

# **NGO submission on the elaboration of article 2, criterion 7 of the draft EU Common Position Defining Common Rules Governing the Control of Exports of Military Technology and Equipment**

**April 2006**

## **Contents**

<b>NGO Endorsements</b>	<b>2</b>
<b>Executive summary</b>	<b>3</b>
<b>Introduction</b>	<b>8</b>
<b>Principles</b>	<b>8</b>
<b>Definitional issues</b>	<b>10</b>
<b>Types and causes of diversion</b>	<b>11</b>
<b>In-country security: assessment and assistance</b>	<b>12</b>
<b>Diversion at different stages in the transfer process</b>	<b>12</b>
<b>Levels of risk</b>	<b>13</b>
<b>Access to information and co-operation among member states</b>	<b>14</b>
<b>Sources of information</b>	<b>14</b>
<b>Inter-state co-operation</b>	<b>15</b>
<b>Information-sharing</b>	<b>15</b>
<b>In-country co-operation</b>	<b>16</b>
<b>Mutual support in event of transgressions</b>	<b>17</b>
<b>Documentation</b>	<b>17</b>
<b>End-use certification</b>	<b>17</b>
<b>Delivery verification</b>	<b>19</b>
<b>Registers of those involved in trade activities</b>	<b>19</b>
<b>Responsibility of industry</b>	<b>20</b>
<b>Elements of an effective system</b>	<b>21</b>
<b>Licence processing</b>	<b>21</b>
Tools to assist risk assessment at the licensing processing stage	22
Controls applied to the shipping process	24
Transit and brokering	25
Post-delivery verification	25
<b>Responding to problematic cases</b>	<b>26</b>
Suspicion of future diversion	27
Responding to actual instances of diversion	27
Co-operation among EU member states	28
<b>Conclusion</b>	<b>28</b>

## NGO Endorsements

The major contributors to this document have been *Groupe de recherche et d'information sur la paix et la sécurité*, *Oxfam GB*, *Saferworld*, and Mike Bourne of the *University of Bradford*.

### The document has been endorsed by the following organisations :

Pax Christi Österreich	Austria
Arbeitsgemeinschaft Entwicklungszusammenarbeit AGEZ (Umbrella Organisation of 32 NGOs in Austria)	Austria
Österreichische MedizinerInnen gegen Gewalt und Atomgefahren OMEGA (International Physicians for the Prevention of Nuclear War, IPPNW)	Austria
Internationaler Versöhnungsbund – Österreichischer Zweig IVB-ÖZ (International Fellowship of Reconciliation IFOR Austria)	Austria
Africa and Europe Faith and Justice Network AEFJN	Belgium
Groupe de recherche et d'information sur la paix et la sécurité GRIP	Belgium
Justice et Paix	Belgium
Pax Christi Flanders	Belgium
Pax Christi Walloon	Belgium
Vlaams Netwerk Lichte Wapens VNLW	Belgium
Transparency International Czech Republic Arms Trade Control Project	Czech Republic
Kansalaisjärjestöjen konfliktinehkäisyverkosto KATU	Finland
Civil Society Conflict Prevention Network	France
Agir ici - Observer member of Oxfam International	France
Caritas Internationalis	France
Oxfam Deutschland	Germany
Transparency International Latvia	Latvia
Instytut Pomocy Roswojowej (Institute for Development Aid)	Poland
School for a Culture of Peace (Autonomous University of Barcelona)	Spain
Swedish Fellowship of Reconciliation SweFOR	Sweden
Swedish Peace and Arbitration Society	Sweden
BASIC	UK
Christian Aid	UK
Oxfam GB	UK
Saferworld	UK
Transparency International UK	UK
Amnesty International, International Secretariat	
Quaker Council for European Affairs	EU

## Executive summary

This paper, working from the *Draft Council Common Position 2005/.../CFSP – Defining Common Rules Governing the Control of Exports of Military Technology and Equipment* (draft for PSC, 28 June 2005), is an initial EU NGO contribution to the process of developing guidelines for criterion 7. It should be noted, however, that some of the ideas contained herein would, if applied more widely, have significant benefits far beyond the issue of diversion.

### Principles

Certain fundamental principles should be kept in mind throughout the process of elaborating criterion 7.

- There is a need for an explicit understanding of the *obligation to deny* a licence where there is a risk of diversion
- The intention of the criterion is to prevent diversion where it might result in a breach of the seven other criteria, for example serious violations of human rights or international humanitarian law. This will require the application of the other criteria once a diversionary risk and the likely end-use/end-user is established.
- Perhaps more than any other criterion, diversion is an issue where there is a need to consider the systems of control that apply to *transfers*, rather than just to exports.
- Due to the attendant risks of serial diversion, member states should be particularly vigilant with regard to criterion 7 when assessing transfers which will assist others to develop their own defence industrial base.
- Current practice with regard to robust checking at the delivery and post-delivery stages is underdeveloped.
- Member states should do more to co-operate in terms of investigations, information-sharing and developing policy responses to suspicion or incidence of diversion.

### Types and causes of diversion

Diversion can take place within country, or can involve detour or retransfer to a third 'unauthorised' country (either before or after the scheduled delivery). It can be of possession (end-user) and/or function (end-use).

Diversion can be initiated at various levels, from deliberate collusion at the level of the state down to the turning of a blind-eye by a border or stockpile guard. It is often carried out in close association with brokers and traffickers of illicit arms. It can result from poorly developed systems or a lack of capacity to manage systems effectively rather than any kind of intent by the state or its agents.

Appropriate policy-responses to cases of potential or actual diversion will depend upon the way these different aspects of the diversion issue interact.

### In-country security: assessment and assistance

Greater efforts should be made by EU member states not just to assess but also to assist in the development of adequate capacities in the importing country to ensure the security of imported military technology and equipment. Examples of the types

of issues that may require attention include stockpile management and arms transfer control mechanisms.

### **Levels of risk**

Some degree of risk of diversion is present with every arms transfer. Thus, in practice, states will assess the level of risk and will then balance that significance against other factors. However, as is clear from the text of the draft Common Position, if a state is unable to conduct a reliable assessment of diversionary risk – or if that assessment is highly ambiguous – no licence should be approved. In other words, the draft Common Position supposes a presumption against transfer unless a thorough risk assessment has established that there is a sufficiently low risk of diversion.

The level of risk will be contingent on the nature of the goods, the identity of the proposed end-user and all the actors involved in the transfer, and the intended end-use. It appears that member states also temper their response to diversion based on the perceived *consequences* of that diversion. The current emphasis on the importance of MANPADS (e.g. because of the threat some may represent to civilian aircraft) has meant that within the Wassenaar Arrangement a number of control measures over and above those applied to most conventional arms have been developed for this class of goods.

### **Access to information and co-operation among member states**

Member states should seek information on diversionary risks from a wide variety of sources including from within their own ranks (not least the intelligence services), from partner governments, international organisations, the defence and transportation industries, media and civil society. However it is important that during such a process the inputs of certain actors (e.g. recipient states) are not privileged at the expense of others simply due to their identity or status – all inputs should be subject to rigorous analysis. Resources should be targeted on those transfers that give most cause for concern.

There is a need for much greater co-operation among member states. While to everyone's advantage, it would be of most notable benefit to smaller states with a limited capacity to carry out all the necessary analysis and checks themselves. Information-sharing should go deeper and wider than is currently the case. Where there are sometimes intelligence 'sensitivities' regarding the passing of information, efforts should be made to work around them. The current situation, where information about individual licence refusals is circulated to all member states, should be supplemented with advice about any special conditions that apply to the general issuance of licences to, for example, certain recipients. This should extend to co-operation by member states 'in-country'. For example, were member states to agree to sharing, seconding or 'borrowing' qualified staff, this would increase both the capacity for relevant checks to be carried out and the leverage that could be applied on states reluctant to allow effective delivery verification or end-use monitoring.

Wherever possible, EU states should seek to use the new international instrument on marking and tracing of SALW to identify points of diversion. The results of any enquiries (including refusals to co-operate with tracing requests) should be circulated and factored into licensing assessments.

The EU should also seek to broaden its co-operation in this area to include other like-minded states. As co-operation increases, the consequences for buyers permitting or participating in diversion, or refusing to co-operate with the exporting states seeking to confirm agreed end-use, would likewise increase.

### **Documentation**

Improved documentation in diversion risk-assessment would not of itself prevent attempts to circumvent arms transfer controls and exploit loopholes. It would, however, make illicit trafficking and diversion more difficult. In addition, systematic use of documentation would assist efforts to hold transgressors to account.

End-use certificates (EUCs) should always be required and authenticated, and should contain 'no re-export without permission' provisions. At the very least, if there are circumstances where exceptions are to be made these should be made explicit and published. In any event, there must always be some form of prior written notification from the importing state.

### **Delivery verification**

EU member states would ideally require delivery verification certificates for all licensed transfers (as is now the case for transfers of MANPADS by Wassenaar Arrangement states). At a minimum, member states should identify (publicly) the situations when delivery verification certificates would be obligatory. Companies named on the original licence application should be held legally responsible for the entire consignment until delivered to the stated end-user. Delivery verification in the country of final destination should include physical inspection to confirm that the equipment delivered to the end-user corresponds to that authorised for export/import and recorded in shipping documents. In order to facilitate such measures, greater use could be made of existing commercial transfer inspection companies in providing delivery tracking services, documentation verification, and conducting physical pre-delivery and delivery verification.

States must however ensure that enhanced delivery verification procedures do not undermine the obligation to deny an export authorisation if there is a clear diversion risk.

### **Responsibility of industry**

Governments should develop, with industry and other stakeholders, clear guidelines for responsible behaviour by industry. A basis for such guidelines is provided by the List of Advisory Questions for Industry, adopted in the Wassenaar Arrangement in 2003.

### **Elements of an effective system**

#### *Assessment and analysis*

An effective elaboration of criterion 7 will specify the elements necessary to assess and minimise the risk of diversion. Measures should be applied at all stages of the transfer process, from pre-licensing through to post-delivery. These will include the following:

- Transfer licences should not be issued without adequate checks on accompanying EUCs, with member states able to draw on the assistance of other member states where required;

- Licences should include 'no re-export without permission' provisions;
- EU members should collate and share details of cases of diversion or suspected diversion or any other relevant information that will help licensing authorities identify problematic cases;
- EU member states should develop a series of 'red flag' indicators to assess risks of diversion at the licence processing stage, including:
  - is the equipment/ technology in question commensurate with the likely requirements of the nominal recipient?
  - does the proximity of the nominal recipient (or the transportation route) to conflict zones, areas of escalating tension, areas where violations of international human rights or international humanitarian law are taking place, embargoed states etc. raise concerns?
  - does the nominal recipient have links with particular actors of concern (e.g. certain armed groups, terrorist or organised criminal networks)?
  - are there (problematic) intermediaries involved in the transfer?
  - is there a history of end-use problems associated with the nominal recipient?
  - does the recipient country have the will and capacity to apply effective transfer controls?
  - what is the level of corruption in the recipient country and among the various actors involved in the transfer?
  - is stockpile management and security of a sufficient standard?
- Companies applying for export licences should be legally responsible for the entire delivery process, including verification that all goods specified on the licence application arrive at the stated end-user;
- In order to physically verify documentation, a comprehensive inventory of all shipments of arms and licensed equipment entering EU territory should occur before shipments are allowed to transit through EU member states;
- All companies involved in facilitating the transfer of the consignment (including supplier and delivery firms) should be registered and have no history of commercial crime.
- Member states should ensure they have sufficient legal powers to impound any shipment or aircraft where problems are suspected or proven;
- Transfer licences should include reserve the right of the licensor government to carry out delivery verification and end-use monitoring inspections (this is on the understanding that such a right would only be exercised where there was a clear concern). Member states should assist each other in carrying out such inspections as necessary.

#### *Responding to problematic cases*

Assessment and analysis is only one half of a comprehensive system of diversion risk management. States must also develop appropriate responses where problems are identified. They must send a clear message that diversion is taken very seriously, that consequences will follow therefrom, and that the EU speaks with one voice on the issue. The consequences should depend upon the extent and scale of the diversion, and the extent of involvement of the recipient state, as well as its willingness and capacity to reform behaviour.

Responses could range from *de facto* embargoes in the most egregious cases, through selective embargoes (on certain types of equipment and/or recipients) and then

special provisions (e.g. extra delivery verification or monitoring obligations), down to special vigilance. States would move down through the steps based on demonstrations of reform and goodwill. Where a 'sinned against' member state puts measures in place, while acknowledging that arms transfer licensing decisions are taken at national level, other member states should seek to respond sympathetically in terms of changes to their own practice.

Member states should also co-operate in terms of helping, where appropriate, recipient states to take remedial action or at least to feed back information about whether the required action has been taken.

## Introduction

EU-based NGOs have for a number of years been arguing that the criteria of the EU Code of Conduct on Arms Exports (EU Code) allow far too much room for interpretation. This has had negative consequences both for EU member states, in terms of hamstringing attempts to achieve their stated goal of “promot[ing] convergence in the field of conventional arms exports”<sup>1</sup>, and for other states that have formally ‘aligned themselves’ to the EU Code but have little idea how to implement this in practice. Civil society therefore welcomed the decision in 2003 to develop elaborative guidelines for criterion 8, and is further encouraged by the decision under the 2005 UK Presidency to begin a similar process for criteria 2 and 7 and the apparent enthusiasm to eventually develop guidelines for all the criteria. NGOs would also welcome the opportunity to discuss this submission with COARM officials, as well as to analyse and respond to any interim drafts produced by COARM.

This paper, working from the *Draft Council Common Position 2005/.../CFSP – Defining Common Rules Governing the Control of Exports of Military Technology and Equipment* (draft for PSC, 28 June 2005), is an initial EU NGO contribution to the process of developing guidelines for criterion 7. While the discussion and the recommendations contained herein are focussed on issues that arise from an examination of the implementation of criterion 7, there are occasions where our proposals may imply action beyond this criterion (e.g. in connection with registration requirements for those involved in trade activities) or beyond the particular scope of the elaborative process as defined for criterion 7. Member states are encouraged not to reject recommendations solely on the grounds that they cannot be comfortably housed completely within the criterion-7 mandate or within the elaboration *per se*. Indeed, herein are ideas which, if applied more widely, could have significant benefits far beyond the issue of diversion.

## Principles

Certain fundamental principles should be kept in mind throughout the process of elaborating criterion 7. Many of these will apply to other criteria, as they are principles which underpin the EU Code itself, however there are some issues particular to this criterion.

The first four of the criteria of the EU Code contain an unambiguous instruction to deny an export licence should certain conditions apply. Unfortunately, under criterion 7 there is no such instruction. Instead, member states are instructed merely to assess the existence of a risk of in-country diversion or re-export. In the report *Taking Control*, EU NGOs suggested new text for criterion 7 which addressed this weakness, however this recommendation has so far not been taken up by member states.<sup>2</sup>

---

<sup>1</sup> As stated in the preamble to the EU Code.

<sup>2</sup> The proposed language was “member states will not license the export of arms where they have knowledge or ought reasonably to have knowledge that transfers of arms of the kind under consideration are likely to be diverted and used in breach of any of the criteria of this Code of Conduct.” (*Taking control: the case for a more effective EU Code of Conduct on Arms Exports*, *EU non-governmental organisations*, Saferworld (ed.), September 2004, p. 41, <http://www.saferworld.co.uk/publications.php?id=33>).

The elaboration of the criterion represents an opportunity to revisit this point. It is a fundamental principle of the EU Code that export-licensing decisions should be made on the basis of risk, rather than proof – it would therefore be an extremely positive step if the elaboration could make explicit that the goal of the criterion is to reduce the incidence of diversion, and that member states should deny licences where there is a risk that this will happen.

One of the key factors in determining risk – for each of the criteria – is past experience (of all member states, which has implications for information-sharing – see below). While evidence or firmly-grounded suspicion of past wrong-doing is not proof of future misconduct, it is significant when calculating risk. By the same token, a lack of knowledge of past misconduct is no guarantee of ‘good behaviour’ in future.

Perhaps more than under any other criterion, diversion is an issue where there is a need to consider the systems of control that apply to *transfers*, rather than just to exports. When considering diversion, the control regimes in place in transit and recipient states are of fundamental importance, and should be taken into account in export licensing decisions. The new criterion 7 refers to “the capability of the recipient country to apply effective export controls”, but it is also imperative that the recipient country can manage the import process and ensure that the goods in question are delivered to the stated end-user. It is also important that transit states are capable of preventing diversion while the goods are in their jurisdiction.

Of particular relevance to criterion 7 is the issue of off-shore production and assembly. The proliferation risks attached to assisting production capacity in other countries are manifestly greater than where the export concerned is a finished weapon, platform or system (except where reverse engineering is an issue). The risk is that the recipient state becomes a self-reliant producer (or at least is no longer reliant on an EU member state), and is therefore able to become a serial re-exporter. Member states should therefore be particularly vigilant with regard to criterion 7 when assessing transfers which will assist others to develop their own defence industrial base.

Although the profile of terrorism is now extremely high, there should be no attempt to give criterion 7 an exclusively anti-terrorism focus. While this criterion is likely to be of particular relevance to the issue of terrorism – as terrorists will frequently seek to obtain weapons through diverted stocks – other beneficiaries and consequences of diversion should not play second-fiddle.

To date, it would seem that EU member states in implementing criterion 7 have concentrated on assessments of diversion risks at the pre-licensing stage. While this is one necessary component in building an effective system, there is a need to recognise the fact that to fully address the risk of diversion member states must also institute robust checks during the delivery stage (e.g. by developing mechanisms for checking on goods in transit) and also post-delivery (e.g. through delivery verification and end-use monitoring mechanisms).

Also important is the need for consistent application and enforcement in all EU member states, especially in light of the extension of responsibility beyond the point

where the goods or technology leave EU territory. For delivery or post-delivery measures to be efficacious, member states must all set and follow the same standards, and co-operate as fully as possible regarding investigations and information flows. There are sensitivities among recipient states about post-delivery inspections or even enquiries regarding end-use. As a consequence, one member state operating alone will find it difficult to assert its will in this area: the 25 states of the EU acting in concert are more likely to enjoy success. Developing this logic further, common understandings and information-sharing should where possible be established with other exporters so as to build this approach into an international norm, with the US as an obvious potential partner.

Finally, it should be noted that elaborating guidelines for criterion 7 cannot take place without considering the impact this will have on other parts of the new Common Position and other elements of the EU arms transfers control infrastructure. For example, this will have direct consequences for article 5 of the draft Common Position (which deals with end-use documentation, and makes specific reference to the export of “military technology or equipment for the purposes of production in third countries”). Chapter 2 section 1 of the User’s Guide<sup>3</sup>, which sets out detailed end-use certification requirements, is also of direct relevance here.

## Definitional issues

*Existence of a risk that the military technology or equipment will be diverted within the buyer country or re-exported under undesirable conditions.*

Unfortunately, this “headline” text of the new criterion 7 is phrased too narrowly to address all aspects of the diversion issue. In particular, this phrasing seems to completely ignore the risk that transfers can be diverted before they reach the intended destination. Nor is it clear whether the reference to “undesirable conditions” refers to diversion within the buyer country as well as to re-exportation, or whether in-country diversion is of itself a target of the criterion (for more detail on these different types of diversion, see below). The general reference in the next sentence of the new criterion 7 to diversion “to an undesirable end-user or for an undesirable end use” would seem to clarify this potential confusion.<sup>4</sup> On the one hand it would seem to extend the concept of diversion to include *en route* issues, while on the other it suggests that diversion *per se* is not problematic unless it includes the risk of one of those “undesirable” consequences. It would, however, be useful if the nature of these undesirable consequences could be made clear, i.e. that these relate to the other seven criteria of the EU Code/draft Common Position, for example the risk that the equipment might be used to commit serious violations of human rights or international humanitarian law.

This reference to undesirable consequences draws attention to the fact that any criterion-7 assessment has two parts: is diversion likely; and, if so, who is the likely

---

<sup>3</sup> ‘User’s Guide to the EU Code of Conduct on Arms Exports’, *Council of the European Union*, 5179/06, PESC 18, COARM 1, p. 18, 11 January 2006, <http://ue.eu.int/uedocs/cmsUpload/st05179en06.pdf>.

<sup>4</sup> The sentence reads: “In assessing the impact of the military technology or equipment to be exported on the recipient country and the risk that such technology or equipment might be diverted to an undesirable end-user or for an undesirable end use, the following shall be considered:”

end-user and/or what is the likely end-use? In the case of likely end-use, this will involve normal application of the other seven criteria. However, where the diversion is in the context of the end-user, the wording of the draft Common Position suggests a different approach, i.e. that the task is only to determine whether that end-user is undesirable, and not to assess the use to which that end-user will put the specific equipment. It would be helpful if the elaboration of criterion 7 could clarify this point, but if such a distinction does exist, there must be agreed procedures in place to determine which end-users are 'undesirable'. And if such an approach is not to undermine the control regime, it should operate to ensure that the likelihood of a criterion-7 refusal increases, rather than decreases.

One other definitional issue concerns the fact that nowhere is it unambiguously stated that to classify as diversion the retransfer or 'detour' must be *unauthorised* (by the relevant EU member state). While this is an obvious assumption, it would be helpful to have it explicitly recognised.

At one level, the focus on consequences is completely logical within the context of the Code (or Common Position) criteria. However, implicit in the phenomenon of (unauthorised) diversion is the fact that the relevant EU member state loses all control over the ultimate recipient of the diverted equipment. The unreliability of end-use/end-user is a problem in itself. A previous 'unproblematic' diversion may raise the risk that future transfers will also be diverted, but it should not give any confidence that subsequent diversion will be without negative consequences. Diversion posits a loss of control; it 'squares the risk' of an undesirable result. It is not clear that this is recognised within criterion 7 as drafted.

## **Types and causes of diversion**

As mentioned above, diversion can take place within country, or can involve detour or retransfer to a third 'unauthorised' country. It can be of:

- possession – the equipment ends up in the hand of different recipient than originally specified in the licence application; and/or
- function – the equipment is used differently from its stated end-use.

The risk of diversion applies to transfers not only of finished systems but also to components, spares, upgrades and sub-systems for weapons already in service in the recipient country as well as cases where the goods exported are to be incorporated into systems or platforms for onward sale.

Diversion can be the result of deliberate collusion at the level of the state. Alternatively, it can involve criminal/illicit activity at a lower level within the recipient country, for example by companies or corrupt officials. Such activity is often undertaken in close association with brokers and traffickers of illicit arms, who are particularly adept at exploiting weaknesses in controls over weapons inventories, stockpile management, customs controls and oversight of the shipping process. And while diversion may involve duplicity on the part of the state or those tasked with administering the system, it may also occur as a consequence of poorly developed systems or a lack of capacity to manage systems effectively. Thus a thorough evaluation of risk of diversion must consider *capacity* as well as *intent*.

For example, leakage from state stocks through theft and subsequent resale is a form of diversion (frequently, but not exclusively, of SALW and ammunition) that in many countries may have more to do with lack of capacity than any deliberate intention of the government.<sup>5</sup>

### **In-country security: assessment and assistance**

Greater efforts should be made by EU member states to assess and assist in the development of adequate capacities in the importing country to ensure the security of imported military technology and equipment. Of particular importance here is the assessment of whether policies and practices ensure the responsible management of stockpiles by the military, police, dealers and other actors in the importing country. Similarly, an assessment should be made of the adequacy of control mechanisms on in-country transfers and re-exports by the importing country. Effective control mechanisms are essential to ensure that importing countries have the capacity to conform with end-use and re-transfer conditions that may be imposed by EU member states.

Indeed, as discussed above, diversion risks are a function of both willingness and the capacity of an importing country to conform with the requirements of exporting countries, for example with regard to preventing falsification of delivery verification certificates. EU member states should therefore continue and, where appropriate, strengthen their efforts to assist importing countries to establish and maintain appropriate national arms control mechanisms.

### **Diversion at different stages in the transfer process**

Member states must take into account the risk of diversion at various stages during the transportation or life-cycle of the controlled goods under consideration.

*En-route diversion* refers to situations where the goods are diverted before they ever come under the control of agents within the stated recipient country. The goods may be diverted at a stop-off point, for example during a refuelling stop, and never reach their stated destination. Or they may reach their stated destination but be diverted immediately on arrival.

This latter type of diversion often takes place in the proximity of conflict zones, particularly when the destination for diversion is subject to an arms embargo or the recipient would be a highly sensitive destination for direct exports. These types of diversion are common methods employed in the illicit brokering and trafficking of arms, which places increased significance on licences issued within the EU for brokering, shipping and transshipment.

---

<sup>5</sup> This aspect of diversion is more explicitly dealt with in other frameworks, such as the Wassenaar Arrangement's *Elements for Export Controls of MANPADS*, [http://www.wassenaar.org/publicdocuments/2002\\_MANPADS.html](http://www.wassenaar.org/publicdocuments/2002_MANPADS.html), parts of which might profitably be imported into the elaboration of criterion 7.

Paperwork is often changed to obfuscate identification of these clandestine deliveries, which makes it all the more important that licensing authorities within EU member states develop systems to collate and verify shipping and delivery information as part of their export licensing processes.

*In-country diversion* refers to cases where the goods reach the country of final destination, but of which are never taken possession by the stated end-user or are subsequently diverted to other users within the destination country. For example, rifles and shotguns licensed for hunting and sporting purposes may be sold clandestinely to criminal networks. Or it could involve diversion to a different section of the country's security forces, for example to a particular unit with a poor human rights record.

Components (including spares and upgrades) can also be subject to diversion. It is therefore important that adequate risk analysis is undertaken at the licensing stage to ensure that these items could not be used in other weapons systems not specified in the original licence application.

In cases of *diversion through re-export* the recipient takes delivery of the goods, but then transfers them on. It is important to note that this can be some considerable time after the original export, e.g. when the original items become surplus to requirements, either via modernisation and upgrade or required reductions in military holdings.

The post-export diversion of components is of particular risk where there is a requirement for spare parts for existing equipment from a recipient that is no longer likely to receive these items direct from EU manufacturers. These could for example include spares for attack helicopters, combat aircraft, military vehicles or artillery systems used by countries which have become subject to an arms embargo. It is very important therefore for EU members to examine the cumulative effect of licences for spares and components issued over a period of time to ensure that exports are commensurate with the stated end-user's current stocks.

## **Levels of risk**

Some degree of risk of diversion is present with every arms transfer. Thus, in practice, states will assess the level of risk and will then balance that significance against other factors.

Member states must then decide, hopefully in cooperation and consultation in line with the spirit of the Common Position, which aspects and levels of risk can be managed through delivery and post-delivery procedures and enhanced shipment security; and which aspects and levels of risk imply a licence refusal.

However, this assumes that the member state is in a position to make a realistic risk assessment. The draft Common Position implies a commitment to deny licences if no sufficient assessment is or able to be made. Article 5 requires that "[e]xport licences shall only be granted on the basis of *reliable prior knowledge of end use* in the country of final destination" (emphasis added). If, therefore, a state is unable to

conduct a reliable assessment of diversionary risk – or if that assessment is highly ambiguous – no licence should be approved.

Different recipients of course pose different diversionary risks. It is also the case that certain types of weapons and technologies are more at risk of diversion than others. In part this relates to the level of demand for particular weapons and technologies in the illicit market. However, some elements of this difference are inherent in the weapons themselves. SALW and ammunition or items of high utility in multiple types of weapons systems (e.g. gyroscopic technologies) may be more prone to diversion than some other types of equipment.

It appears that member states also temper their response to diversion based on the perceived *consequences* of that diversion. It is questionable that Man-Portable Air Defence Systems (MANPADS) are more likely to be diverted than SALW, yet the Wassenaar Arrangement's 2003 *Elements for Export Controls of MANPADS* include a number of unique procedural conditions designed to prevent diversion. For example, paragraph 2.2 requires that "general licences are inapplicable for exports of MANPADS; each transfer is subject to an individual licensing decision" while paragraph 2.3 prohibits exporting states from using "non-governmental brokers or brokering services when transferring MANPADS, unless specifically authorised to on behalf of the [importing] government."<sup>6</sup> This would seem to be due to fears that the target of any diverted MANPAD could be a civilian airliner.

## **Access to information and co-operation among member states**

As discussed above, member states have committed to authorise transfers only where they have reliable prior knowledge of end use. Rather than exporting unless there is a reason not to, licences should be denied unless the authorities are satisfied there is no cause for concern. A lack of knowledge should result in a refusal.

### **Sources of information**

It is therefore crucial that states have access to the information necessary to inform decisions. The range of relevant sources should include:

- intelligence services;
- armed services;
- customs, police and other law enforcement services;
- diplomatic posts;
- relevant government ministries;
- end-use visits and enquiries;
- relevant regional organisations;
- UN reports;
- UN sanctions committee members;
- international peace-support operations;
- SALW tracing requests;
- EU (and other) partner governments;
- the defence industry;
- the civil aviation and maritime transportation sectors, including individual transporters and freight-forwarders etc.;

---

<sup>6</sup> Ibid.

- parliamentary visits and reports;
- media reports;
- academic studies and reports (e.g. SIPRI Yearbooks);
- NGO reports;
- other civil society inputs.

Depending on the circumstances of the particular transfer, member states would be expected to be more or less active in utilising these sources. It would not be a sensible use of limited resources to conduct exhaustive enquiries regarding straightforward transfers to trusted partners. However, where fears of diversion exist, licensing authorities should seek out information and no licence should be issued until such time as the authorities have sufficient information to make an informed decision.

Where conflicting accounts of previous diversion or future diversion risks exist, it will be up to member states to exercise judgement, based on *inter alia* corroborating evidence, the historical credibility of those involved or providing information, and external expert but disinterested opinion. It is important that during such a process the inputs of certain actors are not privileged at the expense of others simply due to their identity or status. For example, claims by recipient states should not be given greater credence than those of armed groups or civil society simply because they are states.

### **Inter-state co-operation**

Unfortunately, capacity constraints can make detailed analysis of the history or risk of diversion a difficult business, especially for smaller member states. For example, a smaller member is less likely to have a diplomatic presence in the buyer country, and if not a significant exporter of controlled goods is unlikely to have large-scale resources within ministries in the capital to devote to licence assessments. How then are the smaller states to conduct effective analyses, drawing upon all appropriate data-sources, in the face of these constraints? It is through co-operation among member states that this circle can be squared. Smaller states would have the most to gain at the 'front end' from increased co-operation (and this could extend beyond pooling information about the situation in-country and the actors – end-users, consignees, brokers, transporters etc. – involved in the transfer (see below), to carrying out delivery verification on behalf of other EU states). However, the downstream benefits for the larger member states could be significant in terms of avoiding arms transfers with a potential harmful impact on development or security, and hence upon development aid or the need for involvement in remedial security measures.

### **Information-sharing**

Member states already share information, for example through the database on licence denials and COARM discussions on particular destinations of concern. It is also becoming more common for licensing officials in different member states to consult one another on specific licence applications. While this is welcome, the systematic data-sharing should go wider and deeper, and difficult cases should not be reliant on the *ad hoc* initiative of individual officials. Implementation of criterion 7, particularly with regard to post-delivery controls, is an area where the benefits of increased information-sharing and collaboration could be immense.

In order to maximise these benefits, the information to be shared should be as sophisticated as possible. For example it may be that the destination concerned has a history of diverting small arms, but not major conventional weapons, in which case a different assessment might be made depending on the type of equipment being exported. This could be done by developing further the existing denial-notifications database within the Council Secretariat.

There may be instances where the authorising member state has concerns to the extent that special conditions are applied to transfers (e.g. the UK has in the past sought special guarantees from Israel that UK-sourced defence equipment would not be used in the Occupied Territories). Guarantees of this nature should be circulated systematically among member states. This is one example of how extra information could be shared not just in response to a particular licence denial but regarding more general diversionary concerns, and even where the member state involved may subsequently grant a licence or licences. Consideration should be given to extending such a principle, and developing methodologies for circulating information on the basis of relevance, in addition to the current narrower basis of licence denials.

Concerns have been expressed that sharing information from intelligence sources is problematic. However it is important here that best is not the enemy of better: while there may be some information that cannot be passed on, not all relevant data will have been sourced through these channels. Furthermore, intelligence information will frequently be drawn from open sources. The fact that data comes from intelligence agencies should not automatically preclude sharing. And where the information is considered particularly sensitive, it may be possible to repackage it in such a way as to protect those sensitivities.

EU states should also seek to take active advantage of the new international instrument on marking and tracing of SALW. Where member states are involved in operations that bring them into contact with confiscated weapons or disarmament processes they should log the provenance of collected weapons and, where there are concerns, tracing requests should be initiated. The results of those enquiries (including refusals to co-operate with tracing requests) should be circulated and factored into licensing assessments.

### **In-country co-operation**

Compared to pre-licensing assessments, post-transfer controls are underdeveloped in terms of criterion 7. Many EU states have extremely limited ability to institute or enforce post-transfer controls, not only because of capacity constraints but because, operating alone, they have limited leverage to apply controls where they do in theory exist. Through greater co-operation there is huge potential to develop this aspect of arms transfer controls.

Member states should share their diplomatic resources in-country. Those states with no diplomatic presence in recipient countries would benefit most, but in many cases, even where there is a diplomatic presence there will be no expertise in this area. This is often for very good reason: it makes no sense to build expertise where it is seldom needed. However, if member states could agree that wherever possible they will have among themselves at least one 'expert' to deal with this for each country (and the nationalities of these experts could be shared out as appropriate), the resource demands of such a policy need not be unmanageable. This would not

necessarily involve an expert being permanently in post, indeed in many cases it would make more sense to involve him or her only where a specific need is identified. Of course, if there are particular transfers where the authorising state does not wish for whatever reason to involve EU partners, there would be no obligation. It is also worth reiterating that it not all transfers would require delivery verification inspections or active end-use monitoring. Instead the focus must be on cases where concerns are most significant.

### **Mutual support in event of transgressions**

Another key aspect of co-operation is that where one member state becomes aware of and acts on a problem, while acknowledging that decisions are taken at the discretion of individual member states, EU partners should endeavour to operate a sympathetic policy (see *responding to problematic cases* in the section on *elements of an effective system* below). This may have implications for the system of consultation. Currently, consultations are based on avoiding undercutting of transfers of 'essentially identical' equipment to essential identical recipients. With regard to criterion 7 it may also be relevant to consult on the basis of essentially identical *arrangements* (e.g. intermediaries or transportation routes etc.).

### *Wider co-operation*

The EU has an opportunity to begin to build an international norm on post-transfer responsibilities. In most countries there has been an attitude that responsibility ends as the shipment leaves the exporter's territory. There has also been a focus on being seen as a 'responsible supplier', i.e. exporting states have been reluctant to refuse to provide follow-up support (spares, maintenance, etc.) to an initial sale as they fear it being seen as an expression of bad faith. Attitudes have begun to shift in recent years, but more needs to be done to promote the idea of the 'reliable recipient'. The US does take post-export control seriously; if the EU were to do the same, and then co-operated with the US (and others) in terms of information-sharing and a joint approach to dealing with transgressors, this would go a considerable way to establishing a new norm. As co-operation increased, the consequences for buyers permitting or participating in diversion, or refusing to co-operate with the exporting states seeking to confirm agreed end-use, would likewise increase.

## **Documentation**

Improved documentation in diversion risk-assessment at the licensing stage and delivery and post-delivery controls would not, by themselves, prevent attempts to circumvent arms transfer controls and exploit loopholes. They would however make illicit trafficking and diversion more difficult. In addition, systematic use of documentation would assist efforts to hold transgressors to account.

### **End-user certification**

End-user certificates (EUCs) and their authentication at the licensing stage should play a central role in counter-diversion policies. This is the rationale behind the reference in article 5 of the draft Common Position where it states that for an export licence to be granted, this "will generally require a thoroughly checked end-user certificate ... and/or some other form of official authorisation issued by the country of final destination."

This is complemented by the best practices on end-user certification stipulated in the User's Guide on the EU Code.<sup>7</sup> The Guide lists minimum standards on the details Member States *should* request when requesting an EUC. These include exporter's and end-user's details; the final destination country; a description of the goods being exported and their quantity and/or value; signature name and position of the end-user; the date of the EUC; and an identification of the end-use of the goods.<sup>8</sup>

In addition, the User's Guide stipulates elements Member States *may* require in an EUC. These concern conditions on end-use and re-transfers a Member State may impose at the licensing stage, including a clause prohibiting re-export of the goods. Less restrictive, an EUC may make *any* re-exportation – or re-exportation to countries other than those previously agreed on – subject to prior written consent of the exporting state. There may also be a specification that the goods being exported will not be used for purposes other than the declared end use.

A further best practice referred to in the User's Guide stipulates that authorities of the exporting country may authenticate the signature on EUCs issued by the government of the destination country and the capacity of the signatory to make commitments on behalf of their government.<sup>9</sup>

While offering a good base for a strengthened EU policy to counter diversions and undesirable re-exports, it is noteworthy that article 5 of the draft Common Position refers only to a *general*, rather than universal, requirement for some kind of end-use documentation. Under this formulation, it would seem that national discretion about when end-use documentation is required is total.

There are compelling arguments that a requirement for end-use documentation should never be waived, but if member states have in mind circumstances where such certification is not required, this should be agreed and made publicly explicit (probably in the User's Guide). It is easier to imagine occasions where authentication of end-use documentation might be foregone, for example where the end-user is the government of another EU member state and the licensing government has other reasons to be confident that the end-use undertakings are legitimate. However, once again these situations should be elaborated and made publicly available, and member states should in any event always reserve the right to verify that the end-use documents are authentic.

EU member states should also adopt a systematic policy on the use of re-transfer and end-use conditions. This should as a matter of course include a prohibition on re-export without permission from the original licensor state. However, once again, if member states are unwilling to institute such a measure, they should at the very least identify the situations under which EU member states will impose such conditions. Certainly, member states should insist that end-use and re-transfer controls will apply to any goods produced as a result of the transfer under the authority of an EU member state of production technology or equipment. In

---

<sup>7</sup> User's Guide.

<sup>8</sup> *Ibid.*, page 18, chapter 2, section 1, points 2.1.1-2.

<sup>9</sup> *Ibid.*, point 2.1.3.

addition, greater use should be made of guarantees that place restrictions on the uses to which the equipment will be put.<sup>10</sup>

For transfers not requiring an EUC, there should still be a requirement for some form of prior written notification from the country of final destination. This notification should state that the import has been authorised by the importing country or that the relevant authorities in the importing country have been made aware of the potential transfer.

### **Delivery verification**

Another area that is underdeveloped in EU export controls is the absence of high common standards on transport security and verification. Notably, EU member states have adopted such a policy within the OSCE and Wassenaar Arrangement in relation to exports of MANPADS. Specifically, these fora have committed to ensure high 'levels of protection and accountability' for transfers. Relevant practices encouraged in these forums include a requirement that the recipient government provides a "written verification of receipt of MANPADS shipments".<sup>11</sup>

EU member states would ideally apply such high levels of protection and accountability, including delivery verification certificates, to all exported equipment. At a minimum, they should identify situations when delivery verification certificates would be obligatory. One obvious example would be where SALW and related ammunition are authorised for exports to end-users neighbouring zones of conflict. Nevertheless, delivery verification certificates should in no way replace the obligation to deny an export authorisation if there is a clear diversion risk.

Responsibility for obtaining delivery verification certificates, signed by the relevant authorities in the importing country, should rest with the exporter. Indeed, member states should hold companies applying for export licences legally responsible for the entire delivery process. Where necessary, transfer control legislation should be amended to ensure that legislative jurisdiction can be applied to the whole shipping process and companies named on the original licence application are legally responsible for the entire consignment until delivered to the stated end-user.<sup>12</sup>

Note that delivery verification measures should also include provision for physical inspection to confirm that the types and quantities of equipment arriving in the country of final destination and at the end-user correspond to those authorised for export/import and recorded in shipping documents. This should extend to verifying that, for example, not only a particular container but also the container's *contents* have arrived at their authorised destination.

---

<sup>10</sup> A relevant example is the condition linked by the UK to arms exports to Israel that the equipment will not be used in the Occupied Territories, and to Indonesia that the equipment will not be used in Aceh (Interviews, UK Department for Trade and Industry, April 2005).

<sup>11</sup> See OSCE, *Principles for Export Controls of [MANPADS]*, 2004, para. 2.7, ([http://www.osce.org/documents/fsc/2004/05/2965\\_en.pdf](http://www.osce.org/documents/fsc/2004/05/2965_en.pdf)); and Wassenaar Arrangement, *Elements for Export Controls of [MANPADS]*, point 2.9.

<sup>12</sup> An example for such in-built measures is provided by Belgian practices. As a means to enhance delivery security, Belgian legislation requires that licences for brokering transactions are conditional on the payment of a deposit by the broker to the Belgian authorities. The deposit is paid back after the completion of the operation and the receipt of a delivery verification certificate, or after the voluntary cessation of operations under an indeterminate licence (*Law of 25 March 2003*, amending art. 10.3 of the Law of 1991).

Governments and industry could consider making greater use of commercial transfer inspection companies in providing delivery tracking services, documentation verification, and conducting physical pre-delivery and delivery verification. These companies already operate globally across a broad range of commercial trade sectors, including agricultural, mining and consumer goods markets.<sup>13</sup>

### **Registers of those involved in trade activities**

Attempts to counter risks of diversion would benefit from a registration requirement for the main actors involved in arms transfers and transportation, i.e. exporters, brokers, transportation and financial agents, without which they would not be entitled to engage in arms transfer activities. Registration, especially when combined with strict record-keeping requirements, would enable states to build a much more detailed picture of how the arms-trade functions. It would also make it easier to keep the sector informed of transfer control developments, and to delegitimise those whom member states deem to be acting inappropriately. Information on those who are refused registration or are struck off should be circulated to all member states. Informing partners that certain entities will not be permitted to be involved in arms transfers sends a very different and much more powerful message than a licence denial.

Several EU member states already operate such a registration system as a gateway to engage in legal arms trade activities.<sup>14</sup> Relevant actors therefore have to obtain a registration in the country where they are resident or established, and, in some cases, also from the countries of which they are a national. However, with a few exceptions, actors involved in the transport of military equipment outside the territory of the country where they are resident or established fall outside the scope of existing registration requirements.<sup>15</sup> So where evidence of undesirable activities by transportation agents is discovered, there may not be the legislation or regulation required to hold them accountable for those activities.

### **Responsibility of industry**

In addition to the extension of company responsibilities to cover the whole delivery process (see *delivery verification* above), governments should develop, with industry and other stakeholders, clear guidelines for responsible behaviour by industry. This should include a 'know your customer' policy. A good basis for such guidelines is provided by the List of Advisory Questions for Industry, adopted in the Wassenaar Arrangement in 2003. This list contains questions intended to "give guidance to when suspicion should be raised and a contact with national export licensing authorities might be advisable", such as whether the customer is reluctant to provide an end-use statement, or was previously unknown to the exporter.<sup>16</sup>

---

<sup>13</sup> 'Marking and Tracing Small Arms and Light Weapons: Physical Inspections', *COTECNA*, published by GRIP, June 2004, <http://www.grip.org/bdg/g4545.htm>. COTECNA is a global trade inspection service (see <http://www.cotecna.com/>).

<sup>14</sup> Examples of EU member states with a registration requirement for brokers are Belgium, the Czech Republic, Estonia, France, Hungary, Italy, Latvia, Lithuania, Malta, Poland, Slovakia, Slovenia, and Spain (see GRIP. 2005. 'Implementing the EU Common Position on the control of arms brokering: progress after two years', Holger Anders, *GRIP*, July 2005, annex B, <http://www.grip.org/bdg/g4579.html>).

<sup>15</sup> One such exception is Germany, which requires transport agents to obtain a general authorisation for transfers of weapons of war between third countries if the weapons are transported on ships sailing under German flag or on air carriers registered in Germany (War Weapons Control Act of 20 April 1961 (as amended)., arts. 4.1 and 4.a.1-2).

<sup>16</sup> See 'List of Advisory Questions for Industry', *Wassenaar Arrangement*, 2003, <http://www.wassenaar.org/2003Plenary/Final%20Questions%20for%20Industry.doc>.

It should be noted that industry in several EU member states already reports suspicions related to diversion risks.<sup>17</sup> Guidelines for industry should therefore seek to consolidate and further build on such existing good practices. However, it is incumbent upon member states to respond appropriately to issues raised by companies, and there are concerns that this is not always the case.<sup>18</sup>

### **Elements of an effective system:**

An effective elaboration of criterion 7 will specify the elements necessary to assess and minimise the risk of diversion. Measures should be applied at all stages of the transfer process, from pre-licensing through to post-delivery. In addition, states must also develop appropriate responses where problems are identified.

#### **Licence processing**

As noted previously in this paper, criterion 7 does not contain an instruction to deny licences on the basis of a risk of diversion. This should be rectified at the earliest opportunity, but in the absence of textual changes to the criteria themselves, it should be clearly specified in the implementation guidelines that such is the case.

Transfer licences should not be issued without adequate checks on accompanying EUCs. While developing robust best-practice guidelines for the end-use certification process may well be outside the scope of criterion 7 elaboration, the two processes are complementary. All EUCs should be checked by the appropriate embassy and the relevant details verified. Where a particular member state does not have a presence (via embassy and diplomatic posts) in the recipient country, they should be able to draw on the assistance of other EU members who have such capacity. At a minimum, if there is insufficient capacity to verify licensing documentation in this manner, the licensing authority must have established direct contact with the stated recipient before any licence approval is granted.

All licences issued should include a legally-binding requirement that equipment must not be diverted or re-exported without the express permission of the original licensing authority. They should also clearly specify the right to carry out physical compliance checks and that penalties and sanctions will be imposed where breaches occur. In order to harmonise policy in this area, as well as help develop best practice that might also inform practice elsewhere, EU members should agree standardised wording to this effect for all transfer licences issued by EU member states.

Criterion 7 elaboration must also complement controls over traffickers and brokers. In order to procure equipment for terrorist organisations, or to embargoed destinations or other illicit end-users, arms traffickers often operate in complex networks, utilising a myriad of front companies, shipping and handling agents. EU

---

<sup>17</sup> An example is a recent case in the UK where an exporter became suspicious when, just prior to export, the presumed end-user, who was non-Iranian customer located outside Iran, specified that markings on the shipping and transportation containers should be done in Farsi. This unusual request was reported by the exporter to the British licensing officials and helped prevent a potential diversion of UK exported military equipment (Interview, British Defence Manufacturing Association, 2 October 2005).

<sup>18</sup> A recent story in the Observer examined the case of 20,318 Beretta 92S guns transferred into Iraq for use by the police via the UK which have since turned up in the hands of al-Qaeda terrorists. It seems that despite the UK arms dealers involved in the transfers finding the eventual diversion completely unsurprising, the UK Government was happy to authorise the transfer. See Mark Townsend & Barbara McMahon, 'UK guns in al-Qaeda hands', *The Observer*, 19 March 2006, <http://www.guardian.co.uk/alqaida/story/0,,1734350,00.html>.

members should rely on advice from *inter alia* relevant intelligence agencies to ensure that they are not unwittingly issuing export licences under these circumstances. This is an area where wider EU and international co-operation is imperative, given the global scope of arms trafficking networks.

To assist the process further, EU members should collate and share – ideally through the EU export licensing data-base – details of cases of diversion or suspected diversion or any other relevant information that will help licensing authorities identify problematic cases. Given the particular diversion risks associated with brokers and traffickers, such information should also contain information on trafficking networks and the individuals and companies behind them (see the ‘red-flag’ indicators below).

Criterion 7 is also extremely relevant to the export of components for ‘incorporation’ into finished systems, especially where these finished systems are exported to countries of concern. It is important, therefore that the licensing authority has full records, including diagrams, photographs or other relevant details of the finished product in which components are for use. Licences should not be issued without this information, as well as other relevant details such as export markets for the finished system. Details of weapons systems containing EU-sourced components should also be circulated to relevant diplomatic posts, so that cases involving the diversion of these goods to un-authorized end-users can be easily identified.

*Tools to assist risk assessment at the licence processing stage*

Following on from work already undertaken within the Wassenaar Arrangement and from best practice developed by the US under its Blue Lantern Scheme<sup>19</sup>, EU member states should develop a series of ‘red flag’ indicators to assess risks of diversion at the licence processing stage. Such indicators are a useful checklist for individuals processing export licences. While not an exhaustive list, the following questions would be essential to include in such a system:

- Is the equipment for export consistent with the requirements for that end-user, either for weapons type, quality or quantities for export? Is the equipment or technology consistent with the existing inventories in the recipient state? If the weapons are from surplus stock, are they of sufficient quality for the regular armed forces of the country (weapons diverted to armed groups in neighboring conflict zones are often relatively old, cheap and of fairly poor quality and generally of a kind and condition not suitable for use by regular armed forces)?
- Does the country of final destination or any part of the transportation route border a conflict zone, or a country subject to an arms embargo of any kind?
- Does the country in question have military forces active in neighbouring conflict zones? Where such engagement is denied by the recipient government, is involvement reported in the media, identified in UN or other credible reports or via an assessment by relevant information sources including intelligence agencies?

---

<sup>19</sup> Wassenaar Arrangement, <http://www.wassenaar.org/>; and Office of Defense Trade Controls, Bureau of Political-Military Affairs, ‘Blue Lantern: A Guide to End-Use Checks of Commercial Defense Exports,’ US Department of State, 1996.

- Does the country have links – official or unofficial – with non-state actors or governments fighting in neighboring conflict zones? Where such engagement is denied by the recipient government, is involvement reported in the media, identified in UN or other credible reports or via an assessment by relevant information sources including intelligence agencies?
- Does the end-user have links to armed groups, military or security forces whose actions are such that they would likely be refused permission under the criteria as set out in the draft Common Position to purchase the items themselves? Where such links are denied, is involvement reported in the media, identified in UN or other credible reports or via an assessment by relevant information sources including intelligence agencies?
- Is the final destination of the transfer or any part of the transportation route in close proximity to a significant black market in the equipment to be transferred?
- Are there any difficulties in verifying the details of the transfer? Are the financial details of the deal transparent and straightforward and is the value of the contract commensurate with the equipment type and quantity?
- Are intermediaries involved in the transaction? Do any of the shippers or brokers involved in the transfer have any history of illicit arms delivery? Are they named as problematic in UN reports or other credible documents, including NGO research and media reports? Are they suspected of links to terrorist or organised criminal networks?
- Have any of the companies involved in the transfer been formulated (as '*brass plate*' companies) in an offshore territory with a history of registering companies implicated in arms trafficking? Is it difficult to identify full company details, for example company address and the names of directors? Is the company address listed as a PO Box, or are there a number of other companies registered or operating from the same address? Does the company appear to be incorporated via a specialised offshore incorporation company, whose address is given when specific company details are requested?
- Does the shipper have any links, including informal links to other notorious arms trafficking networks, either via company ownership, aircraft registration or personnel?
- Does the country of stated end-use have any history of diversion of arms, including the re-export of surplus equipment to countries of concern?
- Does the recipient country apply effective transfer controls? Is there a robust and accountable government process to control the import, export and storage of military goods, including management of government stockpiles? Does the recipient government apply any normative criteria to judge transfer licensing decisions (cf. EU Code of Conduct, OSCE guidelines etc.)? Is there the capacity and the will to enforce the systems that are in place?

- Transparency is an important pre-requisite to an effective and robust export control systems. Does the recipient country report to the UN Register of Conventional Arms; if not, why not? Does it maintain good records of export licensing, imports and exports and inventories of national holdings and stockpiles? Is this information readily obtainable, and if not, why not?
- What is the level of corruption in the recipient country and among the various actors involved in the transfer?
- Is there an effective and thorough system of transit controls in each state through which the goods in question are scheduled to pass?
- Is stockpile management and security of a sufficient standard?

*Controls applied to the shipping process*

These recommendations start from the premise that with 21st century technology, including global communication systems, it should not be possible for licensed goods supplied directly from EU member states to be diverted to unauthorised end-users during the shipping process. That said, there are a number of measures that should be applied to make this system as watertight as possible.

A key conceptual problem with controls over the movement of licensed goods is that it appears that the physical delivery of weapons *does not* form part of the transfer control process. Once the goods are in transit (i.e. have left the jurisdiction of a particular country), the only controls applied are those relating to commercial, technical and administrative procedures utilised for the general international movement of freight.

Clearly, transfer controls should be applied to the whole of the transaction, from the issuing of the licence through to the physical delivery of the equipment to the stated end-user.

Companies receiving licences should be legally responsible for the entire delivery process, including verification that all goods specified on the licence arrive at the stated end-user.

Exporting companies should be required to report back to the licensing authority against all deliveries made under any licence application. This should be done within a specified time limit – for example 21 days from the date of delivery – with strict penalties applied for not meeting these obligations.

This verification should include, but not be limited to, confirmation from the relevant customs authority at ports and airports that the consignment has reached the stated end-use country, as well as verification that the goods have arrived at the stated end-user. It should be noted that every import and export is already automatically logged, recorded and authenticated by customs authorities as part of revenue generation and information processed for trade-statistics purposes, so it should be straightforward to provide this as part of the transfer control process. However, the information routinely provided by customs officials is often insufficient for keeping track of weapons transfers as it does not include information specific to individual weapons or components. A comprehensive inventory at the

start and end of a transfer is ultimately necessary to ensure that no diversion occurs *en route*.

Member states should ensure that transfer-licence processing systems, including databases and computerised records for export licensing, are specially designed to collate and verify delivery information. They should also ensure that reporting systems are modified (where necessary) to ensure this information is made available as part of EU members' obligations to publish reports on strategic exports.

While it is not always possible to specify the shipping and handling agents on the original licence application (as these may not be known at the time) no consignment of licensed goods should leave any EU territory without all those involved in the delivery process being authorised by the licensing authority. This is to ensure that established arms trafficking networks are not unwittingly hired to ship arms from EU member countries. As well as raising several moral and ethical issues, the risks of diversion are increased dramatically by making use of such companies. As proposed in the EU Common Position on Arms Brokering, EU member states should also consider establishing a register of transportation companies, and developing best practice procedures that specify that only registered companies can be used to transport controlled goods.

#### *Transit and brokering*

Given clear evidence that poorly regulated arms brokering activities are a major contributory factor for diversion of arms to unauthorised end-users, it is also vital that controls on transportation developed by EU member states are applied to arms brokering activities by companies or individuals based in or from EU countries.

In addition, it is important to ensure that EU countries are themselves not used as points of diversion during weapons transit. Many countries within the EU are hubs for international transport by road, sea or air. It is imperative that all shipments of arms and licensed equipment entering EU territory and the documentation therefor are physically verified before being allowed to transit through EU member states.

Member states should ensure they have sufficient legal powers to impound any suspect shipment or aircraft whilst documentation is checked. Where irregularities are identified, necessary legal powers should be established to ensure that companies and individuals involved can be prosecuted, even when they do not originate from EU member countries.

#### *Post-delivery verification*

An effective system of on-site verification and monitoring is likely to provide a strong disincentive to divert because of the increased risk of discovery. As stated above, the right of the licensor government to carry out such inspections should be a mandatory element of all licences issued by all member states. Ideally, all member states would apply the same high standards, so as to ensure that the whole EU 'space' becomes a bastion against diversion. Of course it would not be practical, or even desirable, to check every export in such a way. But to be an effective deterrent against diversion, the EU needs to develop a formal post-delivery verification system, and this system must be clear to anyone in receipt of military equipment exported by EU members.

As the EU Code is a risk-based system, member states should prioritise the indicators or concerns that would trigger a physical inspection process. Wherever the line is drawn, there will be marginal cases where although there may be concerns of a diversion risk (for example based on past behaviour of a previous administration in the destination country) the decision is still taken to issue a licence. In such circumstances, the benefits of applying a formal compliance checking system should be clear.

As with checking the information in EUCs, member states should pool resources where necessary, for example by utilising military attachés or other diplomatic posts from other member states where physical inspection is deemed necessary but where the authorising state has no capacity to undertake this activity.

In terms of the checks required during this stage, the exporting state should check exactly when the consignments arrived; when they were received and by which officials and at which ports; and whether the consignment is stored in a secured and authorised site.

### **Responding to problematic cases**

Developing a coherent response to diversion risks is difficult at the national level, let alone across the 25 states of the EU. But it is crucial that where problems are identified, member states send a clear message that diversion is taken very seriously, that consequences will follow, and that the EU speaks with one voice on the issue. When assessing what the consequences should be, the following questions should be considered:

- Is this a 'new' risk, i.e. are concerns centred purely around the prospect of a future diversion, or is there knowledge or suspicion of previous diversion or unauthorised re-export?
- If the latter, is there repeated or a pattern of (suspected) diversion, or is it a one-off?
- What is the scale of the (suspected) diversion and the type and range of equipment involved?
- What is the level of credibility of the information upon which concerns are based? How confident is the authorising state that concerns are justified?
- Does the (suspected) diversion raise issues of active complicity of the state, or is it more a case of slack controls/poor capacity?
- Is the recipient state co-operating with efforts to establish the facts? How far does this co-operation extend? For example, if the recipient state is allowing monitoring visits, what freedom of action/movement/etc. are the monitors allowed?
- Does the recipient state appear committed to addressing the problem? Does it have the capacity to address the problem? Is it willing to accept remedial assistance from the EU or its member states? What constitutes reformed behaviour?

While keeping in mind that decisions and responses are to be based on assessments of risk, when determining the appropriate response, a distinction should be made between cases where concerns are limited to suspicion of future diversion or misuse

and cases where incidents have already occurred, and between one-off risks and patterns of irresponsible behaviour.

#### *Suspicion of future diversion*

Where there are fears that a proposed transfer poses a new diversion risk, in addition to the licence application being refused, other member states should be informed of the aspects of the deal that gave rise to the diversionary concerns and should treat subsequent licence applications that raise the same issues as 'essentially identical transactions' (EIT). It is likely that in some circumstances this would be an extension of the current general understanding of an EIT, however this would take account of the peculiar characteristics of criterion 7.<sup>20</sup> This should continue until such time as the circumstances which prompted the original assessment have changed. Member states may wish to communicate their concerns to the 'problem' recipient, and potentially offer to help institute remedial measures. The benefit of this would be to facilitate a co-operative approach to dealing with diversionary concerns.

#### *Responding to actual instances of diversion*

Where member states have reason to believe that diversion has taken place, there are a number of additional steps that could be taken. Dependent on the answers to the questions above, member states must then decide on an appropriate response (note that if the diversion were of items transferred against a licence issued by a member state, the initial response should be to cancel that licence forthwith). While in the most egregious cases a *de facto* embargo may be appropriate, it is unrealistic and potentially unhelpful to expect a breach of criterion 7 to always result in a blanket ban on exports to that state of all controlled goods and technology. In less severe cases, but where there are still concerns about a pattern of offending, it may be more sensible to apply a 'selective embargo', whereby licences for certain types of equipment and/or to certain end-users within a country are automatically refused. The next step down would be to require specific guarantees regarding end-use for named equipment and/or to named end-users, with explicit provision for delivery verification and end-use monitoring measures and with the understanding that inspections will take place. Of course, where these 'intermediate' sanctions are in place, each licence application should still be subject to the standard criterion 7 assessment as applied to all licence applications.

In terms of determining how and when 'special measures' should be discontinued, it is recommended that member states consider the options above as a 'staircase', which recipient states would negotiate one step as a time. That is, for the less serious problems, it may be the only restriction relates to the specific guarantees, after which the recipient state returns to 'normal' status. But for the worst cases, which result in *de facto* embargo, progress would result in a shift to selective embargo status, and then to the use of specific guarantees.

Time alone should not be enough to permit states to move down the 'steps'. There would need to be evidence of co-operation with the member state(s) concerned and of substantive progress in addressing the problems that led to the (suspected) diversion. The nature of that co-operation and the required remedial action would

---

<sup>20</sup> One example of how member states might extend the concept of EIT and thereby the consultation process would be to take into account intermediaries and/or transport routes in cases where the initial licence refusal was on the basis of concerns about *en route* diversion.

depend on individual circumstances. For example, if the problem involved leakage of SALW from army stockpiles, there would need to be measures to tighten stockpile security. If the problem lay with a particular arms brokering company, that company's activities would need to be constrained and legal redress taken as appropriate. If it were a case of rogue licensing officials, they should be removed from post and possibly prosecuted, but there would also need to be a review of procedures to prevent a repeat. Where there was evidence or suspicion of high-level political involvement, the response would need to take place at the political level.

#### *Co-operation among EU member states*

Except in cases of multilateral embargo, arms transfer licensing decisions are taken at national discretion. It will therefore be the case that unless a concern about diversion or unauthorised re-export is so severe as to lead to embargo, a change in transfer policy by one member state will not necessarily be matched by the same change in other member states. However, it is consistent with the aims set out in the preamble to the EU Code/draft Common Position that members should respond sympathetically to a change in policy based on concerns about diversion by one of its partners.

Following on from the methodology set out above, when a member state changed policy with regard to a specific destination or end-user on the basis of diversion concerns, that member state would then advise all other EU states of this change and the reason for it. At this point, it is to be hoped that other EU states would reconsider their own policy. It may be that the other member states would not choose to follow the first member, but it is to be hoped that they would at least move to within one 'step' of them. So, for example, if one member state were to put in place a *de facto* embargo against a recipient state, others should respond similarly or by putting in place a 'selective embargo' (one step down). Those member states that do not do so should circulate the rationale for their decision.

Member states should also co-operate in terms of helping (if appropriate) recipient states take remedial action or at least in terms of feeding back information about whether the required action has been taken.

## **Conclusion**

The complete elimination of the risk of unwelcome diversion of controlled goods is an unlikely prospect. But in the current environment, whereby most states, including those of the EU, have been slow to acknowledge their post-transfer obligations, arms can all too easily be diverted to inappropriate users and for nefarious purposes. The elaboration of guidelines for the more effective implementation of criterion 7 of the EU Code/draft Common provides an ideal opportunity for EU member states to address this problem, and the recommendations contained in this paper set out a number of practical ways in which the current EU regime could be improved and the risk of diversion minimised. It is hoped that in elaborating criterion 7, rather than merely codifying existing practice, member states will draw upon the recommendations herein to minimise the risks of diversion which result in breaches of any of the other criteria.