PROJECT D-TECT

Countering the diversion of the components of conventional weapons. An assessment of potential technological solutions

Diederik Cops (Flemish Peace Institute)

EXECUTIVE SUMMARY

Although the diversion of conventional weapons components (CWC) has been assigned much less importance compared to other conventional weapons (including SALW), the pivotal role of components in modern warfare and their diversion to unauthorised end-use(r)s is increasingly being acknowledged. The specific nature of (the trade in) such components however makes it challenging to implement effective action to counter their diversion.

Based on a series of stakeholder engagements, this paper examines the possible relevance of 14 technologies to supporting efforts to counter the diversion of CWC: 2D codes, chemical encoding, DNA coding, document authentication, electronic seals, GNSS and mobile tracking, near-field communication, radio-frequency identification, sensors, the Internet of Things, distributed ledger technology, big data analysis, natural language processing and computer vision. All the technologies were assessed as being potentially appropriate in helping to counter the diversion of CWC, even though their impact could differ depending on the life-cycle stage (pre-export, transfer or post-delivery) and the counter-diversion element (prevention, detection or identification). Important barriers to implementing these technologies were equally identified, some of which may not even be feasible in this specific context.

Several avenues for stimulating discussions on the use of technologies to support counter-diversion efforts aimed at CWC were identified: (1) dedicated analyses focusing on specific components, prioritising those components being most critical to the functioning of conventional weapons; (2) initiatives to strengthen cooperation between the authorities and companies involved in the production, sales and transport of components; and (3) implementing pilot projects involving public and private stakeholders as a way of overcoming the lack of familiarity with the technologies and the reality of the diversion of CWC.

August 2024

Acknowledgments

The author wishes to thank the experts who participated in the interviews, surveys and workshops and who provided invaluable inputs during the course of the research. The author is also grateful to the experts who reviewed this paper and provided feedback, including Paul Holtom, Nils Duquet, Maarten Van Alstein, Sarah Grand-Clement, Henry Leach and Keith Krause.

Glossary

- **Components of conventional weapons (CWC)**: A component can be defined as 'one of several or many units of which something is composed'. In the case of conventional weapons, this refers to the different elements and items that are used to develop and build a conventional weapon, irrespective of their export-controlled status. These items could be large or major components such as engines, aeroplane fuselages or turrets, but they could also be smaller items such as the electronic systems or subcomponents used to construct the major components.

- **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. Such diversion can take various forms: (1) An incident of diversion can occur when the items enter an illicit market or when they are 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 in 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]

- **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 specialised aspects of a particular field of endeavour.'[2] In the context of this paper, 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 that fall within the scope of this paper are those which have recently been developed and are emerging in the context of diversion prevention – although this report does not examine technologies that are currently at the lowest levels of technology readiness.

List of abbreviations

2D	Two-dimensional
AI	Artificial intelligence
ATT	Arms Trade Treaty
CWC	Components of conventional weapons
DIEF	Diversion Information Exchange Forum
DLT	Distributed ledger technology
D-TECT	Countering the Diversion of arms using TEChnology Tools
GNSS	Global navigation satellite system
IED	Improvised Explosive Device
IoT	Internet of Things
NFC	Near-field communication
NLP	Natural language processing
PoA	United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects
RFID	Radio-frequency identification
SALW	Small Arms and Light Weapons
UAV	Unmanned Aerial Vehicle
UN	United Nations
UNOTC	United Nations Office of Counter-Terrorism
WMD	Weapons of mass destruction

Section 1: Applying technology to counter the diversion of components of conventional weapons

The diversion of conventional weapons and related ammunition, parts and components to unauthorised end-users and end-uses poses a significant threat to societies across the globe. As a consequence, initiatives have been developed at the national and international levels to counter the diversion of conventional weapons towards an unauthorised end-user or for unauthorised end-use. Countering diversion is essentially at the heart of many national export-control systems. It is also a key objective of several international regimes that have been set up to regulate the trade in (specific types of) conventional weapons. These include the United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (PoA) or the Arms Trade Treaty (ATT).[3]

Whereas the diversion of complete conventional weapons systems and its prevention has therefore been driving many national and international initiatives, the diversion of components used in conventional weapons systems has received much less attention. The few cases that focus on the diversion of components towards unauthorised military purposes do so in the context of so-called dual-use items – civilian goods that can also be used for military purposes – and their diversion towards weapons of mass destruction (WMD) and much less so on their potential role in conventional weapons. This is illustrated by Security Council Resolution 1540, which obliges all States to install effective measures to prevent the proliferation of nuclear, chemical and biological weapons and their means of delivery, and to establish appropriate domestic controls over related materials to prevent their being trafficked illicitly.[4] It is, however, becoming increasingly

clear that in modern warfare and armed conflicts advanced components – often civilian–commercial in nature – are playing an important role in several types of conventional weapons: guided rockets, (cruise) missiles, Unmanned Aerial Vehicles (UAVs), Improvised Explosive Devices (IEDs), battle tanks, electronic warfare, etc.[5] Countering the diversion of such components towards unauthorised end-uses and end-users is therefore increasingly being considered as crucial in limiting the illicit proliferation and production of a wide range of conventional weapons. Recent analyses of such advanced components recovered in conflict zones across the world indicate the challenges being encountered in both monitoring and controlling the international trade in such components and in tracing their chain of custody effectively to identify the specific points of diversion. The wide variety of private actors involved in the international transfer chains of these components and the fact that the components are often not export controlled are important reasons for this (see further in this report).

Often, a combination of systemic and practical measures is required to reduce the risk of diversion of conventional weapons and their components effectively.[6] Along with non-technological approaches, such as information sharing, technology can form one of the different approaches and solutions to the issue of diversion. Technologies can, moreover, also strengthen or facilitate some of the non-technological measures that States use to counter diversion (e.g., using the correct documentation, conducting objective risk assessments).[7] However, despite a growing acknowledgment of and increased attention being focused on the potential added value of technologies to support counter-diversion efforts, the general uptake or implementation of technologies in national or international practices aimed at arms transfer control remains very difficult.

This particular observation was the rationale behind project D-TECT – **Countering the Diversion of Arms using TEChnology Tools**. The overarching aim of this project was 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 of conventional weapons and their components.[8] Whereas the project's first phase developed a general framework[a] for identifying and assessing existing technologies that could be suited to countering the diversion of conventional weapons, the second phase focused specifically on the application of technology to counter the diversion of Small Arms and Light Weapons (SALW) and components of conventional weapons (CWC) respectively.[b] This paper presents initial insights into the relevance and applicability of selected technologies to strengthen efforts to **counter the diversion of CWC**. This analysis draws heavily on the findings from a set of surveys and subsequent workshops involving various stakeholders that were conducted to assess the relevance of the identified technologies, the barriers to their effective implementation and possible avenues to overcoming these obstacles. The 14 technologies (presented and discussed in section 3) that were identified in the project's first phase are at the centre of the technological assessment presented in this paper. A detailed description of the methodology used in this second phase can be found in annex 1.

a This framework comprises three steps. The first step focuses on understanding the risks of diversion, which are tailored to each specific type of conventional weapon, its life cycle and the context it operates in. The second step examines the existing technologies which could help to prevent or overcome the identified risk(s). The third step assesses the identified technologies according to the context(s) in which they would be applied and also against the selected attributes that the technologies should possess. See Grand-Clément, S. & Cops, D. (2023) *Technologies to counter the diversion of small arms and light weapons, and components of conventional weapons*, Brussels: Flemish Peace Institute, https://vlaamsvredesinstituut.eu/wp-content/uploads/2023/08/20230828-FPI_UNIDIR-Paper-Technologies_DIGI-DEF.pdf

b The findings from the application of this framework on SALW can be consulted here: Grand-Clément, S. (2024), *Assessing technologies to counter the diversion of small arms and light weapons*, UNIDIR & Flemish Peace Institute, https://vlaamsvredesinstituut.eu/wp-content/uploads/2024/06/20240626-DTECT2-Online.pdf

Purpose and scope of this paper

The present paper aims to provide an overview of the results of project D-TECT's second phase, in which an in-depth assessment was conducted of the appropriateness of and the barriers to implementation of the identified technologies to counter the diversion of conventional weapons components. In addition, this paper aims to identify possible ways forward to facilitate the implementation of technologies to support counter-diversion efforts. It, together with the previous paper on SALW, is intended as a **proof-of-concept** for the technology-assessment approach and its utility in facilitating reflection on the appropriate technologies in the context of the counter-diversion of conventional weapons and their components. The intention of these findings is, first, to provide insights for national governments, the private sector, civil society, international organisations and all other stakeholders involved across the life cycle of conventional weapons. Second, these findings can provide elements for reflection and consideration whether and how technology could be considered in countering the diversion of conventional weapons. The conclusions reached could be particularly relevant to the different international regimes that have been set up to enhance efforts to prevent, detect and eradicate the diversion of conventional weapons such as the ATT.

Report structure

Section 2 discusses the problem of the diversion of CWC in more detail, focusing on the increased awareness of the necessity to deal effectively with such diversion. Moreover, this section describes the main methods and risks of the diversion of components. **Section 3** provides the overall assessment of the technologies, based on the survey inputs and workshop discussions. This section starts with a concise discussion of the main methods used to divert CWC to unauthorised end-users and end-uses throughout their life cycle. Next, the assessed impact of and barriers to implementation for each of the technologies is described, building on the workshop participants' responses to the surveys. Finally, the section analyses the trade-offs between impact and barriers for each of the different technologies in relation to the identified methods of diversion for CWC. **Section 4** then goes on to discuss possible ways forward and concrete actions identified during the project that could be relevant to mitigating or overcoming these barriers. **Section 5** concludes the report with some reflections on the key findings of this project and on possible next steps in implementing the different technologies to aid in the counter-diversion of CWC.

Section 2: Diversion of components of conventional weapons

The risks and methods of diversion differ according to the type of item, the context and location, and the stage of the supply chain or life cycle. Whereas these aspects are well known regarding other conventional weapons such as SALW, little attention has been paid to and there is only limited knowledge about the issue of diverting the components used in conventional weapons. Therefore, prior to showcasing the ways in which technologies were assessed, this section first expands on the diversion issues facing CWC and the risks and methods of diversion most commonly used to divert components from their intended end-users and end-uses.

Compared to other conventional weapons, including SALW,[9] **attention on and knowledge about the diversion of components of conventional weapons is relatively recent**. An important reason for this relative lack of priority is that parts and components are seen as less sensitive goods

compared to finalised conventional weapons systems. Moreover, some of the components used for the production of conventional weapons are completely civilian in nature and they have therefore drawn very little attention or diligence as to the end-user or potential end-uses. Because many of these components often remain below the thresholds used in existing multilateral and national export control lists, it is very difficult for state authorities to monitor and control the international trade effectively in these items. It is, however, becoming clear that the (illicit) trade in components, including in those available for civilian-commercial use, poses significant challenges. The increasingly globalised and scattered supply chain, involving a wide range of private actors such as wholesalers, import-export companies, distributors and brokers, creates risks of diversion of specific components in locations and transit hubs.[10] This reality results in a greater risk of unauthorised end-use of these components. This is so because these prolonged and internationalised supply chains make it difficult for state authorities and the companies involved in the production and sales of such components to know who the effective end-user will be. In addition, the re-export or retransfer of these components themselves, or after they are integrated into a finalised conventional weapon, renders it difficult to have an ongoing understanding of where these components are effectively ending up and for what purposes they are being used. Illicit networks could procure components at different locations, only to be assembled in a later phase and serve essential functions in a broad variety of conventional weapons. Moreover, they could be used to repair, upgrade or modify existing conventional weapons using technologically more sophisticated components.

Access to and the illicit acquisition of components by both embargoed states and non-state armed groups is increasingly being acknowledged as taking place globally, posing a threat to regional and international peace and security. The increasing availability of the advanced commercial capabilities of such components also raises the likelihood of misuse and the diversion to unauthorised end-users and end-uses.[11] As a consequence, international attention has been intensifying to control and regulate the trade in conventional weapons components. This is, for example, the case in several multilateral sanctions regimes that have been imposed on specific states or non-state actors, or in the context of UN Security Council Resolutions such as Resolution 2370 (2017) that deal with the challenges in preventing non-state armed groups from gaining access to weapons.[12] This attention is strongly driven by findings and conclusions about how components – military, dual-use and civilian-commercial – are found to be playing a pivotal role in the development and production of a wide variety of conventional weapons.[13] The 2022 UN panel of experts report on Libya, for example, states:

> *The ever-evolving technology and relatively low cost of smart electronic fast moving consumer goods, such as optics and unmanned aerial vehicles, and the ease of modification of civilian vehicles to convert them into combat-capable vehicles make such dual-use items ideal for military use in low-level conflicts.*[14]

In a similar way, several countries subjected to international sanction regimes, such as Russia, Iran and North-Korea, have been able to (illicitly) procure a broad variety of foreign-made components, which has enabled them to produce and deploy different types of conventional weapons in current war zones and armed conflicts. The growing number of studies, reports and analyses on the diversion of these types of component have helped to create a better understanding of the main risks and methods of diversion of such items.[15]

The **use of front or shell companies as part of elaborated illicit procurement networks** set up by state or non-state actors, is found to be an important method of diversion of such components used in conventional weapons.[16] This is relevant

throughout all the life-cycle phases and stands out as one of the main ways in which components are being diverted. Such complex acquisition networks are in the first instance set up by states, often to circumvent the international sanctions regimes which they are subjected to. Analyses of conventional weapons used by Russian armed forces in Ukraine clearly indicate how weapons manufactured by Russia, Iran and North Korea almost exclusively consist of components (both export-controlled and non-controlled) which are procured via such illicit procurement networks.[17] In a similar manner, non-state armed groups develop complex illicit networks to acquire components so as to produce conventional military goods such as Improvised Explosive Devices (IEDs) or sound suppressors – as was illustrated by the recent analysis of equipment seized from ISIS in north-east Syria.[18] This method often takes place in conjunction with the use of **transshipment** through different countries **and complex transfer routes** to obscure the real end-user of the goods; alternatively, it occurs by means of changes in the destination during the transfer of items. This method of diversion is particularly relevant in the case of components because their supply chains and life cycles are often more prolonged and complex than those of complete weapon systems. In addition, their supply chains and life cycles consist of a greater number of actors, several of which are civil actors such as private wholesalers, import–export companies, shipping companies, freight forwarders and customs brokers. Identifying such transshipment patterns is often highly challenging as it requires a multi-tier visibility of the goods moving through different countries.[19]

Next, components used in conventional weapons are also found to being diverted using more **generalised or false descriptions of the items in official trade documentation**, with a deliberate view to evading export and Customs controls. Such trade documentation needs to be submitted to Customs/border control agencies for all import, transit or export transactions goods are subjected to during their transport from their point of departure to their (intended) destination. Describing these items wrongly or in a more generalised manner is done to conceal their sensitive or strategic nature with a view to circumvent the risk analysis systems Customs agencies make use of to identify transactions most at risk in the huge amount of trade flows that take place on a daily basis. In a related manner, **falsified documents, such as End-Use Certificates (EUCs)** are equally been identified as a way illicit proliferators divert components from their intended end-use or end-user. This method of diversion is somewhat less relevant in this particular context however, as many of the components found in conventional weapons fall under the threshold for export controls and are thus not subjected to such formal controls.

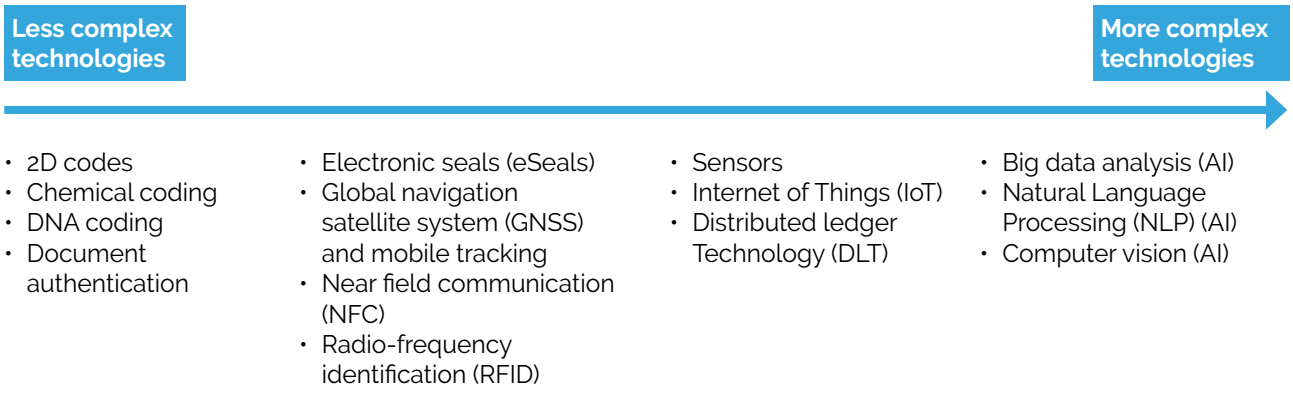
A final method of diverting components, particularly in the post-delivery phase, is making **unauthorised changes to the end-use of the goods after delivery**.[20] This is often due to the multi-purpose use of these components which enables end-users to use the components for other purposes than those originally communicated to the exporter. This diversion method has been clearly illustrated in the findings of, for instance, Conflict Armament Research on the diversion of electromagnetic brakes which were exported by a European company with the intention of their being integrated into medical vehicles – but which were eventually diverted for use in air-to-surface missiles deployed in northeast Syria instead.[21]

Section 3: Relevance of technologies to counter-diversion of components

As mentioned previously, the goal of project D-TECT's second phase was to conduct an in-depth assessment of the relevance of the selected technologies in strengthening counter-diversion efforts, with a specific focus on CWC. This assessment was conducted first through surveys, which collected primarily quantitative data, and then via a series of workshops. All the workshop participants were invited to complete the online surveys ahead of the workshops. The surveys consisted of two parts, with questions tapping, first, into the technologies' **perceived positive impact** on counter-diversion efforts and, second, into the **potential barriers** to the successful implementation of these technologies. During the online workshops, the participants could elaborate on their reasoning behind their responses, add further insights into the application of technology to counter-diversion efforts for the respective items and to reflect on possible ways to overcome the identified barriers to implementation.

Figure 1 provides a short overview of the 14 technologies that were identified as possibly being appropriate to supporting counter-diversion efforts during the first phase of project D-TECT.[a] The identification of these technologies was guided by considerations of their potential appropriateness and ability to counter diversion and by the fact that these technologies already have some level of maturity. Specifically, these technologies were selected because (1) there are some limited cases in which they have been used to counter the diversion of weapons or (2) they have been used in the civilian–commercial realm to prevent the counterfeiting of goods, to identify illicit or fraudulent transactions or to increase the integrity and security of international supply chains. Other industrial sectors such as chemicals, extraction, pharmaceuticals or financials have had experience with effectively implementing technologies for such purposes. In addition, table 1 lists the potential purposes these technologies could serve. A more elaborate description of the different technologies can be found in annex 2.

Figure 1. Overview of the technologies identified in phase 1 of project D-TECT



a Some minor changes were made to the technologies assessed as part of the research for this second phase compared to the long list in the food-for-thought paper. Specifically, physically unclonable functions (PUFs) were not included here because of their immaturity, while the broad category of 'AI' was disaggregated into three specific types of technology to increase its granularity. The food-for-thought paper provides a detailed description of each of these technologies in addition to their current areas of application and where they could be applied to SALW or CWC, and for what purposes. See Grand-Clément, S. & Cops, D. (2023, pp. 9–17), https://vlaamsvredesinstituut.eu/wp-content/uploads/2024/06/20240626-DTECT2-Online.pdf.

Table 1: Longlist of technologies and their purposes

Technology	Potential purpose(s)								
	Accountability	Tracking and tracing	Item-level identification	Inventory and storage	Anti-tampering	Identification and certification	(End-use) monitoring	Data capture/ recording	Data analysis
2D codes	✔	✔	✔	✔					
Chemical encoding	✔	✔	✔	✔					
DNA coding	✔	✔	✔	✔					
Document authentication						✔			
Electronic seals (e-seals)					✔				
GNSS and mobile tracking		✔							
Near-field communication (NFC)	✔	✔	✔			✔			
Radio-frequency identification (RFID)	✔	✔	✔	✔		✔			
Sensors‡						✔	✔	✔	
Internet of Things (IoT)							✔	✔	
Distributed Ledger Technology (DLT)		✔			✔			✔	
Big data analysis†									✔
Natural Language Processing (NLP)†									✔
Computer vision†									✔

‡ *The wide existing range of sensors includes, e.g., cameras, radars, thermal imaging, x-ray scanners, gas indicators, acoustic sensors, time-temperature indicators, RFID, etc.*

† *These are subsets of artificial intelligence (AI).*

Findings from project D-TECT's first phase demonstrate that a **needs-driven and context-sensitive approach** to applying technology to counter-diversion purposes is crucial. In other words, the selection of technology should not be driven by its mere availability, but should in contrast be assessed in relation to the specific diversion risks and methods of the items under study – in this case, CWC. Conscious of the fact that diversion risks and methods will differ depending on the life-cycle stage, each workshop and its associated survey focused on three different phases of the life cycle:

1. **Pre-export stage**, or the stage when items are post-manufacture and within the licensing phase but are not yet ready for export. Front and shell companies are used to hide the effective end-user and end-use of the items from the manufacturers or the exporting state authorities, as are generalised descriptions of the goods to hide their strategic nature to licensing. At this stage, Customs and border-control agencies are important conduits for the diversion of components.

2. **Transfer stage**, or the stage during which the items are being transported via various means (e.g., by land, air or sea) to take them from the country of origin to their country of destination (possibly via different transit countries) and their subsequent importation into a recipient country. The methods used to divert components during this phase are fake documentation, deliberate misdescription of the goods in more neutral or generalised terms or rerouting the goods at transit hubs.

3. **Post-delivery stage**, or the stage starting from the time the intended recipient has received the items until the effective use of the items (after integration into a higher-order conventional weapon) and their eventual destruction. The risks of diversion in this stage include the unauthorised transfer or exportation of the items to another end-user (via front or shell companies acting as the intended recipient), the unauthorised use of the items by the intended recipient or the unauthorised retransfer or re-export of the goods.

Building on the participants' inputs collected in the surveys, this section continues by discussing (1) the possible positive impact the selected technologies could have on countering the diversion of components of conventional weapons, (2) the possible barriers these technologies might be faced with to their implementation, and (3) the trade-offs between positive impact and barriers to the different technologies.

Possible impact of the selected technologies

Overall, all 14 technologies were identified by the workshop participants as being potentially appropriate to helping the counter-diversion of CWC. None of these technologies was identified as having a negative impact on counter-diversion efforts.

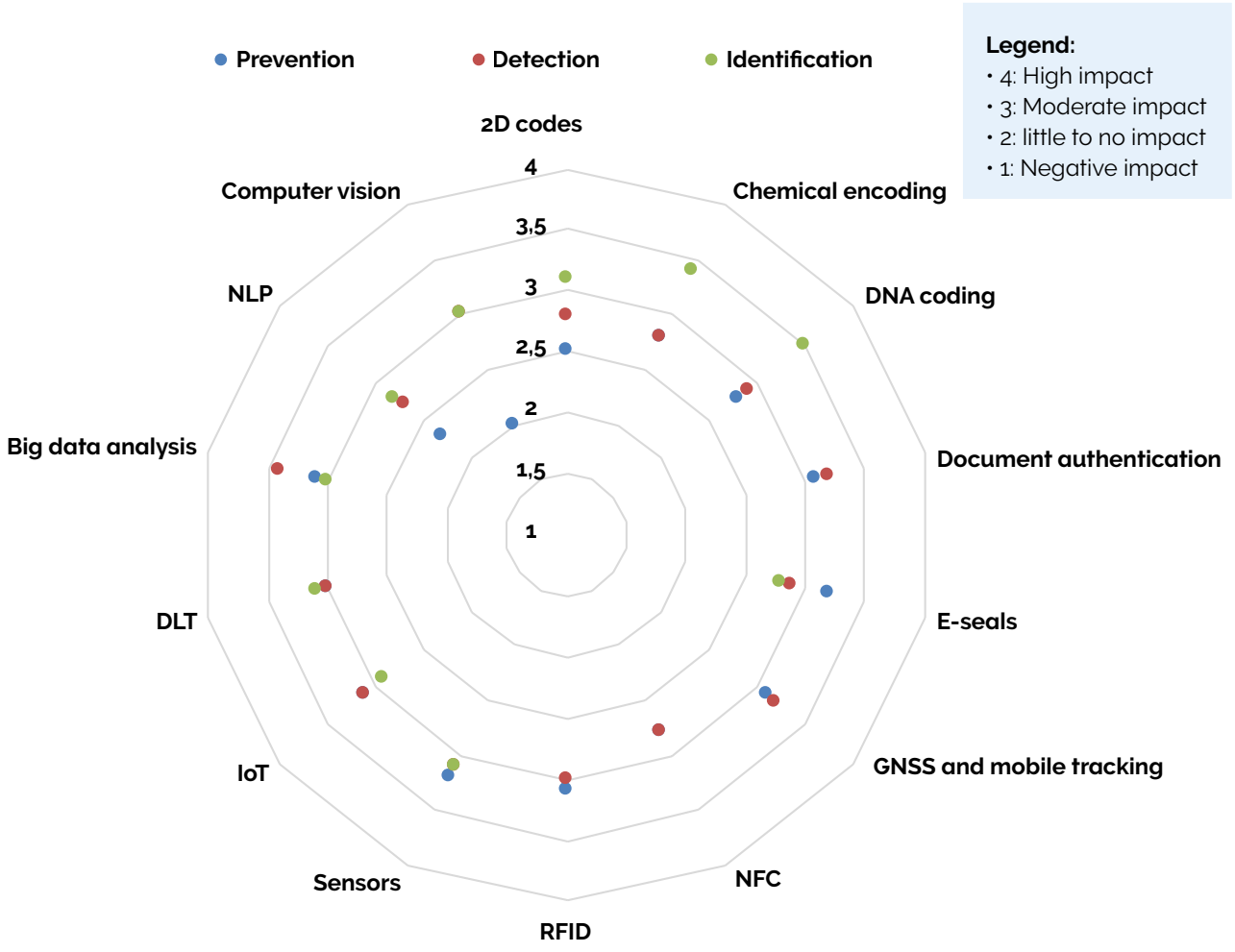
More specifically, **the types of technology identified as most appropriate and potentially impactful in countering diversion tended to differ depending on the life-cycle stage**. In the **pre-export stage**, document authentication, the Internet of Things (IoT), Distributed Ledger Technology (DLT) and big data analysis were assessed as possibly having the greatest impact on countering the diversion of CWC. At the **transfer stage**, the highest-rated technologies were document authentication, e-seals, GNSS and mobile tracking, RFID and big data analysis. These scores reflect transfer-specific considerations, namely, the ability to identify items and false documentation and the ability to prevent the rerouting or theft of items. At the **post-delivery stage**, however, the AI-driven tech-

nologies, document authentication and RFID scored comparatively lower than in the previous life-cycle stages. In contrast, the different marking technologies – 2D codes, chemical encoding and DNA coding – were assessed as being the most promising, especially with a view to strengthening the identification of diversions of CWC. In particular, chemical encoding and DNA coding are considered to be technologies that could have a substantial impact on counter-diversion efforts. Sensors and the IoT were equally assessed as being impactful in the post-delivery stage, specifically for prevention and detection purposes.

In general, the possible impact of the identified technologies appears to differ somewhat between the three life-cycle stages. At the same time, however, a certain level of overlap exists in the extent to which certain technologies are assessed to be appropriate to counter-diversion. This overlap reflects the fact that some technologies have multiple areas of relevance and purposes, as is shown in table 1.

Importantly, the assessed relevance of technology also differed when examining the applicability of each technology to aiding a specific counter-diversion subcomponent (prevention, detection or identification). These differences are illustrated in Figure 2, which shows the differentiation in impact between the different counter-diversion elements. The three marking technologies, for example, are assessed as being particularly appropriate to strengthening the identification of instances of the diversion of components, while being less appropriate to preventing and detecting diversion.

Figure 2. Assessed positive impact of technologies on counter-diversion of CWC (all stages combined)



Document authentication, GNSS and mobile tracking, sensors and RFID, in contrast, would be more appropriate to preventing and detecting, less so for identifying instances of diversion. Interestingly and in a related manner, big data analysis is assessed as being particularly appropriate to preventing the diversion of CWC; the possible impact of the other AI technologies, on the other hand, would be less pronounced and would be more appropriate to the detection of diversion. These findings demonstrate the need to consider carefully the intended purpose when selecting a technology to ensure that it would be effective.

Barriers to technological adoption

In addition to examining (potential) impact of a technology, understanding the barriers to adoption that each technology may face is crucial. To do so, the survey respondents were asked to assess the extent to which each of the requirements outlined in the next box would pose a barrier to the successful implementation of technology for counter-diversion.[a] More specifically, five categories of requirements were to be assessed for each of the technologies regarding their implementation to counter the diversion of CWC, with a specific focus on electronical and drone components.

Overall, the technologies were found to be facing on average **significant barriers** to implementation in all the requirements and the life-cycle stages. However, nuances should be noted: **infrastructural, cost and skills requirements were perceived to be posing the greatest barriers to the successful implementation of the technologies to counter the diversion of CWC**. In contrast, the ethical and social requirements were perceived as posing the smallest barriers. This was the case consistently across all three life-cycle stages and for all the technologies analysed.

Different technologies were also found to face larger or smaller barriers, the results varying slightly depending on the stage of counter-diversion. For each life-cycle stage, table 2 shows the three technologies found to be facing the least versus the most barriers to implementation.

Potential barriers to the successful implementation of counter-diversion technology

- **Skills requirements**: Knowledge of the technology (how to implement it and to use it) and the training accessible and available to gain these skills, in addition to having reliable and trustworthy personnel.
- **Infrastructural requirements**: The availability of both the physical and the virtual infrastructure needed to enable the technology to function, such as secure location, electricity and (security of) connectivity.
- **Cost requirement**: Financial costs related to the development, acquisition and maintenance of the technology and its related enabling infrastructure and personnel needed for the technology to function.
- **Regulatory requirements**: The need to have new or updated regulations or legislation in place to enable the use and implementation of the technology.
- **Ethical and social requirements**: Societal trust and acceptance of the technology to deliver as intended and ensure security of information, and trust between the partners and those involved in using the technology.

a The respondents could indicate whether each requirement would pose (1) 'not a barrier' (i.e., would have no effect on the successful implementation), (2) a 'small barrier' (i.e., can be dealt with relatively easy), (3) a 'significant barrier' (i.e., would be difficult or challenging to overcome) or (4) an 'insurmountable barrier' (i.e., would require action that might not be possible or practicable).

Table 2. Technologies assessed as facing the highest versus the lowest barriers to implementation by life-cycle stage to counter the diversion of CWC

Pre-export stage	
Highest barriers to implementation	**Lowest barriers to implementation**
GNSS and mobile tracking	2D codes
E-seals	Document authentication
DLT	Chemical encoding
Transfer stage	
Highest barriers to implementation	**Lowest barriers to implementation**
DNA coding	Document authentication
Chemical encoding	2D codes
DLT	RFID
Post-delivery stage	
Highest barriers to implementation	**Lowest barriers to implementation**
Natural language processing	Document authentication
Computer vision	IoT
DNA coding	2D codes

Interestingly, two technologies were assessed as having the lowest barriers to implementation in all three life-cycle phases: 2D codes and document authentication. In contrast, DNA coding and DLT were assessed as having particularly high barriers to implementation in the different life-cycle phases.

Yet **low barriers to implementation paint only a partial picture of the potential of a technology**. It is also necessary to consider the suitability of technology to deal with the issue at hand combined with its ability to overcome barriers to implementation. Moreover, even when high barriers might be in place, the potential high impact a technology could have may also be an incentive to take action to deal with the barriers that were identified. Importantly, combining the potential impact and the perceived barriers to implementation is a necessary step to arrive at a more balanced and realistic assessment of the feasibility of implementing potentially high-impact technologies. The survey data and the workshop discussions have led to such a more balanced assessment being possible.

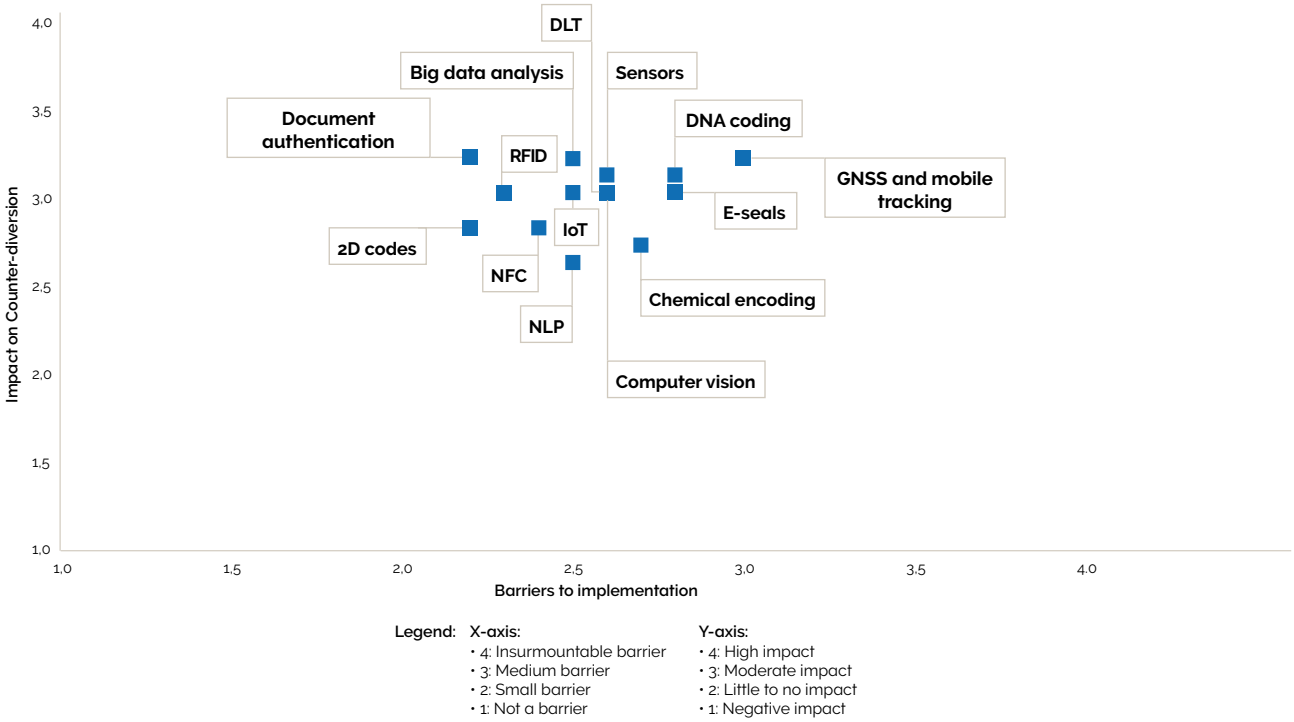
Assessing impact of versus barriers to technology

Examining the trade-off between positive impact and the potential barriers to implementation helps to place the technologies in context. Moreover, it creates a more nuanced understanding of both the appropriateness and feasibility of implementing certain technologies. In this way, such an examination helps to guide the decision-making process by giving decision-makers a better insight into the cost–benefit analysis relating to the implementation of the different technologies. Figure 3 provides the overall results, merging data across the three stages and diversion elements of counter-diversion. This figure shows that whereas

most of the technologies identified in this study could have a moderate to high impact on countering the diversion efforts involving components, their implementation would be accompanied by medium to significant barriers in equal measure.

This becomes apparent with regard to the three different marking technologies included in the analysis: **2D codes, chemical encoding** and **DNA codes**. It has become clear that the enhanced identification of components to allow for better traceability is a crucial step towards understanding the way components have been diverted to unauthorised end-users or end-uses. This could be particularly appropriate to counter-diversion purposes because identifying the chain of custody and the specific point of diversion of components is currently proving to be difficult. This is a consequence of their small size and substantial production numbers, and the lack of unique markings on individual components. These marking technologies could therefore have a significant impact in enhancing the way in which components[22] being diverted are identified. **2D codes** in particular appear to be an appropriate technology to consider, especially as a secondary mark on larger components. Although they have been assessed as having a slightly lower impact compared to chemical and DNA coding – because of their greater visibility (see next box) and the possibility of erasing them – the barriers to implementing 2D codes have also been assessed as being lower. In the case of the chemical and DNA coding marking technologies, more advanced readers of the marks would be

Figure 3. Potential positive Impact versus barriers to successful implementation: mapping technologies with respect to the counter-diversion efforts involving CWC[a]



a This figure shows data aggregated across all three phases of counter-diversion. Y-axis: 4 = Significant improvement to aiding counter-diversion in comparison to current capability or practices, while 1 = A reduction in capability or negative impact on counter-diversion in comparison to current practices; x-axis: 4 = The barriers posed by the requirements would necessitate action that might not be possible or practicable, while 1 = The requirement does not pose a barrier to the successful implementation of the technology (n=28).

needed. Chemical encoding in particular would require important back-end capabilities such as laboratories to process the collected samples.

Deep dive: Reflection from workshop participants on the impact of 'visible' versus 'invisible' technologies.

The visibility of technology – or the absence of it – in relation to its counter-diversion effectiveness was an important element of reflection. On the one hand, the visibility of technology as a physical presence was discussed. The ability of visible versus invisible technology to have a positive impact on counter-diversion appears to depend on the type of technology and the intended counter-diversion purpose (i.e., prevention, detection or identification). For example, 2D codes were noted as being visible and therefore illicit actors would be aware that they could remove the marks. On the other hand, non-visible secondary marks such as chemical encoding or DNA coding may be more resilient due to their invisibility. In other words, more covert markings could be beneficial in preventing counter-action by illicit actors.

Visibility was also discussed in respect of the wider knowledge individuals and corporates possess that technology is being used and not just about what is visible by the naked eye. In the light of this, a deterrent effect could be to inform potential offenders that technology has been applied to components to protect them against diversion and also of the risks of their being identified as illicit actors and the consequences arising from diversion.

Similarly to the marking technologies, Figure 3 indicates that **document authentication** emerged as a promising avenue for preventing or detecting the diversion of specific component types, especially during the pre-export and transfer stages. Moreover, the barriers to successful implementation were also assessed as being relatively low, especially compared to those of many other technologies. This technology is one of the very few that licensing authorities have used effectively, as was mentioned by one of the participants in the workshops – which could be a reason for this favourable assessment. This technology could be particularly appropriate to preventing the use of fraudulent documents to circumvent export controls by concealing the effective country of end-use or the end-user of the items. In the case of CWC, an important limitation with regard to the appropriateness of document authentication technology is that many of the relevant components do not fall within the scope of formal export controls and therefore during transfer they do not require official documents for export-control purposes – such as End-Use Certificates (EUCs). In those cases where such export-control obligations are in place, document authentication technologies can be a relatively feasible option to strengthen the prevention of CWC diversion. In addition, formal documents in general are an indispensable part of the goods transfer process, irrespective of their controlled nature: customs documentation and shipping documents have to be submitted for all transfers of items, irrespective of their controlled status. Here, document authentication technologies for transfers of CWC could equally be appropriate to the different types of actor involved in the international transfer chain.

The analysis of global Customs data and of individual shipment data can play an important role in identifying the sources and intermediaries responsible for the diversion of components – for example, for use in IEDs.[23] However, the staggering number of shipments taking place daily and the accompanying data make it virtually impossible to manually control and analyse these trade flows effectively. But AI-driven applications could make a substantial difference in this regard: the advances in data-collection and computing power provide important opportunities for

analysing the vast amount of data collected by Customs and border authorities every day.[24] **Machine learning techniques** could enable more effective identification of transactions in strategic goods and their patterns.

Of the three types of AI-driven technology identified and assessed in this project, **big data analysis** and **NLP**, and to a lesser extent **computer vision**, could play a role in strengthening the pre-export risk assessment and screening procedures conducted by the licensing and Customs authorities and by private companies involved in the manufacture and sale of such components. Other industrial sectors and private companies, such as the financial sector, already have substantial experience with implementing similar AI-driven applications to identify fraudulent transactions. In addition, it was mentioned during the pre-export workshop that private companies are effectively using AI tools in export licence compliance work to identify suspicious trade patterns and points of diversion. These technologies could therefore play a role in identifying illicit procurement networks and shell and front companies, and could be instrumental in tackling the use of generalised descriptions of the items in Customs declarations.[25]

Detecting **transshipment patterns** is a highly challenging and time-consuming endeavour, largely because it requires 'multi-tier visibility' of goods moving from a country of origin, through a transit country and finally to a destination country.[26] In-depth and systematic analysis of the available Customs data and shipping records has shown itself to be instrumental in helping us to understand diversion methods and identifying so-called 'red flags'. The effective monitoring of international supply chains for sensitive goods using existing data would be paramount as a means of preventing diversion.[27]

Given the fact that components are often (and rather easily) diverted from their intended end-user and end-use during the transfer and post-delivery stages, some of the identified technologies could be appropriate to aiding the prevention, detection or identification of diversion during transportation or after the delivery of the components to their intended end-user. In many instances, **DLT** is described as a relevant technology which would revolutionise supply chain security, including in the field of conventional arms transfers.[28] Interestingly, **DLT** scored relatively high on its potential impact on countering the diversion of CWC. At the same time, however, this technology was also considered to be one of those having the greatest barriers to their successful implementation. It offers great potential to keep track of the full chain of custody, increase transparency on trade flows, decrease counterfeiting and fraud, and reduce the delays in transmitting documents.[29] But its effectiveness depends strongly on the willingness of all the actors involved in the supply chain to link to the system and to submit relevant data and documents to the ledger.[30] However, the broad variety of (public and private) actors involved in international transfers of components, the existence of illicit proliferation networks that deliberately aim to obscure trade flows and the effective end-user and the cost and infrastructural requirements could be significant barriers to successfully implementing DLT.

GNSS and mobile tracking could be a highly relevant technology to track components during their transport with a view to make sure they effectively end up with the intended end-user. This technology could be particularly relevant as it allows a continuous monitoring of their transport and the real-time detection of attempts to divert the items from their intended transport route. These mobile tracking devices also allow implementing specific geographical boundaries in its software – 'geofencing' – which produces a signal when the tracked item leaves these boundaries. As became apparent in the analysis however, the accompanying barriers to implementation are substantial. In particular issues with regard to who is to be responsible for integrating and continuously monitoring such technologies (e.g., the manufacturer, the transport company, licensing authori-

ties, Customs) are important barriers to its effective implementation. While this barrier would be relevant to all types of military items, the barriers to implementing mobile tracking devices for components transfers, would be even more substantial. Their small size and the low cost per item would make it difficult to include such tracking devices on individual components; tracking of packages would therefore be a more feasible option. Moreover, because of the often pure civilian character of components, export control authorities are not always formally involved in their transfers. Changes to the regulatory/legal framework, installing obligations at the manufacturers or transport companies to implement such mobile tracking devices would therefore be needed.

Similar conclusions could be drawn about the trade-offs in implementing other technologies that would allow the continuous monitoring of the effective end-use of exported items. Such end-use monitoring could be particularly appropriate to components that have been delivered to their end-user. The assessment of the **Internet of Things** (IoT) illustrates this clearly. As a technology, IoT refers to the connectivity of items (or 'things') via the internet. This continuous interconnectivity creates – at least theoretical – opportunities to control certain items and components in remotely. Consequently, through this connectivity, the continuous monitoring of items becomes possible. Moreover, the inclusion of a so-called 'kill switch' in an item would permit the exported item to be turned off remotely.[31] Given the appropriateness of this diversion method to components, this technological solution could in theory have an important impact on strengthening counter-diversion efforts. Insurmountable barriers, however, may exist to the successful implementation of such a solution: in particular, the wide-ranging civil applications of components and the large number of manufacturers would make it very difficult in practice. In addition to these practical barriers, more fundamental barriers such as national security and operational–military considerations would equally engender significant reluctance to allow the presence of those 'kill switches' in certain components.

Section 4: Ways forward to technology adoption to counter diversion of components of conventional weapons

The analyses conducted throughout project D-TECT show that the different stakeholders who participated in this project recognise that technology may be a helpful tool to aid counter-diversion efforts. The reasons for using technology are varied and include, but are not limited to, improving knowledge of unknowns through better data utilisation, complementing existing risk-mitigation approaches, overcoming space and time constraints (e.g., the time-consuming and physical nature of post-shipment verification), and enabling sufficient data and information to conduct forensic analysis. A sentiment was also expressed by some participants that if technology is not adopted in certain instances, then the problems will persist, especially regarding the lack of traceability and transparency. Equally, the previous section showed that implementing technologies would not be self-evident. Many barriers to successful implementation were identified and in several instances some barriers were even assessed as being insurmountable. However, this does not mean that steps forward cannot be taken to facilitate the implementation of technologies, especially those with the greatest potential impact. This section therefore discusses the possible ways forward identified throughout this study to overcome the barriers to implementation. Specific attention is devoted to the relevance of existing international regimes, particularly the ATT framework, to facilitate discussions and initiatives on

technology adoption further to counter efforts to divert CWC.

A first important general barrier that was identified relates to **the broad variety of components that could possibly be used in conventional weapons** such as UAVs, missiles or rockets. Further clarification and specification of the components to focus on, and a more detailed understanding of the components most at risk of being diverted, is crucial to any further steps taken to strengthen counter-diversion efforts. More specifically, the criticality of the component, that is, the extent to which a component plays a crucial or critical role in the functioning of a weapon system, could be a relevant criterion with which to prioritise the components to focus on.[32] A granular analysis of the components that play a critical role in specific weapon systems would, moreover, make it possible to identify the actual companies that are effectively involved in the development, production and sale of these critical components. Such a more targeted approach could be particularly appropriate, as a workshop participant mentioned that in some cases the companies producing such components may be small but function as 'hidden champions', controlling a large part of a global market in a very specific segment. While it has become apparent in recent analyses of components found in conventional weapons that electronic components and drone components appear to constitute the most relevant component types, a more specific focus on actual components would still be necessary. One such item that was suggested by several workshop participants was a UAV's engine, which is considered as critical to UAV functioning and appears to be particularly vulnerable to diversion.

A second important issue that was seen as inhibiting the effective counter-diversion efforts involving CWC is **the lack of unique markings on the items and the accompanying registration of the transfers of these items** by both State authorities and the private companies involved in their production and sale. As an interviewee mentioned

> *often this fundamental element, proper registration protocols and adequate systems, is severely lacking. A lot of factors are in play to explain why these fundamentals are absent, such as culture, lack of political will, the lack of IT solutions and internet connectivity and the necessary financial capacity for this.*[33]

The lack of awareness of the risks of these components being 'weaponised' – that is, the use of civilian components for conventional military purposes – is an important reason for this. While the absence of individual markings is thus seen as a crucial barrier, at the same time it implies that substantive progress in countering the diversion of CWC could be made by strengthening the individual markings on certain components. In addition, actions to develop an **adequate infrastructure** for registering component transfers registering would be an important step forward towards strengthening counter-diversion efforts for CWC. The implementation of background data management systems that are capable of capturing data enabled by technology (e.g., on secondary marks, tracking and tracing data) would be an important precondition of the success of these technologies and at the same time be a very practical aspect to develop initiatives on. This should include agreement on the way the data in these management systems and databases are managed and by whom. **For most of the technologies included in this project, digital databases will be crucial.** For e-seals to be effective, for example, they must be accompanied by a host of reading devices and scanners, computer hardware and a suite of underlying IT software systems capable of adequately processing the collected data.[34] In addition, **establishing or strengthening archival processes**, such as through back-up systems, whether digital (e.g., cloud infrastructure) or physical, would be pivotal to overcoming the risk that the use of ICT and digital platforms could weaken archival processes. This archival material is important, particularly with regard to the 'identification' element of counter-diversion. In the ATT working group on effective treaty implemen-

tation, the newly established sub-working group on national implementation issues identified 'information management' as a priority topic.[35] This offers an opportunity to engage with different stakeholders on ways to strengthen data-collection, data-storage and data-sharing between the relevant actors and agencies. This would be a crucial condition for successfully engaging technologies to counter diversion. In any event, systematic marking and **record-keeping** is essential for post-facto 'track and trace' and could enhance the effectiveness of 'real-time location systems', rendering it more difficult to divert weapons to unauthorised users or for unauthorised use.[36] This, however, would not only be a manufacturing issue, but equally a regulatory one, with governments needing to adopt regulations on the marking of components, the registration of transfers (and the archiving of such information) and the sharing of information.

The **often civil–commercial nature of the components** and of the companies developing, producing and exporting them is considered to be another important barrier to successful implementation of (technological) measures to counter the diversion of components. At the same time, however, several solutions for dealing with this threshold were proposed during the workshop discussions. **Strengthening cooperation between State authorities and commercial actors involved in the production, sale and exportation of these components would be a crucial way forward.** Given the often civil nature of these components, the involvement of private actors and the industry will be indispensable to achieving this goal. Essentially, as a workshop participant mentioned, many private companies in different industrial sectors are already looking into supply chain tracing as a means of preventing the introduction of counterfeit components. This ultimately has ramifications for a company's reputation and bottom line. In order to do this, the companies will probably need to place pressure on governments to pass new legislation. The 'weaponisation of components' adds significant weight to the argument that governments should consider passing legislation in support of enhancing supply-chain traceability. Logistics service providers could in a similar manner be included in these initiatives, driven by a shared willingness and objective to strengthen the security of international supply chains.

Given the lack of proper and detailed marking of CWC, such increased cooperation between the private and the public actors could, for example, include dialogues between end-users and manufacturers about the type of information to be included in a secondary mark, the data-management systems that would be needed to collect and store marking information, and how best to harmonise private and public systems. Such discussions could be conducted in existing forums such as the ATT's **Diversion Information Exchange Forum** (DIEF). This forum could enable States parties to discuss the opportunities for and barriers to technology adoption and its use for counter-diversion purposes. Although the focus of such discussions would be broader than merely looking at certain CWC, the inclusion of these items would be appropriate, especially because of their growing relevance in current warfare and armed conflicts. In addition to and parallel with the DIEF, the newly established **sub-working group on 'current and emerging implementation issues'** in the ATT framework could offer a useful forum to set up discussions between public and private actors. In particular, this sub-working group's work on the role of industry in responsible arms transfers could offer an opportunity to voice and clarify the specific expectations and responsibilities of public and private actors. Given the commercial–civil nature of many of the components considered relevant in this context, clear understandings of the responsibilities and roles of public and private actors would be pivotal. Here, linking the issue of due diligence and Know Your Customer practices and initiatives taken by private actors could be important. Again, building on the experiences and policies developed in other industrial sectors, such as the financial or the pharmaceutical sector,

could be an appropriate step towards facilitating these discussions.

The **cost issue** is equally stressed as a crucial aspect that needs to be tackled through increased public–private cooperation. Although public licensing and Customs authorities may struggle with financial and personnel limitations, given the often commercial nature of components, this is an equally valid concern for the private companies involved in the production and sale of such components and which are expected to play a more active role in monitoring and controlling the transfers of their items. Systems designed for such tasks, such as Internal Compliance Systems, are expensive to build and to maintain, particularly for small companies producing specific components.[37] However, as some of these smaller companies can be hidden champions, as mentioned earlier, their involvement would be crucial to the success of any efforts to counter the diversion of these components effectively. A stronger engagement from governments to contribute tools, the provision of entities, etc. to support companies in this process is therefore needed.

Finally, a **lack of familiarity**, not only with the identified technologies but also with the reality of the diversion of components used in conventional weapons was often mentioned by the workshop participants as an important barrier to both reflection about the relevance of and barriers to a specific technology and also to assessing the barriers to its implementation. Initiatives to overcome this lack of knowledge, which is effectively inhibiting more dedicated and focused reflections on the potential impact of technologies, would be needed. The development of **pilot projects** to test the implementation of certain technologies in practice was therefore proposed by several of the workshop participants as an important instrument for overcoming the range of concerns being raised about technology adoption and increasing familiarity with it. Such pilot projects, focusing on actual components, one or a few methods of diversion, the specific actors (industry or government) and the concrete technology, could be beneficial to increasing familiarity and trust in technological solutions to counter-diversion. In this context, the **ATT's Voluntary Trust Fund (VTF)** could possibly be an interesting avenue through which to support the implementation of such pilot projects. Here, including representatives from other industrial sectors such as the extractive, pharmaceutical or the food and beverage industries, which have implemented supply chain tracing systems, may add value to such pilot projects. Such representatives may have much to offer in experience in and insight into the successful development and implementation of such a pilot project. In addition, creating platforms where examples of good practices and lessons learnt related to technology development and adoption could be shared would add value. This could take the form of an online tool or a standing meeting as in the case of existing multilateral instruments and organisations, such as the ATT or the UNOTC.

Overall, it should be acknowledged that the ability to mitigate or overcome barriers could differ depending on the stakeholders involved, the type of barrier, the extent to which the need to adopt technology exists and the willingness to overcome the barrier(s). Even so, it is hoped that demonstrating that there are options available to overcome the overarching barriers can help to advance discussions and expand policy options regarding technology adoption in the context of counter-diversion efforts. It should also be noted that some of these actions can be undertaken with a broader focus on counter-diversion and not only on technology adoption.

Section 5: Conclusion

This paper presented an in-depth analysis of whether and how different technologies could be implemented to help with counter-diversion efforts, with a particular focus on CWC.

Importantly, **three key limitations** should be taken into account when reflecting on the conclusions drawn from this research. First, the findings are based on only a relatively small number of survey respondents and workshop participants, who form only a small subsection of the wider community involved in the counter-diversion of SALW. Second, whereas the project team sought to ensure a wide-ranging representation of perspectives from the participants according to their background, expertise and geographical representation, most of the inputs nonetheless emerged from entities and individuals from the Western European and Other States regional group. Third, the participants differed in their levels of knowledge and understanding of each of the technologies, and also of the different types of need, resource and expectation they considered when participating in the research. The findings presented below have been aggregated and so they do not allow for such differences to emerge; therefore, they may not always reflect each individual response. Overall, the findings should be seen as illustrative rather than authoritative and should not be generalised or extrapolated beyond the constraints of this study. Despite these limitations, however, it is hoped that the findings and conclusions are able nonetheless to offer useful insights into the application of technology to counter-diversion efforts and that they will pave the way for further research and action in this area.

Overall, the 14 technology types identified during the first phase of project D-TECT have, broadly speaking, all been identified as being potentially appropriate to supporting counter-diversion efforts involving CWC. Some of these technology types are more adapted to assisting with certain aspects – such as detection – over others – such as prevention. Nonetheless, **all technologies face barriers to their implementation, although the nature and extent of these barriers is context-specific**. These barriers include the broader infrastructure for arms (transfer) control, the nature of the arms trade, which features a large number of different types of actor, or national security considerations that may emerge due to the use of technology. **Discussing the relevance of technologies to counter the diversion of CWC more specifically**, moreover, **proved to be much more challenging than for SALW**. This should come as no surprise. While countering the diversion of SALW is at the core of many international regimes, treaties and initiatives, the diversion of components, especially those that are of a dual-use or even a civil–commercial nature, is a much more recent topic. A lack of familiarity with technologies and the widely expressed need for practical examples to allow for a more substantive assessment of the relevance of these technologies reflected the general unease or reluctance among the stakeholders of arms transfer control to consider technological advances, even despite the project's deliberate choice to select only more or less 'mature' technologies. And despite a growing acknowledgment of the need to develop initiatives to counter the diversion of CWC, a better understanding of the trends in the acquisition, weaponisation and deployment of such components will be a prerequisite for developing and implementing any meaningful and effective actions, including the use of technologies in counter-diversion efforts.[38] This finding supports the starting-point of project D-TECT, which stresses the need for a contextualised assessment of the technologies, as most of the barriers to implementation are not directly related to the technology itself, but rather to the context in which it would need to be implemented.[39]

Priority appears to be given to the increased and enhanced marking of certain high-priority CWC. For this to happen, a better understanding is needed of what these high-priority components are. And this should be guided by their critical role in certain conventional weapons together with a better understanding of the ways in which these components are diverted. At the same time, advances in data management, collection and storage and the digitisation of (interoperable) data would be indispensable. Such a **'back office' of**

good and relevant digitalised data platforms is crucial to virtually all the identified technologies. Moving away from paper-based and disconnected systems towards a digitalised and integrated approach is required to enhance the security of transfers and reduce the unknowns in the system.

In addition and more fundamentally, the necessity of developing an integrative approach and the need for cooperation and information-sharing between different (non-traditional) actors in the arms transfer chain appear to be crucial. The nature of CWC necessitates close cooperation not only between different public authorities, but also with the industry actors involved in producing, exporting and transporting the items. Implementing other, more advanced and complex technologies such as DLT may therefore not be the best option, especially because doing so necessitates cooperation between a broad diversity of public and private actors and would run up against important concerns about (cyber-)security and operational–military considerations.

Overall, whereas cooperation between the public and the private actors would be essential, particularly in the specific case of CWC, explicit government action and the need for adequate regulatory frameworks will remain indispensable, especially those offering the potential and incentives for existing international bodies and treaties to pay more explicit attention to this topic, as was mentioned on several occasions in this paper.

The paper, however, does not provide a definitive answer as to which one or more specific technologies should be implemented and could be useful to achieving the object of counter-diversion. **This is because the most appropriate technology will differ depending on the context and on the needs behind its implementation.** In other words, it is not possible to provide an answer to the question 'Which is the most suitable technology?' because the technology and the way it is applied is not a one-size-fits-all solution. This is also because our assessment was not able to take regional, national or even local specificities into account. Yet such a perspective would be important to obtaining a more granular understanding of the starting point, level of risk(s) and specific needs to be met. The methods of diversion would or could be different according to the specific region involved – as was, for example, shown in the recent report on UAV acquisition types, which indicated important differences in the acquisition methods according to the participating states.[40]

Technology can act as a supportive tool or force multiplier to counter-diversion efforts, but its successful application nonetheless relies on oversight, an enabling environment, the enforcement of frameworks, instruments and processes, and also the broader political will. **These elements are the 'building blocks' that are required to be in place to enable technology implementation to help with counter-diversion.** These building blocks are composed of both non-technological and technological measures which should work together holistically to contribute to the goal of countering the diversion of conventional weapons. It is upon this basis that technologies can then be applied to best effect. The building blocks are also appropriate to counter-diversion efforts more broadly and not simply focused on paving the way to the use of technology. Certain technologies also need to be in place before others can be considered – for example, adequate individual marking technologies and the availability of a digital information infrastructure would be needed to enable tracking-and-tracing technologies, which in turn would need to be in place in order to enable data-driven technologies such as DLT or AI capabilities. It would, in other words, not be a case of choosing just one technology in developing efforts to counter the diversion of CWC. In the end, the best option for any type of counter-diversion initiatives for CWC would be a combination of several of the technologies discussed in this paper, accompanied by the necessary non-technological measures.

Ultimately, the application of technology to counter-diversion purposes should be an ongoing

conversation as both diversion and technology evolve, change, adapt and advance. Proliferators will continue to find ways to circumvent new measures implemented to counter diversion, with new methods and risks of diversion arising as a result. At the same time, technology continues to develop, with new technologies being developed in different domains. Discussing the role and relevance of technologies to counter the diversion of conventional weapons will therefore remain a continuous and changing, but at the same time worthwhile and interesting, endeavour.

ANNEX 1: Methodological note

This project adapted an existing methodology in order to conduct an assessment of the long list of technologies. This methodology, the Systematic Technology Reconnaissance, Evaluation and Adoption Method (STREAM), serves to assess the relevance of technologies and the opportunities for their adoption to fulfil a specific purpose. STREAM comprises five steps: (1) Framing of the issue; (2) Identification of technologies; (3) Characterisation of the issue; (4) Comparison of options; and (5) Decision.

Whereas the first phase of project D-TECT focused on steps 1 and 2 and resulted in a long list of potentially relevant technologies, this second phase focused on steps 3 and 4. Specifically, step 3 involves the following elements: (1) assessment of the potential impact of the identified technologies; (2) assessment of the potential barriers related to the implementation of these technologies; and (3) assessment of the costs related to the implementation of these technologies. Step 4 consists of a comparison of the technologies based on the assessment in step 3. Building on the insights developed in the first phase of project D-TECT, the overarching purpose of 'counter-diversion' was disaggregated into three subcomponents (see table 3). As technologies could have a differential appropriateness to these subcomponents, this distinction was used in the development of the specific data-collection methods.

A sequential exploratory design was used to collect the data, first via surveys, which collected primarily quantitative data, and then via workshops. The surveys and their associated workshops were organised along different stages in a typical life cycle: the pre-export stage, the transfer stage and the post-delivery stage. All the workshop participants were invited to complete an online survey ahead of the workshops. The surveys consisted of two parts. In the first part, the respondents had to assess the technologies' **perceived positive impact** on counter-diversion efforts for SALW and CWC respectively in each specific life-cycle phase and for three subcomponents of counter-diversion.[40] The second part focused on the **potential barriers** to the successful implementation of these technologies. Skills, infrastructural, cost, regulatory and social and ethical requirements were assessed for each technology, again separately for SALW and CWC. During the workshops, which took place online, the survey findings were presented and discussed. This allowed the participants to elaborate on their reasoning behind their responses, add further insights into the application of technology to counter-diversion efforts for the respective items and to reflect on possible future steps towards overcoming the identified barriers to implementation.

Potential participants from a broad variety of backgrounds were contacted: licensing authorities, Customs and border-control agencies, United Nations entities (e.g., UNODC, UNODA, UNTOC), other international organisations (e.g., World Customs Organisation), regional organisations (e.g., OAS), the private sector and industry, and research organisations. The participants were not selected for their expertise in or knowledge of the technologies per se, but rather for their experience in international trade flows, arms transfer controls

and the practices of diversion of conventional weapons. Four workshops were held in February–April 2024. The first two workshops – on the pre-export and transfer stages respectively – discussed both SALW and CWC. The third and fourth workshops, dealing with the post-delivery stage, focused specifically on SALW and CWC.[40] Table 4 provides an overview of the topics covered during the three workshops that discussed CWC and the number of participants.

In addition, insights from several semi-structured interviews conducted throughout the project and conclusions drawn from a literature analysis are used to substantiate further the insights obtained from the surveys and workshop discussions.

Table 3. Subcomponents of counter-diversion

Element	Description
Prevention of diversion	Takes place before diversion effectively happens and involves interventions to prevent actors from diverting conventional weapons from their authorised end-use or end-user.
Detection of 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 of diversion	Deals with actual instances of diversion, thus after diversion has taken place, and involves interventions to identify such cases and to analyse where the diversion effectively occurred with a view to supporting and optimising future diversion-prevention efforts and initiatives.

Table 4: Overview of the data-collection approach for CWC-specific inputs

Workshop	Life cycle stage	Item types	Number of survey respon-dents	Number of workshop participants	Date
1	Pre-export	SALW and CWC	17	23	26 February 2024
2	Transfer	SALW and CWC	12	18	14 March 2024
3	Post-delivery	CWC	10	12	22 April 2024

ANNEX 2: Overview of technologies

Table 5. Short description of the identified technologies

Technology	Description
2D codes	Small images that can store information both vertically and horizontally which can be applied to packaging or items directly through laser marking. Different types exist: QR codes and data-matrix codes.
Chemical encoding	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 to a wide range of materials. These marks are not visible to the naked eye, only via ultraviolet detection.

DNA coding	A unique DNA code (from synthetic or biological sources, such as plants) placed onto an item or its packaging, which is associated with a set of relevant information about the item. This code can be applied to all types of physical product and cannot be replicated, re-engineered or copied. These marks are not visible to the naked eye, only via ultraviolet detection.
Document authentication	Can be applied to ensure the legitimacy of certain documents, such as End-User Certificates, in order to strengthen protection against forged or other counterfeit copies. Holograms, for example, create an optical effect which acts as an authenticator of the document it is placed on. Ink-based markings can be added to a document and become visible under specific circumstances, depending on the type of ink used.
Electronic seals	A combination of mechanical seals with electronic security to improve the security of the seals. The electronic element most commonly uses either passive or active RFID.
GNSS and mobile tracking	Tracking technologies relying on digital infrastructure. Both GNSS and mobile tracking technologies work using a piece of hardware with receivers which send and receive data to either satellites or mobile communications, enabling the geolocation of the receivers.
Near-field communication	A set of communication protocols for secure wireless communication between electronic devices at a close distance (several centimetres) from each other.
Radio-frequency identification detection (RFID)	Consists of a chip, an antenna 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 readers possessing a greater read-range.
Sensors	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 includes RFID). Sensors can be used for a range of purposes, such as biometrics or intelligent packaging (with sensors monitoring the condition of a packaged product, particularly during transportation and storage).
Internet of Things (IoT)	Refers to an overarching digital platform connecting the physical to the digital world. 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. These data, which are synchronised from various sources on one single platform, can also be used to monitor digitally – or even control – the physical objects to which a sensor is applied..
Distributed ledger technology	A 'distributed record', or 'ledger', in which transactions are stored with cryptographic techniques in a permanent immutable way, ensuring transparency across an entire ecosystem.
Big data analysis	Refers to extremely large datasets which usually employ machine learning in order to make sense of this data. Machine learning describes algorithms that allow machines to learn from data. Big data analysis enables the making of predictions and the identification of hidden patterns in data.
Natural language processing	Field of machine learning in which machines learn to understand natural language as spoken and written by human beings. This allows machines to recognise language, understand it and respond to it, in addition to creating new text and translating between languages
Computer vision	Type of machine learning that enables computers and systems to derive meaningful information from digital images, videos and other visual inputs, and to take action or make recommendations based on that information.

Endnotes

1. UNIDIR, UNIDIR, Conflict Armament Research (CAR), and Stimson Center (2023), *Strengthening shared understanding on the impact of the Arms Trade Treaty in addressing risks of diversion in arms transfers*, Geneva: UNIDIR, https://doi.org/10.37559/CAAP/23/WAM/02, p. 4.
2. Merriam-Webster, Technology, (n.d.), https://www.merriam-webster.com/dictionary/technology.
3. e.g., Varisco, A., Maletta, G. & Robin, L. (2021), *Taking stock of the Arms Trade Treaty. Achievements, challenges and ways forward.* Stockholm: SIPRI, p. 1.
4. Resolution 1540 (2004) adopted by the Security Council at its 4956th meeting, 28 April 2004, *S/RES/1540*, https://documents.un.org/doc/undoc/gen/n04/328/43/pdf/n0432843.pdf
5. Conflict Armament Research (2024), *After the caliphate. Islamic State weapons in high-profile operations in north-east Syria,* London: Conflict Armament Research; Byrne, J. et al. (2022), *Silicon lifeline. Western electronics at the heart of Russia's war machine*, London: RUSI; Albright, D., Burkhard, S. & Faragasso, S. (2022), *Iranian drones in Ukraine contain Western brand components*, Institute for Science and International Security, https://isis-online.org/uploads/isis-reports/documents/Iranian_Drones_Contain_Western_Brand_Components_FINAL_2022.pdf
6. Wood, B. (2022), *The Arms Trade Treaty. Assessing its impact on countering diversion*, Geneva: UNIDIR, p. 17, https://unidir.org/wp-content/uploads/2023/05/UNIDIR_The_Arms_Trade_Treaty_Assessing_its_Impact_on_Countering_Diversion.pdf
7. 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
8. Grand-Clément, S. & Cops, D. (2023), *Technologies to counter the diversion of small arms and light weapons, and components of conventional weapons,* Brussels: Flemish Peace Institute., https://vlaamsvredesinstituut.eu/wp-content/uploads/2023/08/20230828-FPI_UNIDIR-Paper-Technologies_DIGI-DEF.pdf
9. Martinez, Manuel, Malaret, Alfredo, Mumford, Erica & Briggs, Natalie (2021), 'Arms Trade Treaty Issue Brief 3: Diversion Analysis Framework', UNIDIR, Conflict Armament Research, and Stimson Center.
10. e.g., Merrel Wetterwik, A-C & Mara, K. (2012), *Controlling parts and components of conventional weapons in the arms trade treaty – a necessity and a challenge*, Oslo: Norwegian forum for Development and environment, https://www.forumfor.no/assets/docs/Controlling-parts-and-components-of-conventional-weapons-in-the-Arms-Trade-Treaty-_-a-necessity-and-a-challenge.pdf
11. United Nations Office of Counter-Terrorism & Conflict Armament Research (2024), *Global report on the acquisition, weaponization and deployment of Unmanned Aircraft Systems by non-state armed groups for terrorism-related purposes*, p. 2, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_car_aros_report_web_en_mar2024.pdf
12. UN Security Council, Resolution 2370: on preventing terrorists from acquiring weapons, 2 August 2017, https://digitallibrary.un.org/record/1298311/usage?ln=en
13. Albright, D., Burkhard, S. & Faragasso, S. (2022), *Iranian drones in Ukraine contain Western brand components*, Institute for Science and International Security, p. 6.
14. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2233441.pdf, p. 19.
15. See, e.g., Harithas, B. (2024), *Mapping the chip smuggling pipeline and improving export control compliance*, Washington, D.C.: Center for Strategic and International Studies, https://www.csis.org/analysis/mapping-chip-smuggling-pipeline-and-improving-export-control-compliance; *Thirtieth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/394/29/PDF/N2239429.pdf?OpenElement; Panel of Experts (2022), *Final report of 25 January 2022 of the Panel of Experts on Yemen established pursuant to Security Council resolution 2140* (2014), https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2022_50.pdf; UNOCT & CAR (2024), *Global report on the acquisition, weaponization and deployment of Unmanned Aircraft Systems by non-state armed groups for terrorism-related purposes.*
16. *Thirtieth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to Resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/394/29/PDF/N2239429.pdf?OpenElement; Panel of Experts (2022), *Final report of 25 January 2022 of the Panel of Experts on Yemen established pursuant to Security Council resolution 2140*, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2022_50.pdf; Ruehsen, M. & Spector, L. (2015). Follow the proliferation money. *Bulletin of the Atomic Scientists, 71(5)*, 51-58.
17. See, e.g., Conflict Armament Research (2024), *Documenting a North Korean missile in Ukraine, Ukraine field dispatch*, January 2024; Conflict Armament Research (2022), *Dissecting Iranian drones employed by Russia in Ukraine, Ukraine field dispatch*, November 2022; Byrne, J. et al. (2022), *Silicon lifeline. Western electronics at the heart of Russia's war machine*, London: RUSI.
18. Conflict Armament Research (2024), *After the caliphate. Islamic State weapons in high-profile operations in north-east Syria,* London: Conflict Armament Research.
19. Byrne, J. et al. (2022), *Silicon lifeline. Western electronics at the heart of Russia's war machine*, London: RUSI, p. 50.
20. e.g., Conflict Armament Research (2022), *Missile components used in drone attacks in Northeast Syria*, London: Conflict Armament Research.
21. Conflict Armament Research (2022), *Missile components used in drone attacks in Northeast Syria*, London: Conflict Armament Research.
22. Interview representative international research NGO, 23 November 2023.
23. Conflict Armament Research (2023), *Diversion digest. Red flags in trade data*, London: Conflict Armament Research.
24. 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.
25. 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.
26. Byrne, J. et al. (2022), *Silicon lifeline. Western electronics at the heart of Russia's war machine*, London: RUSI, p. 50.

27. Conflict Armament Research (2023), *Diversion digest. Red flags in trade data*, London: Conflict Armament Research, p. 16; 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.
28. Okazaki, Y. (2018), *Unveiling the potential of blockchain for Customs*, WCO research paper n° 45; Coscarella, C. & Minotti, A. (2020), An institutional blockchain as a tool to control the export of dual-use and military goods, *Strategic Trade Review, 6*, (9), 93–112; Yousif, E. & Marshall, W. (2023), *Issue brief: distributed ledger technology for arms control and management*, Washington, D.C.: Stimson Center, https://www.stimson.org/wp-content/uploads/2023/09/Distributed-Ledger-Technology-for-Arms-Control-and-Management.pdf; Miotto, N. (2022), *Blockchain technology: an innovative policy tool for enhancing conventional arms control and verification*, Geneva: Geneva Centre for Security Policy.
29. Coscarella, C. & Minotti; A. (2020), An institutional blockchain as a tool to control the export of dual-use and military goods, *Strategic Trade Review, 6*, (9), 96–97.
30. Interview representative company in the diamond industry, 23 April 2023; interview representative technology company, 5 May 2023.
31. Reinsch, W. A. & Benson, E. (2021), *Digitizing export controls: a trade compliance technology stack?* Washington, D.C.: Centre for Strategic and International Studies, p. 3, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211201_Reinsch_Digitizing_ExportControls.pdf?VersionId=EZ.7BrxaXtjvnwfiD79RZ5ptWs692Ua6
32. Respondent workshop post-delivery CWC, 22 April 2024; respondents interview international research NGO, 25 November 2022.
33. Interview representative international research NGO, 23 November 2023.
34. Lanska, M. & Horak, T. (2012), Current supply chain security technologies in context, *Perner's Contacts, 7*, (2), 80–95.
35. *Draft multi-year work plan for the WGETI sub-working group on exchange of national implementation practices*, Annex B of draft report of the ATT working group on effective treaty implementation, ATT/CSP10.WGETI/2024/CHAIR/783/Conf.Rep
36. Danssaert, P. (2019), *Anti-diversion measures: real-time locating systems*, Antwerp: IPIS, p. 5.
37. Respondents interview international research NGO, 25 November 2022.
38. UNOCT & CAR (2024), *Ibid.*, p. 9.
39. See Kootstra, J. & Kleinhout-Vliek, T. (2021), Implementing pharmaceutical track-and-trace systems: a realist review, *BMJ Global Health, 6*, p. 5. for a similar conclusion in the pharmaceutical context.
40. UNOTC & CAR (2024), *Ibid.*, p. 17.

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 on strategic goods and technologies.

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.

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. The first phase was 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. The second phase is 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 second phase of the research. It focuses on examining the extent to which different technologies could help counter the diversion of components of conventional weapons and the barriers to their implementation.

D-TECT

flemish peaceinstitute

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