CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON

Handbook of best practices for strategic trade control enforcement at ports

Edited by Stephen Osborne

OCTOBER 2023

Table of contents

Introduction 3

Chapter 1: Sanctions 4

Chapter 2: Strategic trade controls 8

Chapter 3: National implementation, licensing, enforcement and outreach 10

Chapter 4: General overview of port privatisation 14

Chapter 5: Screening and tracking of vessels 16

Chapter 6: Boarding and searching vessels 19

Chapter 7: Screening cargo 21

Chapter 8: Inspecting cargo 24

Chapter 9: Port security 25

Chapter 10: Coordination 28

Conclusions 30

Acknowledgements

This handbook was made possible with funding from the US Department of State's Export Control and Related Border Security Assistance program.

The editor wishes to thank the following experts (in alphabetical order) for their inputs to the training course on which this summary is based:

- Dr Cem Boke, Research Associate, King's College London
- Martin Drew, Consultant, British Export Control
- Professor Marleen Easton, Head, Governing and Policing Security (GaPS) Research Group, University of Ghent
- Nick Evans, Asset Manager Marine, Port of London
- Andrew Horton, Senior Technical Policy Advisor, UK Government Export Control Joint Unit
- Dennis Leenman, Strategic Trade Controls/Sanctions Expert, Netherlands
- Stephen Osborne, Research Associate, King's College London
- Dr Christopher J Watterson, Research Fellow, King's College London
- Captain (Retired) Neil Watts, Independent Consultant on Sanctions and Maritime Security
- Yvonne Yew, Maritime Expert, UN Panel of Experts, New York City.

The editor also wishes to thank Dr Sarah Tzinieris for copyediting this document, and an anonymous peer reviewer for their comments.

Edited October 2023: Minor corrections to contributors' affiliations and Figure 5.

Introduction

This handbook outlines best practices for enforcing strategic trade controls at seaports (hereafter 'ports'). The concept of 'strategic trade controls' (STCs) captures both national export controls, for example those placed on high-tech and military-relevant material and technologies, and sanctions, which are broad restrictions on economic engagement with states or individuals issued by national agencies as well as international organisations, such as the United Nations (UN).

This handbook is based on extensive research, consultation with a wide range of government, industry, and academic experts, and King's long-standing programmes of training and outreach designed to strengthen the implementation and enforcement of STCs in countries around the world. It is designed primarily for use by government agencies with responsibilities for enforcing STCs at ports, with typical such agencies including those with responsibilities for customs and border protection, policing and law enforcement, port management and governance, import and export licensing, trade regulation, maritime domain awareness, and industry outreach.

Chapters 1–3 provide an introduction to STCs and the national and international agreements and frameworks that underlie them. Chapter 4 focuses on port privatisation and the implications this carries for STC enforcement. Chapters 5–9 outline best practices in STC implementation and enforcement at ports, covering: vessel screening, tracking, boarding, and inspections; cargo screening and inspections; and port security. And Chapter 10 outlines best practices in coordinating STC implementation and enforcement at the national and international levels.

Above all, this handbook demonstrates that there is an inherent contest, or conflict, between the implementation and enforcement of STCs at a port on the one hand, and that port's rapid and efficient throughput of goods on the other. Overly onerous enforcement will grind legitimate commercial port operations to a halt, while lax enforcement risks the port becoming a hub for STC violations, which carries risks for local, national, and international security. In trying to find the right balance, enforcement

A compromise needs to be struck between enforcement agencies on the one hand, and commercial stakeholders involved in the import, export, and transhipment of goods on the other; one that broadly aligns with international best practices in risk-based STC enforcement.

agencies must adopt a risk-based approach to STC enforcement. A 100% success rate in preventing STC violations (or the illicit shipment of any other goods) is impossible using current methodologies, practices and equipment. A compromise needs to be struck between enforcement agencies on the one hand, and commercial stakeholders involved in the import, export, and transhipment of goods on the other; one that broadly aligns with international best practices in risk-based STC enforcement.

Regardless of who owns or operates a port, STC enforcement responsibilities ultimately rest with the nation in which the port is situated (port state). This carries several implications. First is the need for a constructive and open collaboration between port and state, whether or not the port is owned/operated by a private or public entity, and/or a domestic or foreign entity. Second, the state must ensure that it retains legal rights to access critical port areas and cargo-related data, and that these rights of access are confirmed contractually between the parties, along with penalties strong enough to ensure compliance by the port owner/operator. Third, the port state should impose obligations on (and give guidance to) the private sector: on traders to ensure that licences are sought where needed; on banks and insurers to conduct due diligence checks on parties involved in transactions; and on freight forwarders to check that they are not facilitating the movement of goods in violation of STCs. Taken together, these measures will all contribute to a state's effectiveness at preventing illicit cargo movement through ports.

Chapter 1: Sanctions

Sanctions are a distinct subset of STCs in that they are primarily designed to put pressure on countries, companies or individuals, rather than the focus being on goods. This chapter examines the function and purpose of sanctions, how sanctions apply in the maritime domain and describes sanctions evasion measures, as drawn from extensive UN reporting.

The function and purpose of sanctions

Sanctions are measures imposed unilaterally or multilaterally in the interest of peace and security. Their purpose is to use peaceful means to put coercive and constraining pressure on companies, organisations, governments or individuals, as well as to send strong signals to targets and partners alike.

The commonest forms of sanctions are economic sanctions, which place restrictions on investment and trade, and may restrict imports or exports; arms embargoes, and diplomatic sanctions (such as the expulsion of diplomats or the severing of ties).

Sanctions may be imposed multilaterally – by the UN or the European Union (EU), or unilaterally by individual countries. Article 41 of the UN Charter, for instance, entitles the UN to set sanctions, and obliges all member states to enforce them. Having been agreed at diplomatic level, ratification (such as passing new laws) and enforcement fall to each member state.

The main value of sanctions is that they permit, and oblige, signatories to act to uphold international security. The seizure of the merchant ship *Chong Chon Gang* in Panama in 2013, carrying weapons destined for North Korea, the comparable seizure of the ship *Jie Shun* by Egypt in 2016, carrying weapons from North Korea, and frequent interdictions in the Arabian Gulf of weapons destined for Yemen are all examples of effective enforcement actions based on sanctions.

Sanctions do more than facilitate enforcement actions. They also have a symbolic function: states can demonstrate solidarity with each other or with a wronged party (eg, Ukraine) and show support for international law and for shared norms and values. They also encourage compliance by industry, and carry a risk of commercial and reputational harm, so can be said to have a strong deterrent effect.

In the maritime domain potential involvement in sanctions or STC breaches extends beyond the government agencies (including port authorities, law enforcement, customs, border control and licensing) to the private sector (such as providers of maritime services, banks, trading companies, insurance companies, ship owners and managers).

Sanctions evasion

Countries targeted by sanctions typically respond not by complying, but by resorting to evasion measures. A 2017 UN Panel of Experts report described how sanctions evasion by North Korea was increasing in 'scale, scope and sophistication', as it has continued to do ever since.[1] Nowhere is this more evident than the maritime domain. Law enforcement bodies managing the movements of goods through ports need to be aware of deceptive shipping practices, to better detect criminal behaviour. This section focuses on various evasion tactics in turn (though the list is not exhaustive and new tricks constantly emerge). All information is drawn from actual cases.

Usage of international flag registries, particularly those with a poor due diligence record

Most flag states operate a 'closed' ship registry, in which the ship's owner must be a national or resident of that country. Upwards of 30 countries, however, run a registry that places no such restrictions.[2] Such arrangements are referred to as open flag registries, international flag registries or flags of convenience. This represents normal practice; open registries flag about 70% of the world's merchant shipping tonnage.[3] In the context of sanctions, however, use of an open registry may represent an attempt to conceal a connection between a ship and a country under sanctions. How to detect such malpractice is covered in the screening and tracking section below.

1 United Nations Panel of Experts on North Korea 2017, *Final Report of the Panel of Experts Submitted Pursuant to Resolution 2276 (2016)*, S/2017/150 (New York: United Nations).

2 There is no definitive list of open registries, though the International Transport Workers Federation hosts perhaps the most widely used list: International Transport Workers Federation (no date), 'Current registries listed as FOCs,' https://www.itfseafarers.org/en/focs/current-registries-listed-as-focs.

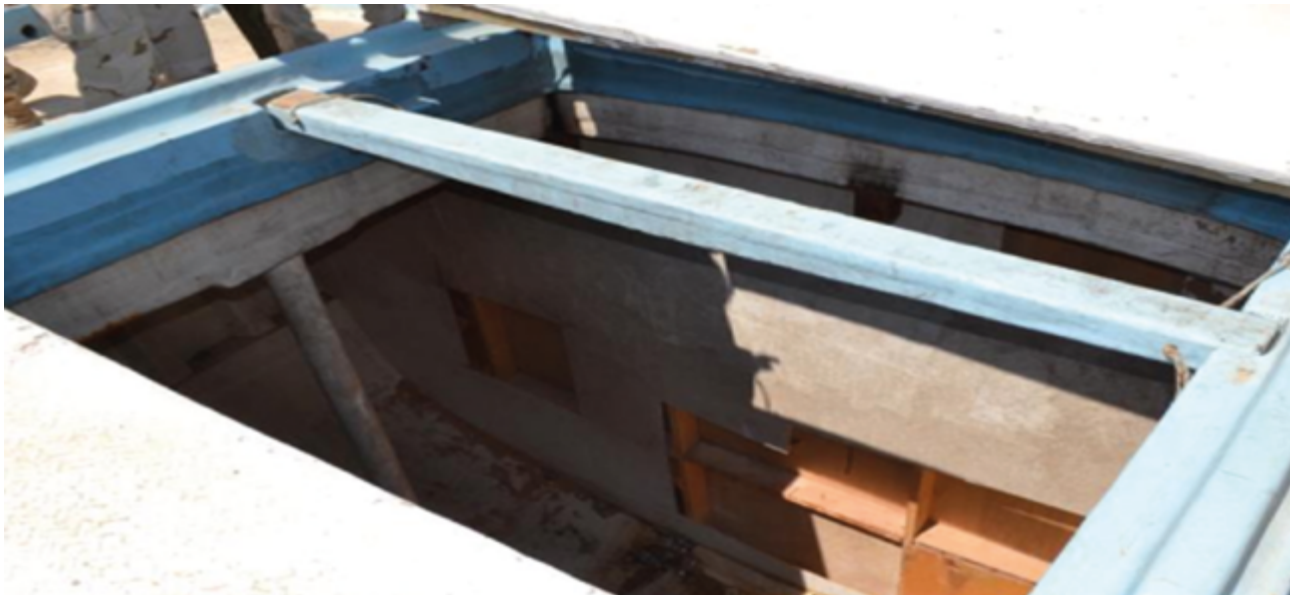
Concealment of illicit cargo

A frequently used tactic is hiding an illicit cargo underneath a legitimate one. When the cargo ship *Jie Shun* was searched in Egyptian waters in 2016, weapons from North Korea were found hidden underneath iron ore.[4] Another ploy is the use of hidden compartments. The dhow *Bari-2* was carrying arms bound for Yemen concealed in hidden cargo compartments (see UN Security Council report S/2021/79).

Figure 1. Weapons concealed under iron ore aboard the *Jie Shun* (2016)

Source: Pictures provided to the UN Panel of Experts by Egypt

Figure 2. Hidden compartment on the dhow *Bari-2*

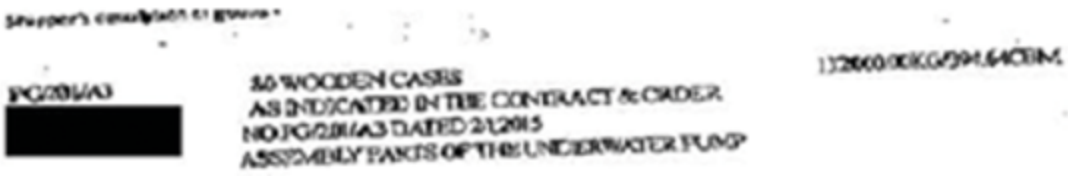


Source: UN Panel of Experts

3 See, for instance: Anna Fleck 2023, 'Flags of Convenience Dominate Maritime Freight,' Statista, https://www.statista.com/chart/29086/flags-of-convenience.

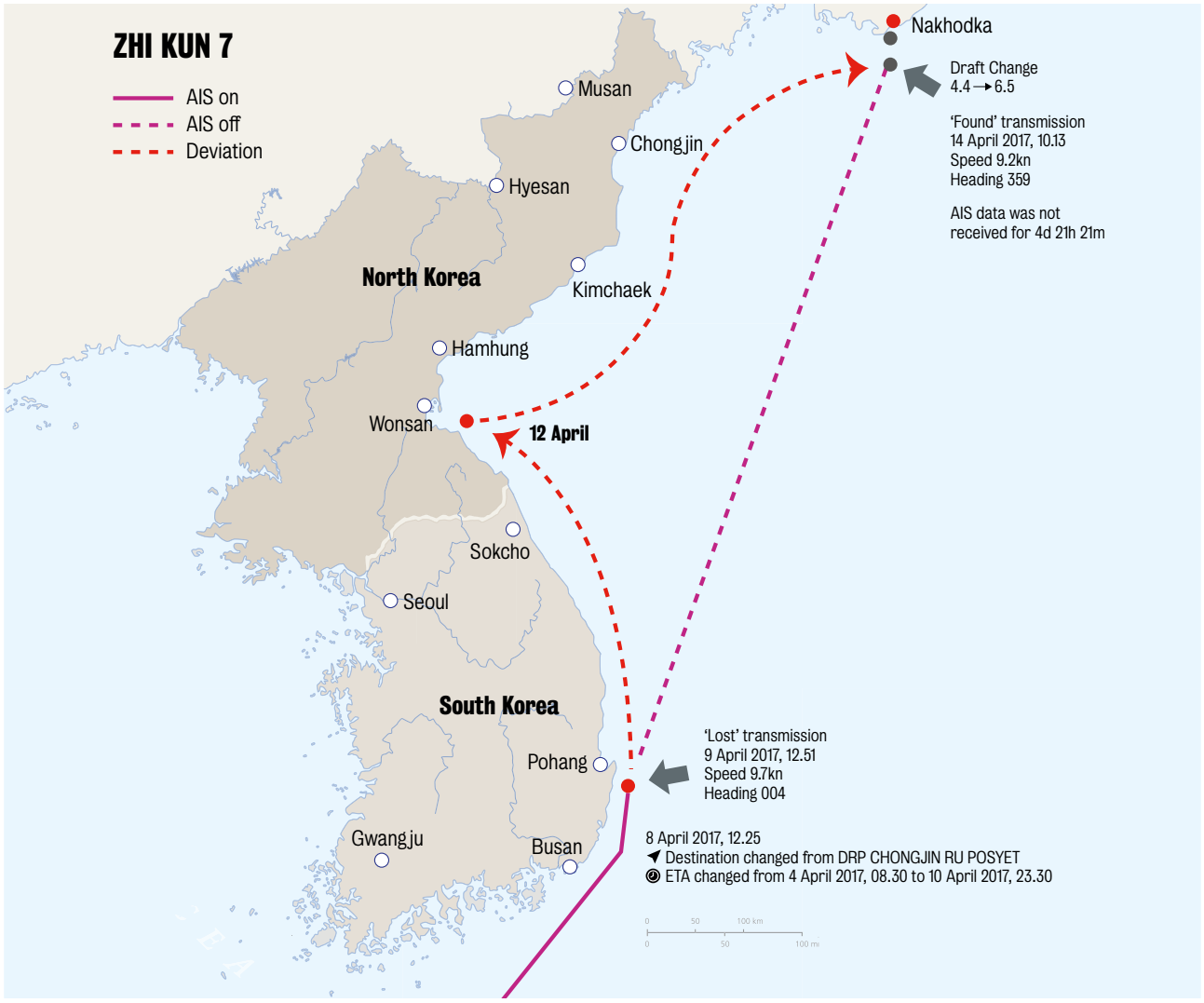
4 United Nations Panel of Experts on North Korea 2017, *Final Report of the Panel of Experts Submitted Pursuant to Resolution 2276 (2016)*, S/2017/150 (New York: United Nations).

Figure 3. Part of bill of lading falsely describing the *Jie Shun's* cargo as pump parts



Source: UN Panel of Experts

Figure 4. Red line showing probable port call in North Korea during AIS blackout



Source: UN Panel of Experts

False information on cargo documentation

Documentation accompanying the cargo, such as the bill of lading or certificate of origin, may mis-describe the goods, or give a false origin. In the case of the *Jie Shun*, weapons from North Korea were described on the bill of lading as pump parts loaded in China.

Deactivation or manipulation of the Automatic Identification System (AIS)

Regular AIS transmissions by a ship, under the International Maritime Organization (IMO) guidelines, identify it and give its course, speed and heading. Sanctions evaders, aware that such information may expose their activity, often switch off the AIS equipment. This makes tracking difficult, but the very existence of gaps in AIS transmission is evident and can be challenged.

Renaming ships; changing MMSI numbers and call signs

After being designated or named in UN reporting in connection with a sanctions violation, it is common for ships to alter elements of their identity. A ship can be renamed, moved to a different flag or transferred to the control of a front company. New Maritime Mobile Service Identity (MMSI) numbers and call signs can be assigned. In addition, these are elements of an AIS transmission that can be falsely entered. Renaming a vessel will have only limited effectiveness against a careful check, as the IMO number, or hull number, remains unchanged. However, creating ambiguity around a ship's identity is a major challenge to enforcement. Techniques to detect such malpractice are found in Chapter 5 of this document.

Deliberately obscure vessel ownership and management arrangements

Entities declared as owners, managers or operators of a ship may have discernible (though deliberately obscure) connections to companies or individuals known to be involved in illicit cargo transfers.

Ship to ship transfers

Transfer of cargo from one ship to another at sea, rather than in port, is a legal and common practice, though in the context of sanctions may constitute a means to conduct trade beyond the jurisdiction and scrutiny of port states. Ports of unloading should investigate if cargo was taken on at sea.

Special note on the importance of the UN Panels of Experts

The role of the panels is to investigate and report breaches of UN sanctions, monitor implementation of the various resolutions, identify gaps, and provide recommendations to assist enforcement and compliance.

Information and reporting from the panels and the sanctions committees they support are some of the most valuable resources to those involved in law enforcement at ports. Comprehensive detail of all restrictive measures and the obligations these place on port states and industry, as well as detailed reporting of breaches, evasion and circumvention, is published on the panels' websites. Although the panels' role concerns sanctions, many of the same evasion tactics apply to any criminal activity in the maritime domain (eg, breaches of STCs).

Chapter 2: Strategic trade control

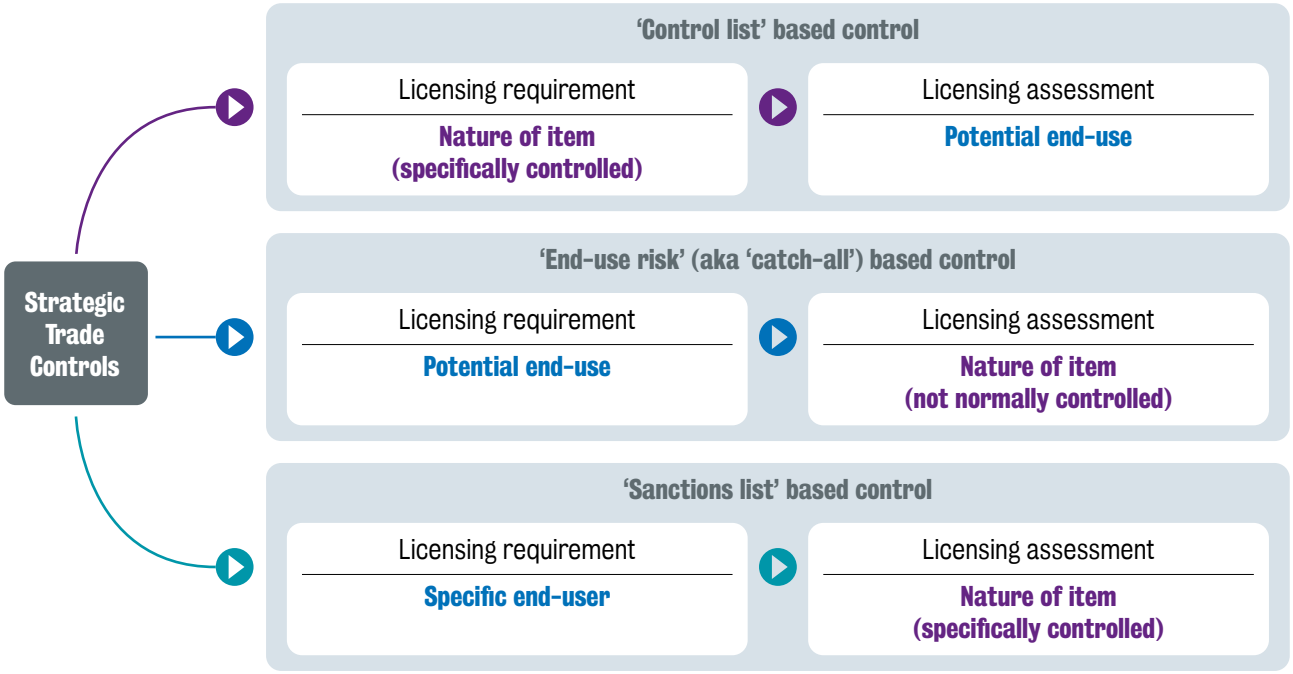
STCs are a complex topic, both in terms of legislation and technical content. A good introduction to the subject is the World Customs Organization's (WCO) Strategic Trade Controls Enforcement (STCE) Implementation Guide. The Guide defines STCs as '.... nationally implemented measures designed to protect society from trans-national acquisition of strategic weapons and goods used to develop or deliver them.'

STCs cover items that could be used to develop, produce or deploy nuclear, chemical and biological weapons, in breach of international legal obligations. Also included here are controls on the spread of conventional arms and conventional military items. The spread of radioactive materials is also of concern in respect of radiological weapons, or so-called 'dirty bombs'.

STCs apply to import, export, re-export, transit, and transhipment, and cover buying, selling and brokering. For goods requiring an export licence, the licensing decision will have been made before the goods are taken to the port. Assuming the exporter is following the legal route (and not attempting to export the goods without a licence), the licence can be checked at the port. In the case of transit and transhipment of controlled goods, enforcement obligations (such as interdiction, inspection or seizure) are not universal but depend on national legislation.

There are three basic frameworks for exercising STCs. First, 'control list'-based controls, where the basis is a specific list of items requiring export approval by a government authority. Whether an export licence is granted or not is based on the end use and end user, but the key trigger is the item itself. Second, end user-based controls (also known as catch-all controls), where the goods themselves are not controlled but may be deemed to have a weapons of mass destruction (WMD)-related application due to the end user. An example might be heat-resistant paint sought by a company linked to the manufacture of ballistic missiles. The licensing assessment is focused on the risk that the items may be used in connection with an activity of concern, and investigations will focus on whether the end user can be linked to entities or activities of concern. This means that there is usually a 'watch list' or database of entities of concern held by national authorities. The third frameworks for exercising STCs is sanctions-based controls. Sanctions measures target companies, organisations, governments or individuals, and specify goods (or entire sectors) that are controlled for those sanctioned entities. Sanctions are covered in more detail in Chapter 1 above.

Figure 5. Schematic showing three basic grounds for export controls



Source: UK Export Control Joint Unit

The schematic in Figure 5 shows the three grounds on which STC are based. If the items are dual-use or otherwise controlled, the assessment is based on the potential end use. If the goods are not controlled but may be destined for an end use or end user of concern, then the assessment is based on the nature of the item. In the case of sanctions, specific targets and goods are named in sanctions lists.

The following international obligations form the framework for export controls.

- UN Security Council (UNSC) resolution-based sanctions and embargoes that are focused on specific countries and entities, for example sanctions on North Korea or Iran. UN Security Council Resolution 1540 requires countries to implement measures to prevent the acquisition of WMD by non-state actors.

- The Biological and Toxin Weapons Convention (BTWC) is an international treaty that aims to prevent the proliferation and use of biological material and biologically derived toxins. This includes controlling transfers of such materials and goods related to their manufacture or deployment.

- The Chemical Weapons Convention (CWC) seeks to prevent the proliferation and use of chemical weapons, and places export controls on chemicals that could be used in such weapons, and any other materials and goods related to their manufacture or deployment. Like the BTWC above, the CWC is a treaty that countries can opt to join.

- The Treaty on the Non-Proliferation of Nuclear Weapons (NPT) is a treaty aimed at stopping the proliferation of nuclear weapons and includes provisions for controlling the transfer of nuclear related items.

- Flows of conventional arms, and some dual-use items, are controlled by the Wassenaar Arrangement and the Arms Trade Treaty, or ATT.

- The Missile Technology Control Regime (MTCR) is not a treaty but nevertheless is a multilateral export control regime, currently with 35 members. It seeks to limit the proliferation of missiles and missile technology, as delivery systems for WMD, and focuses on missiles, rockets and UAV capable of delivering a 500kg payload over 300km.

The CWC, BTWC, NPT, MTCR and the Wassenaar Arrangement form the basis for Multilateral Export Control Regimes, which maintain lists of controlled items and help member states coordinate export controls. The EU's dual-use list consolidates all these lists, and so constitutes a valuable and up-to-date guide to all goods subject to export controls. Dual-use goods are those that have both a military and a civilian use. To give two examples, a lathe may be used in the manufacture of cars or ballistic missiles, while fermenters are essential for vaccine manufacture as well as the production of biological weapons. Implementing UNSC resolutions is obligatory for all UN member states. The other export control regimes operate on a membership basis.

Additional resources

World Customs Organization Strategic Trade Control Enforcement (STCE) Implementation Guide

- http://www.wcoomd.org/en/topics/enforcement-and-compliance/instruments-and-tools/guidelines/wco-strategic-trade-control-enforcement-implementation-guide.aspx

Wassenaar Arrangement lists and best practice guidance

- https://www.wassenaar.org/control-lists
- https://www.wassenaar.org/best-practices

MTCR lists and handbook

- https://mtcr.info/wordpress/wp-content/uploads/2017/10/MTCR-Handbook-2017-INDEXED-FINAL-Digital.pdf

Nuclear Suppliers Group (NSG) lists

- https://www.nuclearsuppliersgroup.org/en/guidelines

Australia Group (AG) lists and handbooks (the Australia Group maintains lists concerned with chemical and biological weapons)

- https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/controllists.html
- https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/controllisthandbooks.html

EU dual-use list

- https://web.archive.org/web/20230115182552/https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159198.pdf

UK export control list

- https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation

Chapter 3: National implementation, licensing, enforcement and outreach

Once agreed at international level, it falls to each country to implement STCs. There is no one correct system or method. Each country has its own structure, its own legal framework, and its own methods. This chapter examines essential components of the process and aims to put the work done at ports to enforce STCs into a broader national context.

Legislation

International agreements such as UNSC Resolution 1540 need to be implemented by all UN member states. The multilateral treaties such as the CWC, BTWC, NPT and MTCR operate on a membership basis, but once states join up, they need to implement the relevant provisions at the national level. In most countries, enforcement relies on legislation. The first step, therefore, is to pass national laws dealing with strategic goods and/or sanctions. This is often the responsibility of the individual state's Ministry of Foreign Affairs or the Ministry of Justice, but consultation with enforcement agencies is advisable to avoid enforcement problems at a later stage.

Powers and responsibilities

National laws must grant sufficient powers to enforcement agencies to enable inspections and criminal investigations. These will include the power to enter premises, to check goods or take samples, to force cooperation and to request documents. Criminal investigations will require powers to carry out arrests, telephone and email intercepts, and house searches. These powers must apply at any location. This means that they apply even if a port is owned or operated by a private or foreign entity.

During the implementation process, responsible agencies for enforcement should be appointed. It must be clear which authority is responsible for different elements such as policy, licensing, intelligence and enforcement.

The licensing process and the role of the licensing authority

Chapter 2 described the three types of export controls: list-based controls, catch-all controls and sanctions-based controls. These form the basis for the licensing process, which is a vital component of a country's export control efforts. A responsible trader will seek a licence before attempting to export a dual-use item, meaning that once the goods reach the port the licence should be in place and can be checked at the port. Where an attempt is made to export goods without a licence the port may detain the goods and refer them back to the licensing body for an assessment. Either way, the key elements in the licensing process are the end user checks and a technical assessment.

End user checks should aim to establish whether the stated end user or other entities involved in the export have any discernible links to WMD. This is intended to defeat scenarios such as an attempt by a ballistic missile entity in, say, Iran, from using a front company, based in Iran or elsewhere, to procure dual-use items from another country. The end user check is based on reference to sanctions lists, watch lists or other databases. Sanctions lists need to be publicly available information, as they are useful to industry and financial institutions as well as the licensing authority. Confidential watchlists are also essential, based on previous illicit activity, or on information held by intelligence and law enforcement agencies.

“
Sanctions lists need to be publicly available information, as they are useful to industry and financial institutions as well as the licensing authority. Confidential watchlists are also essential, based on previous illicit activity, or on information held by intelligence and law enforcement agencies.
”

The 'technical assessment' stage is where a determination is made regarding whether items being exported are subject to control, based on various control lists. The technical assessment is normally undertaken by specialists who have a scientific or technical background. It is useful, therefore, for the licensing team to maintain useful contacts in the state's Ministry of Defence and its universities or other higher education institutions. In many cases, personnel at the exporter or manufacturer of the item being exported are the only ones who can make this assessment, so there is often an element of trust placed in the exporter by the licensing authorities.

Each item on the dual-use list has a unique control list code. This appears on any UK or EU export licence. Harmonised System (HS) codes and the EU Combined Nomenclature (CN) code are also useful, although less specific than the control list code.

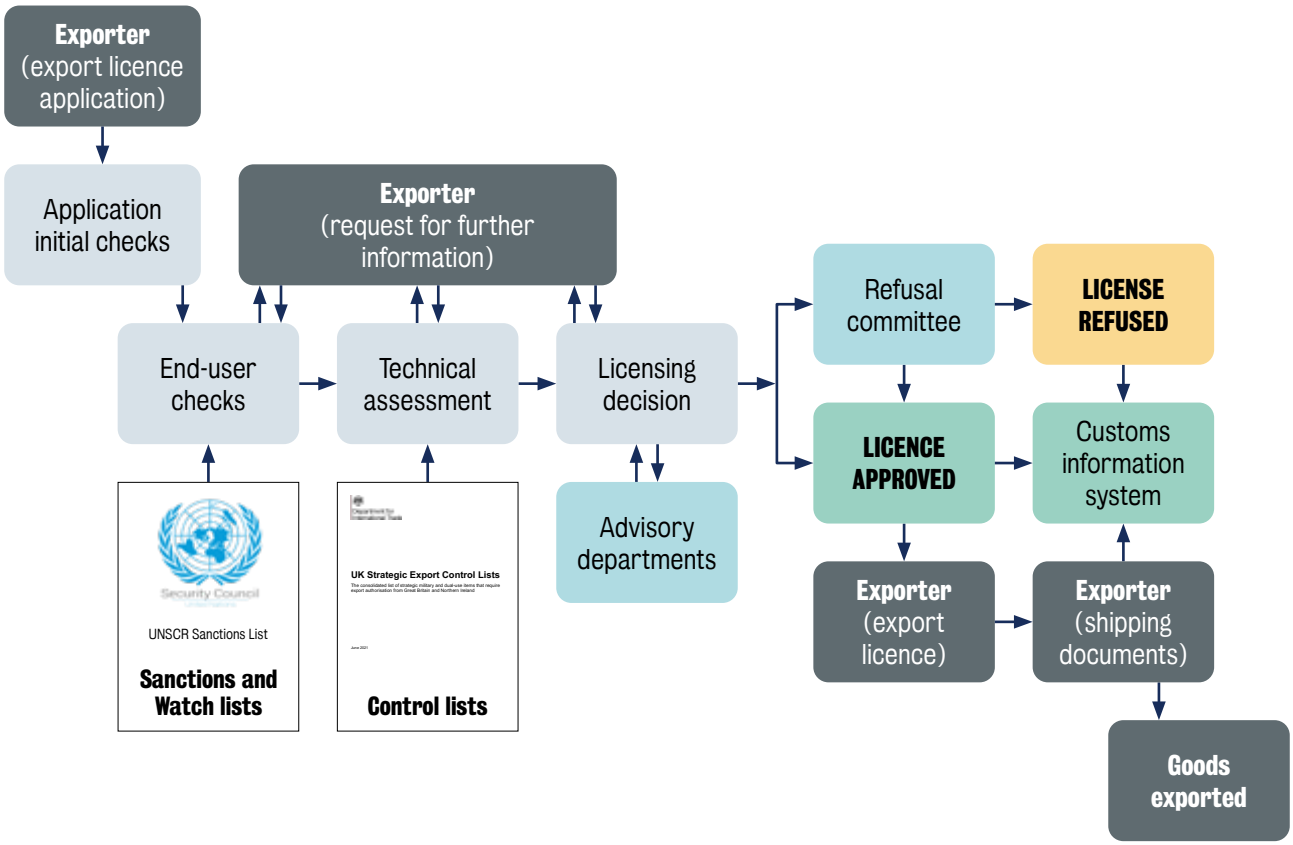
As well as conducting checks and assessments, the licensing authority has an important advisory role to the public. It should maintain a clear and up-to-date website explaining the licensing process and listing all goods requiring a licence. It should invite inquiries from companies as to whether a planned export requires a licence.

The licensing team may be the first point of contact if goods are detained at a port by frontline officials. Customs at the port may have concerns that the goods do not match the licence, or that goods requiring a licence are being exported without one. The licensing authority will attempt to determine the control status of the shipment.

In this way the licensing authority can usefully act as a 'single window' for questions both from customs officers and from industry. Providing a clear point of contact where companies can apply for licences, submit requests, or ask any questions related to STCs will help companies in their efforts to comply with export control laws.

Figure 6 shows how all these components work together. On receipt of a licence application, the licensing team first conducts an end user check (drawing on sanctions lists and watch lists), then a technical assessment (drawing on control lists). The applicant may be asked for more information. After consulting advisory experts where required, a decision is made either to grant or to deny an export licence. Customs are informed of denials, to alert them to attempts to export the item without a licence. If granted, the licence is sent to the exporter, which can prepare shipping documents, enter details (customs declaration) into the customs database and export the goods.

Figure 6. Schematic of licensing process (UK)



Source: UK Export Control Joint Unit

Interagency cooperation

Once responsible authorities are identified, mechanisms to help them cooperate with each other should be set up. This might include regular inter-agency meetings (in the UK these take place fortnightly), where all departments and agencies involved in STCs can discuss current cases (eg, non-straightforward licence applications) and agree actions, as well as discuss longer-term issues such as policy decisions or amendments to the law.

Training and education

Not only must there be sufficient staff, but these staff also require training. Dual-use goods are a challenging area. Battle tanks, arms, and ammunition may be easy to recognise, but dual-use items are much harder to identify. The EU dual-use regulation contains hundreds of pages full of complex technical description. Alongside technical knowledge, staff need good knowledge of legislation. Furthermore, staff need regular training to keep their knowledge up to date, as dual-use regulations are updated frequently to keep pace with evolving technology.

Particularly for enforcement officers, training in auditing and investigating companies is also essential. Training is required in investigative techniques, checking records and conducting questioning, as well as knowledge of criminal methodology in this area (eg, the use of front and cover companies, false or vague description of goods, etc)

Reachback

Customs administrations are, in addition to export controls, generally responsible for enforcing many different regulations, for example, import duties, illicit drugs and counterfeit goods. Not every customs officer can be an expert in all these areas. Therefore, effective STC depends on the availability of technical reachback.

The WCO's Implementation Guide on strategic trade controls recommends two distinct levels of reachback services in two different contexts:

- The first one is a rapid determination during the examination of documentation or the initial inspection of goods at a port. A customs officer who suspects that a consignment may contain strategic goods can contact an advisory expert. This might be an officer who has more in-depth training on export controls and commodity identification. The principle is to reach a quick decision to avoid unnecessary delays.

- The second is if the advisory expert needs additional expertise or a violation is suspected, a full item rating can be requested. This will take longer and must generally be performed by the licensing authority, especially if the judgment will be used in subsequent enforcement and prosecution actions.

Outreach

Outreach is about helping companies meet their obligations. Most companies wish to comply with the rules and avoid committing offences. However, complex legal frameworks and long technical lists of goods make STC a challenging area of compliance, especially for smaller companies that may not have the resources to run a compliance team. Outreach is a useful way to inform companies about their STC-related obligations and the risks to international security.

An informative website, handbooks, factsheets, seminars and visits to companies are frequently-used tools to assist compliance. In the Netherlands for example, the authorities provide an online handbook of strategic goods[5] which explains the law and the rationale behind it, gives information about licence options and explains how to apply for a licence.

Another useful model is the guidance on the export of dual-use items issued by the export control Organisation in the UK.[6] This document explains that under UK and EU export control legislation a licence is required to export certain types of technology and gives detailed information about the legal requirements.

Online and paper-based factsheets can be used to address specific topics, such as 'intangible technology'. As mentioned, STC is a challenging topic, and companies, banks and academic institutions may not be fully aware that exporting or publishing technology or know-how (eg, formulae that may have applications in the manufacture of chemical warfare agents) fall under the same rules as exporting goods.

Seminars and webinars are interactive and allow officials from different agencies to explain processes such as rating/classification, licence applications, internal compliance programs and enforcement. Company visits are a more direct way to remind an individual company, say a manufacturer of dual-use goods, of its compliance obligations.

Enforcement at the border

The most recognisable and visible part of STCs takes place in ports and airports, where export declarations are checked and where inspections take place. This handbook has already discussed the relevance of technical reachback in ports which relates to the technical nature of the goods. However, to be able to select the right export declarations and to select the riskiest shipments for inspection, risk management is important, and setting up 'risk profiles' can improve efficiency. Risk profiling is covered in more depth in Chapter 7 (Screening cargo).

Post-shipment audits

Not every illicit shipment can be detected or stopped. Customs declarations may be misleading or vague, referring to 'consolidated cargo' or 'spare parts'. Furthermore, many customs administrations traditionally focus more on imports than exports, and specifically on those imports (such as alcohol and tobacco) where excise duty is earned. And finally, customs are under constant pressure not to impede the fast and smooth operation of the port.

Recognising these challenges, post-shipment audits can be used as an enforcement tool. By analysing trade flows, and customs data, from public information on the internet and the chamber of commerce, for example, a selection can be made of more relevant entities. Supported perhaps by intelligence gathering, this can be used to create a database of higher-risk entities, whose recent exports can then be audited. The advantage of audits is that they allow a closer look at records, not hindered by the time pressure of trade flows. Auditing can also help select which companies to visit or to invite to seminars or other training opportunities.

Criminal investigations and prosecution

Prevention and education will not always work, for instance in cases of wilful or repeated circumvention of export control laws. Sometimes cases may need to go forward for criminal investigation and prosecution. Important here is that investigators are thoroughly trained in STC legal requirements. It is advisable also to have prosecutors who are well versed in export control law.

5 Netherlands Enterprise Agency (no date), 'Import and export of strategic goods and services,' Business.gov.nl, https://business.gov.nl/regulation/import-export-strategic-goods.

6 Gov.uk 2021, 'Export controls: dual-use items, software and technology, goods for torture and radioactive sources,' https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources.

Chapter 4: Port privatisation and its implications for STC enforcement

This chapter begins by looking at the main features of ports, and then outlines the various models of port privatisation seen around the world. It goes on to examine the implications of port privatisation for the enforcement of STCs, and finally suggests strategies that may help host governments to manage these implications.

There are three main types of operation at any given commercial seaport. First, regulatory functions, concerned with law enforcement, security, safety, customs and immigration. These functions will be typically performed by government agencies. Second, infrastructure functions, concerned with developing and maintaining the port's buildings, berths, cranes, breakwaters, roads and any other structures at the port. Third, port services, including cargo handling, loading and unloading, towing, pilotage and bunkering. Different models of privatisation apply to the second and third types of operation in different ways.

Currently two models of port privatisation prevail. The first is the 'tool port' model, where private entities take on the service functions only. The public port authority manages all infrastructure, as well as performing all regulatory and law enforcement functions. The second is the 'landlord port' model, where private entities take on both the service and infrastructure functions at the port. Under the landlord model, the public port authority will typically lease land to private entities, which then build and operate a port. The various functions carried out by ports are depicted in Figure 7, along with annotation showing which functions are likely to be carried out by public or private entities under the tool port and landlord models.

In practice, many of the private port owners and operators are partly or wholly controlled by a government. Terminal operator Dubai Ports World is controlled by the government of the United Arab Emirates, and PSA International is owned by the Singaporean government. By far the biggest national government stakeholder in foreign port operations, however, is China. Through a network of over 30 state-owned enterprises specialising in terminal operations, shipping, construction, and logistics, the Chinese government now operates in dozens, if not hundreds of ports around the world.

A potential conflict of interest can arise between STC enforcement and the priorities of private port operators. Maximising the rapid and efficient throughput of cargo increases profit, as well as the port's ability to compete with other ports in the region. Private port operators might therefore be concerned that cargo inspections could affect their profit and their reputation. Additionally, enforcement agencies may struggle to keep pace with a rapidly expanding port.

Figure 7. Models of port privatisation

	Regulatory functions	Infrastructure functions	Service functions
	• Licensing port works • Customs and immigration • Port safety and environmental standards • Vessel screening for entry • Emergency services • Vessel traffic safety • VTS services	• Project management and supervision of civil engineering works • Constructing berths, sea locks, breakwaters etc • Maintenance and renovation works • Procuring and servicing mobile assets, eg container cranes, x-ray scanners	• Pilotage and towage • Cargo and passenger handling • Warehousing • Security • Line handling • Waste disposal
Tool port	**PUBLIC**	**PUBLIC**	**PRIVATE**
Landlord port	**PUBLIC**	**PRIVATE**	**PRIVATE**

This apparent conflict of interest is tempered by the fact that no private port would wish to attract a reputation for customs violations, or any other breaches of security. But on a day-to-day basis, any delay to the port's smooth operation is a threat to profit and reputation. A further risk to STC enforcement arises where the port operator is owned by a foreign government. Specifically, those operators may facilitate STC violations if doing so is in the interest of the government that controls them.

Figure 8 shows how some STC-related functions may be carried out by a private port owner or operator, especially under the landlord port model. Put another way, private entities, and potentially the governments that own them, may gain control over STC-relevant port services and infrastructure. In all privatised ports, cargo handling operations, and many security functions, will be performed by the private company.

The following strategies can help ensure STC compliance at ports controlled by private operators, including those controlled by foreign governments.

- Ensuring STC compliance obligations are included in written contracts with private terminal operators.
- Building STC infrastructure needs into contracts with terminal operators, such as provision of inspection terminals and office space for customs liaison officers.
- Ensuring that penalties for STC violations are clearly defined and communicated and are strong enough to deter non-compliance. Penalties would allow for criminal and civil liabilities, and might result, in the most severe cases, in the termination of private terminal contracts.
- Ensuring that enforcement officers have necessary legal authorities, and access to all port areas and documentation; and are indemnified against legal action resulting from an enforcement action. This should be formalised in law, then agreed with the private owner/operator.

Figure 8. STC-relevant functions that may be carried out by private entities

STC-relevant functions	Regulatory functions	Infrastructure functions	Service functions
	• Licensing port works	• Project management and supervision of civil engineering works	• Pilotage and towage
	• Customs and immigration	• Constructing berths, sea locks, breakwaters etc	• Cargo and passenger handling
	• Port safety and environmental standards	• Maintenance and renovation works	• Warehousing
	• Vessel screening for entry	• Procuring and servicing mobile assets, eg container cranes, x-ray scanners	• Security
	• Emergency services		• Line handling
	• Vessel traffic safety		• Waste disposal
	• VTS services		
Tool port	**PUBLIC**	**PUBLIC**	**PRIVATE**
Landlord port	**PUBLIC**	**PRIVATE**	**PRIVATE**

Chapter 5: Screening and tracking of vessels

Screening is about checking the details of a ship, and any people and companies associated with it. Tracking is the process of identifying a ship's current and recent locations. As well as screening and tracking, this chapter also covers how open-source checks can complement screening and tracking to help STC and other law enforcement.

Officials at ports, or in more central roles, concerned with STC enforcement need to know various information in advance of a ship's arrival. These include whether it is connected through its flag history to a country under sanctions; whether any of the several companies typically associated with any merchant ship can be linked to entities or activities of concern; whether the ship has visited countries of concern, made undeclared port calls or made attempts to conceal its location. They also need to know if it, or companies linked to it, are named on sanctions lists or come up in UN reporting. Such information will help enforcement agencies decide whether to take a closer interest in that ship's cargo or, in certain circumstances, refuse access to the port.

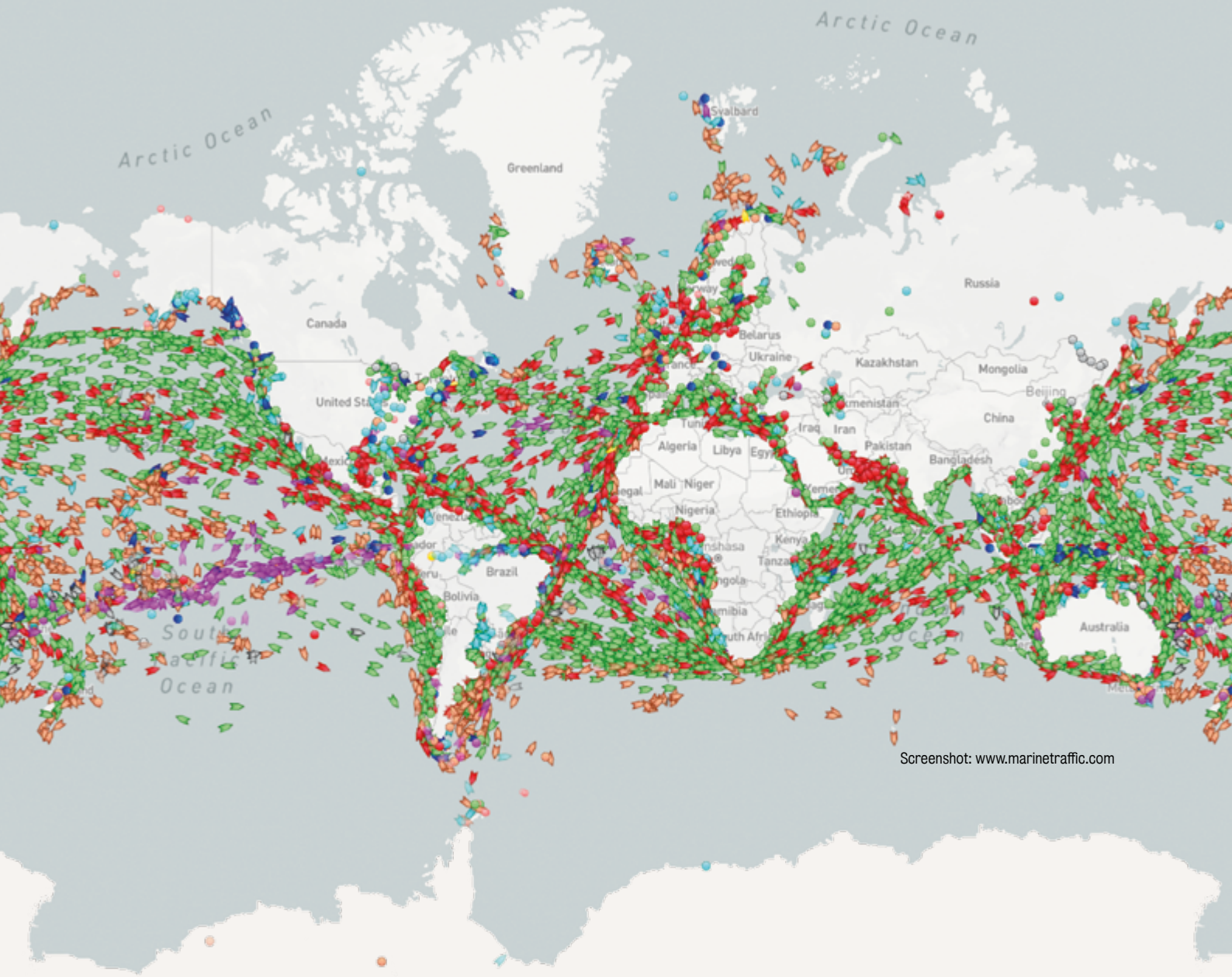
Which agency carries out such checks varies from country to country, but the main elements should be a fast and consistent checking process, whose results are recorded and shared with relevant partners. Screening, tracking and open-source checks may be carried out by each port, or by a central resource.

Under IMO rules a ship should give at least 24 hours' notice of its intention to enter a port. This is communicated in the form of a Pre-arrival Notification (PAN). The PAN form contains a ship's details, its previous ten ports of call and any ship-to-ship transfers undertaken. Receipt of the PAN form can be the trigger for shore-based authorities to carry out screening, tracking and open-source checks.

Each country should develop its own process, but we recommend the following screening, tracking and open-source checks:

Table 1: Screening, tracking and open-source checks

Recommended check	Suitable data sources
Check the current flag and the flag history. Ships with a North Korean or Russian flag are subject to port bans in many countries. Ships that have recently moved from a North Korean or a Russian flag to another registry may have done so as a sanctions evasion tactic. Frequent changes of flag (flag hopping) – legal but commercially unnecessary – warrant closer inspection on the same grounds.	Equasis, GISIS, subscription-based tools such as PurpleTrac or Marine Traffic.
Check all companies associated with the ship (registered owner, ISM manager, operator and beneficial owner) for any links to sanctioned entities. Check for front companies operating out of the same address, or controlled by the same individuals, as sanctioned entities. Check previous companies too – the vessel may have ostensibly changed hands yet remain under the control of companies linked to illegal activities.	Equasis, GISIS, subscription-based tools such as PurpleTrac or Marine Traffic. Sanctions lists.
Check the locations of the ship over the last 12 months, including ports of call. Compare findings against information provided in the PAN. Check for any significant AIS gaps (what counts as a significant gap is open to debate, but a 24-hour gap may be sufficient to allow an undeclared port call or ship-to-ship transfer).	Subscription-based tools such as PurpleTrac, Marine Traffic or Fleetmon. Current location information is free, but previous locations require subscription.
Check whether the ship, or any associated companies or individuals, can be found in sanctions lists, UN reporting or media reporting in connection with sanctions breaches.	UN Panel of Experts reports. UN and national sanctions lists. General internet searches.



Screenshot: www.marinetraffic.com

Screening and tracking information are drawn from two main sources. The main source of data on the characteristics of a ship (including information on flag, owner etc) is collected and made available by the IMO. Tracking information is based on transmissions from the onboard Automatic Identification System (AIS). IMO and AIS information has been used to develop a range of screening and tracking tools. Some of the tools available are as follows:

Marine Traffic, Fleetmon. Two tools offering a similar range of screening and tracking services. Both have a free version, offering a vessel's characteristics (based on publicly available IMO data) and its current location (based on the latest AIS transmission). Previous locations require a subscription, but this pay-walled data allows more functionality, such as the identification of any AIS gaps over the 12 months prior to the search, or the setting up of 'watch zones' around a port or coast, electronically tipping off the subscriber if any ship enters it. 'Watch lists' of ships of particular concern can be set up also.

- https://www.marinetraffic.com
- https://www.fleetmon.com

Sea-web and AIS-Live. Subscription-only service giving comprehensive detail of merchant ships and maritime companies. Sea-web provides screening information, and AIS-Live tracking information.

- https://maritime.ihs.com

Equasis. Free service providing current and previous flags and company information for any merchant vessel. Equasis allows searching by ship or company.

- https://www.equasis.org

GISIS. The Global Integrated Shipping Information System is the IMO's own database. Free to use, it gives present and previous flags, and current companies, associated with a ship, and indicates whether a ship or associated company is subject to sanctions.

- https://gisis.imo.org

PurpleTrac. Subscription-only service offered by Pole Star. Providing screening and tracking data, PurpleTrac also has some sanctions functionality, generating automated 'warning' or 'critical' reports if the ship being searched on has visited a sanctioned port or country, or is owned/managed by a sanctioned entity.

- https://www.purpletrac.com

Both IMO and AIS data have their limitations, and by extension, so do the tools that rely on such data. The IMO depends on receiving regular updates from flag registries giving details of all ships on their register. Some information is therefore inaccurate, incomplete or out-of-date, and there are many ships that do not appear to belong to any registry, and about which the IMO therefore has no current information. The limitations of AIS data are that the equipment can be switched off, making tracking by AIS impossible, and false information can be entered, to report a ship as being in a different place or create ambiguity around its identity. IMO and AIS data sources are still useful, but users should be aware of the limitations.

Performing a series of checks such as those suggested above should allow port authorities and operators to reach a risk assessment on any given ship. There may be a clear breach, such as a North Korean owner, but the risk assessment is more likely to be built up from several factors. If the checks throw up any concerns, the options are as follows: refuse the ship entry to port; challenge the ship's captain about any concerns before deciding whether to grant the ship entry to port; or allow the ship to enter port but carry out specific searches etc.

Using sanctions lists to complement screening and tracking

Sanctions are imposed by the UN, the EU and many individual countries. UN listings are applicable to every member state. However, unilateral listings, even if not binding outside the country that applied them, are nevertheless valuable resources, particularly as maritime security incidents typically cut across multiple jurisdictions.

Due diligence must not just be performed; it must be demonstrably performed. It is important:
a) to have a process, and to form a dedicated and trained team familiar with necessary tools. Update this process to meet new risks and to make use of new tools.
b) to ensure that the process is followed consistently, and that the team knows what to do and who to contact when a suspicious vessel is identified. A checklist may ensure consistency as well as make the process easier and faster.
c) to keep records of all checks performed. That way, if an inadvertent breach does occur, authorities and operators can prove that they followed a strong, consistent process, and did everything they could.

Table 2: Consolidated sanctions lists

Sanctions list	URL
UN Security Council Consolidated Sanctions List	https://www.un.org/securitycouncil/content/un-sc-consolidated-list
EU Sanctions List	https://www.sanctionsmap.eu
US Treasury's list of Specially Designated Nationals (SDN) List. The SDN List contains details of all individuals, ships and companies sanctioned by the US.	https://sanctionssearch.ofac.treas.gov
UK Sanctions list	https://www.gov.uk/government/publications/the-uk-sanctions-list
Australian Consolidated Sanctions List	https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list
Consolidated Canadian Autonomous Sanctions List	https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng

The limitations of AIS data are that the equipment can be switched off, making tracking by AIS impossible, and false information can be entered, to report a ship as being in a different place or create ambiguity around its identity.

Chapter 6: Boarding and searching vessels

STCs apply not just at the point of export or import, but also to transits and transshipments. This means that the boarding and search on reasonable suspicion of STC violations, within one's own jurisdiction, forms an integral part of STC enforcement. The Proliferation Security Initiative (PSI) is attempting to coordinate activities in this area.[7] A decision to board and search a vessel may be based on an intelligence tip-off, or on the results of vessel screening and tracking. This chapter looks at the issues of whether to conduct the operation at sea or in port, and then looks at the process itself, from pre-inspection planning, through the search itself to the post-inspection management.

Boarding a vessel at sea will probably only be considered if it is transiting through or near a territory with no intention to head to a port, or if the ship does not comply with a request to divert to a port. Boarding at sea is more challenging than portside boarding for various reasons, including:

- Sea and weather conditions are likely to be more challenging, combined with the need to use helicopters and/or fast patrol boats.
- It is harder to ensure availability of specialist personnel and specialist equipment, as the at-sea boarding would be carried out by a relatively small team.
- It may be harder to access cargoes, as containers cannot be moved around, or bulk cargoes moved.

For these reasons it may be preferable to divert the ship either to a nearby port or to a safe location just offshore. Likewise, if an at-sea boarding indicates STC violations but a thorough examination is impossible at sea, diversion to port may be needed.

> **A decision to board and search a vessel may be based on an intelligence tip-off, or on the results of vessel screening and tracking.**

A state's authority to act depends on whether the ship is within or outside that state's territorial waters, and on the ship's flag status. The following guidance may be followed:

- **Own flag-state vessels.** The state has full authority to act.
- **Foreign-flagged vessels in transit passage.** The Law of the Sea guarantees the right of free and uninterrupted passage. Any enforcement action requires the consent of the flag state. The flag state should respond quickly. In the case of the Turkish-flagged *Rosaline I,* boarded by a German enforcement team under the IRINI mission in November 2020 on suspicion of violating the arms embargo on Libya, a German Defence Ministry spokesman said that no reply was received within four hours, which was seen as tacit consent. As that case demonstrated, having to ask permission from the flag state may open a political/diplomatic dimension to a case.
- **Any vessel heading into a state's port.** The port state has jurisdiction and full authority to act.
- **Stateless or de-registered vessels, or vessels with unconfirmed status.** Every country has the right to board a ship on the high seas to ascertain its flag status (although reasonable grounds for suspicion required).

7 See Federal Foreign Office, Germany (no date), 'The Proliferation Security Initiative,' https://www.psi-online.info/psi-info-en/-/2075520.

Pre-boarding considerations, whether at sea or in port, should include the following:

- **Personnel.** The combination of enforcement officials constituting the boarding team. As search and inspection teams are typically small, there is limited flexibility regarding their make-up. It may be helpful to have a line of communications to expertise on standby ashore, for example to deal with any hazardous materials found.
- **How the team will embark (and disembark) the vessel** if not quayside.
- **Rules of engagement** in the event of resistance or non-cooperation.
- **Tasks to be carried out.** The team should be clear in its objectives before boarding, and what equipment is needed. The cargo manifest and a plan of the vessel's layout are useful.
- **Communications** within the team and with experts ashore.
- **Information and documents** that need to be gathered, and any measures required to prevent the destruction of evidence.

The search itself should include the following considerations:

- Illicit cargo may be concealed under legitimate cargo. North Korea used this ploy in the cases of the *Chon Chong Gang* and the *Jie Shun*. Moving aside bulk cargo at sea is problematic, so it may be preferable to divert the ship to port.
- Opening containers is difficult at sea, as is moving them to a more accessible location on deck. Again, directing the ship to port may be preferable.
- It is important to keep track of the inspection team as they move through the vessel, and to adhere to pre-agreed communications protocols (such as required times to check in with the team leader).
- Managing the crew in a safe and secure manner.
- All documentation should be preserved as evidence needs to be secured.
- Illicit cargo may be concealed in hidden compartments (note the case of the *Bari-2*, discussed in Chapter 1 above).

Post-interdiction considerations should include the following:

- **Management of the vessel.** If a decision is taken to seize the vessel or cargo, a suitable berth must be found, either inside or outside port. Security arrangements need to be put in place. Under certain circumstances a seized vessel may be sold to defray costs or offset unpaid fines.
- **Management of captain and crew.** Crew may be transferred to a secure facility that takes crew welfare into account. Crew should be given access to respective embassies. The port state should consider approaching an international NGO such as the Red Cross to oversee crew welfare.
- **Disposal of the cargo.** The UN Security Council authorises states to dispose of seized items whose supply is prohibited under UN Security Council resolutions. Goods may be destroyed, rendered inoperable or transferred to another state.
- **Reporting** to the UN is mandatory for breaches by North Korea, but should be considered for any sanctions- or STC-related seizure. Feedback to the flag state should also be considered.

Chapter 7: Screening cargo

Although presented here as separate chapters, cargo screening and cargo inspection are two parts of the same overall task of preventing illicit movements through ports. The screening occurs first and is a large factor in determining whether a physical inspection is required. Whereas screening will be applied to as high a percentage of the cargo as possible, only a very small percentage of it will end up being physically inspected.

Cargo screening and inspection are undertaken to determine if a consignment is STC-compliant. Even if goods are controlled, the transfer may be legal if, say, a licence is in place, or the goods' specifications fall below thresholds of concern. The technical analysis often required makes this a challenging area of enforcement.

To illustrate this challenge, consider the following examples. A shipment of heroin, in any context, is likely to be illicit. But this is not the same for controlled strategic goods. For example, a jurisdiction may place export controls on hydrazine, a chemical compound used in jet and rocket fuels. But this does not mean that every export of hydrazine from that country will be illicit. Rather it will only be illicit if, for example, it exceeds the legally allowed specifications, or if it is being shipped to a banned entity, or if the shipment is without the proper licences. The STC officer must determine therefore not only whether goods are subject to controls, but also whether the shipment complies with the law.

Cargo screening entails the gathering and analysis of any documentary data. This may include invoices, certificates of origin, bills of lading, import and export licences, packing lists and insurance certificates. Information not only on the goods themselves, but also on their importer and exporter and any intermediaries, the goods' origin and destination, and any transhipment, may be relevant.

Cargo screening requires three steps. First, obtaining a detailed description of the goods, using sources such as the product description, HS code or manufacturer. Second, determining whether import, export or transhipment of those goods is controlled. This can be done by checking against a definitive list, such as the EU's list of dual-use goods. If controls exist, then the third step is to establish whether licensing and certification are in place to make transfer of the controlled goods legal. If the requirements are not met, the goods should be detained. Reaching a decision may require 'reachback' to technical experts in industry, academia or government, or a request for further documentation from the consignor.

Enforcement officers should bear in mind that a deliberately vague description of the goods is often used to conceal a non-compliant cargo. For instance, a description 'reactor vessel' covers many controlled as well as many non-controlled items. In such a case, a check of the HS code, or a close check of the entities involved, may be appropriate.

Cargo screening and inspection are undertaken to determine if a consignment is STC-compliant. Even if goods are controlled, the transfer may be legal if, say, a licence is in place, or the goods' specifications fall below thresholds of concern

Following the goods check, cargo screening moves on to check all entities involved, to determine and screen the source of the goods, the end user and any intermediaries. If any entity appears on a sanctions list, or a watch-list maintained by the investigating country, then there may be grounds to detain the goods even if they are not controlled (on end user grounds or under so-called catch-all provisions).

Screeners should be alert to documentary anomalies, which would result in the investigation being escalated. Below are some red flags of STC-relevant misdeclarations:

- Contradictory information provided on a consignment's documentation is a red flag. For example, the importer's address may be different between the bill of lading and the end use declaration. Contradictory information suggests an attempt to misrepresent the goods or entities involved in the consignment, or a sudden change to the consignment.

- A consignment appearing unusual or out of character for one or more of the parties is a red flag. An example would be a consignment of 50 tonnes of titanium alloy to a pet store, or a consignment worth US$15 million purchased by a company with an operating budget of only US$100,000. This suggests the use of shell companies to hide the true source or destination of a consignment. Out of character consignments can also manifest at the national level. For example, an export of uranium from the UK should be considered suspicious as the UK currently has no commercial uranium mining or milling operations.

- Any documentation that appears forged or is otherwise not authentic, for example fabricated export or end use licences, is a red flag. Forgeries are a strong indicator of an attempt to misrepresent the goods or entities involved in the consignment.

- The importer or exporter having a history of STC non-compliance is a red flag. It suggests that the importers or exporters may lack the willingness or capacity to comply with STCs. Information on the compliance histories of importers and exporters may be gathered internally, for example through records on previous transactions, seizures, investigations, audits and licence applications. Or it could be gathered from external sources, such as media reporting.

- A consignment not having a clear commercial rationale is a red flag. Recognising that trade is a business, legitimate traders will generally pursue commercial efficiency in their trade. Thus, for example, if a consignment of coal is purchased at double the prevailing market price, or if that coal is traveling to the end user via a slow and expensive shipping route, the objectives of the importer and/or exporter come into question.

- The importer and/or exporter having links to designated entities, even if they are not designated entities themselves, is a red flag. For example, an importing business may be co-located with a designated entity or be part-owned by a designated entity. Links to designated entities suggest the use of shell companies to hide the true source or destination of a consignment.

- The importer and/or exporter having similar names to designated entities is a red flag. A common evasion tactic for designated entities is to make slight changes to their personal or business names so that they are not matched to designated entity lists. For example, an individual may use an alternative Romanisation of their name. Another common technique used by North Korean entities is to declare themselves as based in just 'Korea', making it difficult for cargo screeners to determine whether the entity is in South Korea or the sanctioned North.

- Late presentation of customs documentation, or an agent pressing for the release of a consignment, is a red flag, as it suggests that the agent is trying to rush the approval process in order to minimise scrutiny of the consignment.

- Unusual terms of payment, for example barters, cryptocurrency or gold, are a red flag, as it suggests that the true importer may be barred from regular financial channels and is thus more likely to be a designated entity.

- The mode of transport, or transport or insurance costs being inconsistent with the goods is a red flag. For example, a consignment of toys may be shipped in a reefer container, or insurance costs for a consignment may be well above the market rate for that particular commodity. Such red flags suggest that the goods have been mis-declared.

- First time importers or exporters are a red flag, as newly established trading companies may be shell companies for other, more established traders.

- And finally, shipments to trading companies are a red flag, as it suggests that the consignment will then be forwarded to another non-declared party.

An approach recommended by the WCO is to implement an Authorised Economic Operator (AEO) system, which allows importers and exporters with strong records on trade control compliance to bypass some of the checks associated with cargo screening.

As well as documentation, other indicators that contribute to the screening process, and may inform a decision on whether to inspect a cargo, include:

- Physical indicators, such as the weight of the cargo not corresponding to the goods described, the presence of radiation or explosive residue, or the condition of the cargo container or the tamper seal.

- Intelligence, eg, from informants, investigations or international partners.

A clear challenge to cargo screening is the sheer volume of cargo. A port's reputation depends on the rapid and efficient throughput of goods, but alongside this is the requirement to screen incoming and outgoing goods for potential breaches of STC. This screening process must be thorough enough to satisfy regulatory requirements, yet fast enough to avoid disrupting the port's smooth operation. Furthermore, a country's approach and methods must be kept confidential, both from the public and from partner countries, to prevent 'patterning' by criminals.

An approach recommended by the WCO is to implement an Authorised Economic Operator (AEO) system, which allows importers and exporters with strong records on trade control compliance to bypass some of the checks associated with cargo screening. An AEO may be able to submit fewer documents to cargo screening agencies or be exempt from having their consignments weighed before release. For STC enforcement, such a system offers two benefits. First, it incentivises importers and exporters to strive for high STC compliance to gain the benefits of reduced regulation. And second, officials can focus resources on importers and exporters at higher risk of non-compliance.

In many larger ports the number of declarations is too high to inspect every single shipment. Therefore, the use of **risk profiles** could help to select more relevant ones. The risk profile is an aggregation of several risk indicators. Most common indicators relate to goods and to end-users, but will also consider any previous non-compliance by a particular exporter, and the risk of diversion. Risk profiling is not practicable for each port to do by itself. Rather it is a role for the licensing body or a central customs office, which would collect relevant information from different stakeholders across the export control system.

The ability of customs and other officials to carry out cargo screening tasks assumes a free sharing of cargo data between government agencies and the port operator, whether in public or private hands. The contract between the port state and the private port owner/operator must include provisions for data sharing, and the infrastructure and systems required to enable it.

Chapter 8: Inspecting cargo

The previous chapter described the challenges to effective cargo screening at ports. Thousands of tonnes of goods may be passing through each day, most of which furthermore are sealed inside shipping containers. Despite these challenges, enforcement officials at the port must screen incoming and outgoing cargo for possible breaches of STCs. This chapter describes the elements of the cargo inspection process.

A cargo may be selected for physical inspection if any of the following apply:

- Screening of documentation shows the described goods appear on published dual-use lists.
- Any of the named entities appear on sanctions lists or the country's own watchlists.
- Any deficiencies, inconsistencies or anomalies in documentation are detected.
- Screening links the vessel, or any associated company, to an entity or country subject to sanctions or to previous illicit transfers such as breaches of STC violations.

An intrusive inspection involves the opening of a shipping container, which requires breaking the seal. Non-intrusive methods such as the use of X-ray equipment may appear to offer a more streamlined approach, but unfortunately X-ray scanning is relatively ineffective for STC enforcement, as it rarely provides a sufficiently detailed image (for instance it would not be able to distinguish between a pump that is subject to export controls and one that is not). Non-containerised cargo, such as large items of machinery, may be more conducive to non-intrusive inspection, allowing the identification of goods through model numbers or the manufacturer's name.

Even if the decision to open a container is made during a boarding at sea, the inspection itself is best carried out at a port. In port, the container in question can be accessed and offloaded even if at the bottom of a stack, and the costs of accessing the cargo are lower. The port will have a dedicated hangar where inspections can be carried out, and the port operator should bring the container to the search area on request. Whether the port is owned/operated publicly or privately, the port should provide the dedicated search facility, and cooperate with the request by customs or other law enforcement agencies to make the container available to search. This collaboration needs to be specified in the contract between port state and port owner/operator.

Some STC-controlled goods are hazardous – comprising explosive, nuclear, chemical, radiological or biological materials. Enforcement agencies should make use of sensors where possible and ensure that staff have full training and physical protection. Pages 34–35 of the WCO's Strategic Trade Control Implementation Guide[8] gives useful guidance on training and equipment.

Enforcement personnel at the port may need specialist assistance from technical experts based elsewhere. Sustaining an effective reachback service requires maintaining a network of experts practised in the process of assessing the status of potentially controlled goods, and a secure data- and file-sharing capability, enabling, for instance, the sharing of photographs.

Inspection personnel need to be protected from liability for any damage or delay caused to cargoes during inspection. Indemnity should be formalised both in national law and, where the port is owned or operated by a private or foreign entity, in the contract between the port state and the port operator/owner.

Following inspection, the goods will either be released or detained, depending on the outcome of the search. Detention may trigger a criminal investigation, and potentially a prosecution. Those found in breach of STC regulations should expect to face penalties ranging from a warning or small fine to a custodial sentence. To enable prosecutions, the following need to be offences in law, and penalties clearly stated: submitting a false customs declaration; attempting to export controlled goods without a licence; and the creation or use of false paperwork.

Enforcement agencies may wish to inform the consignor and/or consignee about the detention of their cargo. They should also engage international bodies (Organisation for the Prohibition of Chemical Weapons, OPCW, or International Atomic Energy Agency, IAEA) in the event of seizures of chemical, nuclear or radiological material.

8 World Customs Organization 2019, *Strategic Trade Control Enforcement (STCE) Implementation Guide* (Brussels: World Customs Organization).

Chapter 9: Port security

Ports are part of a country's critical national infrastructure (CNI) in enabling the import of essential goods and commodities such as food and oil, and in facilitating exports and trade. They are also border entry points, at which formal procedures must be followed to ensure all movements of goods and people across the border conform to the country's laws.

Ports need strategies to deal with any security threats. Illegal entry to the port, smuggling and, more recently, cyber-attacks, are typical threats to a port's security. Ports may be targeted by actors ranging from individuals to large organised crime networks.

Accountability for security at a port rests with the government and the port authority, but within a port some security tasks may be performed by private security firms.

Every port should adhere to the International Ship and Port Facility (ISPS) Code.[9] ISPS standards apply to all ports. In general, a comprehensive port security architecture consists of three interconnected components: Personnel Security, Physical Security and Cyber Security. These three components will now be discussed in turn.

Personnel security

Vigilant port workers, trained to look out for any suspicious or illicit activity at the port, are a crucial asset and the first line of defence against security risks. Yet personnel can also be the weakest link in the security chain. Negligence or ignorance of procedures could lead to breaches of STC. Furthermore, any port worker who knows the port's routine, has details of cargo handling operations, or has access to data or IT systems, would pose a high security threat if they collaborated with criminal individuals or groups – known as an 'insider' threat. Best practice for ports would consist of the following elements.

Pre-employment screening. The foundation of good personnel security, it verifies the credentials of job applicants and aims to identify any concealed or misrepresented information. This must be done for all people whose work gives them access to port facilities. Checks should include previous work history, career gaps, payslips, references, contacting previous employers to learn why they left, and a social media check.

Avoid single points of failure. To guard against a single point of failure (either through human error or corruption), ports should ensure that more than one person is on duty at any one time, on tasks with direct security implications, such as container/cargo handling or customs clearance functions. IT specialists (in public or private organisations within the port) are more vulnerable to being targeted by criminal groups as they have access to databases and control privileged access to systems, processes and facilities.

Training to all personnel on security. Training should include not only classroom-based or self-paced learning, but regular drills and exercises.

9 The ISPS Code is a mandatory set of security measures administered by the IMO.

Physical security

Best practice includes the following multi-layered approach:

- **Monitoring the perimeter and the interior of the port.** This will include CCTV (along with signage making everyone aware of its presence), and physical patrols. Patrol routines should be (or appear to be) random, to make them harder for criminals to 'pattern', and details of patrols should be kept on a need-to-know basis.

- **Fencing.** Ports should maintain high-security fencing with the least possible portals (entry and exit points). Fencing should be used not only for the perimeter of the entire port complex, but to subdivide the port into separate areas to which access can then be separately managed. It is important that such boundaries are not only difficult to overcome, but also that they give a strong message of being physically and technically secure (eg, through signage, warnings, lighting, etc) to act as a deterrent.

- **Checking the container seal.** The container seal is an important component of physical security. Container seals are a complex topic, but for STC enforcement at ports the following details are relevant. Each shipping container is sealed as soon as it is packed, and the seal should remain intact until the container reaches its final destination. Each seal has a unique number, which is recorded on the ship's manifest. The purpose of the seal is to show whether the container has been illegally accessed en route either to remove legitimate cargo or to add illicit cargo. When the container is accepted at the container terminal the seal should therefore be checked for evidence of tampering and to ensure that the seal number corresponds with the manifest. Any anomaly should result in the container being pulled aside for inspection. It is also possible for seals to break accidentally during stacking and moving. Before leaving the terminal, the container has to be re-sealed whether the seal has broken accidentally or following a customs inspection. Most containers, however, will pass through the port with their seals intact.

Cyber security

As digitalisation and automation at ports increase, so does connectivity between Information technology (IT) and operational technology (OT) systems. At the same time, volumes of data being created, processed, exchanged, and stored continue to grow rapidly. Cyber threats, therefore, and the measures required to counter them, are also rapidly growing and changing.

Ransomware attacks and denial-of-service attacks are common forms of cyber-attacks against port facilities and are often delivered via malicious email attachments. Ransomware attacks can take between seven and 14 days to recover from and attackers may have already breached the backup systems. Ports should consider cloud-based backup systems to ensure some IT and OT continuity.

In June 2017 the Maersk shipping company was hit by a cyber-attack using the NotPetya virus. The virus entered Maersk's systems through an unpatched computer in a local office, but spread across Maersk's network, making all the company's applications and data unavailable for several days. Port operations – including its Rotterdam terminal – were seriously affected, with estimated losses in the region of US$200–300 million.

In July 2021 a cyber-attack against Transnet, a public body which operates major South African ports and most of its railway networks, disrupted container operations at the ports of Cape Town and Durban. Port workers had to resort to a paper-based clearance process for cargo.

Cyber-attacks and STCs

The loss, or compromise, of one or more of the operational services where technology plays an increasingly important role will undermine a port's ability to carry out its functions and may disrupt port operations for days or even weeks.

- Compromised port control, customs and border control, cargo/container reception, handling, storage and monitoring systems, vessel control systems can result in illicit data manipulation which may lead to:
  – Challenges in tracking the locations of dual-use or controlled goods.

  - Changing of cargo details which can increase the risks to safety or allow for the unauthorised release of cargo.
  - Delaying submission of documents required for customs clearances, undermining the ability to process and track cargo/containers properly.

- Compromised security control systems (eg entry controls, vehicle controls) may allow authorised access to the port or to specific containers.

Mitigation measures

Ports should conduct a baseline cyber security assessment to identify critical assets and infrastructure, key processes at the port, key risks, as well as countermeasures. These cyber security assessments should translate into cyber security plans to address the issues identified.

A continuous programme of training for both security and all other staff is a vital component of cyber defence. Training should adopt the International Ship and Port Facility Security Code (ISPS Code) and more specific to cyber security, the IMO's Guidelines on Maritime Cyber Risk Management, issued as MSC-FAL.1-Circ.3.[10]

Regular cyber security exercises and drills should be conducted to increase awareness and promote cooperation among Border Force, police and port staff. These might include:

- Monthly videos distributed among staff to raise awareness of cyber threats.

- Internal (aka 'ethical') phishing and penetration tests to challenge staff and systems.

In the UK, the Centre for the Protection of National Infrastructure (CPNI) provides visual training material regarding personnel, physical and cyber security to help reduce the vulnerability of CNI, including ports, to cyber threats. The CPNI's See Check and Notify (SCaN) training module is designed to increase vigilance among all staff to security threats.[11] Please refer also to the International Association of Ports and Harbors' 2020 report on cyber security at ports.[12]

Security implications for ports owned or operated by private or foreign entities.

Regardless of who owns or operates a port, the port authority and/or other government agencies must be involved in and satisfied with the vetting of all staff working at the port. Security roles at the port may either be carried out by government personnel or private security personnel, or a combination. Whether the security is provided by national or private entities, vetting for all staff involved in security is particularly important, as these functions are most likely to be targeted by criminal actors.

Training, security exercises and drills, as well as IT, OT and cyber security, guards and patrols are all functions that may be managed by the private port operator. Yet the port authority must have oversight and be satisfied that arrangements conform to the country's standards and laws. This entails close cooperation, and written agreement, between the private port operator and the port authority.

10 IMO, *Guidelines on Maritime Cyber Risk Management,* MSC-FAL.1/Circ.3 (London: IMO).
11 National Protective Security Authority, UK 2023, 'SCaN for All Staff,' https://www.cpni.gov.uk/scan-all-staff.
12 International Association of Ports and Harbors 2020, 'Port Community Cyber Security,' World Ports Sustainability Program, https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf.

Chapter 10: Coordination

The final chapter in this handbook focuses on mechanisms for timely and reliable information sharing among the various stakeholders.

Section 1 looks at the internal stakeholders, and outlines the importance of, and processes for, establishing roles and chains of command, maintaining inter-agency communication, and training. Section 2 looks at international entities, whether conventions and codes of practice, or actual bodies with which to consult and collaborate.

Internal stakeholders

Structures and priorities are decided by each country, but stakeholders likely to be involved in the implementation and enforcement of STC are as follows:

- **Ministry of Foreign Affairs (MFA).** Involved in the process of agreeing international measures at, say, the UN, and communicating these back home. Many enforcement actions are also likely to have an international dimension: any illicit cargoes will be en route either to or from another country, and it may become necessary to inform the overseas consignor/consignee. It is advisable to consult the MFA on any international aspects of a case. The MFA will also play a significant role in creating any STC laws.

- **Coast Guard.** In many countries the Coast Guard is responsible for maintaining safety and security within territorial waters.

- **Navy and other military forces.** The Navy in many countries is responsible for maintaining security in areas outside territorial waters. The Navy and other military services may have useful expertise in such challenging areas as hostile boarding, boarding at sea in all conditions or the handling of dangerous goods or materials.

- **Police.** A police force may maintain security within a port, though such duties are often performed by private security firms. Police may be a branch of the national police force, or be affiliated to another ministry, such as the Transport Ministry.

- **Customs.** Customs in most countries will have primary responsibility for screening and inspecting cargoes, for decision making on whether to release or detain cargoes, and for any resulting investigations. Customs may also have a role in outreach to industry. Customs officers at a privately owned port need a cooperative working relationship with the owner/operator to enforce STCs effectively.

- **Port authorities.** These are public bodies responsible for ensuring that all necessary activities at the port, including the enforcement of STCs, are carried out. This responsibility applies regardless of whether the port is publicly or privately owned or operated.

- **Licensing authorities.** The licensing authority is responsible for rating goods, and for granting or denying export licences. It is also likely to play a key role in advising and liaising with companies on all licensing matters.

- **Shipping registry and maritime authority.** Ships flagged to a particular country may be involved, anywhere in the world, in some breach of STCs. Although plausible, even likely, that the ship's captain was unaware that the ship was being used to carry an illicit cargo, the maritime authority should aim to cooperate fully with the country that has taken the enforcement action. If a UN member state suspects a breach of STCs or sanctions involving a ship that is flying that country's flag and is currently on the high seas, then the ship can only be boarded or directed to port with the consent of the flag state. Again, the aim should be to cooperate fully with any such requests.

- **Public prosecutor.** The public prosecutor will be involved in building and bringing a case against individuals or companies that have breached STCs.

- **Ministry of Defence.** Scientific and technical experts are of great value in helping to assess the potential for military end use.

- In some countries security in and around territorial waters, as well as tasks such as screening of merchant ships prior to their arrival, is carried out by a purpose-designed **multi-agency organisation.** Good examples are the National Coast Watch Center (NCWC) in the Philippines and the Maritime Security Centre (MSC) in Oman.

Effective cooperation among all government agencies may be assisted by a regular cross-agency meeting, probably chaired by the licensing authority or customs, at which representatives from many of the above ministries or departments can discuss current investigations and (non-routine) licence applications and assign tasks and actions. Outside these meetings, all stakeholder organisations should be able to communicate confidentially/securely with each other.

Each of the stakeholder agencies needs personnel trained to a high level in STCs – export control legislation, a good level of technical understanding of dual-use technologies as well as methodologies of illicit trade.

International cooperation

Several key initiatives have been introduced to set international standards on STC implementation and enforcement. The following are among the most useful:

The International Ship and Port Facility Security (or ISPS) Code. The ISPS Code is a set of measures specifically aimed at improving the security of ships and ports. The ISPS Code is part of the Safety of Life at Sea Convention (SOLAS), and compliance is mandatory for all countries.

The Container Control Programme (CCP). Based in Vienna and set up around 2009, this joint initiative between the UN Office of Drugs and Crime (UNODC) and the WCO focuses on building capacity to improve the security of containerised trade. It recommends setting up dedicated teams at ports and offers in-depth training to that purpose. Its remit covers all illicit trade (not just STCs).

The Customs Trade Partnership Against Terrorism (CTPAT). This is focused on preventing weapons for terrorists entering the US, so is only loosely connected to international STC enforcement. However, it is a useful example of a public-private initiative, in that it is based on collaboration between government and industry. By opting to join, manufacturers, exporters/importers and freight forwarders agree to implement various security measures and best practices, allowing them in return a smoother transit at the border (fewer checks etc). This resembles the WCO-recommended Authorised Economic Operator (AEO) concept discussed in Chapter 7 above.

The Container Security Initiative (CSI). Launched by the US in 2002, this aims to improve security by pre-screening high-risk containers at the port of origin instead of waiting until they reach the port of destination. This relies on intelligence sharing (eg, on exporters of concern), and the use of screening equipment at ports, and consists of partnerships between US Customs and non-US ports/governments, involving the reciprocal deployment of customs officers to ports in the partner country. Approximately 60 ports outside the US are currently part of CSI.

EU P2P (Partner-to-Partner) Export Control Programme is a programme of outreach, in which EU experts work with partner countries outside the EU to build capacity in dual-use trade control and arms trade control.

World Customs Organization's Regional Intelligence Liaison Offices (RILO) network. These regional offices gather and share tip-offs on vessels and cargoes of concern.

Standardised terms. International cooperation, and enforcement at port level, also benefit from the use of standardised terms, such as the customs codes (HS Codes) to describe goods, and the unique identifiers applied to each item on the EU's dual-use list.

Conclusions

Ports are the most important, and most visible, component of effective STC enforcement. It is at ports that all elements – the screening and tracking of ships; the screening and inspection of cargo; the searching and inspection of ships, and a secure, accountable cargo handling process – combine to maximise effectiveness in STC enforcement. However, ports are part of wider national networks that they rely on and can also leverage to assist their work. This wider network includes legislation, technical support, licensing, outreach, and potentially a central ship screening and tracking capabilities.

Legislation is the process by which international frameworks can be ratified at the national level. National laws need to be in place covering export controls and sanctions. These laws assign responsibilities and grant powers (for instance to obtain information and require cooperation) and specify offences (such as submitting a false customs declaration, attempting to export goods without a licence or creating false paperwork).

STCs are a complex and technically challenging area for law enforcement. Customs at a port can expect a licence to be in place by the time an item requiring one reaches the port. However, they need to be alert to discrepancies between the goods and the licence or attempts to import or export goods without a licence (such as by mis-describing or concealing goods). Customs officers or other port employees involved in cargo screening or handling cannot be expected to be expert in all dual-use technologies, so a process of reachback provides a useful mechanism by which local law enforcement at ports can consult experts.

Licensing, although handled centrally rather than at any given port, is an essential component of STC implementation. The licensing authority should conduct end use checks and a technical assessment. They, along with customs, may maintain watchlists of entities of concern (eg, companies involved in previous attempts to evade STCs), and are a source of advice to traders on licensing matters. The licensing body should maintain an up-to-date website for this purpose, as well as offer direct advice.

Outreach and education to the private sector go beyond the licensing authority. If customs and other agencies have a programme to identify exporters at potential risk, and inform them of their obligations, that should reduce the enforcement burden at ports. Leading on from this, a 'trusted exporter' system may allow exporters with good reputations a more streamlined experience at ports, thus incentivising them to conduct appropriate due diligence.

Regardless of whether a port is publicly or privately run, responsibility for STC enforcement lies with the port state rather than any private operator. Rights of access to cargoes and information, as well as full cooperation from the port operator, must be agreed in the contract between the state (or port authority) and the private operator. Even though many STC-relevant functions, such as cargo handling, and security patrols, may be carried out by private contractors, the state has a role in the selection, recruitment, vetting and training of staff. Recent cyber-attacks at ports worldwide demonstrate how quickly security threats are evolving.

So, what does best practice for enforcement of STCs at ports look like?

In the briefest terms, best practice describes a system that encompasses all STC-relevant functions carried out by or for a port: the screening and tracking of ships; the screening and inspection of cargo; the searching and inspection of ships; and a secure, accountable cargo handling process. It leverages technical expertise held by the licensing body, customs and industry itself. It relies on good cooperation between authorities and private port operators. Above all it must maximise the port's ability to enforce STCs while minimising the impact on port operations.

Centre for Science & Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

www.kcl.ac.uk/csss
@KCL_CSSS