FOOD-FOR-THOUGHT PAPER

# PROJECT D-TECT

## Technologies to counter the diversion of small arms and light weapons, and components of conventional weapons

*Sarah Grand-Clément - United Nations Institute for Disarmament Research*

*Diederik Cops - Flemish Peace Institute*

## EXECUTIVE SUMMARY

There are many ways in which technology could help to counter the diversion of conventional weapons. Yet despite some discussions in international meetings on conventional arms control, we see limited evidence of technologies being used to strengthen or enhance efforts to prevent, detect, and investigate the diversion of conventional arms, their ammunition, and parts and components.

This paper seeks to bridge this gap by presenting a needs-driven, systematic, and context-sensitive framework to identify and assess technologies that could strengthen efforts to counter the diversion of conventional arms and related components. The first step of this framework requires an understanding of the risks and methods of diversion, tailored to each specific type of conventional weapon and its life-cycle context. The second step examines the existing technologies which could help address the identified risk(s). The final step assesses the identified technologies according to the context(s) in which they would be applied, as well as against selected attributes the technologies should possess. The paper also provides two illustrations to show how the framework could be applied to small arms and light weapons on the one hand, and components of conventional weapons on the other.

This paper presents an introduction to the first phase of a joint UNIDIR-FPI initiative to explore the utility of different technologies for strengthening efforts to counter diversion and eradicate the illicit trade in conventional arms.

*August 2023*

# Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. The preparation of this joint report has been supported by generous funding for UNIDIR's Conventional Arms and Ammunition Programme by Germany and for the Security and Technology Programme by Germany, the Netherlands, Switzerland and Microsoft. The Flemish Peace Institute is funded by the Flemish Parliament.

The authors wish to thank the experts who participated in the interviews and provided valuable inputs during the course of the research. The authors are also grateful to the experts who reviewed and provided valuable inputs to the report, including Paul Holtom, Nils Duquet, Giacomo Persi Paoli, Hardy Giezendanner, Mark Bromley, Jonathan Rickell, and Christian Straubert.

# Glossary

**Diversion:** "The rerouting and/or the appropriation of conventional arms or related items contrary to relevant national and/or international law, leading to a potential change in the effective control or ownership of the arms and items. Instances of such diversion can take various forms: (1) An incident of diversion can occur when the items enter an illicit market, or when redirected to an unauthorised or unlawful end user or for an unauthorised or unlawful end use; (2) The rerouting and misappropriation of the items can take place at any point in the transfer chain, including the export, import, transit, trans-shipment, storage, assembly, reactivation or retransfer of the items (3) The transaction chain facilitating a change of effective ownership and/or control can involve various forms of exchange, whether directly negotiated or brokered – grant, credit, lease, barter, and cash – at any time during the life cycle of the items.".[1]

**Small arms and light weapons (SALW):** "'Small arms' are, broadly speaking, weapons designed for individual use. They include, inter alia, revolvers and self-loading pistols, rifles and carbines, sub-machine guns, assault rifles and light machine guns; 'Light weapons' are, broadly speaking, weapons designed for use by two or three persons serving as a crew, although some may be carried and used by a single person. They include, inter alia, heavy machine guns, hand-held under-barrel and mounted grenade launchers, portable anti-aircraft guns, portable anti-tank guns, recoilless rifles, portable launchers of anti-tank missile and rocket systems, portable launchers of anti-aircraft missile systems, and mortars of a calibre of less than 100 millimetres."[2]

**Technology:** There is no single definition of technology. For example, the Merriam-Webster dictionary defines it as follows: "(1a) the practical application of knowledge especially in a particular area; (1b) a capability given by the practical application of knowledge, (2) a manner of accomplishing a task especially using technical processes, methods, or knowledge, and (3) the specialized aspects of a particular field of endeavor."[3] In the context of this report, the definition of technology most closely resembles the second definition – "a manner of accomplishing a task, especially using technical processes, methods, or knowledge". Specifically, the technologies within the scope of this paper are those which have been recently developed and are emerging in the context of diversion prevention– although this report does not examine technologies at the lowest technology readiness levels.

# Section 1 - Introduction

## Applying technology as one of the tools to prevent diversion

**The diversion of weapons systems into the hands of unauthorised users or for unauthorised use causes many adverse effects.** These include crime, terrorism, armed violence, situations of conflict; and they may cause mental and physical harm to and the death of individuals. In addition, diversion can have negative impacts on state stability, development, human rights, education, and other socioeconomic circumstances or factors. Countering the diversion and unauthorised end-use of conventional weapons therefore lies at the heart of international and regional conventional instruments intended to control arms transfers.

In recent years, significant attention has been devoted to setting international standards, strengthening national controls, and improving processes to support the implementation of these regional and international instruments, with the aim of preventing the diversion of conventional arms – especially SALW. In the context of the Arms Trade Treaty, for example, a non-exhaustive list of practical measures that governments can implement has been disseminated.[4] Next to measures of a non-technological nature, various specific technologies that have been put forward as good practices are being discussed, developed, and tested in specific contexts or are being marketed by technology development companies with the aim of strengthening existing diversion-prevention efforts. However, the general uptake and implementation of technologies to counter the diversion of conventional arms, their ammunition and parts and components remains relatively limited in practice and the emphasis of discussions on the matter is mainly on the challenges that have arisen rather than on the potential of technologies to enhance control opportunities.[5] Overall, **there appears to be a gap between the increasing discussions on using technologies in counter-diversion efforts and initiatives, on the one hand, and their effective broad-scale implementation on the other**.

**Some technologies, however, could be highly beneficial, efficient, and effective in supporting and strengthening existing measures aimed at preventing, negating, or mitigating diversion risks.** Numerous technologies have been implemented in the commercial and industrial sectors to ensure the security of legitimate trade flows and to prevent the smuggling, theft, and diversion of commodities from authorised to unauthorised users. Such technologies, already in use across other industrial sectors, could also, when repurposed, be effective in preventing, negating, or mitigating the risk of unauthorised diversion and detecting attempts at diversion. They could lead to a better understanding of the diversion methods and help to strengthen the end-use or end-user controls of conventional weapons systems. Using technology as a tool to collect and share information on instances of diversion can also be most useful in building advanced information and strategic intelligence to support the identification of high-risk transactions and illicit facilitation routes transnationally and to deploy technologies more accurately to prevent and detect future diversion efforts.

## Purpose and scope of this paper

The aim of this project (Countering the Diversion of arms using TEChnology Tools, or D-TECT) is to develop and test an approach to identifying and assessing the utility and feasibility of using specific technologies for preventing, detecting, negating, or mitigating diversion. Project D-TECT consists of two consecutive phases:

- First, to identify existing technologies that could be suited to countering the diversion of conventional weapon systems, including small arms and light weapons (SALW), ammunition, parts and components (hereafter, "conventional weapons and related components"), and develop a framework that makes it possible to identify and assess technologies used to counter diversion.

- Second, to assess, refine, and validate the list of identified technologies in relation to specific types of conventional weapon systems.

**This paper presents the results of the first phase; it contains an exploration of how technologies could contribute to enhancing efforts to counter the diversion of conventional arms and ammunition.** Although several technologies have been suggested, tested, discussed, and marketed as potential solutions to support the prevention of diversion, their effective uptake or implementation in international arms-transfer controls remains comparatively limited. This paper aims to help bridge this gap by presenting a framework that uses a needs-driven, systematic, and context-sensitive approach to identifying and assessing potential technologies so as to strengthen initiatives to counter the diversion of conventional weapons and related components. It is important to mention at this point that this framework is still a work in progress, which will be refined and validated as the project advances. Therefore, the analysis of the identified technologies, their attributes, and the contextual analysis presented in this paper are by no means final, but they are intended to guide discussion, with a view to developing a more comprehensive picture of technology adoption towards countering the diversion of conventional weapons and related components.

By setting out this framework, **the paper therefore aims to provide a common vocabulary with which to discuss, evaluate, and share knowledge on the barriers, preconditions, and context for implementing technologies** to counter diversion among all the actors involved in conventional arms-transfer controls. For this reason, this framework and paper are aimed at relevant state authorities and the various stakeholders involved in a weapon's or a component's life cycle.[6]

Several disclaimers should be noted. First, the aim of this paper is not to explore the reasons behind the barriers that have prevented technologies being more widely adopted to prevent diversion; nor does it explore the role and relationship of the various private and public actors in this regard. These elements will be explored via the application of the framework as part of the second phase of the project. Second, it should be noted that technologies cannot be seen as standalone initiatives. Rather, this paper argues that technology should be viewed as those instruments or tools that can contribute to the achievement of some desired goals to complement and enhance existing measures.

## Methodology

The analyses and conclusions presented in this paper were developed using various methods to collect relevant information for the subsequent stages of the project. More specifically, the first step in developing the framework drew upon the existing relevant literature on the diversion of conventional weapons and related components to unauthorised end-users into embargoed countries and actors and also the illicit market. Interviews with experts in this domain were used to further refine and contextualise these findings. In a second step, the literature on supply chain management, security, and resilience was consulted, and in-depth interviews with academic experts who specialise in supply chain management and technologies, industry representatives from sectors such as the diamond, chemical, critical minerals, and technological industries, and from technology companies were conducted to identify existing technologies and the challenges and preconditions related to their implementation. The literature review spanned the period from September 2022 until May 2023, while the interviews were conducted between October 2022 and May 2023.

## Report structure

**Section 2** of this paper describes the framework that was developed to enable the identification and assessment of technologies that are used or could be used to counter diversion. This section also includes a long list of technologies that could possibly be valuable in strengthening counter-diversion efforts in international arms transfer controls. In **section 3**, two examples are provided to demonstrate how this framework could be applied in identifying and assessing technologies to counter the diversion of two different types of conventional weapon and their components. The paper concludes with an overview of the main conclusions drawn from the development of a structured and systematic approach to identifying and assessing relevant technologies that could be used to counter the diversion of conventional weapons and related components (**section 4**).

# Section 2 - Identification and assessment of technologies for counter-diversion applications: a general framework

We focus on identifying technologies to strengthen counter-diversion efforts, which resonates with other recent efforts to analyse the relevance of specific technologies to be implemented in conventional arms trade controls. Several analyses and studies have assessed the possible relevance of certain technologies to counter the diversion of conventional weapons and related components.[7] Certain specific technologies have notably been at the centre of more attention and uptake than others: one is Radio Frequency Identification (RFID) tags, which have, for example, been applied to help with ammunition[8] and firearm[9] inventory record-keeping, as well as physical security and stockpile management (PSSM). Beyond RFID, certain technologies have been in the spotlight more than others in the context of both international conventional arms transfers and more widely, such as artificial intelligence (AI)[10] and distributed ledger technology (DLT).[11] However, other potentially valuable technologies are not discussed in as much detail.[12] In addition, the speed at which and the extent to which these technologies – even those that are put forward or promoted in this context – are implemented on a generalised scale remain limited. This may be caused by the difficult and elusive process of assessing, planning for, and integrating technological change into international conventional arms transfer controls.[13]

To this end, a framework has been developed to **structure the process of identifying and assessing potentially relevant technologies** to counter the diversion of conventional weapons and related components. This framework presents a consistent approach to guiding decision-making regarding technology in the context of the international trade in conventional weapons and related components. At the same time, it allows for a tailored and specific approach to different types of conventional weapon and related components and contexts of application.

Reflecting similar approaches that provide guidance on technology decision-making[14] and on supply chain risk management,[15] the **guiding principle that underpins the framework is that the use of technology should be needs-driven rather than driven by its mere availability.**[16] Consequently, the reality of diversion functions as the starting point for the framework rather than the technologies and their functionalities.

The framework consists of three steps. The first step focuses on understanding the risks of diversion, which are tailored to each specific type of conventional weapon and the context it operates in.

The second step examines the existing technologies which could help prevent or overcome the identified risk(s). The third and final step assesses the identified technologies according to the context(s) in which they would be applied and also against selected attributes that the technologies should possess. These three steps are illustrated in figure 1.

The remainder of this section elaborates on these three steps that make up the general framework.

## Step 1. Specifying the aim of using technology and mapping item-specific risks of diversion

The use of any measure – whether technological or not – **needs to be clear about why it is being adopted and what it aims to achieve or resolve**. To this end, a clear understanding of what technology can help with – and where it is superfluous or not adapted to aid with the issue – is important. Consequently, a thorough analysis and deconstruction of the problem at hand and the intended aim of a technology application is the first step in the framework set out in this paper.

In this particular context, the aim of technology is to counter the diversion of conventional weapons and related components at different points in their life cycle and supply chain. Diversion is a very complex, multi-faceted, and multi-layered phenomenon, and countering it can take different forms. **It is crucial to unpack the various elements which comprise countering diversion, as different technologies can contribute differently to these elements.** Table 1 provides an overview of these different elements.

At the same time, **an analysis and definition of the specific item-level[17] risks of diversion is also needed, which should also be specific to the context in which it exists**. Knowledge on the main risks and methods of diversion across the different phases in the supply chain of conventional weapons and related components has notably been integrated in the comprehensive "Diversion

Figure 1: Framework to identify and assess technologies to counter the diversion of conventional weapons and related components

| | |
|---|---|
| **Step 1:** Specifying the aim of using technology and mapping item-specific risks of diversion | **This step includes conducting an assessment regarding the aim of applying technology as well as of the specific item level risks of diversion.** |
| **Step 2:** Identifying potential technologies | **This step consists of identifying the technology/ies which would respond to the purpose and risk assessment.** |
| **Step 3:** Analysing the context in which technologies are to be implemented | **This step examines the context in which technologies would need to be applied, and to identify the necessary preconditions and possible barriers to overcome to successfully apply the selected technology solution(s).** |

Analysis Framework (DAF)", developed by UNIDIR, CAR and the Stimson Center. The DAF provides a comprehensive overview of possible methods and risks of diversion in the different stages of the life cycle and supply chain of a conventional weapon. These stages include: (1) manufacture, (2) transfer (which includes export, transport, import and transit), (3) stockpile, (4) active use, and (5) destruction. It is therefore very well suited as a starting point for such a risk mapping.

Beyond a framework such as the DAF, the risk analysis would require an assessment through a more specific item-level lens as well as a location-specific lens. On the first element, the specific risks and methods of diversion can be more or less pronounced for different types of conventional weapons or related components. For example, it may be easier to divert certain items over others, or certain items can have a greater effect on peace and security. The same can be said about the second element, where risks differ according to the specific regional and national contexts. This can also be linked to what measures are already implemented – or not – in different locations, and form part of a capability gap analysis, which feeds into the broader risk analysis. Not taking these issues into account can impact the successful application – or lack therefore – of a technology. It is therefore important to acknowledge the differences between the different types of military goods as well as their geographical context, in order to provide targeted solutions that best respond to specific contexts of diversion.

## Step 2. Identifying potential technologies

In the second step of the framework, **potentially relevant technologies to counter diversion are identified**. For the purposes of this paper, a total of 13 overarching technologies are presented, each of which could be further subdivided into different types of application.[18] It should be noted that this long list of technologies is not necessarily exhaustive and should therefore be viewed as a starting point. Indeed, the technologies within scope of this report are those which have been used or considered for use to aid with countering diversion (or similar issues found in the civilian domain, such as product tampering or counterfeiting). Specifically, technologies included in the long list are either:

- used to counter the diversion of weapons but remain limited in their use and are not widespread; or

Table 1: Elements for an effective approach for countering-diversion

| Element | Description |
|---|---|
| **Prevention** | This form of countering diversion takes place before diversion effectively happens and involves interventions and measures to prevent actors from diverting conventional weapons and related components from their authorised end-use or end-user. |
| **Detection** | This form of countering diversion takes place during the diversion efforts and involves measures and interventions to detect when diversion is happening with a view to setting up measures or interventions to be taken to prevent the diversion efforts being successful. |
| **Identification** | This form of countering diversion deals with actual cases of diversion; thus, it occurs after diversion has taken place and involves interventions and measures to identify such cases and to analyse where the diversion effectively happened with a view to supporting and optimising diversion prevention efforts and initiatives in the future. |

- used in the civilian commercial realm to increase the integrity and security of supply chains, but have not been used for sensitive military or security items.

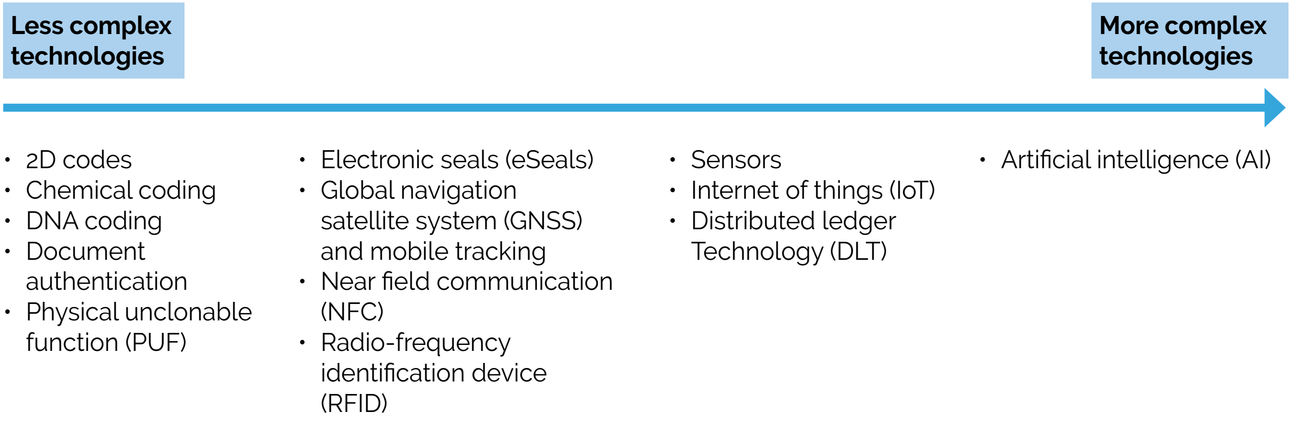
For the latter category, we explored technologies used by the food industry, the chemical industry, or the diamond, critical minerals or pharmaceutical sector. These industries were selected because their features are similar to that of the arms trade and transferable lessons can be learnt. Notably, these industries also face challenges regarding the risk of diversion to unauthorised end-users and end-uses. Although the motivations, methods, and effects of diversion may differ depending on the industrial sector, these sectors could be using technologies that could be relevant to conventional arms control.

This **focus allows for an assessment based on existing knowledge and experiences of applying these technologies**, including lessons learnt and information on the preconditions necessary for their successful implementation. Consequently, this report does not examine technologies at the lowest technology readiness levels.[19] Therefore, while there may be future technologies that could present potential solutions to counter diversion, these technologies are not within the scope of our study.

Figure 2 provides an overview of the technologies in the long list. It illustrates the technologies included, providing an indicative overview of the way they range from more application-specific and less complex to higher-end and more application-diverse technologies. Table 2 contains descriptions of the various technologies and describes their current and potential applications based on existing information about their use. At this stage, users of the technology are not in scope or examined in this long list.

While table 2 provides only a quick look at a wide range of technologies, two additional points should be noted. First, the technologies mentioned in the table are presented as standalone technologies which have specific applications. However, in reality, the use of technology often means combining several such technologies, which may lead to additional applications not necessarily included or even foreseen in the table above. Second, it should be borne in mind that each of the technologies presented above requires wider supporting infrastructure in order to function optimally. This can range from electricity or an internet connection to data inputs, an overarching record-keeping system in the form of a digital database, and trained personnel, which should also be taken into account when selecting a particular technology, as will be discussed in Step 3 below.

Figure 2: Overview of technologies



**Less complex technologies**

**More complex technologies**

- 2D codes
- Chemical coding
- DNA coding
- Document authentication
- Physical unclonable function (PUF)

- Electronic seals (eSeals)
- Global navigation satellite system (GNSS) and mobile tracking
- Near field communication (NFC)
- Radio-frequency identification device (RFID)

- Sensors
- Internet of things (IoT)
- Distributed ledger Technology (DLT)

- Artificial intelligence (AI)

Table 2: Description of the identified technologies[20]

| Technology | Description | Applications |
|---|---|---|
| **2D codes** | 2D codes are small images that can store information both vertically and horizontally. 2D codes can be applied on packaging or items directly through laser marking. Laser marking applies a mark on the surface of an item without affecting the properties of the item on which they are placed; they can be used to input a large amount of information in a small space.[21] 2D codes not only require a coding system and equipment to generate and mark the code, which can be done only on flat surfaces, but also equipment to read the code. Two different 2D codes are highlighted as part of this long list: QR and data-matrix codes.<br>• **QR codes** are a type of 2D code which can store a very large amount of numeric, alphanumeric, binary, and kanji/kana characters. QR codes are fairly resilient to a small amount of damage or dirt and their data will still be readable.<br>• **Data matrix codes** can store slightly less information than QR codes, although they can store more characters in a smaller amount of space. Data-matrix codes are also seen as being more robust than QR codes in that even if a data-matrix code gets damaged, scanners may still be able to scan the code. | 2D codes are already in use in civilian supply chains. For example, QR codes can be laser marked onto ammunition as a way to identify and trace these items.[22] 2D codes can be used to identify items across the different stages of their life cycle. They are particularly suited to the PSSM context, where damage to the surface of conventional weapons, such as SALW, and related components is minimised in a controlled environment.<br>Data about an item's life cycle and diversion based on this marking could also be combined with data from other cases of diversion to help to identify suspicious activities and areas of weakness, feeding into an early warning mechanism. The use of such codes could also help automate data input, reducing errors compared to the manual transfer of data from paper-based records to a computerised database.<br>2D codes can be applied at different stages of an item's life cycle (e.g., manufacture, pre- or post-transfer, stockpile) and to a variety of items – SALW, their components, and ammunition. |
| **Chemical encoding** | Chemical encoding is the use of individual combinations of chemical particles to mark a product and identify it with a unique marking. This type of mark can be applied onto and integrated into very small and medium-sized products, and also to a wide range of materials. These marks are not visible to the naked eye but can be seen using ultraviolet detection. Furthermore, they are designed to withstand the environmental extremes that conventional weapons and related components are exposed to. However, such marks require specific, proprietary laboratory tests to identify the marking and decode the related data.[23] | Chemical encoding is already in use in various sectors, including as a pilot method to mark ammunition.[24] Chemical encoding is particularly well suited to identifying marked items during their entire life cycle, from manufacture to destruction, as well as post-diversion, to trace it back to its last legal custodian or storage facility.<br>Data about an item's life cycle and diversion based on this marking could also be combined with data from other cases of diversion to help to identify suspicious activities and areas of weakness, feeding into an early warning mechanism.<br>Chemical encoding can be applied at different stages of a life cycle (e.g., manufacture, pre- or post-transfer, stockpile) and to a variety of items, but in particular components and ammunition. |

| Technology | Description | Applications |
|---|---|---|
| **DNA coding** | DNA coding involves placing a unique DNA code (from synthetic or biological sources, such as plants) onto an item or its packaging, which is associated with a set of relevant information about the item. DNA codes can be applied to all types of physical product, particularly those which are small, numerous and flexible where other types of tag are less suited, such as RFID tags. Such marks are easy and quick to apply, and preservation techniques enable them to remain stable and permanent. These marks do not affect the properties of the item on which they are placed. Such marks, however, cannot be viewed by the naked eye but can be seen using ultraviolet light. Specific laboratory tests must be performed to identify the marking and extract the related data.[25] | In practice, DNA coding is already in use in various sectors, including as a way to identify counterfeit electronics in the military supply chain.[26]<br>While DNA coding can be used to identify items during their entire life cycle – from manufacture to destruction – the stability of marks without preservation techniques makes them more suited to aiding with PSSM. Subsequent data extracted from this marking could also be combined with data from other cases of diversion and help to identify suspicious activities and areas of weakness, feeding into an early-warning mechanism.<br>DNA coding can be applied at different stages of a life cycle (e.g., manufacture, pre- or post-transfer, stockpile) and is most relevant to components of conventional weapons, such as electrical sub-components. |
| **Document authentication** | Various technologies can be applied to strengthen physical document identification. Two such categories are described here: holograms and ink-based marking:<br>• **Holograms** create an optical effect which acts as an authenticator of a document it is placed on. Holograms can be divided into two broad categories: "traditional" and "complex".[27] In each, different types exist, the main difference being that traditional holograms only authenticate a document, whereas complex ones include additional hidden information which can be read only with specific tools, such as lenses or microscopes.[28]<br>• **Ink-based markings**, such as ultraviolet, iridescent or infra-red inks, or magnetic inks, are, similarly to holograms, used to authenticate documents. They become visible under different circumstances, depending on the type of ink used, which can include ultraviolet light or an infra-red reader. Or they are read by special character recognition devices.[29] | Document authentication is already applied to certain official documents, such as bank notes and passports. The use of such technology does not preclude undertaking existing checks on the information included in the certificates.<br>This technology could be applied in combination with artificial intelligence in order to aid staff distinguish between a real and a fake hologram or are able to review ink-based markings.<br>Physical document authentication can be applied to end-user certificates in order to strengthen protection against forged or other counterfeit copies. To this end, this technology is best applied at the earlier stages of the life cycle. It is most applicable during the transfer stage of an item's life cycle. |

| Technology | Description | Applications |
|---|---|---|
| **Physical Unclonable Function (PUF)** | Physical Unclonable Function (PUF) technology can be used to generate unique identifiers from the microscopic imperfections in chips to authenticate original chips and detect cloned chips.[30] A PUF is a physical object that for a given input and conditions (challenge) provides a physically defined "digital fingerprint" output (response) that serves as a unique identifier.[31] At a higher level, a PUF can be thought of as analogous to biometrics for human beings – they are inherent and unique identifiers for every piece of silicon. Every PUF device initially needs to be registered with the server so that it can be used with any cryptographic method. During the registration phase, the server uses a stimulus to challenge the client's PUF and as a result a corresponding original response is produced. This challenge and response pair is stored in the server's memory. During the authentication process, the server uses the same challenge for the client's PUF to extract the corresponding response. Consequently, PUF technology requires a link to the online server for stimulus–response control. | PUFs are being applied in applications related to cyber security: software licensing, secret key generation, payments, and also for device authentication.[32] PUF responses can therefore be used to authenticate a device or they can serve as a secret key for cryptographic operations such as encryption and digital signatures to enhance security beyond authentication.<br>PUFs can be applied at different stages of the life cycle and in particular to items containing an integrated circuit. As this technology makes use of variations in the manufacturing process of integrated circuits, it should be applied early on in the life cycle – particularly in the ICs that are used in the production of the items. However, this personalisation process during fabrication may be expensive, as it adds extra processing steps to the manufacturing process.<br>PUF technology can, for example, be applied to the chip in an RFID tag in order to make that RFID tag (more) tamperproof. Therefore, this technology can be used in the same situations and for the same purposes as the RFID tag (passive, active, semi-passive) it is identifying and authenticating.[33] |
| **Electronic seals (e-seals)** | Mechanical seals are generally used to secure containers and cargo; however, they are not tamper-proof. E-seals, which combine mechanical seals with electronic security, therefore seek to improve the security of seals.[34] The electronic element most commonly uses either passive or active RFID, with similar advantages and constraints as individual tags: read-range, cost, etc. Other equivalent technologies (e.g., NFC) can also be used. In this way, e-seals "build on [electronic technology] to provide digital data-capture, storage and readability functions in addition to [a mechanical seal's] physical anti-tampering functions".[35] Whether or not a seal has been tampered with is therefore immediately detected when a seal is scanned. E-seals require an internet connection so that they can upload and update scanned data to online databases. | This type of technology is already being used by customs organisations. E-seals can therefore help to prevent both diversion and the detection of any diversion attempts. The known presence of e-seals can increase accountability and provide an alert in cases of tampering.<br>As with other technologies, data collected based on seal tampering could be combined with other types of data to help to identify suspicious activities and areas of weakness, feeding into an early warning mechanism.<br>E-seals are most relevant to the transfer stage of the life cycle and to application to the cargo or container of conventional weapons and related components. |

| Technology | Description | Applications |
|---|---|---|
| **GNSS and mobile tracking** | Several types of tracking technologies exist that rely on a digital infrastructure. Two in particular are highlighted in this long list:<br>• **GNSS tracking** technology is added to specific technologies, such as RFIDs or sensors, or onto an item, its package or an entire container to track them using satellite technology (GNSS).[36]<br>• **Mobile tracking** technology includes the Global System for Mobile Communications (GSM) and the General Packet Radio Service (GPRS) technologies. GPRS technology is more sophisticated than GSM, enabling improved mobile service. As with GNSS, mobile tracking is added to specific technologies and tracks them using mobile phone networks.<br>These tracking technologies require the use of both a device and software that gathers the tracking data. However, if there is a poor signal, or none, transmissions will stop in certain areas. | This type of tracking is already used to track both commercial civilian and military objects. GNSS and mobile tracking can therefore help to detect any attempt at diversion. Indeed, the known presence of tracking technology can increase accountability and give an alert in cases of any divergences – for example, during transportation.<br>As with other technologies, data regarding any issues during transfer could be used on their own or can be combined with other types of data to help to identify suspicious activities and areas of weakness. These could then feed into an early warning mechanism.<br>GNSS and mobile tracking are most relevant during the transfer stage of the life cycle, and to application to the cargo or container transporting conventional weapons and related components. |

| Technology | Description | Applications |
|---|---|---|
| **Near field communication (NFC)** | NFC technology is a "set of communication protocols for secure wireless communication between electronic devices"[37] at a close distance (several centimetres) from each other. While NFC is like RFID in that it also possesses a tag (small chips that can be inserted into stickers, magnets, and labels) and reader, it enables two-way communication. NFC technology can also be incorporated in active RFID tags as a way of improving the security of the data communication.<br>As with RFID, there are both active and passive NFC devices. Active devices entails both devices sending and receiving data; with passive devices, one side (the initiator) has to send power to the other (the target) to power it up. Due to the similarities with RFID, it is necessary to outline the differences: for instance, because the NFC read range is shorter than for RFID, it can be more difficult for hackers to gain access to the data or identify the signal. Additionally, only one tag can be read at a time for NFC (unlike several for RFID), making NFC less efficient for PSSM purposes. | With NFC embedded in many smartphones (e.g., to make contactless payments), it is widely used daily and it has also been used to some extent for logistics and warehouse management for civilian products, although it is less mature and less extensively used than RFID. NFC has also been used to enable a certified user to fire a weapon, as is the case with certain so-called "smart guns".[38]<br>NFC technology can be applied at different stages of the life cycle, depending on the purpose of the NFC. Overall, NFC is best suited to helping with record-keeping and the tracking and tracing of individual SALW. NFC could, for the most part, be applied to the same items as RFID tags. For example, NFC could be used as a way to mark items directly as a way to track them or be applied to packaging or pallets to help to track items during transfer.<br>Data about an item's life cycle and diversion based on this marking could also be combined with data from other cases of diversion and in this way help to identify suspicious activities and areas of weakness, feeding into an early warning mechanism.<br>The use of such codes could also help to automate data input, reducing errors compared to the manual transfer of data from paper-based records to a computerised database. |

| Technology | Description | Applications |
|---|---|---|
| **RFID** | RFID technology consists of a chip, an antenna which is attached to the chip, and an external reader. Data are encoded in the chip, transmitted via the antenna, and read by the reader. Readers can be either static or mobile, with static ones possessing a greater read range. RFID tags can be either passive or active, or distinguished by their frequencies.<br>• **Passive tags** do not have an internal power source. They rely on the wave signal emitted by the reader to power themselves. They operate at different frequencies, ranging from low to high to ultra-high frequency. Both the frequency and the activeness or passiveness of a tag determine the range at which it can be read, with ultra-high-frequency tags having the greatest read range.[39]<br>• Unlike passive tags, **active tags** have an embedded battery. This can limit the length of the life cycle of active tags. They are also larger than passive tags due to the integrated battery. As a result, however, active tags can be read from a greater distance than passive ones.[40] Some active tags can include sensors that monitor environmental factors (e.g., temperature) and also satellite communication technology or mobile telephone networks. The latter two enable real-time visibility of the tag and product,[41] and also authentication capabilities and cryptographic functionalities, thus ensuring the security of the data.[42] | RFIDs are already in use, particularly for tracking and tracing transfers. For example, RFIDs can be applied directly on objects to track these throughout their life cycle, as is notably the case regarding civilian products; to the packaging and pallets of items, in which case it can be used to track a variety of items, including SALW, the components of conventional weapons, or ammunition during the transfer stage; or to enable a certified user to fire a weapon, as is the case with certain so-called "smart guns".<br>The use of RFID also aids the automation of data input, reducing errors compared to the manual transfer of data.<br>Subsequent data extracted from RFID data could also be combined with data from other cases of diversion to help to identify suspicious activities and areas of weakness. Such data could feed into an early warning mechanism.<br>RFID tags can be applied at different stages of the life cycle, depending on the purpose of the RFID, but also as a result of their versatility and the different types of RFID that exist.[43] RFIDs can notably support tracking, marking, record-keeping, and PSSM, and are most relevant for SALW. |

| Technology | Description | Applications |
|---|---|---|
| **Sensors** | While RFID and NFC tags are a type of sensor, a wide range of other types of sensor exist. They include image sensors (e.g., cameras, radars, thermal imaging, X-ray scanners) and monitoring sensors (e.g., gas indicators, acoustic sensors, time-temperature indicators, which also include RFID[44]). Sensors can be used for a range of purposes, including but not limited to:<br>• **Biometrics**: Biometric data include the physical, morphological, and behavioural measurements of certain characteristics linked to an individual. Some of the most commonly used biometric characteristics include fingerprints and facial and voice recognition. Biometric scanners can be used to grant access to certain locations (e.g., stockpiles) or to certain systems (e.g., databases), and even the use of weapon systems only for pre-approved individuals.<br>• **Intelligent packaging**: This is "packaging which senses and informs."[45] Such packaging has embedded sensors that monitor the condition of a packaged product, particularly during its transportation and storage. Sensors include, for example, time–temperature indicators, gas indicators, and RFID.[46] This can ensure product protection – for example, identifying whether packaging has been tampered with.[47] Embedding RFIDs and NFC can also help to track and trace items, particularly during transit.<br>Not only do such sensors require electricity and sometimes an internet connection, but there is also a cybersecurity risk linked to their use, particularly if information security management is inadequate. This can be mitigated by implementing appropriate cybersecurity measures. | Sensors can be placed directly on items, as in the case of RFID and NFC. They can also be used to monitor certain locations (e.g., thermal cameras) and help with access control (e.g., biometrics). In these ways, sensors play a preventive and detection role across the life-cycle stages; and, in fact, different types of sensor are already in use in the civilian commercial realm (e.g., the food and pharmaceutical industries) and with conventional weapons.<br>Subsequent data extracted from sensor activity could also be combined with data from other cases of diversion and in this way help to identify suspicious activities and areas of weakness, feeding into an early warning mechanism.<br>Sensors can be used across different stages of the life cycle of a weapon or related components for a variety of purposes. For example, they can be used pre-, during, and post-transfer to monitor the security of the objects and their packaging (e.g., intelligent packaging, X-ray scanners). |

| Technology | Description | Applications |
|---|---|---|
| **Internet of Things (IoT)** | IoT refers to an overarching digital platform connecting the physical to the digital world. Specifically, IoT is enabled by physical devices such as sensors, RFIDs, and other similar (internet) connected technologies that collect and exchange data, which is therefore captured digitally.<br>These data, which are synchronised from various sources on one single platform, can also be used to digitally monitor – or even control – the physical objects onto which a sensor is applied. For example, if a sensor indicates a change in the environment, such as temperature, then, if the thermostat is also a connected device, it can be modified from a distance.<br>The use of IoT technology requires an infrastructure of connected devices, without which it cannot exist. The use of connected devices also implies a potential cybersecurity risk, particularly if there is poor information security management. | IoT is already used for warehouse management for certain commercial civilian products.<br>IoT technologies could help automate data input, reducing errors compared to the manual transfer of data from paper-based records to a computerised database. Data related to weapons and related components can be captured across their life cycle by IoT devices. This is conceptually quite similar to DLT in that IoT requires data capture throughout, even though the data storage and use differ. To this end, IoT is particularly well suited to detecting instances of diversion, including areas of weakness. |
| **Distributed Ledger Technology (DLT)** | DLT[48] is a “distributed record”, or “ledger”, in which transactions are stored with cryptographic techniques, ensuring transparency across an entire ecosystem. [49] Data held on a DLT is very hard to manipulate, thus enhancing trust in the data stored.<br>There are two main types of DLT: open (i.e., permissionless) platforms and permissioned platforms. Permissionless platforms are publicly available and anyone can become a user, own a copy of the data, add data, verify transactions, etc. Permissioned platforms are accessible only to those who have been given permission, and who can read, write, and verify transactions. There can also be a hybrid of the two systems. Permissioned platforms are safer from harm of attack compared to permissionless platforms.[50]<br>DLT can improve trust in stored data stored, so long as it is of quality, while also increasing the transparency and visibility of items throughout their life cycle. The use of DLT does require a significant logistical footprint as data needs to be captured at all relevant stages and by all relevant actors in the life cycle. For example, by using marking and tracking and tracing technologies (e.g., 2D codes, RFID, sensors). | DLT has already been applied to certain specific sectors, such as the food and diamond industries.<br>Regarding weapons, a proof-of-concept examined the use of DLT to reduce the risk of chemical weapons proliferation.[51] To this end, DLT could be particularly well suited to export and import licensing and clearance and to detecting instances of diversion, including areas of weakness.<br>Data related to weapons and related components can be stored in a DLT across their life cycle. This can include data regarding the item itself (or their containers or pallets), which is captured across every stage of the life cycle. |

| Technology | Description | Applications |
|---|---|---|
| **Artificial intelligence (AI)** | AI is an umbrella term that includes different types of algorithm learning techniques and abilities. All AI models require data for training, whether that be to understand anomalous patterns or specific aspects of images. More broadly, AI is well suited to assist with tasks such as data collection, data synthesis, and data analysis. To that end, AI has a wide range of applications, though, as with other digital technologies, the use of AI entails a cybersecurity risk. | AI is already in use: for example, to help identify financial fraud and as a way to identify supply chain risks in the automobile industry.[52]<br>AI is applicable at different stages and also across the life cycle of conventional weapons and related components. In particular, it helps to improve and render transfer controls more effective and safer. In this way, AI can aid various tasks across the supply chain of an item, notably by using its analytical and pattern analysis capabilities. This includes, but is not limited to:<br>• Supporting human-led risk assessments by enabling automated data analysis and assessment.<br>• Identifying document fraud using optical character recognition (OCR) combined with AI.<br>• Analysing sensor data, such as X-ray images at border controls via computer vision.<br>• Analysing big data, as in screening financial flow data or analysing data captured by sensors across a life cycle in order to identify unusual patterns or ensure sanctions compliance.<br>• Automating image analysis (e.g., by X-ray machines at border control) and conducting big data analysis (e.g., financial flow data). |

## Step 3. Analysing the context in which technologies are to be implemented

The third and final step of the framework is to assess the practical implementation of the technologies. This involves determining the conditions that need to be met in order to apply technologies in a given context, and also ensuring that the technologies possess the attributes considered most important to the users.

Importantly, apart from the direct goal related to the countering of diversion, system-related factors should also be weighed up when assessing potential technologies. Such factors could be derived from a broader contextual analysis and the reality in which technologies would be implemented. Both the existing literature and interviews with relevant experts helped to identify general contextual attributes that are crucial to use in any assessment of the identified technologies and their proposed usefulness in the specific context of international conventional arms transfer control.

First, it is necessary to understand the **context of application**. This will differ between cases and therefore requires a case-by-case assessment. This includes, for example, understanding the following:

- Which non-technological measures exist? For example, do we have the appropriate policy and legal framework in place to facilitate technology use? And if not, what is required? Are issues regarding the standardisation of information between different actors addressed?

- At what level is the technology being adopted or applied? For example, is a particular technology intended for use only at the national level or would it necessitate inputs from or application at the regional or the international level by other stakeholders active at another national level? This may affect considerations of which technology to apply where, as well as lead to differences regarding use, uptake and accessibility.

- What physical and non-physical infrastructure is required, and what is currently missing? For example, this could refer to the existence of sound buildings and also to the presence of a reliable electricity supply.

- What resources are required to apply the selected technologies and do we have these at our disposal? These could include monetary resources, human resources, know-how, institutional capacity, expertise, training programmes, etc.

- Do certain arms-control instruments restrict or otherwise regulate aspects of marking, tracking, or tracing? And would this affect or prevent the use of certain technologies?

In addition, technology comes with its own set of advantages and challenges, so it should not be seen as a panacea. However, beyond that set, **several other overarching challenges should be considered and responded to prior to applying technologies** for conventional arms transfer controls. These challenges include:

- Patchy or irregular use of technologies can undermine their effectiveness. For reasons related to national security or for geopolitical reasons, end-users can be highly reluctant to integrate certain technologies because they are concerned about who will have access to the software and to what extent the information would be accessible to the developers of the technology.[53]

- One needs to take a whole-of-system approach to deploying technology, and consider such factors when embedding technologies within a process. Specifically, inadequate human resources and infrastructure can undermine or prevent the use of technology, such as:

  - the infrastructure may simply not be strong enough to prevent illegal users from entering it;
  - the remoteness of the storage location could make it impossible to connect to online data platforms;
  - there may be unreliable electricity; or
  - untrained personnel can make unintentional mistakes or omissions.[54]

- Even with consistent use and cooperation, it is still possible for malicious actors to circumvent or weaponise technology. This includes diverting conventional weapons and related components enabled by governments themselves, making it even more difficult to collect and share information or to cooperate.[55]

Second, it is important to **identify the qualities or elements that technology can or should have – in other words, the attributes a user determines to be of most importance for a particular technology to possess**. Technologies all possess differing advantages and barriers to implementation. These need to be paired with certain characteristics or qualities that a user would like a technology to possess so that it can adequately fulfil its aim. Building on the insights expressed in the literature review and also in expert interviews, nine key attributes have been identified (see Table 3), which can be tailored to the needs of the framework users to help them determine whether the selected technologies possess the required attributes. These attributes could also be a way to engage all stakeholders in a common dialogue. Importantly, these attributes also function as variables. For example, the assessment of the affordability of a technology will differ between technologies. This will enable stakeholders depending on available resources or funds to take such factors into account in their assessment of a technology. These attributes are also relative: some stakeholders may be willing to accept a high cost if the benefits are also high, while others may not.

**Table 3: Technological attributes**

| Attribute | Explanation |
|---|---|
| **Affordability** | If the cost of a technology is high, then the willingness and ability to apply it will differ across the various stages in the life cycle of an item. There may also be questions of who becomes responsible for bearing this cost.[56] The cost of a particular technology should be assessed in relation to the value of the item in question: highly sensitive or valuable products may require and justify more expensive technologies. |
| **Embeddedness** | Technologies do not operate in a vacuum; they are not "standalone" solutions. Technologies operate in an existing context of rules, regulations, and approaches. It therefore behoves users to ensure it is possible to embed a technology seamlessly within this existing context, and to undertake the necessary steps for this to be the case. |
| **Ease of use** | Many stakeholders are involved at all stages in the supply chain, with varying levels of digital literacy and facility with technology. A particular technology should therefore be accessible and easy to use, and spare parts and maintenance must be easily accessible.[57] |
| **Interoperability** | Supply chains are complex, involving many different stages and stakeholders. The complexity of supply chains that involves many different stages and stakeholders requires the development either of a common technology that can be used by all or of a particular technology that can be interoperable with others. Ascertaining the technological interoperability of a particular technology or technologies is therefore important. |
| **Layered** | Multiple technologies, whether of the same type or of different types, could be used to complement each other and overcome the limitations of any singular technology. The use of multiple technologies can also provide additional redundancy in case of any issues or failures in one of the technologies. It would therefore be important to ensure that a particular technology could be layered with others. |
| **Robustness** | Robustness refers to both physical condition and security concerns. For example, throughout transit and later active use, weapons will be placed in several different and at times challenging environments. Technologies should therefore be robust enough to withstand both very high and very low temperatures, rough handling and also other environmental factors such as rain, wind, and dirt.[58] At the same time, they should be robust in the sense that they are tamper proof against both physical and digital intrusion. |
| **Scalability** | Volumes of items or user needs will probably fluctuate over time. Ensuring that a particular technology is scalable – meaning that it is still able to function despite changes in volume – is important to ensure its long-term usability. |
| **Sustainability** | The ability to maintain or support a technology over a long period of time ensures both continuity and dependability. Sustainability may also have an impact on affordability, as not having to replace it cuts costs. A long-term technology also enables better absorption of any up-front costs over time, leaving only any running-costs to be factored in the affordability attribute. |
| **Trust** | Trust is an essential factor to ensure the successful adoption of technology.[59] However, it is also complex and multidimensional. Multiple types and levels of trust exist. These include trust in the technology (does it do what it is meant to do?), trust in the security of the technology (is the technology and/or its data secure?), trust in the provider of the technology (are they a trusted vendor and can they keep the technology safe?), and trust between the different actors in the supply chain to share relevant information.[60] There is therefore not one single clear interpretation of "trust", which is an amalgamation of all these different and context-specific facets. |

# Section 3 - Applying the framework in real-life: a primer

The previous section set out the framework with which to identify and assess potentially relevant technologies to counter the diversion of conventional weapons and related components. This section aims to provide two illustrations to demonstrate how the framework might work in practice with, first, the components of conventional weapons (CWC), more especially electrical components (3.1) and second regarding SALW (3.2). Importantly, these descriptions are not in-depth case studies in which a thorough and comprehensive assessment process is undertaken, but they serve primarily as a first attempt at illustrating how the framework presented in section 2 could be instrumental in analysing diversion risks, identifying potentially relevant technologies and assessing the possibilities and challenges that need to be considered in order for these technologies to be implemented effectively in arms transfer controls. Such a comprehensive assessment would necessitate more dedicated discussions and input from all the different stakeholders – state authorities, relevant industry representatives, technology companies, international organisations, and civil society.

## Technologies to counter the diversion of components of conventional weapons and related components: an illustration

While policymaking focused traditionally on countering the diversion of complete weapon systems, awareness is gradually growing that components play a crucial role in the development, production, and maintenance of conventional weapons. Given their size and appearance, however, they are easier to conceal, more difficult to identify and therefore easier to divert. Moreover, the international trade in components often runs through prolonged and complex supply chains, making it difficult to keep an eye on the effective end-user, thus creating a greater risk of unauthorised end-use. The fact that these components could also be intended for use in civilian products and thus do not have an exclusively military use, also adds to the challenge of understanding and controlling transfers of such items. A specific type of components – electronic components, such as semiconductors, integrated circuits or microprocessors – is particularly relevant in this discussion as they have been found to be diverted to different embargoed destinations, where they are used as critical components in a broad variety of weapon systems. The main methods used to divert such components are the development of elaborate procurement networks with shell or front companies in various countries, with the aim of obscuring the effective end-use of the goods and the country of end-use. In this context, the identification of such transfers during customs controls is rendered more difficult by describing the goods in a general manner and thus hiding their strategic and controlled nature.[61]

**Step 1. Specifying the aim of using technology and mapping item-specific risks of diversion**

The principal methods of diversion for the electrical components of conventional weapons used occur in the (pre-)export phase of these items:

- Shell or front companies are used to obscure the effective end-user. This is possible because such items are typically not transferred directly to governments but pass instead through various export and import companies before reaching their effective end-user. This complexity of the supply chain and life cycle of these goods makes it difficult to identify the chain of custody and the specific points at which the goods are diverted.

- Goods are deliberately described in a general manner in customs declarations in order to circumvent controls.

As a consequence, specific technologies that could strengthen identification of risks during the **pre-export or transit** risk assessment process by the competent export authorities should be the main focus of detection measures. These should be implemented prior to either authorising or denying the transfer of goods. Such technologies should therefore be applied to counteract diversion by supporting governments' work in **preventing diversion**. This should be achieved in two ways: by identifying fraudulent procurement networks and by **detecting diversion** (attempts) by enhancing the identification of transfers of such components when they pass through customs controls in the countries through which the goods transit or from which they are exported.

**Step 2. Identifying potential technologies**

An important technology that could be relevant in this context is **artificial intelligence** (AI). AI could be used in the pre-export phase, where it could contribute to preventing diversion from effectively taking place by identifying suspect, front or shell companies in the first place. Such technologies are being used extensively in the financial sector for various applications: data collection, organisation of market information, and fraud and risk assessment. However, regarding fraud and risk assessment, the lack of real-life data is making it difficult to implement AI to combat financial terrorism and identify instances of money laundering.[62] Regarding this challenge, Canhoto (2021: 441) has offered a possible solution:

*"Therefore, there is limited scope for using supervised machine [(ML)] learning to tackle this problem. However, it is possible to use reinforced ML and, to an extent, unsupervised learning to model unusual financial behaviour, not actual money laundering."*[63]

With regard to identifying illicit procurement networks set up for international sanctions-busting, though, several organisations claim to have used AI tools to uncover illicit procurement networks, for example, to identify the vessels used to circumvent international sanctions[64] or the supply chains for electrical components to sanctioned countries).[65]

Next, AI could also be used in the transfer phase to detect attempts at diversion by identifying transfers of controlled items for which more generalised descriptions are used in customs declarations. However, the substantial amounts of goods that are being transferred and which pass through customs every day make it difficult to identify such transactions. But ML techniques could be applied to profile international transfers of strategic goods in particular: they could do so by identifying patterns that may enable customs authorities to recognize these transactions more effectively.[66]

**Step 3. Analysing the context in which technologies are to be implemented**

The successful implementation of these technologies would, however, be confronted by several barriers and preconditions, as becomes clear when we consider the attributes identified in step 2 of our framework. Overall, AI software appears to be quite **robust** and **scalable**. However, such technologies are relatively costly to procure, to keep up-to-date (**"sustainability"**) and to **embed** in existing programmes and processes. But in the current context there are some advantages to using AI: data entry and checking for false flags would be the very tasks that would become automated and less demanding of human time and effort and therefore on cost. In addition, implementing such technologies could also result in the identification of more suspect cases and transactions needing human analysis, interpretation, controls and follow-ups – possibly increasing the need to employ additional staff. But since international trade flows are in any event characterised by vast amounts of data collected by customs authorities through shippers' export, transit or import declarations, perhaps additional effort and staff might not be needed. This is because AI would certainly be capable of using the huge datasets for training and optimising the algorithms that will serve to identify shell companies and strategic goods transactions in the huge amount of trade transactions that take place worldwide every day. Digitization, which is a major prerequisite of any meaningful use of AI, therefore appears to be generally present to perform analyses of trade flows.

Staff should also be trained properly and continuously in how to use these technologies efficiently and technical expertise should be available to keep the software up-to-date and secure. A crucial question in the specific context of international arms transfers in which both private actors and government control agencies are involved would also be this: **Who is to be responsible for implementing such AI tools?** On the one hand, private actors such as manufacturers, shipping companies and financial institutions could do this as part of their enhanced due diligence processes and "know your customer" procedures. On the other, public agencies – export control and customs authorities – could include such tools in their existing risk assessment and monitoring programmes. These considerations will also be relevant to matters pertaining to the cost of implementing these AI tools and of the staff that will need to be trained in using these tools.

Another crucial condition is that a **layered approach** is necessary: AI requires databases with substantial amounts of information to be available that the AI software could analyse. Here, the information collected by customs authorities in export, transit and import declarations could be highly useful, as could existing company and trade registers. Gathering all these data presupposes **interoperability** between the different actors involved and the owners of these databases, which in practice has proven to be a challenge to date.[67]

Finally, concerns about the ethical dimensions and bias of AI software may be a barrier to its uptake, and this could have an impact on the level of **trust** in the technology. In a similar manner, trust in the quality of the datasets used is also a crucial precondition. However, it should be borne in mind that implementing algorithms does not necessitate close cooperation between the various actors throughout the transfer chain as it can be carried out autonomously by private and public actors in the countries of export or transit. **Trust** between the different actors in the supply chain should therefore not be a necessary precondition.

## Technologies to counter the diversion of SALW: an illustration

SALW are at increased risk of diversion compared to other, larger military equipment for several reasons:

- Their **ease of use**, as SALW do not require particular technical skills or equipment to operate, making them accessible and attractive to a wide range of users, including but not limited to state and non-state armed forces, security forces, police forces, and civilians.
- The **ease of diversion** of such items, given their small size, making them "easy to conceal".[68]
- Their **long life cycle**, increasing the opportunities for diversion across their lifetime.
- The **high scale of production** of SALW, which can make individual products more difficult to keep track of.[69]

In this context, it is also important to consider that SALW is a broad category comprising many different types of weapon. Some of these will be at greater risk of diversion, simply because they are more appealing to users. Others will pose greater risk to international security, such as man-portable air-defence systems (MANPADS) and man-portable anti-tank systems (MANPATS), due to their ability to threaten and affect larger military (and civilian) equipment to a greater extent than other SALW.

The following presents a hypothetical example to explain how the framework presented in Section 2 could be applied to the issue of SALW diversion. By way of context, Country A has had a turbulent recent history. Over the past several decades, it has been the location of a civil war which lasted several years. The conflict has now ended; however, pockets of rebellious actors who are not happy with the status quo remain. Therefore, certain parts of Country A's territory are still the site of attacks by armed groups, which predominantly use assault rifles, general-purpose machine guns, and mortars. This is also compounded by instances of armed violence in neighbouring countries which at times spill over into Country A, again mostly using SALW.

These ongoing localised conflict situations are enabled by areas of structural fragility which are exploited to enable the illegal flow of SALW – which are the main types of weapon used by local and neighbouring armed groups. Indeed, based on evidence collected, it was determined that many of the weapons currently being used have been obtained from state stockpiles.

Country A already has several counter-diversion measures in place, notably by having robust national arms control legislation in place; efforts to implement international arms-control norms, instruments, and processes; and by ensuring the registration of all weapons at the time they are imported. However, such measures have not been sufficient to prevent the illicit diversion of SALW, and the use of technology to bolster existing mechanisms is therefore being considered.

**Step 1: Specifying the aim of using technology and mapping item-specific risks of diversion**

The main aim of applying technology was identified as improving detection of diversion as well as identifying of how diversion occurred in the first place. Based on a risk assessment undertaken in-country, one of the main risks of diversion that emerged within Country A is the (lack of) security and integrity of national stockpiles. This risk was found to be primarily driven by the poor implementation of procedures for managing SALW in national stockpiles, which is notably linked to limited record-keeping, inventory management, and reporting and investigation of weapons diverted from the stockpiles.

**Step 2: Identifying potential technologies**

Several technologies were identified as being able to help respond to the identified risk; they can be divided into improving weapon identification and securing stockpiles. For improved weapon identification, **laser marking data matrix codes on SALW** was identified as a potential technology. For securing stockpiles, the solutions include placing **passive RFIDs** on the weapons to automatically log weapons entering and leaving the stockpile, using a **digital database** both to track the movement of weapons through RFID data and to store specific weapon data obtained from the data matrix code, and then to implement the use of **biometrics** at the entrance of the stockpile to ensure that only pre-approved individuals could enter the area.

**Step 3: Analysing the context in which technologies are to be implemented**

In the final step of the framework, users then need to consider the possible barriers and preconditions to using these technologies. This analysis should ideally be undertaken by all relevant users and other stakeholders involved at this stage of the life cycle of SALW to identify any challenges or issues beyond those specific to each technology. The discussions should also involve technology experts.

Focusing on passive RFIDs, in this example, the context of the existing regulatory and legal framework would need to be examined to identify whether new laws, norms, or other policies would be required to implement the envisaged technologies (e.g., **embeddedness and interoperability**). Similarly, the physical infrastructure of the stockpiles would also need to be examined and any non-technological issues resolved before technologies can be implemented. The **costs** of the tags and the required digital infrastructure would also be assessed, together with their **robustness** and resistance to environmental factors. With passive tags not possessing a battery, this improves their long-term **sustainability** and therefore drives down the costs of having to change tags frequently. Also examined is the extent to which the tags are determined to be **easy to use** and whether technical knowledge or training is required by those handling the weapons or fitting the RFID devices to the weapons. As noted above, RFID can work well with other technologies, not least of all the use of a digital database to capture and store the data, highlighting that a layered approach is important when considering this technology. Finally, an examination of trust in this context may demonstrate queries whether the data are secure – which can be mitigated by applying good cybersecurity principles – and whether, and to what extent, RFID tags could be subject to battlefield detection, which could pose an operational security risk. The latter possibility could be mitigated by investigating the use of tags with a very short read-range.[70]

# Section 4 - Concluding remarks: Assessing the application of technologies to counter diversion

This paper presents a framework which aims to offer a systematic and consistent approach, language, and method with which to identify and assess technologies that counter the diversion of conventional weapons and related components. Overall, **the framework demonstrates that the application of technology to prevent or counter diversion in international conventional arms transfer control requires a multi-step approach**:

- first, define the aim of the technology and understand the specific risks to be mitigated or prevented;
- second, identify the technology or technologies which could deal with these risks and aim(s); and
- finally, analyse how technology would be applied in practice by assessing the context and barriers of application and the preconditions of the use of the identified technology, and then assess the technologies against the attributes seen as most relevant and important to the stakeholders involved.

**The paper presents a long list of technologies, which demonstrates that a wide range of relevant technologies exist** and can be explored by the international conventional arms transfer control community to help strengthen counter-diversion efforts. Owing to the approach taken by this paper, to focus on existing technologies applied in supply chain management, there is a bias in the technology long list towards those which apply either to the entire life cycle or to the transfer stage specifically. Despite this limitation, the long list of technologies nonetheless demonstrates the range of options available to stakeholders, from more to less complex, not only aimed at improving data collection and diversion prevention or detection measures, but also to help users undertake risk assessments, adopt early warning mechanisms, enable transparency, and build cooperation and trust.

Yet, as shown through the framework, a considered approach to technology is needed. First, **technology does not and cannot replace non-technological measures** – from standardising data inputs to adopting the necessary legal and governance frameworks to prevent diversion. In addition, alongside those benefits that can be provided by technologies, an objective review of the challenges, barriers, and preconditions of use, including the necessary non-technological measures, is necessary.

Second, the **siloed nature of conventional arms transfer control** makes it particularly challenging to apply technologies where coordination, information sharing, and collaboration are necessary. This is compounded by:

- the wide variety of actors involved in the life cycle of a weapon or ammunition;
- the lack, in some instances, of existing regulations and standards on record-keeping; and
- the practical and political difficulties regarding information-sharing between actors in different countries.

These are just some of the barriers to the development and implementation of technologies.

Third, **technologies that allow for continuous and real-time tracking of conventional weapons and their components throughout the complete value chain remain scarce**. This indicates that no single technology can singlehandedly prevent or counter diversion across the entire life cycle of a weapon, and therefore a single technology should not be relied on.

Finally, **certain stages in the life cycle of conventional weapons and related components appear to have fewer technologies relevant to countering diversion**. This applies particularly to the active use and destruction stages and may be due to the study approach taken, as already noted. However, it also shows that while it is important to examine technologies which have been tried and tested in other domains, there is also scope for exploring more nascent solutions at a future stage and for helping to develop and mature such promising technologies.

Overall, the inclusion of technology in international conventional arms-transfer control brings together a range of questions, diverging opinions, views and approaches about the willingness, effectiveness, and ability to implement. This identifies the need to conduct a dialogue among all stakeholders: the technology development companies, the industrial sectors which would need to deploy and adapt to such technologies, civil society, and state representatives for whom arms-transfer controls serve specific goals and objectives. Doing so would help with understanding which barriers and challenges exist, and how to overcome them. Proponents, enthusiasts, or doubters – all of them need to be brought together to give a substantive push forward regarding the questions – and answers – about using technology in controlling international conventional arms transfers.

## Endnotes

1. UNIDIR, Conflict Armament Research (CAR) and Stimson Center (n.d.), *Strengthening shared understanding on the impact of the Arms Trade Treaty in addressing risks of diversion in arms transfers*, https://www.unidir.org/publication/strengthening-shared-understanding-impact-att-risks-diversion-arms-transfers-compendium#:~:text='Strengthening%20shared%20understanding%20on%20the,referred%20to%20as%20the%20Consortium

2. UNODC (2005), *International instrument to enable states to identify and trace, in a timely and reliable manner, illicit small arms and light weapons*, https://www.unodc.org/documents/organized-crime/Firearms/ITI.pdf, 3.

3. Merriam-Webster (n.d.), Technology, https://www.merriam-webster.com/dictionary/technology

4. Arms Trade Treaty (n.d.), Possible measures to prevent and address diversion, https://www.thearmstradetreaty.org/hyper-images/file/Article%2011%20-%20Possible%20measures%20to%20prevent%20and%20address%20diversion/Article%2011%20-%20Possible%20measures%20to%20prevent%20and%20address%20diversion.pdf.

5. Tech4Tracing (2022), Bringing new tech to arms control. T4T report from UN PoA BMS8, Policy brief, August 2022, https://static1.squarespace.com/static/6081e2a18f1c88179800e119/t/63f77128b8e3ac29b7eb23cf/1677160745692/T4T-PolicyBrief1-Aug2022.pdf. It should also be noted that while technology has been examined in various multilateral processes, the focus has not been on technology as a tool to counter diversion, but rather on new and evolving weapon materials and production processes.

6. See, for a similar approach, National Academies of Sciences, Engineering, and Medicine (2013), *Strategic issues facing transportation, volume 3: Expediting future technologies for enhancing transportation system performance*. Washington, DC: The National Academies Press.

7. See, for example, Conflict Armament Research (2021), *Field forensic firearm exploitation; developing RFID solutions in support of stockpile management and post-diversion tracing*, https://www.conflictarm.com/technical/developing-rfid-solutions-in-support-of-stockpile-management-and-postdiversion-tracing/; Danssaert, P. (2019),*Anti-diversion measures: Real-time locating systems*, Antwerp: IPIS, https://ipisresearch.be/wp-content/uploads/2019/05/1905-Anti-diversion-v2.pdf; Candano Laris, D. (2021), Blockchain applications for export control compliance and global supply chain integrity, in C. Vestergaard (ed.), *Blockchain for international security. Advanced sciences and technologies for security applications*, Springer, Cham, 89–107.

8. Indian Ministry of Defence (2022), Indian army implements radio frequency identification (RFID) of ammunition stock, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1797008; Lewis, M. & Maletta, G. (2022), Post-shipment on-site inspections and stockpile management assistance: Bridging gaps, SIPRI Policy Brief, August 2022, Stockholm: SIPRI, https://www.sipri.org/sites/default/files/2022-08/pb_2208_post-shipment_on-site_inspections_and_stockpile_management_assistance.pdf

9. Laporta, J., Pritchard, J. & Hall, K.M. (2021), AP: Military units track guns using tech that could aid foes, AP, 30 September, https://apnews.com/article/rfid-military-weapons-guns-62c88008478f4ac403047c21f3184677

10. Lück Nico (2019), PRIF Report: Machine learning-powered artifial intelligence in arms control. https://www.hsfk.de/fileadmin/HSFK/hsfk_publikationen/prif0819.pdf

11. Marshall W., McAllister C., Vestergaard C. (2023), Nonproliferation: Reconciling Discrepancies in the International Trade of Dual-use Chemicals: The Potential of Blockchain Technology. https://www.stimson.org/2023/reconcilingdiscrepancies-in-the-international-trade-of-dual-use-chemicals/

12. Tech4Tracing (2022), Bringing new tech to arms control. T4T report from UN PoA BMS8, Policy brief, August 2022.

13. National Academies of Sciences, Engineering, and Medicine (2013), *Strategic issues facing transportation, volume 3: Expediting future technologies for enhancing transportation system performance*. Washington, DC: The National Academies Press, 1.

14. National Academies of Sciences, Engineering, and Medicine (2013), *Strategic issues facing transportation, volume 3: Expediting future technologies for enhancing transportation system performance*. Washington, DC: The National Academies Press.

15. For example, Ho, W., Zheng, T., Yildiz, H. & Talluri, S. (2015), Supply chain risk management: A literature review, *International Journal of Production Research*, 53 (16), 5051.

16. World Customs Organization and World Trade Organization (2022), WCO/WTO study report on disruptive technologies, 105, https://www.wto.org/english/res_e/booksp_e/wco-wto_e.pdf

17. "Item level" refers to examining a specific type of weapon (e.g., MANPAD), ammunition (e.g., small-calibre ammunition), or component (e.g., semiconductors), as opposed to focusing on the broader category in which they belong.

18. Based on an analysis of the existing literature on technologies implemented in supply chains across industrial sectors and in-depth interviews with academic experts in supply chain management, representatives of various civil industrial sectors and of companies that have developed or implemented technologies to strengthen supply chain security and visibility were used to identify this long list of potentially relevant technologies.

19. Technology Readiness Levels, or TRLs, are a categorisation used to classify the maturity of a particular technology. They range from level 1 to level 9, with 1 being where "basic principles [are] observed" and 9 where it is an "actual system proven in an operational environment". Low TRLs are understood to be TRLs 1 to 3; these relate to technologies that are not commercially available or not deployed in commercially available products.https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

20. This long list of technologies presented here does not constitute a recommendation that they be used; it is provided solely for informative purposes and to enable discussion of the matter of technology adoption in the counter-diversion domain.

21. Grand-Clément, S. & Kondor, R. (2022), *Exploring the technical feasibility of marking small calibre ammunition*, Geneva: UNIDIR, https://unidir.org/publication/exploring-technical-feasibility-marking-small-ammunition

22. Grand-Clément, S. & Kondor, R. (2022), Exploring the technical feasibility of marking small calibre ammunition, Geneva: UNIDIR, https://unidir.org/publication/exploring-technical-feasibility-marking-small-ammunition

23. The European Observatory on Infringements of Intellectual Property Rights (2021), *Anti-counterfeiting technology guide*, https://euipo.europa.eu/tunnel/web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

24. Grand-Clément, S. & Kondor, R. (2022), Exploring the technical feasibility of marking small calibre ammunition, Geneva: UNIDIR, https://unidir.org/publication/exploring-technical-feasibility-marking-small-ammunition

25. The European Observatory on Infringements of Intellectual Property Rights (2021), *Anti-counterfeiting technology guide*, https://euipo.europa.eu/tunnel/web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf; Paunescu, D., Stark, W.J. & Grass, R.N. (2016), Particles with an identity: Tracking and tracing in commodity products. *Powder Technology*, 291, 344–350, doi:10.1016/j.powtec.2015.12.035; Doroschak, K., Zhang, K., Queen, M., Mandyam, A., Strauss, K., Ceze, L. & Nivala, J. (2020), Rapid and robust assembly and decoding of molecular tags with DNA-based nanopore signatures, *Nature Communications*, 11 (1), doi:10.1038/s41467-020-19151-8

26. Mak, T. (2013), Plant DNA markers help the Pentagon detect counterfeit electronics in the military supply chain, *Washington Examiner*, https://www.washingtonexaminer.com/plant-dna-markers-help-the-pentagon-detect-counterfeit-electronics-in-the-military-supply-chain^

27. The European Observatory on Infringements of Intellectual Property Rights, (2021), *Anti-counterfeiting technology guide*, https://euipo.europa.eu/tunnel/web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

28. The European Observatory on Infringements of Intellectual Property Rights (2021), *Anti-counterfeiting technology guide*. https://euipo.europa.eu/tunnel/web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

29. The European Observatory on Infringements of Intellectual Property Rights (2021), *Anti-counterfeiting technology guide*. https://euipo.europa.eu/tunnel/web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

30. Davies, J. & Wang, Y. (2021), Physically Unclonable Functions (PUFs): A new frontier in supply chain product and asset tracking, *EEE Engineering Management Review*, 49 (2), 116–125, https://ieeexplore.ieee.org/document/9388862

31. Kamal, Y., Muresan, R. (2019). Mixed-signal physically unclonable function with CMOS capacitive cells, *IEEE Access*, 7, 130977–130998.

32. Joshi, S., Mohanty, S. & Kougianos, E. (2017), Everything you wanted to know about PUFs, *IEEE Potentials*, 36 (6), 38–46.

33. Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T. & Khandelwal, V. (2008), Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications, IEEE 2008 IEEE International Conference on RFID (IEEE RFID 2008), Las Vegas, NV, USA, 58–64.

34. World Customs Organization (2018), Container security/tracking devices, Permanent Technical Committee 221st/222nd Sessions, https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/ressources/permanent-technical-committee/221-222/pc0526e1a.pdf?la=en

35. The European Observatory on Infringements of Intellectual Property Rights (2021), *Anti-counterfeiting technology guide*. https://euipo.europa.eu/tunnel/web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

36. Interview respondent 7 (technology company, 13 January 2023).

37. The European Observatory on Infringements of Intellectual Property Rights (2021) *Anti-counterfeiting technology guide*. https://euipo.europa.eu/tunnel/web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

38. See, for example, Trotta, D. (2022), Exclusive: Smart guns finally arriving in U.S., seeking to shake up firearms market, Reuters, https://www.reuters.com/technology/exclusive-smart-guns-finally-arriving-us-seeking-shake-up-firearms-market-2022-01-11/

39. Interview respondent 8 (academia, 25 January 2023).

40. The European Observatory on Infringements of Intellectual Property Rights (2021), *Anti-counterfeiting technology guide*. https://euipo.europa.eu/tunnel/web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

41. Danssaert, P. (2019), *Anti-diversion measures: Real-time locating systems*, Antwerp: International Peace Information Service; Wood, B., Kytomaki, E., Shiotani, H. & Wilkin, S. (2019), *Enhancing the understanding of roles and responsibilities of industry and states to prevent diversion*, Geneva: UNIDIR, https://www.unidir.org/sites/default/files/2019-09/enhancing-the-understanding-of-roles-and-responsibilities-of-industry-and-states-to-prevent-diversion-en-819.pdf

42. The European Observatory on Infringements of Intellectual Property Rights (2021), *Anti-counterfeiting technology guide*. https://euipo.europa.eu/tunnel/web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

43. It should nonetheless be noted that there are a number of technical and logistical challenges linked to RFIDs: first, certain RFID tags may not work as efficiently if used on or around metal components and liquids; second, RFID tags can also increase the visibility of tagged items, which could be exploited by nefarious actors either by undermining the data security of the tags or by revealing the location of weapons during operational use.

44. Aliakbarian, B. (2019), Smart packaging: Challenges and opportunities in the supply chain, *Supply Chain Quarterly (20 February 2019)*, https://www.supplychainquarterly.com/articles/1853-smart-packaging-challenges-and-opportunities-in-the-supply-chain

45. Aliakbarian, B. (2019), Smart packaging: challenges and opportunities in the supply chain, *Supply Chain Quarterly (20 February 2019)*, https://www.supplychainquarterly.com/articles/1853-smart-packaging-challenges-and-opportunities-in-the-supply-chain

46. Aliakbarian, B. (2019), Smart packaging: Challenges and opportunities in the supply chain, *Supply Chain Quarterly (20 February 2019)*.

47. Høyer, M.R., Oluyisola, O.E., Strandhagen, I.O. & Semini, M.G. (2019), Exploring the challenges with applying tracking and tracing technology in the dairy industry, *IFAC-PapersOnLine*, 52 (13), 1727–1732.

48. The terms DLT and blockchain are often used interchangeably; however, blockchain is a subset of DLT, similarly to the way machine learning is a subset of AI.

49. Persi Paoli, G. & Vestergaard, C. (2021), *Exploring Distributed Ledger Technology for arms control and non-proliferation*, Geneva: UNIDIR, https://unidir.org/sites/default/files/2021-09/DLT_in_Arms_Control_and_Non-Proliferation.pdf

50. Persi Paoli, G. & Vestergaard, C. (2021), *Exploring Distributed Ledger Technology for arms control and non-proliferation*, Geneva: UNIDIR, https://unidir.org/sites/default/files/2021-09/DLT_in_Arms_Control_and_Non-Proliferation.pdf

51. Marshall, W., McAllister, C. & Vestergaard, C. (2023), MATCH: Leveraging blockchain for chemical weapons nonproliferation, Washington, D.C.: Stimson Center, https://www.stimson.org/2023/match-leveraging-blockchain-for-chemical-weapons-nonproliferation/

52. Simmonds, N. & Lynch, A. (2023), Mitigating supply chain threats: Building resilience through AI-enabled early warning systems, The Alan Turing Institute, https://cetas.turing.ac.uk/publications/mitigating-supply-chain-threats-building-resilience-through-ai-enabled-early-warning

53. Interview respondent 2 (international NGO, 17 October 2022); interview respondent 6 (international NGO, 28 November 2022).

54. Interview respondent 9 (academia, 1 February 2023); interview respondent 2 (international NGO, 17 October 2022); interview respondent 6 (international NGO, 28 November 2022); and interview respondent 10 (research organisation, 7 March 2023).

55. Interview respondent 3 (international organisation, 9 November 2022); interview respondent 1 (international organisation, 11 October 2022).

56. Interview respondent 6 (international NGO, 28 November 2022).

57. Interview respondent 6 (international NGO, 28 November 2022; interview respondents 4 & 5 (research organisation, 25 November 2022).

58. Interview respondent 6 (international NGO, 28 November 2022).

59. Interview respondent 2 (international NGO, 17 October 2022).

60. Interview respondent 6 (international NGO, 28 November 2022).

61. Interview respondent 3 (international organisation, 9 November 2022); Interview respondent 1 (international organisation, 11 October 2022).

62. Milana, C. & Ashta, A. (2021), Artificial intelligence techniques in finance and financial markets: A survey of the literature, *Strategic Change*, 30 (3), 189–209.

63. Canhoto, A. I. (2020). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. Journal of Business Research, 131, 441-452.

64. Planet Labs PBC (2023), Planet.com.: Planet's Data Leveraged To Identify Dark Vessels And Monitor The Illicit Russian Oil Trade. https://www.planet.com/pulse/planets-data-leveraged-to-identify-dark-vessels-and-monitor-the-illicit-russian-oil-trade/

65. See Byrne, J., Somerville, G., Byrne, J., Watling, J., Reynolds, N. & Baker, J. (2022), Silicon lifeline. Western electronics at the heart of Russia's war machine. London: RUSI, in which the Altana Atlas (https://altana.ai/atlas) was used.

66. Nelson, C. (2020), Machine learning for detection of trade in strategic goods: An approach to support future customs enforcement and outreach, World Customs Journal, 14 (2), 119–130, https://worldcustomsjournal.org/Archives/Volume%2014%2C%20Number%202%20(Oct%202020)/1902%2001%20WCJ%20v14n2%20Nelson.pdf?_t=1603239884

67. Aarvik, P. (2019), Artificial intelligence – a promising anti-corruption tool in development settings? *U4 Report*, 1, 15, https://beta.u4.no/publications/artificial-intelligence-a-promising-anti-corruption-tool-in-development-settings.pdf

68. Wood, B. (2020), *The Arms Trade Treaty: Obligations to prevent the diversion of conventional arms*, Geneva: UNIDIR, https://unidir.org/publication/arms-trade-treaty-obligations-prevent-diversion-conventional-arms

69. Griffiths, H. & Wilkinson, A. (2007), *Guns, planes and ships: Identification and disruption of clandestine arms transfers, Sarajevo*: SEESAC, https://issuu.com/undphr/docs/guns__planes___ships_-_identificati

70. See Conflict Armament Research (2021), *Field forensic firearm exploitation; developing RFID solutions in support of stockpile management and post-diversion tracing*, https://www.conflictarm.com/technical/developing-rfid-solutions-in-support-of-stockpile-management-and-postdiversion-tracing/; interview respondent 10 (research organisation, 7 March 2023).

## Flemish Peace Institute

The Flemish Peace Institute was established in 2004 as a para-parliamentary institution within the Flemish Parliament. It provides thorough analyses, informs and organizes the public debate and promotes peace and the prevention of violence.

## Author

**Diederik Cops** has been working as a senior researcher at the Flemish Peace Institute since January 2016. Within the research domain "weapons-peace-violence", he focuses mainly on the aspect of export control.

Email: diederik.cops@vlaamsparlement.be

## UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

## Author

**Sarah Grand-Clément** is a Researcher in the Conventional Arms and Ammunition Programme and the Security and Technology Programme at UNIDIR. Her work focuses on the intersection of technology with conventional arms, exploring both the benefits that technology can bring to prevent violent conflict and enable peace, as well as the challenges and threats technology can pose to international security.

Email: sarah.grandclement@un.org

## Project D-TECT

Countering the **D**iversion of arms using **TEC**hnology **T**ools (D-TECT) is a joint project by the Flemish Peace Institute (FPI) and the United Nations Institute for Disarmament Research (UNIDIR). The aim of Project D-TECT is to develop and test an approach to identifying and assessing the utility and feasibility of using specific technologies that could be used to support or strengthen existing initiatives aimed at detecting, preventing, and mitigating the diversion of conventional weapons. Project D-TECT consists of two consecutive phases. First, to identify existing technologies that could be suited to countering the diversion of conventional weapon systems and develop a framework that makes it possible to identify and assess technologies used to counter diversion. Second, to assess, refine, and validate the list of identified technologies in relation to specific types of conventional weapon systems. This current paper is a product of the first phase of the research, which focused on the relevance of existing technologies to help counter the diversion of small arms and light weapons (SALW) and components of conventional weapons.

D-TECT

flemish
peaceinstitute

Leuvenseweg 86, 1000 Brussels \ tel. +32 2 552 45 91 \ vredesinstituut@vlaamsparlement.be \ www.flemishpeaceinstitute.eu