AND ACTIVITIES COVERED BY A STRATEGIC TRADE CONTROL SYSTEM

WHAT: ITEMS AND ACTIVITIES COVERED BY A STRATEGIC TRADE CONTROL SYSTEM

3.1 ITEMS (GOODS, SOFTWARE, AND TECHNOLOGIES)

In order to establish an effective STC system, a wide range of tangible and intangible items may be considered for any of the various reasons exposed *supra*.[72] These can consist of goods, software, and technologies. Although each category of items may have its own specific definitions, in general terms, 'goods' refers to tangible systems, equipment, components, and materials; the term 'software' refers to a collection of one or more programs (i.e., a sequence of instructions to carry out a process in, or that isconvertible into, a form executable by an electronic computer) fixed in any tangible medium of expressions; and finally, the term 'technology' refers to any information—which may take the form of technical data (such as blueprints, plans, diagrams, models, formulae, algorithms,) or technical assistance (such as instructions, skills, training, working knowledge and consulting services)—necessary for the development, production, or use of an item.

72. **See section "Why: rationales behind a strategic trade control system".**

Technology transfers, in particular, pose a challenge to the enforcement of STCs. This is notably the case in academia and research, where sharing research results is of paramount importance in the context of a 'publish or perish' culture. The idea of 'research involving dual-use items' has gained particular attention and presents potentially conflicting interests: scientific progress on the one hand, and security on the other. Research papers and publications in the biotechnology research field, for instance, are usually aimed at generating scientific knowledge and improving the early diagnosis, treatment, and prevention of disease. However, scientific knowledge shared by teaching, collaborating, or working on research involving sensitive technologies with dual-use potential could also end up in the wrong hands and pose biosecurity threats. An STC system should also consider the strategic and dual-use nature of research to prevent security-related risks when sensitive technology is transferred.

Items covered by an STC system can be divided into three main categories according to their potential application: i) conventional weapons and defence-related items; ii) dual-use items; and, iii) other strategic items depending on national interests.

CONVENTIONAL WEAPONS AND DEFENCE-RELATED ITEMS

In very broad terms, conventional weapons are weapons other than WMDs which comprise, in accordance with the United Nations Register of Conventional Arms (UNROCA), seven categories: battle tanks, armoured combat vehicles, large-calibre artillery systems, combat aircraft and unmanned combat aerial vehicles (UCAVs), attack helicopters and rotary-wing UCAVs, warships, and missiles and missile launchers.[73] Other defence-related items are also part of this category and comprise components and technology used for the development, maintenance, and operation of conventional weapons. While conventional weapons and defence-related items are essential for national defence and security reasons, some of these goods and technologies could beeasily accessible to state and non-state actors. Hence, it is important they fall under the scope of an STC system to prevent their transfer and use in armed conflict, human rights violations, or terrorist activities. For its part, the Arms Trade Treaty (ATT), adopted in 2013 to regulate international trade in conventional arms, contains a brief list of 'conventional arms' to which the treaty applies (article 2) and which mirrors the abovementioned UNROCA categories, with the addition of a supplementary category covering small arms and light weapons (SALWs). Also worth mentioning is the Common Military List of the European Union,[74] which places items specially designed for military use under export controls within the EU in order to prevent illicit trafficking in conventional arms, internal repression, international aggression, or contributions to regional instability. From a non-legally binding perspective, the Wassenaar Arrangement is a MECR in which participating states informally agree to maintain national export controls on items included in two control lists: the Munition List, which contains conventional arms; and the List of Dual-Use Goods and Technologies.[75] Its Munition List covers twenty-two categories of equipment specially designed for military use, such as ammunition, parts and components, and related software and technology.

73. For a more precise definition of these conventional arms, see https://www.unroca.org/categories.

74. Common Military List of the European Union adopted by the Council on 17 February 2020 (equipment covered by Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment).

75. Wassenaar Arrangement, Control lists, https://www.wassenaar.org/control-lists/.

DUAL-USE ITEMS

The concept of 'dual-use items' refers to goods, software, and technology that can be used for both civil and military purposes. Despite the lack of an internationally agreed definition, dual-use items have been widely discussed and their control considered a key component of an effective STC system. Dual-use items are certainly not new, but the concept has gradually broadened as the understanding of such has evolved. The term includes tangible and intangible items, i.e., dual-use goods, software, and technology. Indeed, there is increasing concern regarding intangible transfers of technology and their control. Knowledge and information, for instance, can be transferred through electronic means—such as email attachments, cloud-based storage services, or simply uploads and downloads on electronic platforms—to be used for civilian and/or military purposes. Also, dual-use items have traditionally been linked to WMDs, but the concept extends far beyond this. Items that might be misused cannot be merely categorised as military or non-military; rather, a wider range of items with legitimate commercial applications have dual-use potential, and can be used for peaceful or non-peaceful, benevolent or malevolent, ends[76].

76. Cfr. Sánchez Cobaleda, A. 'Definition of concepts : dual-use goods', in Michel, Q. et al, A decade of evolution of dual-use trade control concepts : strengthening or weakening non-proliferation of WMD, European Studies Unit, 2021, p. 12.

Strategic dual-use items might include the following:

WMD-related items and delivery systems

WMD-related items are goods, software, and technology that can be used for the design, development, production, or use in nuclear, biological, and chemical weapons. Their delivery systems—the means to transport and deploy WMDs—should also be considered strategic dual-use items, and include, for instance, ballistic missiles, cruise missiles, combat aircraft, and unmanned aerial vehicles (UAVs).

UNSCR 1540 obliges all states to 'take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery' (OP 3). Despite the lack of a list of items attached, UNSCR 1540 explicitly refers to 'relevant multilateral treaties and arrangements', thus linking the resolution to WMD international non-proliferation and disarmament treaties and MECRs.

WMD-related items are listed in various international WMD non-proliferation treaties and MECRs.

Concerning the treaties, the CWC contains Schedules 1, 2, and 3 that classify chemical substances and precursors based on their risk to the treaty's objectives. While chemical items in Schedule 1 are highly dangerous and have few or no legitimate commercial applications, Schedules 2 and 3 include dual-use chemicals that pose significant ormoderate risk but can be used for civil and military ends. Yet, neither the NPT nor the BWC contain nuclear nor biological control lists, respectively. This gap is addressed by the relevant MECRs.

The roles of the MECRs include developing guidelines and control lists of WMD items and their delivery systems. The Zangger Committee—initially created for the interpretation of the terms "especially designed or prepared for" of Art. III.2 of the NPT—established a list of key nuclear fuel cycle items whose transfer triggers the need for IAEA safeguards: the Trigger List. The Nuclear Suppliers Group (NSG) provides two control lists, one covering nuclear-related items that trigger IAEA safeguards when exported for peaceful purposes to any non-nuclear weapon state (NSG Trigger List, INFCIRC/254/Part 1), and the other covering nuclear-related dual-use items (NSG Dual-Use List, INFCIRC/254/Part 2). The AG's Common Control Lists covers both biological and chemical weapons-related items. AG participants are all states parties to the BWC and CWC and support their implementation.[77] Finally, the MTCR provides a control list covering a broad range of equipment, material, and technology, both military and dual-use, that are relevant to missile development, production, and operation in order to prevent the proliferation of WMD delivery systems.

77. See: https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/controllists.html.

Cyber-surveillance items

Cyber-surveillance items can be defined as 'dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting

or analysing data from information and telecommunication systems'.[78] These can be potentially used—especially by state authorities—for internal repression purposes or to commit serious violations of human rights and international humanitarian law. The importance of cyber-surveillance items has increased since the events of the so-called Arab Spring that started in Tunisia in December 2010, where surveillance technology was widely used in various Arab countries to suppress protests and social uprisings. In 2013, the Wassenaar Arrangement amended its List of Dual-Use Goods and Technologies to include cyber-surveillance software, thereby marking the first multilateral recognition of the dual-use nature of cyber-surveillance items. Also, the EU dual-use Regulation (EU) 2021/821 places a strong emphasis on cyber-surveillance items,[79] introducing a 'human rights' perspective. More particularly, the EU dual-use Regulation requires authorisation 'for the export of cyber-surveillance items not listed in Annex I' (Article 5) in order to prevent human rights violations committed with European software and strategic technologies.

78. Cfr. Commission Recommendation (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council, p. 5.

79. The Regulation (EU) 2021/821 of 20 May 2021 understands 'cyber-surveillance items' as 'dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems' (Article 2 (20)).

Conventional weapons-related dual-use items

Certain dual-use items—goods, software, and technologies—that have both civilian and military applications are closely related to conventional weapons because they either enable their use or can aggravate the consequences of such.

The Wassenaar Arrangement was precisely established to control transfers of conventional arms and dual-use items in order to prevent destabilising accumulations, as well as their acquisition by terrorists. While the Wassenaar Arrangement Munitions List covers conventional arms, the List of Dual-Use Goods and Technologies contains over 1,000 items that can be used for civil purposes but may also be used to develop military capabilities, such as electronics, navigation systems, advanced materials, and software, that can contribute to the development or production of conventional weapons.

Based on the Wassenaar Arrangement agreements, the Common Military List of the European Union (EU CML) covers items 'specially designed for military use'. Although some conventional weapon-related dual-use items controlled in the EU Dual-Use Control List may also be included in the EU CML, the technical parameters of the items included in the two lists differ, with those in the EU Dual-Use Control List being more precise and restrictive than those in the EU CML.

Emerging technologies

The latest developments in the spheres of artificial intelligence, additive manufacturing (e.g., 3D printing systems for metals), quantum technologies (e.g., quantum computers), and biotechnology (e.g., DNA synthesis, microencapsulation technology, and genetic engineering) are clear examples of emerging dual-use technologies, while other critical technologies have received attention for their implications regarding the EU's economic security.[80] Such technologies are characterised by rapid development, a novel character, and a high disruptive or destabilising potential, and could contribute, for example, to the production or development of WMD capabilities. Because of their great potential, unpredictable development and resulting applications, emerging

80. European Commission, Annex to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, C(2023) 6689 final, Strasbourg, 3.10.2023.

technologies require more extensive controls—for instance, through catch-all clauses—which enable scientific innovation for peaceful purposes while at the same time mitigate the risk of misuse. Quantum technology is a recent example of an emerging technology that was initially controlled on an occasional basis through 'catch-all controls' and then subjected to systematic control as listed dual-use items.[81]

81. European Commission, 2025 Update of the EU Control List of Dual-Use Items, 8 September 2025, available at : https://policy.trade.ec.europa.eu/news/2025-update-eu-control-list-dual-use-items-2025-09-08_en.

OTHER STRATEGIC ITEMS ACCORDING TO NATIONAL INTERESTS

The consideration of 'strategic items' differs depending on states' national interests. National security is definitely a particular concern, although it is certainly not the only one. Other strategic items might be regarded as critical to a country's security, in the broadest sense of the word. Economic and social well-being might also influence decision making in order to ensure competitiveness, global influence, and economic growth and prosperity. As a result, critical items or technologies could also be covered by an STC system. Considering the differing interests among countries, there are no universal lists in the international realm defining 'other strategic items' that might be of relevance. As an exceptional example, the European Union, Japan, the United Kingdom, and the United States compiled a List of Common High Priority Items covering goods regarded as critical for Russian military systems in the war against Ukraine. The list is divided into four tiers that identify items according to the Harmonised System codes and include dual-use and advanced technology items which are also covered under international sanctions against Russia, such as integrated circuits, radio frequency modules, antennas, ball bearings, and machine tools.[82]

82. Cfr. Bureau of Industry and Security, Common High Priority Items List, US Department of Commerce, 23 February 2024, available at: https://www.bis.gov/licensing/country-guidance/common-high-priority-items-list-chpl.

However, national lists are more likely to be developed according to national interests. The Australian Government, for instance, developed two different lists of minerals that are considered of great importance to the country, not only in terms of defence technology and military capabilities, but also regarding sustainable development, economic prosperity, and other geopolitical considerations. More specifically, the Australian STC system includes a Critical Minerals List and a Strategic Materials List, which cover, for instance, nickel, to ensure a progressive energy transition and a strong resources industry.[83]

83. Cfr. Australian Government, 'Australia's Critical Minerals List and a Strategic Materials List', Critical Minerals Office, 20 February 2024, available at: https://www.industry.gov.au/publications/australias-critical-minerals-list-and-strategic-materials-list.

3.2 ACTIVITIES (TANGIBLE AND INTANGIBLE)

STC regulations may cover a wide range of activities along a supply chain of sensitive items. These can include export, re-export and temporary export, import and temporary import, transit and trans-shipment, technical assistance, brokering services, in-country/Union transfer, financing services, and other services. The specific activities covered may

depend on the regime in question (e.g. dual-use, military items), the type of targeted items (e.g., import controls are often more restrictive for military items than for dual-use items), the economic or political organisation a country belongs to (e.g., controlling intra-transfers may be relevant for the European Union or the Eurasian Economic Union), and the geographical position (e.g., trans-shipment may be particularly relevant in areas that serve as trans-shipment hubs).

It is important to note that activities can occur in both tangible and intangible forms. A common example is the transfer of technology by intangible means, such as a phone call or email, which constitutes an intangible export or intangible technology transfer. Similarly, technical assistance can be provided by giving instructions to repair or maintain a sensitive item, whether in person, in the same laboratory, or remotely through a webinar or lecture. Certain activities, however, can only take place in a tangible form, such as transit or trans-shipment, which, by definition involve the physical movement, loading, or unloading of goods.

Before outlining the different activities that may be subject to control, it is worth noting that the maturity of an STC system may sometimes be assessed according to the types of activities it covers. Similarly, the 1540 Committee evaluates states' implementation of UNSCR 1540 based on country matrices, which include questions on export, re-export, transit, trans-shipment, financing of exports, and services related to exports.[84]

84. "Approved 1540 Committee Matrix", National Implementation – 1540 Matrices, United Nations, accessed September 4, 2025, https://www.un.org/en/sc/1540/documents/Final%20Matrix%20Template%20(E).pdf.

Against this background, below is a general outline of the main activities that may be covered by an STC system.

EXPORT

Export refers to the physical movement or intangible transfer of any item (goods, technology, software) outside the customs territory in question. Examples include selling and shipping a good to a third country, or physically carrying an item abroad in a suitcase. However, in some STC systems, export does not necessarily require the item to leave the customs territory; it may also occur when controlled technology is transferred to a person of a different nationality who is subject to the controls. This is the case of the US 'deemed export', which occurs when controlled technology is released or shared with a foreign person inside the national territory.[85] Additionally, the definition of 'export' also covers scenarios such as the electronic transmission of software or technology, including sending files via email or uploading data to cloud servers accessible from outside the country's customs territory. It is therefore important to appreciate that export controls apply not only to classical commercial transactions but also to research and academic contexts. Closely related to export is re-export, which occurs when a previously imported good is exported again to a third country without undergoing any significant modification or alteration. Controlling re-exports may prove to be crucial to countering circumvention, and for this reason may be restricted or prohibited under sanction regimes in addition to export controls. For instance, authorities may require the inclusion of a "no re-export to Russia" clause in export, sale, supply, or transfer

85. US Department of Commerce, Bureau of Industry and Security, What is a deemed export?, https://www.bis.gov/learn-support/deemed-exports/what-deemed-export.

86. EU "No re-export to Russia" clause

87. For example, the EU provides for the Union General Export Authorisation No EU004 for temporary export for exhibition or fair; 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), Annex II, D. See also US 15 CFR 740.9.

contracts.[86] Finally, temporary export can also be subject to controls. For instance, a licence may be required to temporary export an item for exhibition or fair purposes.[87]

IMPORT

Import is the bringing of an item into a country from abroad. In some cases—such as for weapons or military-related equipment—an import licence may be required. For example, an import could involve ordering and acquiring the chemical agent 'sarin' from a foreign company for scientific or medical research. In a system controlling the import of military items, this transfer may require a licence because sarin appears on the national control list. Import controls can play an important role in tracking, record-keeping, and monitoring the international flow and exchange of sensitive items. They also help ensure compliance with national and international regulations and reduce the risk of diversion to unauthorised end users or prohibited end uses. Additionally, such mechanisms may enable authorities to verify that imported items are used in accordance with regulations and for their intended purpose. Finally, temporary imports may also be subject to controls and require a licence, e.g., for marketing, or for display at an exhibition or trade fair, inspection, test, calibration, or repair.[88]

88. See for example US 15 CFR 740.9.

TRANSIT/TRANS-SHIPMENT

Transit refers to the movement of items through a country's territory en route to a destination outside the customs area. Transit may include the passage of a cargo through a country to reach another country, or temporary storage in a bonded warehouse or an aircraft stopping in another territory without unloading cargo. If goods are physically unloaded and reloaded from one means of transport to another during their passage through a foreign territory, this is considered a trans-shipment. A key reason for controlling such activities is to reduce the risk of circumvention and diversion to unauthorised end users or uses. One example of such controls is the EU's restrictions on the transit of dual-use items via Russia, as set out in its various sanction packages.[89]

89. Enzo Caponetti, "Overview of EU sanctions against Russia and Belarus - EU reaction to Russia's war of aggression against Ukraine", ESU, March 3, 2025, https://www.esu.ulg.ac.be/wp-content/uploads/2025/03/Overview-of-EU-sanctions-against-Russia-Belarus-2014-2025-final.pdf.

TECHNICAL ASSISTANCE

Technical assistance refers to any technical service, including support for the repair, development, manufacture, assembly, testing, or maintenance of an item. Assistance can take many forms, such as instruction, advice, training, electronic communication, or verbal guidance of a different kind. Under certain regulations, such as the EU framework, controls are triggered as soon as technical assistance is provided to listed items (even though catch-all clauses might also apply), if the provider has been informed by the authority, or if the provider is aware that the items are intended for any use in connection with WMDs and related delivery means, military end-use in a country subject to arms embargo, or listed military items illegally exported.[90] Examples include lecturing abroad on controlled drone technology or providing consultation on controlled items to axforeign person within the national territory.

90. Article 8 of Regulation (EU) 2021/821.

BROKERING SERVICES

Brokering services involve any arrangement, including negotiation, buying, or selling, for the supply of an item from one country to another. A hypothetical example is a person from Country A arranging the sale of controlled quantum technology acquired in Country B and subsequently shipped to Country C for its final end-user.

IN-CUSTOMS/UNION TRANSFER

For certain controlled goods (e.g., defence items), countries may impose controls on internal transfers. This can include requiring a licence for movement within the national territory.[91] Furthermore, when a customs union exists—e.g., the EU or the Eurasian Economic Union (EAEU)—specific controls may be imposed, lifted, or facilitated regarding the movement of items within the union's customs territory. In the EU, for example, most controlled items can transit or be transferred freely within the customs area, except for particularly sensitive items (e.g. nuclear items, military items) that may require prior notification or 'transfer' authorisation.[92]

FINANCING SERVICES

Financing services refers to any activity providing financial support. Illicit trade often begins with financing—whether for a development project, assembly, acquisition, or another stage of the supply chain—so STC systems need to consider covering this aspect and ensuring the legality of financial transactions. For example, a Western company could invest in the development of critical technologies by a third-country company, which could then sell those items to sensitive end users, including sanctioned entities. Because of risks related to illicit trade and weapons proliferation, financial activities and assets should also be subject to case-by-case monitoring.

OTHER SERVICES

Other services may include ancillary services, such as transportation and logistical services, insurance or re-insurance, and general advertising or promotion, as well as other activities such as warehousing and storage. Entities providing these services may share responsibility under trade control regulations.

91. See for example: "Expansion of Export, Reexport, and Transfer (in-Country) Controls for Military End Use or Military End Users in the People's Republic of China, Russia, or Venezuela," BIS, April 28, 2020, https://www.federalregister.gov/ documents/2020/04/28/2020-07241/expansion-of-export-reexport-and-transfer-in-country-controls-for-military-end-use-or-military-end.

92. The term 'transfer' refers to the movement of goods from one Member State to another within the customs territory of the Union.

Figure 3: Scope of STC systems

4

HOW: IMPLEMENTATION AND ENFORCEMENT OF A STRATEGIC TRADE CONTROL SYSTEM

HOW: IMPLEMENTATION AND ENFORCEMENT OF A STRATEGIC TRADE CONTROL SYSTEM

4.1 SYSTEM (RE)DESIGN

In the process of designing or redesigning an STC system, national authorities should adopt a structured and inclusive approach. The following are some of the core elements, not necessarily in consecutive order, to review or build a robust, effective, and internationally compliant STC framework.

POLICYMAKING BY NATIONAL AUTHORITIES

The crucial step of defining and updating a national STC policy involves the development of a coherent national strategy that aligns with both legally and politically binding international trade control state commitments, such as UNSCR 1540 and, if relevant, the guidelines of various MECRs. To facilitate the process, authorities are encouraged to designate a lead agency or establish an interagency coordination mechanism to oversee the system. National security and economic priorities must be clearly articulated, and international commitments fully integrated. Securing political will and ensuring sustainable funding are essential to support long-term implementation and effectiveness.

STAKEHOLDERS' CONSULTATIONS

Inclusive and transparent stakeholder consultations are critical to ensuring that the STC system is practical, effective, and widely supported. Authorities should engage a broad range of stakeholders, including representatives from industry, shipping companies, brokers, research centres, academia, and civil society. Structured consultation formats—such as public hearings, roundtables, surveys, and advisory committees—can facilitate meaningful dialogue. Feedback from these consultations should be systematically incorporated into both policy development and legal drafting to ensure relevance, feasibility, and review. Ultimately, such engagement also helps to raise awareness among public and private stakeholders, and build trust and share responsibilities among them, thereby promoting a stronger culture of compliance and a more resilient STC system.

REVIEWING AND DRAFTING THE LEGAL FRAMEWORK (LAWS AND BY-LAWS)

A strong legal framework is the foundation of any effective STC system, granting legal certainty to all stakeholders involved. It is essential to draft or review both primary legislation—which usually defines the scope, mandates, and penalties—and secondary legislation, which outlines licensing procedures, control lists, and enforcement mechanisms. It is important to highlight that considering the necessity to update regularly control lists of items to include latest technology developments, the legal procedure should allow smooth and rapid adaptation. Ideally, the legal framework should comprehensively cover all relevant activities (both tangible and intangible), including export, re-export, brokering, transit and trans-shipment, and technical assistance of controlled goods, software, and technologies.

TRAINING OF NATIONAL AUTHORITIES

To ensure effective implementation of the legal and policy frameworks, national authorities must invest in capacity building. Tailored training programmes should be developed and delivered on a regular basis for customs officials, licensing officers, judicial authorities, and enforcement personnel. These programmes should include modules on risk assessment, dual-use goods, and compliance auditing. Practical training through simulation exercises, case studies, and interagency workshops can enhance operational readiness. Sharing best practices with partner countries and collaborations with international organisations such as the World Customs Organisation (WCO) can provide valuable expertise and support.

AWARENESS-RAISING

Raising awareness among operators and the general public is essential to fostering a culture of compliance. Outreach campaigns should target key sectors such as industry, academia, and logistics providers. Authorities should develop accessible guidance materials, digital tools, and online resources to support understanding and adherence to the control system. Workshops, webinars, and national compliance days can serve as effective platforms for fostering engagement and dialogue between authorities and the public and private sectors. Promoting the adoption of internal compliance programmes and voluntary self-regulation mechanisms will further strengthen the overall effectiveness and resilience of the STC system.

4.2 IMPLEMENTATION

In the context of setting up or reviewing an STC system, implementation refers to the process of establishing a policy and its legal framework in order to put them into effect. It involves defining political and technical guidelines, allocating resources, developing procedures and protocols, as well as disseminating knowledge and implementing capacity-building initiatives among relevant stakeholders. The following sections elaborate on the key components of the implementation process.

POLITICAL AND TECHNICAL DIRECTIVES FOR IMPLEMENTATION

The formulation of political and technical directives serves as the foundational step in implementing an STC system. Political directives are derived from national and international commitments, such as treaties and MECRs.[93] These directives are defined by the government to outline the overarching goals, principles, and priorities of the STC system, ensuring alignment with national security, non-proliferation objectives, and economic interests.

93. See supra Chapter "Why: rationales behind a strategic trade control system », section « Alignment with the international framework".

Technical directives, on the other hand, translate political objectives into actionable measures. They involve the development of standardised criteria for risk assessment, classification of controlled items, and the establishment of thresholds for licensing requirements.

The harmonisation of political and technical directives ensures that the system is both legally sound and operationally feasible, facilitating compliance and enforcement.

AUTHORISATION MECHANISMS

Types of licences and exemptions

An STC system, generally, relies on a licensing regime to regulate the transfer of controlled items so that it is illegal to transfer such goods without authorisation. Licences may be categorised based on the nature of the transaction, the sensitivity of the items, and the end use or end user. The various types of authorisations reflect the risk management measures put in place by the regulatory authority, which aim to mitigate proliferation risks while facilitating legitimate trade. Common types of authorisations include:

- General authorisation: general authorisations for low-risk transactions, available to all exporters, subject to certain conditions and specific requirements,[94] and covering pre-defined items for pre-defined destinations.

- Individual authorisation: case-specific authorisations, particularly favoured for high-risk and sensitive transactions, or for occasional transactions.

94. For example, exporters may be required to register with the competent authorities before transferring controlled items subject to the general licence and/or report information relating to exports made.

• Global authorisation: authorisations for multiple shipments available to highly trusted operators to specific destinations (end users and/or countries).

In addition, if the item to be exported is not controlled but the destination is problematic or the customs code of the product is similar to that of a listed item, a "no licence required" (NLR) certificate may also be required. An NLR serves as proof of compliance and facilitates customs clearance by demonstrating to authorities that the exporter has verified the transaction's eligibility for a licence.

Operators generally apply for the type of licence that best suits their needs (e.g., number of shipments, processing time for licence applications, licence validity period) and as dependent on the conditions for issuing the licence (e.g., keeping track of serial numbers of exported items, reporting obligations, implementation of a robust ICP—often mandatory for global licences).

An STC system may also provide for exemptions or facilitated procedures that may be granted for specific scenarios, such as temporary exports for exhibitions, transactions in connection with government or law enforcement activities (e.g., peacekeeping and humanitarian missions), information already in the public domain or concerning "basic scientific research", or the minimum necessary information for patent applications.[95]

95. See General Technology Note of Annex I to EU Dual-Use Regulation (Commission Delegated Regulation (EU) 2024/2547 of 5 September 2024 amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items, C/2024/6093, OJ L, 2024/2547, 7.11.2024).

Licences procedures

The licence application process is a core element of STC systems and involves various procedures. It typically includes:

• Submission of licence applications: operators must submit a completed licence application form (in paper or electronic format), often available through the national export control authority's website. The form generally includes details about the operator, the items to be exported (including their export control classification number), and the consignee/end user. The form is accompanied by other documentation such as a technical description of the items, end-user and end-use documentation (e.g., an end-user certificate), commercial documents (e.g., a proforma or commercial invoice), a company registration certificate, and compliance documentation.

• Licence assessment: the review of licence applications is a risk-management mechanism that consists of an administrative and technical/geopolitical analysis of the application. The administrative analysis verifies that the form is complete and includes all required documents. The technical/geopolitical analysis checks item classification and assesses risks related to destination, end use, end user, as well as shipping route and other elements aimed at mitigating the risk of diversion.

Therefore, granting a licence implies the satisfaction of various conditions, i.e., objective and verifiable facts concerning, inter alia, the item (listed, not listed but requiring the implementation of a catch-all clause, or not controlled), destination country (sanctioned, sensitive, or low-risk), end user (distributor or operator based in a free trade zone, tied

to the military/defence industry or a governmental body, little information in open sources), end use (related to WMD proliferation, military applications, human rights considerations, or civilian applications), shipment (unusual shipping arrangements)—and criteria—more subjective (political) considerations used for risk assessment and generally related to, inter alia, national foreign and security policy; the recipient state's behaviour towards the international community (respect of UN sanctions, international law and other international commitments on non-proliferation, its attitude to terrorism); preservation of regional/international peace, security and stability; the internal situation in the country of final destination (existing tensions or armed conflicts); and compatibility of the exports with the technical and economic capacity of the recipient country.

A key aspect of the technical assessment is the appropriate classification of the item. Generally, exporters are best placed and indeed have the legal obligation to classify their products. However, it is the responsibility of the licensing authority to verify the item classification in order to ensure an adequate risk assessment. Determining the classification of an item is a complex and highly technical task, and authorities may require support from technical experts (e.g., scientists, engineers, or military/defence experts) to evaluate the items' technical specifications and potential applications. Technical reachback strengthens the accuracy and reliability of export control decisions by leveraging specialised knowledge, thereby reducing the risk of unauthorised transfers of sensitive items. Such technical expertise may be developed in-house—i.e., in specialised agencies or government departments having a technical knowledge about the controlled items—or outsourced to an external service provider—e.g., research institutes or specialised entity—under a contractual partnership guaranteeing the non-disclosure of sensitive data.[96]

Interagency coordination: applications are assessed in coordination with relevant authorities, usually including the ministries of trade, defence, foreign affairs, customs, and intelligence to ensure a comprehensive assessment of proliferation risks and consistency with international commitments, national security, and economic interests (for more information, see infra Interagency coordination).

- Decision Making: based on the conclusions of the technical assessment and in compliance with national and international obligations, licences are granted, denied, or conditionally approved. Furthermore, in case of doubt, and when the line separating civil from military is subtle, licensing authorities may opt for a stricter control and require a military licensing procedure.

Post-licensing phase

The post-review process ensures accountability and transparency in licensing decisions. It includes:

- Appeal mechanisms: appeal mechanisms can vary significantly from one country to another. Depending on the jurisdiction, appeals may be introduced by the applicant and civil society,[97] and take the form of administrative and/or judicial procedures.

96. For instance, the Korean Security Agency of Trade and Industry (KOSTI) is an external agency tasked by the South Korean government with assessing whether or not an item is considered a strategic item (see: https://www.kosti.or.kr/cms/content/view/439).

97. See, for instance: "Belgian Council of State suspends export licences for arms to Saudi Arabia", European Studies Unit (ESU), University of Liege, 9.3.2021, available here; or "Coalition appeals Dutch court ruling for failure to uphold obligations under international law", Centre for Research on Multinational Corporations (SOMO), 5.3.2025, available here.

The administrative appeal may be internal—i.e., organised within the licensing authority itself, generally at a higher hierarchical level—or external—i.e., taking place before an independent administrative tribunal.

• Licence modifications: previously granted licences may be amended, suspended, cancelled, or withdrawn by the competent licensing authorities in response to changing circumstances, such as new intelligence or non-compliance by the operator.

• Post-licensing requirements: subsequent to a licence being granted, operators have to fulfil various obligations designed to ensure that the exported items are used in accordance with the terms of the licence and to mitigate risks of diversion. The following are amongst the most common requirements and are critical for ensuring the effectiveness and integrity of the export control system:

• Record-keeping: exporters are required to maintain detailed records of transactions, including documentation related to the shipment, end user, and final destination of the items. This may involve keeping copies of commercial invoices, shipping documents, end-user certificates, and correspondence with the consignee. Such records must often be retained for a specified period (e.g., five years) and made available for audit or inspection by national authorities.

• Reporting obligations: after obtaining the licence, operators may be required to inform the competent authority of any changes concerning the end use, end user, or destination of the controlled items. Exporters may also be required to submit post-shipment reports confirming that the goods have reached their intended destination and are being used as declared.

• Compliance audits: export control compliance audits aim to assess the efficacy of implemented control measures and to identify compliance deficiencies within an organisation. Audits can be realised internally—by internal compliance experts, or with the help of outside independent auditors, as a prevention measure to identify compliance gaps, prepare for government inspections, and demonstrate due diligence—or by government authorities, where operators undergo periodic reviews to verify that they are fully compliant with the terms of the licence. These audits involve examining records, internal compliance programmes, and transaction documentation, as well as conducting on-site inspections—if such a clause was attached to the export, for example, in the end-user certificate—to ensure that goods are used as declared.

Failure to comply with these post-licensing requirements may result in penalties or the withdrawal of the licence, while confirmed compliance may enhance an operator's credibility.

INTERAGENCY COOPERATION

STC systems rely on collaboration between multiple agencies to comprehensively assess risks and effectively combat illicit trafficking in strategic goods. Such cooperation generally includes a ministry of trade, which oversees licensing and regulatory compliance; defence and military agencies, which contribute to assess the strategic and security implications of exports; foreign affairs departments, which align export controls with diplomatic objectives and international obligations; intelligence services, which provide valuable information and early warnings; law enforcement bodies, which investigate violations and enforce penalties; and other relevant bodies, such as financial services authorities. To operationalise and facilitate such collaboration, STC systems may employ various institutional mechanisms, such as:

Interministerial Working Groups and Joint Task Forces

Dedicated bodies or units for coordinating licensing procedures (e.g., commodity identification and licence issuance) and enforcement actions (e.g., detection, investigation, and prosecution) which, by centralising decision making and response capabilities, reduce delays and improve the system's flexibility to deal with emerging threats.

Information Sharing

Facilitated by secure digital platforms and information-sharing protocols, information sharing is an essential component of interagency cooperation as agencies need to exchange classified and unclassified data—including export licence applications, risk assessments, law enforcement files, and intelligence reports on proliferation actors—in order to implement an effective STC system. International cooperation—specifically, the exchange of information among authorities across countries (e.g., allies or members of a MECR)—represents another dimension of interagency cooperation. This cooperation is crucial for achieving non-proliferation objectives and enhancing the collective effectiveness of STCs.

Memoranda of Understanding:

Formal (but non-legally binding) agreements aimed at establishing an operational framework defining roles and responsibilities among agencies, thereby helping to prevent jurisdictional overlaps and gaps.

In conclusion, interagency cooperation enhances the system's ability to detect and disrupt proliferation networks while minimising bureaucratic redundancies.

OUTREACH FROM NATIONAL AUTHORITIES

Public and private sector engagement is critical for the success of an STC system. Industrial operators, in particular, play a fundamental role, as they are at the very core of the supply chain; they know their products and business partners, and can identify red flags. National authorities may employ various outreach initiatives to promote awareness and compliance, such as:

Annual forums and workshops

Platforms for dialogue between regulators and industry/academic stakeholders.

Company visits

On-site visits can be highly effective for raising awareness about compliance obligations. These visits help highlight risks—such as audit consequences and legal penalties—while engaging management and fostering mutual understanding. For authorities, such visits offer a practical, on-the-ground perspective of a company's products, operations, and challenges. This direct interaction allows them to provide targeted guidance and address industry-specific risks.

Dialogue with professional federations

Professional federations can play an important role in ensuring that all stakeholders (especially SMEs) are represented, providing regulatory monitoring and training, and disseminating best practices, while providing regulatory authorities with collective feedback from the sector concerned. Establishing an open and informal dialogue will help build trust and present the relationship with industry as a partnership.

Newsletters

Regular updates on regulatory changes or communications regarding upcoming events.

Online Resources

Web portals providing relevant legislation, tools (for instance, for item classification[98]), frequently asked questions (FAQs), explanatory notes, and compliance handbooks and guidelines.

While establishing a dialogue can raise awareness among industry and academic stakeholders regarding dual-use trade risks (including the legal, financial, and reputational consequences of non-compliance faced by the company/institution/individual), providing tools and online resources empowers them to comply with regulations and implement best practices. Together, these initiatives foster a culture of compliance by informing, clarifying, engaging, and connecting the regulatory authorities and regulated entities.

98. An example of such a tool is TARBEL, a web application of the Belgian Federal Public Service Finance enabling consultation of measures relating to the Belgian customs tariff and notably regarding possible licensing requirements for a dual-use item via its footnote CD464 (see Michel, Q. (Ed.), Caponetti, E. (Ed.), Paile, S., et al. (2023). Analyzing Strategic Trade Compliance Tools. Liège, Belgium: European Studies Unit (ESU), University of Liège).

OPERATORS' COMPLIANCE

Operators from industry and academia and other relevant sectors (e.g., including exporters, importers, brokers, and providers of technical assistance, financial institutions, and freight forwarders) bear primary responsibility for complying with STCs. Compliance measures include:

Internal Compliance Programmes (ICPs)

Develop and implement tailored policies and procedures to identify, assess, and mitigate risks associated with dual-use items, regularly reviewed and updated to reflect changes in relevant regulations.[99]

Due diligence

Conduct thorough checks on customers, suppliers, end use, and end users to ensure transactions do not contribute to unauthorised or illicit activities. This includes screening against sanctions lists, verifying end-use statements, and assessing the legitimacy of all parties involved. The concept of due diligence is introduced in STC systems with the intent to highlight and strengthen the responsibility of operators in the fight against weapons and WMD proliferation, and human rights violations—including, in the context of conflict minerals and the rough diamond trade, where due diligence replaces the licensing-based system.[100]

Compliance with customs procedures

Accurately classify goods using the correct Harmonised System (HS) codes and provide complete, transparent documentation to customs authorities. Operators must also cooperate with customs inspections, audits, and any requests for additional information to facilitate lawful trade.

Training and awareness

Deliver regular training sessions for employees to ensure they understand control lists, licensing requirements, and red flags (e.g., unusual payment methods, vague end-use declarations, or high-risk destinations). Awareness programmes help foster a culture of compliance and vigilance within the organisation.

Operators who demonstrate robust compliance may benefit from simplified procedures or incentives, such as trusted trader programmes.

99. The European Commission published two recommendations on internal compliance programmes in order to provide operators with a common framework. The first recommendation, published in 2019, is tailored to companies (see: Commission Recommendation (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009, C/2019/5528, OJ L 205, 5.8.2019, p. 15-32), while the second one, published in 2021, to research organisations (see: Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, C/2021/6636, OJ L 338, 23.9.2021, p. 1-52).

100. See, for instance: Organisation for Economic Cooperation and Development (OECD), OECD Due Diligence Guidance for responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, 2013.

TRANSPARENCY MEASURES

Transparency is essential for building trust and accountability in STC systems and promoting international cooperation. Key measures include:

National Reports

Publication of annual reports detailing licensing statistics, enforcement actions, and policy developments. These reports offer stakeholders and international partners insights into the functioning and effectiveness of the national control system.

Public Consultations

Proactive engagement with stakeholders (e.g., industry, academia, and civil society representatives) to solicit feedback on proposed regulations or policy changes. Such consultations can ensure that trade controls are more practical, balanced, and reflective of diverse perspectives, while also increasing public awareness and compliance.

International Reporting

Submission of reports to MECRs and international organisations (e.g., IAEA, OPCW, or the UN 1540 Committee) to demonstrate compliance with global standards, facilitate peer review, and support collective non-proliferation efforts.

In conclusion, transparency enhances the credibility of the system and facilitates international cooperation.

4.3 ENFORCEMENT

An effective STC system requires not only sound policy and legal frameworks but also robust enforcement and compliance verification mechanisms. The enforcement objectives are usually to investigate and prosecute violations, stop illegal exports and seize goods, prevent the illegal export of strategic items, identify and disrupt illicit procurement efforts, promote awareness and compliance among stakeholders, and support legitimate trade activities. All agree to ensure that strategic items are not diverted for unauthorised uses. The following components are essential to a comprehensive enforcement architecture:

CUSTOMS CONTROL AND RISK MANAGEMENT

Customs authorities play a frontline role in enforcing trade controls. Their responsibilities include risk management, company audits, and the application of clearance and post-clearance procedures. Risk-based targeting allows customs to focus resources on high-

risk shipments, while audits help verify the accuracy of declarations and the integrity of internal compliance systems. Post-clearance reviews are critical for detecting discrepancies and ensuring ongoing compliance.

POST-SHIPMENT VERIFICATION

Post-shipment verification (PSV) is a key tool for confirming that exported goods have reached their declared end use and end user. This process may involve on-site inspections, document review, and cooperation with foreign authorities. PSV helps prevent diversion and strengthens the credibility of the national control system in the eyes of international partners.

INVESTIGATION AND COMPETENCE

When violations are suspected, competent authorities—such as specialised police units or customs investigation branches—must be empowered to conduct thorough investigations. These units require technical expertise in dual-use items, export control regulations, and international trade practices. Effective investigation capabilities are essential for detecting illicit activities, gathering evidence, and preparing cases for prosecution.

INFORMATION EXCHANGE AND INTERAGENCY COOPERATION

Timely and secure information exchange is vital for effective enforcement. This includes both national-level coordination among agencies (e.g., customs, licensing authorities, intelligence services) and international cooperation with partner countries and multilateral organisations (e.g., Proliferation Security Initiative). Mechanisms such as joint task forces, shared databases, and liaison officers can enhance coordination and reduce enforcement gaps.

PROSECUTION AND PENALTIES

To ensure accountability, violations of STCs must be subject to prosecution. Specialised prosecutorial units with expertise in export control law can improve the quality and consistency of legal proceedings. Penalties should be proportionate and dissuasive, ranging from administrative sanctions (e.g., licence revocation, fines) to criminal penalties (e.g., imprisonment) for serious offenses. In some legal systems, self-disclosure mechanisms have been implemented to encourage transparency and cooperation between companies and public authorities. These mechanisms often function as mitigating circumstances, allowing companies to voluntarily report violations of export control legislation prior to authorities discovering them. By doing so, businesses can demonstrate good faith and a commitment to compliance, which may result in reduced penalties. A credible enforcement regime reinforces compliance and deters illicit trade.

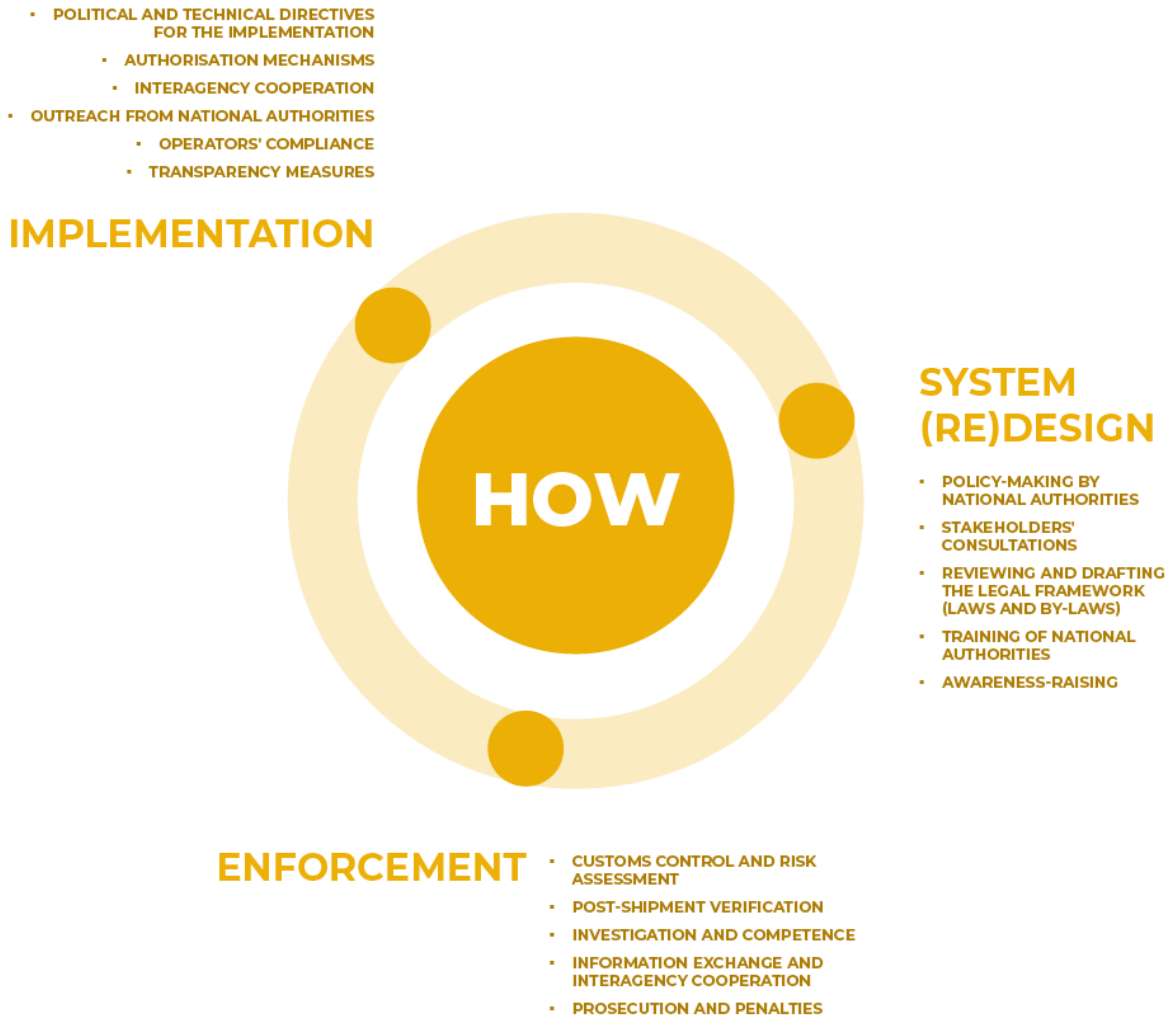


Figure 4: Core elements for implementation and enforcement of STC systems

AUTHORS

Enzo CAPONETTI	**Associate Lecturer and Researcher, European Studies Unit, University of Liege**
Veronica VELLA	**Researcher, European Studies Unit, University of Liege**
Mónica CHINCHILLA ADELL	**Lecturer and Researcher, University of Navarra**
Quentin MICHEL	**Full Professor, European Studies Unit, University of Liege**

PARTICIPANTS OF THE 14TH AND 15TH CHAUDFONTAINE GROUP CONFERENCE

Branislav ALEKSIC	Fraunhofer Institute
Wim BOER	Ministry of Finance, The Netherlands
Kolja BROCKMANN	SIPRI
Lotte BRUYNEN	Deloitte
Lia CAPONETTI	SPW Economy, Walloon Region
Christos CHARATSIS	European Commission – Joint Research Centre
Arnaud DEVIENNE	Ministry of Economy and Finance, France
Johan EVERS	imec
Lauriane HEAU	SIPRI
Marcello IRLANDO	Ministry of Foreign Affairs, Italy
Georgios KOLLIARAKIS	EUP2P Programme for Dual-Use Goods
Werner KNAPP	Federal Office for Economic Affairs and Export Control, Germany
Irena KOLAKOWSKA	Ministry of Foreign Affairs, Poland
Ivana MIĆIĆ	Ministry of Foreign and European Affairs and Foreign Trade, Luxembourg
Matjaz MUROVEC	EUP2P Programme for Dual-Use Goods
Sylvain PAILE-CALVO	University of Liege
Rosa ROSANELLI	Patria Group
Kamshat SAGINBEKOVA	International School of Economics, Maqsut Narikbayev University
Ana SANCHEZ COBALEDA	University of Barcelona
Filippo SEVINI	European Commission – Joint Research Centre
László STÉFAN	Government Office of the Capital City of Budapest, Hungary