ANTI-DIVERSION MEASURES: Real-Time Locating Systems

By Peter Danssaert

IPIS

COLOPHON

Title: Anti-Diversion Measures. Real-Time Locating Systems

Antwerp, April 2019.

Cover picture: Lt. Col. Brad Culligan, 838th Trans. Bn. (U.S. Department of Defense)

International Peace Information Service (IPIS) vzw is an independent research institute providing governmental and non-governmental actors with information and analysis to build sustainable peace and development in Sub-Saharan Africa. Research is centred around four programmes: Natural Resources, Business & Human Rights, Arms Trade & Security, and Conflict Mapping.

Author: Peter Danssaert

D/2019/4320/ 01

TABLE OF CONTENTS

ANTI-DIVERSION MEASURES: Real-Time Locating Systems

Diversion is largely a self-inflicted problem that stems from negligence by states, militaries, and civilians (Small Arms Survey, 2008).

The illicit trade of small arms and light weapons remains a serious problem internationally and in many countries. The European Union expressed its concerns as such "Illicit firearms and small arms and light weapons (SALW) continue to contribute to instability and violence in the European Union, in its immediate neighbourhood, and in the rest of the world. Illicit weapons are fuelling global terrorism and conflicts, thwarting the EU's development and crisis-management, humanitarian and stabilisation efforts in parts of the EU's neighbourhood and Africa. Within the EU, illicit firearms have a clear impact on internal security, by fuelling organised crime and providing terrorists with means to carry out attacks on European soil".[1] To prevent the illicit trade States call for responsible arms export control systems to be put in place. One solution is to prevent diversion. Mostly limited to an assessment of the risk of diversion prior to export, and the insistence on the use of a robust stockpile management system by the recipient.

This paper highlights the use of Real-Time Locating Systems (RTLS) as a possible option to combat some forms of diversion. The newer active radio-frequency identification tags use global navigation satellite systems and the mobile telephone network to transmit their location. RTLS allows for a breadcrumb trail in the supply chain from the beginning all the way to the final recipient.

The use of RTLS to track and trace shipments should not be confused with "track and trace" method that has developed in the literature and in State practice regarding the regulation of small arms and light weapons (SALW)[2] including firearms.[3] This method comprises, firstly, the systematic marking of small arms and light weapons with unique serial numbers and symbols or letters, which identify the manufacturer (art. 8(a) ITI). The International Tracing Instrument (ITI),[4] requires "appropriate simple marking on each imported small arm or light weapon, permitting identification of the country of import and, where possible, the year of import" (art. 8(b) ITI). When SALW are transferred from government stockpiles to permanent civilian use marks are applied "permitting identification of the country from whose stocks the transfer of the small arm or light weapon is made" (art. 8(c) ITI). The ITI also requires comprehensive record keeping of all marked SALW manufactured, exported and imported in each State's territory. Thus, the basic "track and trace" idea is that when SALW or their ammunition are seized from suspected criminals, or retrieved in the field because the items are related to a crime or present a danger to the public, the markings on the weapons should help lead law enforcement authorities to the manufacturer, government stockpile, importer and/or exporter from where the authorities can determine the provenance of the weapon and if possible its chain of custody. A similar methodology has been used to mark and trace the provenance of ammunition.[5] The limitation of this approach is simply that it is designed in each

1 Working paper submitted by the European Union, Third United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, New York, 18-29 June 2018 (A/CONF.192/2018/RC/WP/EO/3).

2 See in particular Parts III, IV and V of the United Nations General Assembly (2005). International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner Illicit Small Arms and Light Weapons [International Tracing Instrument, ITI], A/60/88 of 27 June (annexe) adopted by the General Assembly in resolution 60/519 of 8 December.

3 United Nations General Assembly (2001). Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, Supplementing the United Nations Convention against Transnational Organized Crime ('UN Firearms Protocol') adopted by the General Assembly in resolution A/RES/55/255 of 8 June. Article 12, paragraph 4, of the Protocol requires States parties to cooperate in the tracing of firearms that may have been illicitly manufactured or trafficked, and this cooperation must include the provision of prompt responses to requests for assistance in tracing such firearms.

4 United Nations General Assembly (2005). International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner Illicit Small Arms and Light Weapons [International Tracing Instrument, ITI], A/60/88 of 27 June (annexe) adopted by the General Assembly in resolution 60/519 of 8 December.

5 Marking and recordkeeping, Modular Small Arms Control Implementation Compendium (MOSAIC 05.30:2012(E)V1.0), United Nations, 2018.

case to only begin after the diversion or other illicit trade has already taken place and been discovered.

Here, it is proposed that, in addition to the post-facto 'track and trace' method, it is now feasible to track and trace entire shipments of SALW and related items in real time, and thus make it possible for the authorities to take action as soon as the diversion takes place. In any case systematic marking and record keeping of all SALW is essential for post-facto 'track and trace' and can enhance the effectiveness of 'real time location systems' making it more difficult to divert weapons to unauthorized users or for unauthorized use.

1. DEFINING DIVERSION[6]

The Arms Trade Treaty (ATT) requires each State Party involved in the transfer of conventional arms to take measures to prevent the diversion of those arms. The Treaty does not offer a definition of diversion or many other key terms in its provisions, because the ATT text was the result of a complex political consensus. However, the preamble of the ATT does provide some clue what diversion might entail: "to prevent... diversion to *the* ***illicit market***, or for ***unauthorized*** end use and end users, including in the commission of terrorist acts."

Nevertheless, some States have defined the concept of 'diversion' in their national regulations and official guidance.[7] For example, the United States Government Accountability Office defines diversion as "the transfer or release, directly or indirectly, of a good, service, or technology to an end user or an intermediary that is not an authorized recipient of the good, service, or technology"[8]. The United States Department of Commerce's Bureau of Industry and Security (BIS) uses the term 'unlawful diversion' as follows: "Unlawful diversion occurs when an item intended for an authorized end-use and end-user is instead directed toward an unauthorized end-user for an unauthorized end-use."[9] This definition implies the existence of "lawful diversion" (for example the lawful re-routing of a shipment because of unforeseen circumstances). In the literature diversion has a general negative connotation, usually linked to some form of illicit act. I would prefer to keep it like that, and stick to diversion at one end and "lawful re-routing" at the other end. The Small Arms Survey recently defined diversion as "a delivery to an unauthorized end user or unauthorized end use by an authorized end user."[10]

To summarize: in literature diversion in the arms trade is seen as the unauthorized or unlawful re-direction of arms or a related item intended for an authorized end-use(r) toward an unauthorized end-user and/or unauthorized end-use.[11] According to Casey-Maslen[12] "unauthorized" refers to "not simply the movement of arms from the legal to the illicit sphere, but is rather the unauthorized change in possession or use". In my opinion there is an over-reliance on the concept of "unauthorized". In all these interpretations "unauthorized end user" is exclusively interpreted from the perspective of the exporting State. A transfer could be authorized by the exporting State, but in my opinion still be illegitimate according to the laws of the importing State. This line of reasoning is reflected in the preamble of the ATT where it says that the State parties "re-affirm … the sovereign right of any State to regulate and control conventional arms exclusively within its territory, pursuant to its own legal or constitutional system".[13] Paragraph 7 of the guidelines for international arms transfers in the context of General Assembly resolution 46/36 H of 6 December 1991 defined illicit arms trafficking as "that international trade in conventional arms, which is **contrary to the laws of States and/or international law**".[14] Thus if arms are transferred contrary to

6 Defining diversion was discussed at length with my colleague Brian Wood who was so kind to let me review his paper on diversion. For further discussion see also: P.A. Arrocha Olabuenaga, C. Gramizzi: Article 11 – Diversion. In: C. Da Silva, B. Wood (eds): *Weapons and International Law: The Arms Trade Treaty, Law Annotated*. Larcier, Brussels, 2015: p. 191-201; S. Casey-Maslen, A. Clapham, G. Giacca, S. Parker: *The Arms Trade Treaty: A Commentary*. Oxford University Press, Oxford, 2016: pp. 342-365.

7 See for instance 22 U.S. Code Subchapter III – Prevention of Diversion of Certain Goods, Services, and Technologies to Iran; .

8 *Export Controls: Compliance and Enforcement Activities and Congressional Notification Requirements under Country-Based License Exemptions*. United States Government Accountability Office, GAO-13-119R, 16 november 2012.

9 *BIS "Best Practices" for Industry to Guard Against Unlawful Diversion through Transshipment Trade.* Bureau of Industry and Security (BIS), U.S. Department of Commerce, 31 August 2011.

10 *Arms Transfers Dialogue: First Meeting - Diversion of Arms*. Small Arms Survey/UNIDIR, Geneva, 1 February 2017

11 P.A. Arrocha Olabuenaga, C. Gramizzi: p. 192; S. Casey-Maslen, A. Clapham, G. Giacca, S. Parker, 2016: p. 349.

12 S. Casey-Maslen, A. Clapham, G. Giacca, S. Parker, 2016: p. 349.

13 F. Felsenstein, I. Güzel, S. Hoti, F. Roosens, A. Syknej: *Non-State Actors and Transfers of Arms: The Issue of Diversion*. Legal Clinic IPIS, Universiteit Antwerpen, 2018, 7 p. The Security Council can overrule sovereign rights in particular limited circumstances as spelled out in the UN Charter – arms embargoes, sanctions etc.

14 Report of the Disarmament Commission. UN General Assembly, Official Records · Fifty-first Session Supplement No. 42 (A/51/42), Annex I. Article 6 ATT: A State Party shall not authorize any transfer of conventional arms covered under Article 2(1) or of items covered under Article 3 or Article 4: 1) if the transfer would violate its obligations under measures adopted by the United Nations Security Council acting under Chapter VII of the Charter of the United Nations, in particular arms embargoes; 2.) if the transfer would violate its relevant international obligations under international agreements to which it is a Party, in particular those relating to the transfer of, or illicit trafficking in, conventional arms; 3.) if it has knowledge at the time of authorization that the arms or items would be used in the commission of genocide, crimes against humanity, grave breaches of the Geneva Conventions of 1949, attacks directed against civilian objects or civilians protected as such, or other war crimes as defined by international agreements to which it is a Party.

the laws of the importing or exporting State that trade enters the illicit market. This is made clear in the guidelines for international arms transfers in the context of General Assembly resolution 46/36 H of 6 December 1991 which emphasized that an exporter should require an import licence to prevent diversion of arms to unauthorized destinations and persons.[15] The issuance of the import licence here is the explicit consent by the importing State that the transfer has been authorized also by the importing State.[16]

Likewise arms transferred contrary to international law enter the illicit market, and therefore, seen as diversion. This would include arms embargo violations. Note that article 6(2) ATT emphasizes that States Parties shall not authorize arms transfers that would violate its relevant international obligations under international agreements to which they are a Party. Thus for example parties to the 2005 International Tracing Instrument (ITI)[17] would, according to article 6 of the International Tracing Instrument, be in violation if (a) they are transferred in violation of arms embargoes decided by the Security Council in accordance with the Charter of the United Nations, and (b) they are transferred without a licence or authorization by a competent national authority. The competent national authority being here those of the exporting and importing State.[18]

Based on the above "unauthorized end use" needs to interpreted as the illegitimate use of the transferred weapons, thus contrary to national or international law. For instance the use of weapons in the violation of international humanitarian law or human rights law need to be seen as unauthorized end use. It should be noted that article 6(3) ATT prohibits the transfer of conventional arms covered under article 2(1) ATT or of munitions and parts and components for those conventional arms covered under article 2(1) if the State Party at the time of authorization has knowledge that the arms or items would be used in the commission of genocide, crimes against humanity, grave breaches of the Geneva Conventions of 1949, attacks directed against civilian objects or civilians protected as such, or other war crimes as defined by international agreements to which it is a Party.

The following definition of diversion is proposed[19]:

Diversion", for the purposes of the Arms Trade Treaty, is 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.

1. *Such diversion can occur through the transfer of the items into the illicit market, or to an unauthorized or unlawful end user or for an unauthorized or unlawful end use.*
2. *The re-routing and misappropriation of the items can take place at any point in the supply chain, including the export, import, transit, trans-shipment, storage, re-activation or re-transfer of the items.*
3. *The transaction chain 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.*

At present it is not known how many conventional weapons and munitions are entered into the illicit market through unlawful redistribution by governments. However, there are numerous ongoing credible reports of illicit redistribution and acquisition, for example in the UN investigative reports on Security

15 Report of the Disarmament Commission. UN General Assembly, Official Records · Fifty-first Session Supplement No. 42 (A/51/42), ANNEX I - Guidelines for international arms transfers in the context of General Assembly resolution 46/36 H of 6 December 1991: § 33.

16 At the April 2013 plenary meeting of the UN General Assembly the Cuban ambassador objected to the text of the Arms Trade Treaty because Cuba felt that "the treaty would legitimize transfers without the consent of the receiving country, contravening the principle of non-intervention into State affairs" (United Nations, GA/11354, 2 April 2013). See also A. Clapham: Weapons and Armed Non-State Actors, in: S. Casey-Maslen (ed.): Weapons Under International Human Rights Law. Cambridge University Press, Cambridge, 2015: p. 163-196.

17 International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons.

18 See also article 3(e) of the 2001 Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime: "'Illicit trafficking' shall mean the import, export, acquisition, sale, delivery, movement or transfer of firearms, their parts and components and ammunition from or across the territory of one State Party to that of another State Party if any one of the States Parties concerned does not authorize it in accordance with the terms of this Protocol...".

19 This definition has been developed with Brian Wood to whom I am grateful.

Council arms embargoes, and in court cases.

Diversion can happen at all stages of the supply chain: at point of embarkation, during transit/transhipment, at point of delivery, or post delivery. Included various examples for illustrative purposes:

Example 1 (Point of embarkation):

On 12 July 2005 the m/v Sloman Traveller sailed from Ploce (Croatia), containing around 78,000 surplus AK47 assault rifles and some light machine guns, destined for British and German arms dealers, plus 955 tonnes of obsolete and obsolescent armoured vehicles, all to be unloaded at the port of Immingham in the United Kingdom. Nobody knows how many assault rifles were actually loaded.

A discrepancy note stated that on 1 July 2005 in Ploce, truck registration 734J640/266M476 was unloaded at the quayside alongside the m/v Sloman Traveller, when it was discovered that 6 pallets of boxes of AK47 assault rifles were missing. 18 pallets were recorded as being loaded at Tuzla and, according to the driver's records, were on the truck; yet only 12 pallets were found when the truck was unloaded. Six pallets equates to 720 assault rifles. The Shipper's Note, which accompanied the consignment, graphically illustrated the lack of physical security of this consignment: *"693 pallets said to contain 7,389 cases of surplus weapons. Pallets control:- steel stripe bands loosened. Used Cases. cases are not sealed. carrier shall not be liable for the number and content of cases"*.[20]

Sloman Traveller, Immingham, 23 July 2005

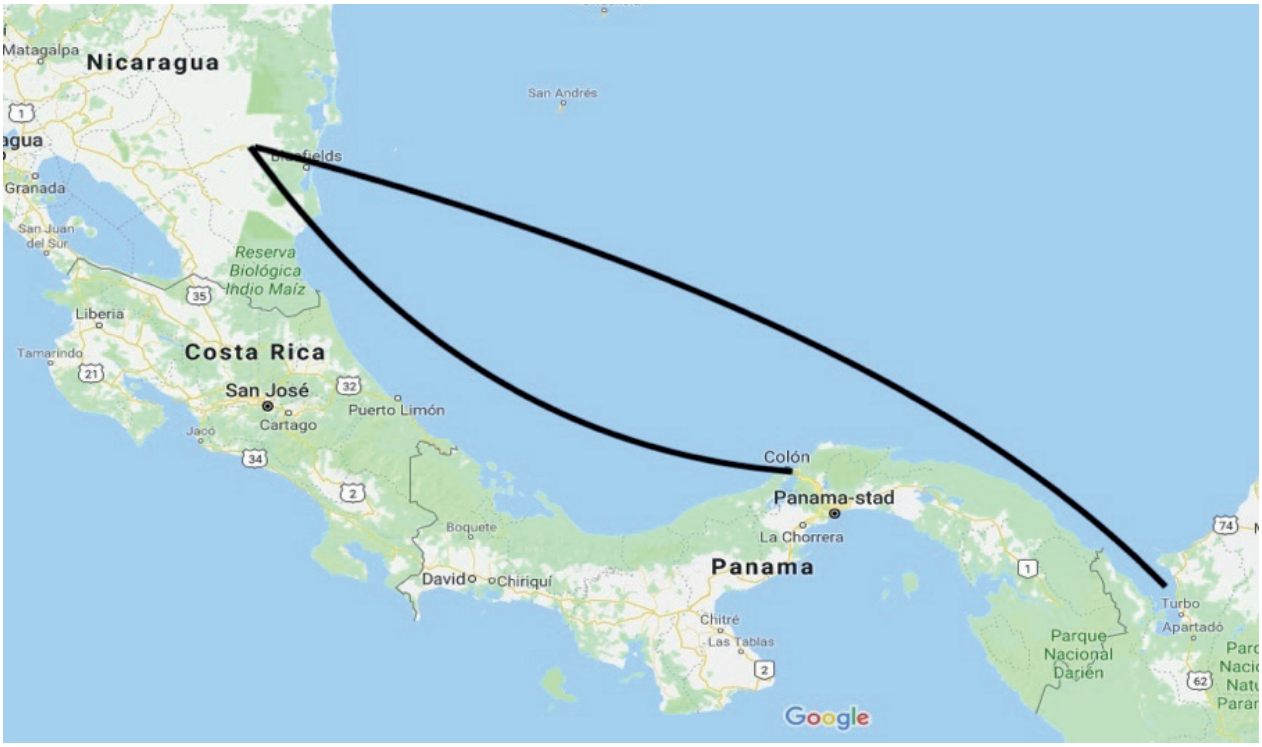
Photographer: Alex (http://www.shipspotting.com/gallery/photo.php?lid=88756)

20 P. Danssaert, J. Capelle, B. Johnson-Thomas: *Recent arms deliveries from the successor States of the former Yugoslavia*, IPIS, 2007.

Example 2 (In transit):

Between October 1999 and June 2000 the Nicaraguan National Police negotiated a barter deal with the Guatemalan arms dealer GIR S.A.[21] The deal was to swap 5,000 surplus AK47s and 2.5 million rounds of ammunition from the police stockpiles for brand new Israeli pistols and mini-Uzi's. To get the maximum amount of money out of this deal between July 2000 and June 2001 GIR tried to find a buyer for the surplus AK47s. The Israeli arms broker Shimon Yelinek, based in Panama, was interested. He allegedly bought the weapons for the Panamanian police but the purchase order/end user certificate he used turned out to be a forgery. Nobody had taken the time to verify Yelinek's paperwork. After inspection of the weapons Yelinek deemed the weapons to be unserviceable. GIR thus made a new deal with the Nicaraguan Army, which accepted the 5,000 surplus AK47s from the police, and gave GIR in return 3,117 new AK47s. 3,000 rifles were intended for Yelinek, and 115 were sold to the Guatemalan armed forces. The Nicaraguan Army also agreed to provide GIR with an additional 2.5 million rounds of ammunition and 3,000 bayonets, in return for bullet-proof vests, and weapons training for the Nicaraguan Police.

On 11 July 2001 a Mexican national established a new shipping company in Panama, Trafalgar Maritime Inc., with one vessel (m/v Otterloo) to its name. On 3 November 2011 the m/v Otterloo sailed from the Nicaraguan port of El Rama, carrying 14 containers of arms and ammunition, with destination allegedly the port of Colon (Panama). The vessel instead docked in the port of Turbo (Colombia) on the 5 November 2011 where it was unloaded. The cargo was then transferred to the paramilitary Autodefensas Unidas de Colombia (AUC). Trafalgar Maritime was dissolved in April 2002.[22]



Map 0: El Rama – Colon / El Rama - Turbo

21 Owned by the Israeli's Ori Zoller and Uzi Kissilevich.

22 *Report of the General Secretariat of the Organization of American States on the Diversion of Nicaraguan Arms to the United Defense Forces of Colombia*, OAS, 6 January 2003, CP/doc. 3687/03.

Example 3 (Point of delivery):

Between 14 September 2007 and 1 September 2008, three ships – the Radomyshl, the Beluga Endurance, and the Faina - loaded hundreds of tons of military equipment at the Ukrainian port of Oktyabrsk/Nikolayev. According to documents the shipments were destined for (and eventually delivered to) the Government of South Sudan. However, in the cargo manifests of the MV Faina and MV Beluga Endurance the consignee was reported as the "Ministry of Defence – Republic of Kenya", even though the contracts related to the cargo and named in the documents were titled "DOD/GOSS", followed by a date and number. On 25 September 2008 the story hit the news headlines when the Faina was hijacked by Somali pirates.

On October 8, 2008, the BBC published the cargo manifest of MV Faina and stated that "GOSS" was an acronym for "Government of South Sudan", while the Kenyan authorities insisted that GOSS meant "General Ordinance Supplies and Security". An email from the U.S. Department of Defense dated 25 September 2008, and released under the Freedom of Information Act, states that the shipment was "part of a contract signed between Ukraine and the Sudanese People's Liberation Movement/Army in DEC 06".[23]

The vessel was released on 5 February 2009. After docking in Mombasa the arms and ammunition were transferred by rail and road to Juba in South Sudan.[24]

Image 0: M/V Faina hijacked by Somali pirates, 2008 (Photo Credit: Jason R. Zalasky, U.S. Navy)

Example 4 (Post delivery):

In early 2014 the United Nations arms embargo Monitoring Group on Somalia and Eritrea pursuant to Security Council resolution 2111 (2013) reported in a confidential report of "high level and systematic abuses in weapons and ammunition management and distribution" by the Federal Government of Somalia

23 FOIA 17-F-0640, submitted 28 September 2011 by Peter Danssaert, response received 29 March 2019.
24 S. Finardi, P. Danssaert: *Rough seas. Maritime transport and arms shipments*. IPIS/Transarms, 2012.

(FSG).[25] Their 19 September 2014 report spoke of "a number of serious anomalies and concerns regarding weapons deliveries from Uganda, Djibouti and Ethiopia". Some of these arms shipments to the FSG could not be accounted for. The Monitoring Group suspected that at least 1,000 had been diverted from the government stockpiles to al-Shabaab. The Group was also informed that large quantities of ammunition supplied to the FSG had been leaked by rogue elements of the Somali National Army into Mogadishu arms markets.[26]

Example 5 (covert supplies):

When the Libyan civil war broke out in February 2011, various States rapidly shipped arms and ammunition to the opposition forces. The United States secretly approved Qatar and the United Arab Emirates shipping arms to Libyan opposition groups.[27] France and Italy also armed opposition groups. Italy shipped weapons that had been previously intercepted during the civil war in Yugoslavia.[28] Following the collapse of the Ghadaffi government weapons stockpiles were overrun by former government groups on the run and/or victorious opposition groups. All the weapons and ammunition that had been supplied to Libya under the Ghadaffi regime as well as the new supplies entering Libya to support the armed groups resulted in widespread proliferation of arms and ammunition not only in Libya but also across North Africa (Algeria, Egypt, Tunisia), parts of Sub-Sahara Africa (Central African Republic, Chad, Mali, Niger, Nigeria, Somalia and Sudan) and the Middle East (Gaza, Syria) through arms trafficking networks that continue to operate.[29]

25 Letter dated 6 February 2014 from the Coordinator of the Somalia and Eritrea Monitoring Group addressed to the Chair of the Committee, S/AC.29/2014/COMM.13.

26 Letter dated 6 February 2014 from the Coordinator of the Somalia and Eritrea Monitoring Group addressed to the Chair of the Committee, S/AC.29/2014/COMM.13; Letter dated 10 October 2014 from the Chair of the Security Council Committee pursuant to resolutions 751 (1992) and 1907 (2009) concerning Somalia and Eritrea addressed to the President of the Security Council, S/2014/726; P. Danssaert, B. Johnson-Thomas: *Pentagon Accidentally Arms Al Qaeda Affiliate*, IPIS, 2014.

27 U.S.-Approved Arms for Libya Rebels Fell Into Jihadis' Hands, New York Times, 5 january 2012.

28 P. Danssaert, B. Wood: Surplus and Illegal Small Arms, Light Weapons and their Ammunition: the consequences of failing to dispose and safely destroy them, IANSA, 2017: p. 10-11.

29 N. Marsh: Brothers Came Back with Weapons. The Effects of Arms Proliferation from Libya, in: Prism, 6 (2017), 4: p. 79-96. See also: Letter dated 17 February 2012 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council, 20 March 2012, S/2012/163; Letter dated 15 February 2013 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council, 9 March 2013, S/2013/99; Swede behind Syria arms smuggling, Radio Sweden, 31 October 2013 (*http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5690625*); Letter dated 15 February 2014 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council, 19 February 2014, S/2014/106; Letter dated 23 February 2015 from the Panel of Experts established pursuant to resolution 1973 (2011) addressed to the President of the Security Council, 23 February 2015, S/2015/128; Letter dated 4 March 2016 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council, 9 March 2016, S/2016/209; Letter dated 1 June 2017 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council, 1 June 2017, S/2017/466.

2. MEASURES TO TACKLE DIVERSION[30]

2.1. Pre-Export Risk Assessment

Various measures can be taken to address the issue of diversion. These can be divided between pre-export and post-shipment measures.

Marking: pre-shipment

In relation to the transfer, acquisition, storage and stockpile management of small arms and light weapons the marking of such weapons is recommended. Common minimum standards for marking SALW pre-shipment include[31]:

1. Marking at the time of manufacture;
2. Markings need to be unique, as well as reliable, visible, easily recognizable, readable and user-friendly;
3. Unique marking needs to be applied to one or more of the following locations: frame, receiver, barrel and slide;
4. The information contained in the marking at the point of manufacture would include the following information: country of manufacture and serial number;
5. Exchange of information on national marking systems;
6. The same part of the same model of a small arm or light weapon would always receive the manufacturer's unique mark so as to avoid the trafficking of spare parts that would make it possible to reconstitute an unmarked weapon;
7. The manufacturer's unique mark would be applied to an essential (structural) component of the weapon, the destruction of which would make it definitively inoperable.

Recent innovations include microstamping of the firing pin of SALW. When fired an imprint is made on the cartridge. This can be used by forensic experts to trace the weapon to the last registered owner.

Risk assessment for diversion

One of the crucial steps that starts before the export has even been approved is to assess the risk of diversion. National export control authorities must take into account the potential use of the conventional arms in the recipient country and of the risk that the conventional arms might be transferred to an unauthorized or unsuitable end user. To address this uncertainty companies and individuals will be required to formally submit a range of information as part of the export licence application process. This can be information on the final end user and end use, the intermediate and final consignees, the type, characteristics, value and quantities of the arms to be exported, reference to the contract or order number concluded with the end user, and relevant import authorization documents from the country of final destination. It might also include which freight forwarders are going to be used, or information on transit points to be taken...

30 For measures see B. Wood, P. Danssaert: Study on the development of a framework for improving end-use and and-user control systems. UNODA Occasional Paper 21, UNODA, December 2011.

31 United Nations General Assembly: Report of the Group of Governmental Experts established pursuant to General Assembly resolution 56/24 V of 24 December 2001, entitled "The illicit trade in small arms and light weapons in all its aspects". United Nations, A/58/138, 11 July 2003; International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons; Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime.

Vetting parties

The licence application has to be reviewed by the national export control authorities. Such a review will include assessing the export and licensing history of the exporter, or broker; verify the credentials and good standing of the entities (exporter, broker, end user, freight forwarder...) that are party to each transaction. Law enforcement and intelligence agencies can be asked to provide data. Parties can be cross-referenced against "watch lists" or "Lists of debarred entities". Companies, entities, and persons found on such a list are sanctioned by a State and individuals, companies from said State may not engage in economic activities with these sanctioned companies or individuals[32]. For example the U.S. Treasury Department maintains a "Specially Designated Nationals and Blocked Persons" list (SDN). The assets of these SDN listed nationals are blocked and U.S. persons are prohibited from dealing with them. The Office of Foreign Assets Control (OFAC) is responsible for the list.[33] The United States also has an "Excluded Parties List System". On Federal level now included in the "System for Award Management".[34] While debarred or suspended, the Government will not solicit offers from, award contracts to, renew, or otherwise extend contracts with, or consent to subcontracts with entities or individuals that appear on the Excluded Parties List.

Requirement for additional documentation

In order to help assess the potential risk of diversion end-use documents, such as end-use(r) certificates or end-use(r) statements are used. States may also request the following information: a commitment by the end user and/or the importing State to provide the exporting State a delivery verification certificate; a clause allowing the exporting State to carry out, upon its request, on-site inspections of the transferred items. If the exporting State requires such information and commitments from the importer or final consignee/end user, but the information or commitments are not submitted and received by the export authorities at the time the export authorization is considered, then approval for the arms export should be refused.

The end-use(r) document needs to be authenticated and verified by the authorities of the exporting State:

Authentication: Authentication of an end-use document is the legal formality by which the authorities of the exporting State certify the authenticity of the signature, the capacity in which the person certifying the document has acted and, where appropriate, the identity of the seal or stamp which it bears. Upon request, the importing State should assist the exporting State in the end-use(r) document authentication process, a procedure usually undertaken by embassies or consular agents.

Verification: Verification is not limited to the official certification of the signature and authenticity of the document but is the whole process by which the authorities of the exporting State check the validity of the documents and the accuracy of the information contained in those documents regarding the risk of diversion and the suitability of the end use(r). Not only the authenticity of the documents is verified. More importantly also the security of the transfer and storage, the accuracy of assurances regarding the end use, the end user and re-export, and crucially the legitimacy of the end user and end use have to be verified before an export licence is granted.

The Wassenaar Arrangement includes the following optional requirements in the list of end-use/user certificate elements, presumably measures that at least some of the participating States require from importing States in sensitive cases: (i) certification that the goods will be installed at the premises of the end user or will be used only by the end user; (ii) agreement by the importer/end user to allow on-site verification; (iii) assurance from the importer/end user that any re-exports will only be carried out under the authority of the importer's/end user's export licensing authorities; (iv) an undertaking from the importer/

32 See for instance "List of Statutorily Debarred Parties" by Directorate of Defense Trade Controls (*http://pmddtc.state.gov/compliance/debar.html*); the "Specially Designated Nationals And Blocked Persons List" by U.S. Department of the Treasury (*https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx*).

33 *https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx*

34 *https://www.sam.gov*

end user not to divert or relocate the goods covered by the end-use certificate/statement to another destination or location in the importing country.

Exchange information

Upon request the importing State should assist the exporting State. The importing State can provide relevant information to verify the end-use(r) document. It can also clarify the existence of documents which certify the import.

Compliance

The national export control authority can demand from exporters to commit to maintain a company policy to comply with relevant national and international laws and regulations. This compliance policy will outline the procedures for dealing with licensing and compliance matters, including identification of the management structure responsible for implementing internal compliance, screening procedures, regular audits, re-export procedures, detailed record-keeping of specific documentation for licensed exports: e.g. a description of the item, quantity, transaction date, destination, means of transport... These records can regularly be checked by the national export control authority.[35]

Pre-shipment inspections

In general, international guidelines for arms control do not mention pre-shipment inspection of the arms cargo to be delivered. However, international standards for customs administrations do encourage the 'pre-shipment inspection' of higher risk cargoes.[36] The World Customs Organization proposes that Customs administrations develop the ability to inspect and screen cargo and transport conveyances before it arrives: "Using automated targeting tools, Customs administrations identify shipments that are high-risk as early as possible in the supply chain, at or before the port of departure. Provision should be made for the automated exchange of information. Systems should therefore be based on harmonized messages and be interoperable".[37]

This not to be confused with a pre-shipment inspection (PSI) service offered by international companies (Bureau Veritas, Intertek, SGS...). In this context PSI serves to maximize duty collection. Contracted goods are prior to shipment inspected to ascertain their quality, quantity or price. In general arms and ammunition are exempted from PSI contracts.[38]

2.2. Post-Shipment Measures

End-use monitoring

The Organization for Security and Cooperation in Europe (OSCE) recommends that the end use of the goods should be verified, when possible. Post-shipment verification can take two forms: (a) the physical inspection *in situ*, or (b) the final consignee provides the exporter with a delivery verification certificate once the export has reached the final destination. The customs authority in the recipient country will sign

35 *Internal Compliance Programme. Richtlijnen voor het opstellen van een Intern Nalevingsprogramma voor Strategische en Foltergoederen, Technologie en Sancties*. Ministerie van Buitenlandse Zaken, Den Haag, juni 2018.
36 For example the World Customs Organization SAFE Framework of Standards to Secure and Facilitate Global Trade, June 2012.
37 World Customs Organization SAFE Framework of Standards to Secure and Facilitate Global Trade, June 2012: p. 7.
38 The exemptions vary: Haiti has exempted from PSI ammunition and weapons other than for hunting and /or sport (SGS Importer Guide PSI in Haiti); the Democratic Republic of Congo has exempted from PSI weapons, ammunitions imported by the Government (Bureau Veritas PSI of Imports for the Democratic Republic of Congo).

the delivery verification certificate. Under article 10.4 of the United Nations Firearms Protocol, the importing State party shall, upon request, inform the exporting State party of the receipt of the dispatched shipment of firearms, their parts and components or ammunition.

In order for such post-shipment controls to be carried out, a clause on post-shipment control should be inserted into the contract, the end-use(r) certificate or the arms export regulations requiring a delivery verification certificate or a post-delivery inspection.

Examples of post-shipment verification programs are: Blue Lantern (US Department of State), Golden Sentry (US Department of Defense), article 5a Kriegsmaterialverordnung (Switzerland). For instance, under U.S. law all Department of Defense government-to-government transfers or exports of defence articles and/or defence services are subject to end use monitoring with the purpose "to verify that defense articles or services transferred by the United States Government (USG) to foreign recipients are being used in accordance with the terms and conditions of the transfer agreement or other applicable agreement"[39]. The Golden Sentry program employs two post-delivery monitoring methodologies: Routine End Use Monitoring and Enhanced End Use Monitoring. The level of monitoring is determined by the type of defence article or service.[40]

Stockpile management

Diversion can also be caused by ineffective stockpile management. The States participating in the Wassenaar Arrangement agreed to take into account the stockpile management and security procedures of the importing State.

The United Nations Group of Governmental Experts established pursuant to United Nations General Assembly resolution 61/72 with regard to the issue of conventional ammunition stockpiles in surplus proposed that a comprehensive and effective stockpile management system has the following basic components[41]:

1. National stockpile management planning;
2. Classification systems;
3. Marking systems;
4. Accounting systems;
5. Inspection;
6. Physical storage conditions;
7. Transportation procedures;
8. Stockpile security systems.

Storage and stockpile management is greatly enhanced by the use of automatic identification (s*ee infra*) and data collection technology. This includes use of biometrics (e.g. fingerprint recognition) to recognize authorized users; use of radio frequency identification (RFID) and barcodes to tag items to automate record-keeping. The logistics department of the Dutch Armed Forces has developed the Small Arms Registration System. Small arms and light weapons for the Armed Forces are fitted with a passive RFID tag. When the weapon is issued to a soldier the tag is linked to the soldier in question.[42]

39 Security Assistance Management Manual: Chapter 8 - End-Use Monitoring (*https://www.samm.dsca.mil/chapter/chapter-8*)
40 See: Security Assistance Management Manual: Chapter 8 - End-Use Monitoring.
41 United Nations General Assembly: Problems arising from the accumulation of conventional ammunition stockpiles in surplus. United Nations, A/63/182, 28 July 2008.
42 "RFID: vijf kilometer lopen of honderd meter sprint?", logistiek.nl, 10 juni 2008 (accessed 6 August 2010).

Marking: post-shipment

In relation to the acquisition, storage and stockpile management of small arms and light weapons the marking of SALW is recommended. Common minimum standards for marking SALW post-shipment include[43]:

1. Marking at the time of import by the importer;
2. Unmarked or inadequately marked weapons that are confiscated, seized or collected are marked or destroyed;
3. Markings need to be unique, as well as reliable, visible, easily recognizable, readable and user-friendly;
4. Unique marking needs to be applied to one or more of the following locations: frame, receiver, barrel and slide;
5. The information contained in the marking at the time of import (if necessary) would include the country and, when possible, date of import;

Tracing

Much is written about tracing. Usually interpreted as a post-diversion activity: the markings on seized or confiscated SALW are used to identify the manufacturer and possibly the importer. The ECOWAS Convention on Small Arms and Light Weapons, Their Ammunition and Other Related Materials defines tracing as the systematic monitoring of the movements of conventional arms and their ammunition and other related materials, from the manufacturer until the end user, with a view to helping member States' competent authorities to detect illicit manufacture and trading.

The latest technologies allow entire shipments of conventional weapons and ammunition to be tracked and traced as they happen. Real-time end-to-end visibility is possible through the use of radio frequency identification (RFID) technology, global navigation satellite systems, satellite communications, and cellular communications technology and software to track the identity, status, and location of cargo from origin to destination in real-time. Moreover containers can be fitted with intrusion detection devices. These RFID tags are secured inside the container. The tag will monitor a number of tampering indicators such as shock, light exposure, or door openings. Unauthorized intrusion into the container will be alerted to the RFID interrogator. (See infra.)

Border control

Customs, law enforcement and licensing agencies can often obtain a range of relevant information, prior to shipments, during the journey and upon delivery, to assess risks related to sensitive cargoes. This could be vital for verification of the end user, the lawful end use and the prosecution of offenders. For the supply chain to function legally, a series of documents are required that precede and accompany the shipments. The types of documents include commercial invoices; pro-forma invoice; dispatch advice; bill of lading; international rail consignment note; international road consignment note; dangerous goods declaration; goods declaration for export (Kyoto Convention); goods declaration for transit (Kyoto Convention); Single Administrative Document...

43 United Nations General Assembly: Report of the Group of Governmental Experts established pursuant to General Assembly resolution 56/24 V of 24 December 2001, entitled "The illicit trade in small arms and light weapons in all its aspects". United Nations, A/58/138, 11 July 2003; International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons; Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime.

Exchange of information

For high-risk shipments customs administrations along the supply chain should consider customs-to-customs electronic data exchange. These electronic messages can include details about the goods (value, quantity, export licence, …), the custom control results along the supply chain, as well as a corresponding arrival notification.

3. REAL-TIME IN-TRANSIT VISIBILITY

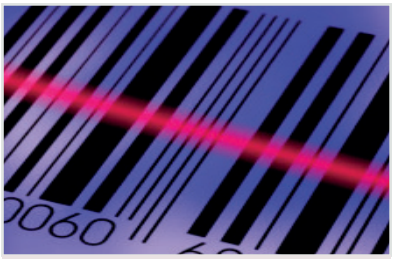
"Simply put, sensors attached to containers for the straightforward purpose of identifying the whereabouts of goods at any given moment revolutionize how logistics is conducted. Customers have the ability to hold their carriers and other vendors accountable in a way they can't today." (Peter Tirschwell: "New era emerges for cargo visibility", Journal of Commerce, 10 March 2017)

A major innovation to track and trace conventional arms shipments was the introduction of real time locating systems which allow to identify the location of cargo along the entire supply-chain. The ability to track and trace cargo from origin to consignee or destination in near real-time increases security of in-transit cargo significantly, and thereby reducing the possibility of diversion. The system requires the combination of various technologies: tags with or without sensors are attached to containers, in combination with Global Navigation Satellite Systems technology (e.g. GPS, Galileo, GLONASS, BeiDou,...), or the Global System for Mobile Communications technology, communication satellites, software (web-based maps...), etc.

3.1. Radio-Frequency Identification

Automatic Identification Technology (AIT) has been around for quite some time. The most familiar examples of AIT are bar codes, magnetic stripes, and shoplifting deterrent tags. The widely used linear or one-dimensional barcoding is gradually replaced with two-dimensional barcoding (2D matrix code, for example, QR code or Quick Response code) (see illustration below).

2D matrix code



one dimensional barcode

Labelling can also be achieved by using radio-frequency identification (RFID) tags. These tags are used to identify containers or pallets and their content. They allow identification at a distance by transmitting information using radio waves. The basic tag is nothing more then a small transponder. It consists of a chip to carry data and an antenna.

The first tags to be developed were passive tags. Passive tags draw electromagnetic power from an RFID reader to transmit their data to the reader. These are the most simple in design and the least expensive tags. The readers can be fixed or handheld, and are connected to a network. Major drawbacks of passive RFID technology is that RFID readers need to be located along the route or at point of destination, and the tag needs to be held close to a reader, so that the data on the tag can be read. The pioneers for the adoption of RFID on a large scale were Walmart, Tesco, and the U.S. Department of Defense.[44]

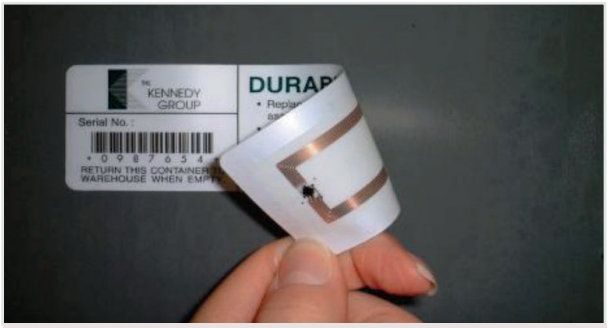
In October 2003 the Department of Defense developed an initial RFID policy establishing business rules and requirements for implementing passive RFID technology in the integrated DoD supply chain.[45] As such RFID became mandatory for all DoD suppliers on solicitations issued on or after October 1, 2004 for

44 Select bibliography: J. Banks, et. als.: *RFID Applied.* John Wiley, 2007; K. Finkenzeller: *RFID Handbuch.* Hanser, 2006; E.C. Jones, C.A. Chung: *RFID in Logistics.* CRC, 2008; K. Michael, M.G. Michael: *Innovative Automatic Identification and Location-Based Services.* IGI Global, 2009; A. Malik: *RTLS for Dummies.* Wiley Publishing, 2009; S.B. Miles, et. als. (eds.): *RFID Technology and Applications,* Cambridge University Press, 2008; P. Sweeney II: *RFID for Dummies.* Wiley Publishing, 2005; G. Tamm, C. Tribowski: *RFID.* Springer Verlag, 2010; R. Want: *RFID Explained: A Primer on Radio Frequency Identification Technologies.* Morgan & Claypool, 2006.

45 *Better Strategic Planning Can Help Ensure DoD's Successful implementation of Passive Radio Frequency Identification.* GAO-05-345, 12 September 2005. See also: *DoD RFID Policy.* 2 October 2003; *DoD RFID Policy.* 30 July 2004. Web links to be found here: http://www.acq.osd.mil/log/sci/ait.html.

delivery of materiel on or after January 1, 2005.[46] But the ultimate aim of the Pentagon was to achieve real-time visibility. Passive tags can tell you where a shipment was at a certain point-in-time, but only when a tag has passed a reader.

Real-time visibility became possible with the introduction of active RFID tags.[47] Active tags carry their own power source in the form of a battery to communicate. The battery allows the radio signal to carry more information, and to travel further. The internal battery allowed sensors (heat, pressure, light...) to be added which can tell if and when containers are opened. Active tags can be combined with specialized components such as global navigation satellite systems, and telecommunication technologies. Instead of only identification of the cargo, the transmission of positional data in real time makes it possible to locate the cargo at all times, and not just when passing a fixed or handheld reader.[48] Thus the creation of Real-Time Locating Systems.[49]



Passive tag

Active tag

3.2. Real-Time Locating Systems

RFID is just one example of many technologies and systems to locate people, equipment and other assets in real-time. For instance infrared, ultrasound, Bluetooth, Wi-Fi, ZigBee, Ultra Wideband, and many other technologies can be used to create a real time locating system.[50] The advent of the smart phone, tablets, and other innovations in wireless communication has opened many possibilities for real-time asset visibility. Some (infrared, ultrasound, Wi-Fi, ZigBee, ...) are only useful to create a local area RTLS (warehouses, container terminals,...) because of their limited range.

46 *DoD RFID Policy*, 30 July 2004.

47 RFID and DoD select bibliography: *DoD RFID Policy.* 2 October 2003; *DoD RFID Policy.* 30 July 2004; *Better Strategic Planning Can Help Ensure DoD's Successful implementation of Passive Radio Frequency Identification.* GAO-05-345, 12 September 2005; *Radio Frequency Identification Technology in the Federal Government.* GAO-05-551, 27 May 2005; *More Efficient Use of Active RFID Tags Could Potentially Avoid Millions in Unnecessary Purchases.* GAO-06-366r, 8 March 2006; *Tactics, Techniques, and Procedures for In-Transit Visibility (ITV).* US Transportation Command, 1 March 2004 (incorporates changes 17 March 2006); *Efforts to Improve Supply Chain Can Be Enhanced by Linkage to Outcomes, Progress in Transforming Business Operations, and Reexamination of Logistics Governance and Strategy.* GAO-07-1064T, 10 Juy 2007; *Lack of Key Information May Impede DoD's Ability to Improve Supply Chain Management.* GAO-09-150, 12 January 2009; *Preliminary Observations on DoD's Progress and Challenges in Distributing Supplies and Equipment to Afghanistan.* GAO-10-842T, 25 June 2010.

48 E.C. Jones, C.A. Chung: RFID in Logistics. CRC, 2008: p. 233-234; Col. K. Ryan: Exploring Alternatives for Strategic Access to Afghanistan. US Army War College, 20 March 2009.

49 Satellite navigation and satellite communication are not a requirement for an RTLS network. A warehouse, or terminal can be fitted with RFID technology. As long as the active tags can connect to the RFID infrastructure their location can be determined.

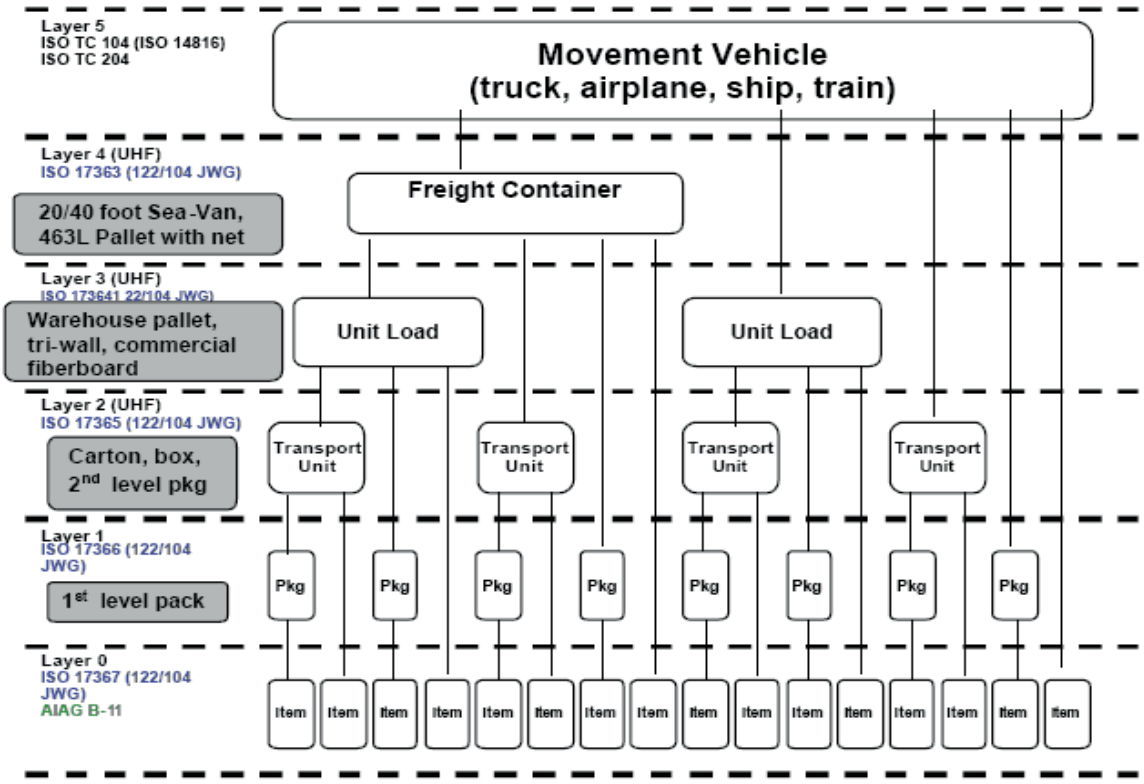
50 A. Malik: *RTLS for Dummies*. Wiley Publishing, 2009.

3.2.1. Use of satellite communication: The U.S. Defense Transportation In-Transit Visibility System[51]

All unit movement equipment, cargo, ammunition, and prepositioned materiel and supplies shipments to a destination outside of the continental USA have to be packed in a **RFID Layer 4 freight container**. The RFID Layer 4 freight container corresponds to the 20 or 40 foot freight container or the 463L air pallet fitted with active RFID tags written at the point of origin. The RFID tag data must be updated when the content of the container or pallet is altered during transit.[52]

The following diagram identifies 5 layers in increasing degree of packaging:

- Layer 0: Product item
- Layer 1: Package
- Layer 2: Transport unit – box (passive RFID used)
- Layer 3: Unit load – pallet (passive RFID used)
- Layer 4: Freight container – 20 or 40 foot freight container (active RFID used)
- Layer 5: Movement vehicle – vessel, aircraft, truck, train (active RFID used)



Packing Layers (https://wawftraining.eb.mil/wawfwbt/xhtml/unauth/web/wbt/other/rfid/RfidPackLayers.xhtml)

51 'RFID Technology: Keeping Track of DoD's Stuff'. *Defense Industry Daily*, 12/11/2009. "*The scope of the Radio Frequency Identification (RFID) infrastructure includes four business process servers, strategically positioned globally to mitigate communication limitations. There are in excess of 2400 nodal read and write sites located in 30 countries worldwide. These nodes are placed at strategic choke points throughout the Defense Transportation System (DTS) (i.e., all Defense Logistics Agency (DLA) depots and strategic aerial ports and seaports). Locations include, but are not limited to, the United States, Great Britain, Republic of Germany, Iraq, Kuwait, Egypt, Luxemburg, Belgium, Norway, Netherlands, Qatar, Bahrain, Djibouti, Spain, Korea, Japan, Hungary, Kyrgyzstan, Greece, Macedonia, United Arab Emirates, Turkey, and Italy.*" (Radio Frequency In-Transit Visibility (RF-ITV), http://jitc.fhu.disa.mil/washops/jtcb/rfitv.html, accessed 9 August 2010.)

52 U.S. DoD RFID Policy 2004; United States Department of Defense Suppliers' Passive RFID Information Guide Version 14.0 (http://www.acq.osd.mil/log/rfid/index.htm)

Cases, pallets, and packaging for Unique Identification (UID)[53] items are tagged with passive RFID tags at the point of origin (including vendors), except for bulk commodities[54]. The tags contain data on identity of pallet, case or UID item associated with the tag, the identity of the supplier, and a unique serial number.

The level of detail of the information on the active RFID tag has two components: (1) the **asset level detail**, these are data elements that describe the asset, and (2) the **content level detail**, these are data elements that minimally identify each level of a complete shipment entity (being a single shipment unit or a consolidated shipment). All this data is sent to the In-Transit Visibility servers.[55]

ASSET LEVEL DETAIL The minimum data elements required to describe the physical characteristics of a single asset, and the characteristics that identify that asset.	
* National Stock Number (NSN)	* Item Weight
* Nomenclature/Description Model Number	* Item Cube
* Unit Price	* Line Item Number (LIN) / Package Identification (PKGID)
* Condition Code	* Ammunition Lot Number
* Serial Number/Bumper Number	* DoD Identification Code (DoDIC)
* Serial Number Enterprise Identifier (or UID eligible)	* Hazardous Cargo Descriptor Code
* Part Number (if UID eligible, as applicable)	

53 *"A system of establishing globally ubiquitous unique identifiers within the Department of Defense, which serves to distinguish a discrete entity or relationship from other like and unlike entities or relationships."* (DoD Directive 8320.03 "Unique Identification (UID) Standards for a Net-Centric Department of Defense", DTD 23 March 2007) *"IUID (Item Unique Identification) is accomplished by marking each qualifying item with a permanent 2-dimensional data matrix. The data matrix is encoded with the data elements necessary to construct a Unique Item Identifier (UII) which is globally unique and unambiguous. The data elements required to form a UII include an identifier for the enterprise assigning the UII (e.g. manufacturer's CAGE code) and the item's serial number. If the manufacturer serializes within part number, that data element may also be encoded. Because the data matrix is machine-readable, IUID marking greatly reduces human error and improves the accuracy of inventory and acquisition records. UIIs are stored in a comprehensive database called the IUID Registry, which allows easy access to a limited set of data. The available data varies for newly acquired assets and legacy assets. In general the available data are "birth record" types of information (e.g. description, part number, serial number.) The IUID Registry is maintained by the Defense Logistics Information Service (DLIS). Every IUID delivery includes the required data elements describing the end item and the "pedigree" of embedded items. This data is captured during the acceptance process via the Wide Area Workflow (WAWF) application, or after acceptance via direct data submission. Items marked with IUIDs accelerate the receipt and acceptance process, allowing DoD to submit payment to its vendors in a timely fashion, thereby saving on late charges."* (http://www.acq.osd.mil/dpap/pdi/uid/faq.html, accessed 5 August 2010.)

54 For example sand, gravel, bulk liquids, ready-mix concrete, coal or combustibles, agricultural product.

55 Department of the Army: *Distribution of Materiel and Distribution Platform Management*. Army Regulation 56-4, 17 September 2014: p. 33-34; United States Transportation Command: *Defense Transportation Regulation – Part II. Chapter 208: Packaging and Handling*. 17 April 2017; Under Secretary of Defense: *Radio Frequency Identification (RFID) Policy. Memorandum*. 3 July 2004.

CONTENT LEVEL DETAIL VISIBILITY FOR EACH SHIPMENT UNIT

The most basic transportation entity is a single box or unpacked item governed by a shipment unit identifier. The data elements are contained in the requisition document, Transportation Control and Movement Document (TCMD), commercial carrier transaction, and the Consolidated Shipment Information transaction that describes the shipment and shipment movement characteristics. Minimum data elements necessary to provide content level visibility for each shipment unit are:

* Requisition Document Number
* Required Delivery Date or expedited shipment and handling codes
* Project Code
* Asset (Item) Quantity
* Unit of Issue
* 'From' Routing Indicator Code (for DoD shipments)
* Inventory Control Point
* 'From' Routing Indicator Code (for contractor/vendor shipments)
* Shipment Transportation Control Number for single shipment unit
* Intermediate Shipment Transportation Control Number for a multi-level consolidated shipment
* Conveyance (lead) Shipment Transportation Control Number for a consolidated shipment
* Commercial Carrier Shipment Tracking Identifier
* Transportation Priority
* Sender (Consignor) (DoDAAC/CAGE) Code
* Ship Date
* Port of Embarkation (POE) Code
* Port of Debarkation (POD) Code
* Shipment Total Pieces
* Shipment Total weight
* Shipment Total Cube
* Oversize Length/Width/Height
* Receiver (Consignee) (DoDAAC)
* Commodity Class
* Commodity Code
* Special Handling Code
* Water Type Cargo Code
* Net Explosive Weight
* Unit Identification Code (UIC)
* Unit Line Number
* Operation/Exercise Name
* Hazardous Material Shipping Characteristics: United Nations Identification Number, Class or Division Number, Package Group, Compatibility Group.

To be able to generate transaction records linked to RFID events in the DoD logistics system the RFID tag data with the associated material information must be present in the DoD servers so that information systems can access this data each time the tag is read.[56] In the DoD In-Transit Visibility system active RFID tags are written as either a data-rich format (the full shipment data is encoded on the tag and sent to the system) or as a license plate format (RFID shipment data is not encoded on the tag but is sent to system: the unique identifier of the RFID tag is linked to the data in the system).[57] For security reasons the Department of Defense is encouraging the transition to license plate RFID tags.[58]

Truck drives through the Savi Signpost system, which helps the Trailer Transfer Point keep track of all inbound and outbound trailers, at Contingency Operating Base Speicher (Iraq). The Savi Signpost system is an interrogator system that tracks the RF ID tags as they enter and exit the Trailer Transfer Point. (Photo Credit: Sgt. Ryan Twist, 139th Public Affairs, U.S. Army)

56 Department of the Army: *Distribution of Materiel and Distribution Platform Management*. Army Regulation 56-4, 17 September 2014.

57 United States Transportation Command: *Defense Transportation Regulation – Part II. Appendix K – Active Radio Frequency Identification (RFID) In-Transit Visibility (ITV) Data Requirements*. 17 April 2017.

58 Office of the Assistant Secretary of Defense for Logistics & Materiel Readiness: *RFID Supplier Info & FAQs* (https://www.acq.osd.mil/log/sci/rfid_FAQs.html)

Electronic communication occurs through various servers strategically positioned across the globe. Thousands of nodal read and write sites are scattered around the world. "These nodes are placed at strategic choke points throughout the Defense Transportation System (DTS) (i.e., all Defense Logistics Agency (DLA) depots and strategic aerial ports and seaports). Locations include, but are not limited to, the United States, Great Britain, Republic of Germany, Iraq, Kuwait, Egypt, Luxemburg, Belgium, Norway, Netherlands, Qatar, Bahrain, Djibouti, Spain, Korea, Japan, Hungary, Kyrgyzstan, Greece, Macedonia, United Arab Emirates, Turkey, and Italy."[59]

The system is not full proof against tampering. Therefore the U.S. military developed active RFID tags which are equipped with sensors, the **container intrusion detection devices (CIDD)**. The anti-pilferage sensors are activated using a hand held reader. Unauthorized intrusions into the container when detected are alerted at the next RFID reader, or through a messaging system. Selected personnel are pre-addressed to automatically receive email notification of breach so that immediate response is initiated. Intrusion detection is monitored using multiple sensors - like shock, light exposure, door openings, humidity, temperature,...[60] - to ensure the highest probability of accurately detecting and reporting a container breach.61 If containers are pilfered "DOD can attempt to determine the approximate area where the pilferage took place based on the last [active] RFID tag signal obtained by an interrogator inside Pakistan. Additionally, some RFID tags have intrusion-detection capabilities that provide information on when and where the cargo has been broken into"[62].

An Early Entry Deployment Support Kit—a radio-frequency identification interrogator—that is positioned at a chokepoint for passing cargo and equipment (Photo Credit: U.S. Army)

The battery of an active tag also allowed other technologies to be added. In 2007 the Department of Defense and industry set up a joint R&D project to integrate satellite communication technology into existing active RFID tags to be able to continuously monitor high value assets while outside the RFID infrastructure.[63] In 2014 the Alexandria based (Virginia) Savi Technology was awarded a five year contract by the Department of Defense to supply active RFID tags, readers, a Real-Time Locating System (RTLS), satellite communication (SATCOM) and related technologies for global tracking of personnel, equipment and sustainment cargo worldwide.[64] Savi's ST-694 GlobalTag combines active RFID with satellite communication technology and global navigation satellite systems. The tag automatically switches on the satellite transmitter when no longer in range of the RFID infrastructure.[65] By 2017 the system included 36 countries, 1,600 tag interrogator sites with over 470 satellite-enabled tracking systems making it the largest active

59 Radio Frequency In-Transit Visibility (RF-ITV), http://jitc.fhu.disa.mil/washops/jtcb/rfitv.html, accessed 9 August 2010.

60 "How to correct "First Seen" anomalies when using Smart Chain for Mobile Devices (SCMD)/EZ Sensor Software", *PM J-AIT ITV Operations and Training Newsletter*, October 2009; "Container intrusion detection device (CIDD)", *DTO & MO Quarterly Newsletter*, Volume 5 (2009) issue 2: p. 6; Col. K. Ryan: *Exploring Alternatives for Strategic Access to Afghanistan*, US Army War College, 20 March 2009.

61 "Container intrusion detection device (CIDD)", http://www.eis.army.mil/AIT/News/news/news_cidd.html (accessed 9 August 2010); "Container intrusion detection device (CIDD)", *DTO & MO Quarterly Newsletter*, Volume 5 (2009) issue 2: p. 6; "RFID Technology: Keeping Track of DoD's Stuff", *Defense Industry Daily*, 12-Nov-2009.

62 United States Government Accountability Office: *Preliminary Observations on DOD's Progress and Challenges in Distributing Supplies and Equipment to Afghanistan*, GAO-10-842T, 25 June 2010. See also: Col. Kurt Ryan: *Exploring Alternatives for Strategic Access to Afghanistan*, US Army War College, 20 March 2009.

63 U.S. TRANSCOM, Numerex Corp. join forces for improved cargo tracking, 28 August 2008 (http://www.scott.af.mil/News/Article-Display/Article/161594/us-transcom-numerex-corp-join-forces-for-improved-cargo-tracking/); Hybrid tag includes active RFID, GPS, satellite and sensors, RFID Journal, 24 February 2009.

64 https://www.savi.com/news/u-s-defense-department-selects-savi-sole-provider-rfid-iv-contract/

65 Hybrid tag includes active RFID, GPS, satellite and sensors, RFID Journal, 24 February 2009.

RFID network in the world.

NATO and various NATO countries have also begun to use tracking technology.

3.2.2. Use of the Global System for Mobile Communications

A newer active RFID tag is available from SCT Technology: the ST-900 (Savi Mobile Security Parent) tag is offered in combination with SCT Technology's consignment management application software. The ST-900 tag uses a global navigation satellite system (e.g. GPS) in combination with General Packet Radio Service (GPRS) on the Global System for Mobile Communications making communication cheaper compared to satellite communication. "The container security tag uses a global navigation satellite system (here GPS) to get its location and it then reports directly back to the consignment management application (CMA) via the mobile phone network (GPRS). Thereby negating the need for any fixed readers and providing a more detailed 'breadcrumb' trail on the consignment management application's embedded map. Using GPS reports like this also means that we can geo-fence the route and checkpoints for the authorised journey and CMA then triggers alerts to the user if a tagged container strays off route or is late etc and if there is an unauthorised removal of the tag that also triggers an immediate real-time alert."[66] When out of reach of a GPRS signal "the tag continues to record its GPS position and security status and when it is able to get a GPRS signal it uploads GPS and status messages that had been cached"[67].

3.2.3. RFID safety

An issue to be taken into consideration when active RFID tags and readers are used in the transport or storage of ammunition is that the electromagnetic radiation does not interfere with the electrically initiated detonators installed in the ammunition. The radiation might inadvertently actuate or disable the detonator. This radiation hazard is known as Hazards of Electromagnetic Radiation to Ordnance (HERO). Before using any automatic identification technology (AIT) in the presence of ordnance the AIT equipment needs to be evaluated and certified for use.[68] For example a certified tag that is safe to be used with ammunition is the ST-900 tag.

3.2.4. RFID security

Another matter to be taken into consideration is RFID security. There are two components to this:(a) back-end network security (communication between the reader and the network servers via the internet protocol): there are lots of security technologies available to ensure data security (implementation of certificates for authentication, use of Secure Sockets Layer (SSL),....); (b) the weakest link is the front-end radio frequency security (data transmitted from the tags to the reader): the communication between reader and tag can be intercepted, or any reader can communicate with the tags. This security breach can be overcome by using encryption, or as a cheaper option, use license plate tagging. All the shipment data is stored on the server, but not on the tag, and all the data collected during transit is send as a string of digits to be translated by the software application.[69]

The ST-900 tag works on this principle: "data transmitted is not encrypted but does not contain any read-

66 Email conversation SCT Technology, 22 November 2017.
67 Email conversation SCT Technology, 20 February 2018.
68 DoD: *DoD Ammunition and Explosives Safety Standards: Explosives Safety Construction Criteria*. DoD manual 6055.09-M Volume 2, 2012; US Naval Sea Systems Command: *Electromagnetic Radiation Hazards (Hazards to Ordnance)*. NAVSEA OP 3565/NAVAIR 16-1-529 Volume 2, 2007; Defense Information Systems Agency: Hazards of Electromagnetic Radiation to Ordnance. In: *Explosives Safety Bulletin*: June 2011.
69 RFID Security Issues: Generation2 Security. Thingmagic (*http://www.thingmagic.com/index.php/rfid-security-issues?tmpl*); T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips: Guidelines for Securing Radio Frequency Identification (RFID) Systems. Special Publication 800-98, National Institute of Standards and Technology, 2007; Y. Zhang, L.T. Yang, J. Chen: RFID and Sensor Networks. Architectures, Protocols, Security, and Integrations. CRC Press, 2010.

able text, simply a string of digits that has to be translated by the consignment management application to determine location, status etc and any association to the cargo is held in the server not the tag so interception of the tag message does not give away details".[70]

3.2.5. Solution to all diversion issues?

Not all diversion problems can be solved by using RTLS. Clearly RTLS will not address the deliberate arming of armed opposition groups or militias by exporting or importing States, nor the change in end-use by an importing State. Nor will it stop theft. We must see it as an extra security layer on top of existing security measures. If the integrity of containers is compromised or containers deviate from pre-determined routes an alert will be triggered, and adequate measures can be taken. For example, Kenya is a transit country for shipments to Uganda, Rwanda or the eastern DR Congo. In 2010 a consignment of ammunition transported by road on behalf of the United Nations Mission in Congo (MONUC) was hijacked in transit between Mombasa and eastern Congo. The Kenyan officials were very displeased with the lax security provided by MONUC.[71]

In the before mentioned Panama example (see above Example 2, Section 1) the passing of Colon would have been immediately reported by a container tag. Since July 2002 all ships of 300 gross tonnage and upwards engaged on international voyages have to be fitted with an automatic identification system (AIS)[72]. AIS was not designed to be a security system, but a collision avoidance system. Since its introduction AIS is also used for maritime security and fleet tracking. It automatically sends to shore stations and other ships the ship's identity, type, position, course, speed, navigational status and other safety-related information. Starting from 2006 AIS was also introduced onto smaller ships. AIS has a limited range, therefore a satellite-based AIS was developed as a global ship surveillance system.[73]

It should be noted that AIS was conceived as an open system, and therefore anyone with an AIS receiving station can access AIS data. Much of this data is available on the internet by/for the maritime industry or maritime enthusiasts. In 2004 the Maritime Safety Committee (MSC) condemned the publication of AIS data on the internet, and urged member States, "subject to the provisions of their national laws, to discourage those who make available AIS data to others for publication on the world-wide web".[74] The argument used is that this open data can be exploited by pirates or terrorists. Although a risk, there is no evidence that supports this argument. A more plausible explanation for this stance is the insistence on commercial confidentiality and secrecy within the maritime industry.[75]

70 Email conversation SCT Technology, 20 February 2018.
71 Interview with Kenya Revenue Authority, 17 June 2010.
72 SOLAS, Regulation 19. The ship's maneuvering status determines the intervals at which AIS data is transmitted. AIS data is send autonomously and continuously, and contains dynamic data (navigation status, speed...) and static data (IMO number, call sign, ...). For further information see, M.N. Murphy: Lifeline or Pipedream? Origins, Purposes, and Benefits of Automatic Identification System, Long-Range Identification and Tracking, and Maritime Domain Awareness, in: R. Herbert-Burns, S. Bateman, P. Lehr (eds.): Lloyd's MIU Handbook of Maritime Security. CRC Press, Boca Raton, 2009, p. 13-28.
73 Y. Chen: Satellite-based AIS and its Comparison with LRIT. In: Transnav, the International Journal on Marine Navigation and Safety of Sea Transportation, 2014 (8), 2: p. 183-187.
74 Report of the Maritime Safety Committee on Its Seventy-Ninth Session, International Maritime Organization, MSC 79/23, 15 December 2004: p. 59.
75 M.N. Murphy: Lifeline or Pipedream? Origins, Purposes, and Benefits of Automatic Identification System, Long-Range Identification and Tracking, and Maritime Domain Awareness, in: R. Herbert-Burns, S. Bateman, P. Lehr (eds.): Lloyd's MIU Handbook of Maritime Security. CRC Press, Boca Raton, 2009, p. 16.

Long-Range Identification and Tracking (LRIT) system

A true ship tracking system came into being when the International Maritime Organization introduced the Long-Range Identification and Tracking (LRIT) system which provides for the global identification and tracking of ships.[76] Every six hours the ship transmits automatically the identity of the ship; the position of the ship (latitude and longitude); and the date and time of the position provided.[77] During the development phase of the LRIT system the Maritime Safety Committee instructed its Sub-Committee on Radiocommunications and Search and Rescue (COMSAR) "to bear in mind the lessons learnt from the publication on the world-wide web or elsewhere, of AIS data transmitted by ships when developing the LRIT system".[78] The data generated by this system is only accessible by the contracting States.

4. CONCLUSION

One needs to recognize that the current commonly used definitions and descriptions of 'diversion' are inadequate. A working definition for acts of diversion should include the unlawful and unauthorized physical re-directing of the arms or related items in the supply chain, as well as the unlawful or unauthorized change of ownership and effective control in the chain of custody. Both elements shed light on diversion. In addition, as is argued above, it is important to consider the "unlawfulness" of a diversion in relation to international legal obligations, and not only in relation to national laws. Both may entail individual criminal responsibility. This is especially the case for international transfers between territorial and national jurisdictions. A neglected aspect in some literature is the requirement for the prior consent of the importing State, and not only the exporting State. This is addressed to some extent in the UN Firearms Protocol and is also in line with the obligations set out in the Arms Trade Treaty, which, *inter alia*, recognizes the "sovereign right of any State to regulate and control conventional arms exclusively within its territory". The only exception is provided for in the UN Charter.

The latest real time tracking technology could help prevent acts of illegal diversion of arms and related items at all points in the physical supply chain, and deter illegal transactions to divert ownership and control of the items. The use of Real-Time Location Systems leaves a visible breadcrumb trail making diversion harder. The tracking of containers could even be combined with the tracking of the vessel using the Long-Range Identification and Tracking system. Perhaps the use of active RFID tags for SALW and ammunition shipments should become mandatary. Cost should not be an issue here taken into consideration the cost to society at large if shipments are diverted and misused.

76 http://www.imo.org/en/OurWork/Safety/Navigation/Pages/LRIT.aspx
77 Resolution MSC.202(81), adopted on 19 May 2006.
78 Report of the Maritime Safety Committee on Its Seventy-Ninth Session, International Maritime Organization, MSC 79/23, 15 December 2004: p. 59.