Strategic Trade Review

Spring 2016

Procurement Methods and Trends

How proliferators evade controls to procure dual-use goods

Proliferation Financing

Impact of the Iran nuclear deal

Surveillance Technology

Trade policy and human security concerns

SPECIAL SECTION

Strategic trade controls in Southeast Asia

Issue 02

Strategic Trade Review

E-ISSN: 2406-5269

STR serves as an open source international forum for advanced exploration of the strategic trade field. STR's mission is to provide its readers with valuable resources regarding the current state of this area of study. STR pledges to publish articles of only the highest calibre that have gone through double-blind peer review and make them available to scholars and interested members of the public.

Website

http://www.str.ulg.ac.be/

Copyediting/Proofreading/Design

Andrea Viski

Publisher

University of Liege
Place du 20-Août, 7
4000 Liège
Belgium

With support from the University of Liege, European Studies Unit and the Institute for Transuranium Elements, Nuclear Security Unit of the European Commission's Joint Research Centre.

Contents

Letter from the Editor

In the twelve years since United Nations Security Council resolution 1540 (2004) made the implementation of strategic trade controls mandatory for all UN Member States, the field has undergone significant evolution and transformation. From the transactions and activities involved to the definition of the field itself, aspects of the objectives, content and practice of strategic trade controls have remained unresolved and unclear.

Like any academic field, strategic trade offers ample research areas to dissect and develop these unresolved or unclear issues. The Strategic Trade Review brings together a diversity of viewpoints and seeks to continue promoting the field's development through confrontation between different perspectives.

The first issue of STR established fundamental definitions and drew lines around emerging topics. This second issue demonstrates the complexity and range of questions and obstacles still to be resolved such as proliferation finance, countering methods used by proliferators, and the broadening scope of controls to areas such as information and communications technology (ICT). In addition, a special section focused on Southeast Asia shows the level of detail and the importance of political, economic, geographic and legal factors in the process of developing and effectively implementing strategic trade controls.

The broad range of research topics, perspectives and ideas in this issue reflects the importance of knowledge-sharing between the diverse stakeholders involved in strategic trade. As the journal serves as a vehicle moving communication, awareness and understanding of strategic trade forward, I invite submissions for future issues from all those who seek to advance scholarship in this important field.

ANDREA VISKI

Points of Deception: Exploring How Proliferators Evade Controls to Obtain Dual-Use Goods

GLENN ANDERSON[1]

Abstract

This paper examines the question of how proliferators go about evading nonproliferation controls to obtain dual-use goods. It argues that the proliferator must determine a suitable 'point of deception' for proliferation to succeed. Some of the factors involved in determining this point are outlined. The use of 'points of deception' in procurement for the nuclear and missile programs of several countries is considered. The paper concludes by considering how nonproliferation controls can best address the risks identified through the points of deception model.

Keywords

Nonproliferation, procurement, illicit trade, smuggling, nuclear, export controls, strategic trade controls

Introduction

This paper examines the methods by which proliferators carry out illicit procurement to obtain dual-use goods for use in nuclear weapons and missile delivery system programmes. Since the entry into force of the Nuclear Nonproliferation Treaty in the 1970s and the creation of the Nuclear Suppliers Group, the ability of states to proliferate by procuring complete facilities from international suppliers has been significantly reduced. There continue to be the occasional exceptions, such as Syria's acquisition of a nuclear reactor from North Korea in the late 2000s, which was almost completed before Israel acted to destroy it.[2] However the general trend is clear: states generally cannot procure complete facilities outside of International Atomic Energy Agency (IAEA) safeguards.

Consequently proliferators have generally changed tack, with the focus of procurement shifting towards the component and material level, and towards obtaining technology (both tangible technology and intangible 'know-how') that furthers their capability to manufacture such items for themselves. Many of the 'dual-use' goods sought have been either not included in export control lists or, although listed, also had plausible

[1] Glenn Anderson is a research associate at Project Alpha within the Centre for Science and Security Studies at King's College London.

[2] IAEA, "Implementation of the NPT safeguards agreement in the Syrian Republic," Board of Governors Report: GOV/2011/30, May 24, 2011.

benign uses which could allow an export license to be granted.[3,4] In some cases goods have simply been smuggled to avoid controls altogether.

Of interest to this paper is the question of how it is that determined proliferators have been able to forward their programmes despite the increasing coverage of controls since the 1970s. Specifically, this paper explores what could be the considerations of a proliferator when planning a procurement. It is argued that the procurer's prime task is to successfully set at least one "point of deception," which is the point at which the details of the true end use or end user of the goods to be procured becomes obfuscated. Upstream of this point, there are entities that are consciously working to a proliferator's agenda, and seeking to deceive, suborn, persuade or manipulate those entities downstream into acting in such a way that a procurement objective held by the proliferator is met. Immediately downstream there may be only innocent parties, ignorant that there is anything illicit going on, or there may be entities that are aware that the business is illicit.

This paper builds upon the observation of the author that the procurement efforts of different programmes have often utilised similar approaches over the last four decades. For example, Pakistan was perhaps the first country to systematically utilise illicit procurement methods on a large scale to procure goods for its nuclear programme after international counter-proliferation controls were introduced following the Indian 'peaceful nuclear explosion' in 1974.[5] Iraq's nuclear programme also utilised clandestine procurement techniques extensively in the 1980s to procure goods.[6] The use of clandestine procurement and illicit trade techniques by the Abdul Qadeer Khan network has been extensively analysed.[7] It is notable that the customers of A.Q. Khan, both before and in some cases after interaction with the network, relied extensively on their own clandestine procurement networks. Libya, for example, had a clandestine nuclear programme before being offered the Pakistani designs and subsequently maintained a parallel capability to procure technology and materials for its missile programme.[8] Less is known about the procurement channels used by North Korea, but it is certainly the case that the North Korean nuclear programme has relied extensively on illicitly procured dual-use technologies for the decade since the Khan network was dismantled.[9] Since the unravelling of the Khan network, however, it was perhaps Iran that utilised illicit procurement techniques with most vigour, with Iran's president admitting to the use of such techniques in 2014 because he saw sanctions as illegitimate.[10,11,12]

---

[3] 'Dual use' goods are goods that can be used for both civil and military applications. They can range from materials to components and complete systems, such as aluminium alloys, bearings or lasers. Definition derived from guidance at <www.gov.uk/controls-on-dual-use-goods>.

[4] Illicit trade occurs when states or other entities use deceptive and fraudulent methods to circumvent export controls and sanctions to obtain the goods and services that they need to sustain their WMD efforts.

[5] For an overview of Pakistani illicit procurement, see Feroz Khan, "Eating Grass: The Making of the Pakistani Bomb," Stanford Security Studies, November 7, 2012.

[6] For example, see account in Graham S Pearson, *The UNSCOM Saga* (New York: Palgrave MacMillan, August 2000).

[7] "Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks – A Net Assessment," The International Institute for Strategic Studies, 978-0-86079-201-7, May 2, 2007, <https://www.iiss.org/en/publications/strategic%20dossiers/issues/nuclear-black-markets--pakistan--a-q--khan-and-the-rise-of-proliferation-networks---a-net-assessmen-23e1>.

[8] Wyn Bowen. "Libya and Nuclear Proliferation: Stepping Back from the Brink," Adelphi Paper 380, The International Institute for Strategic Studies, May 16, 2006. <http://www.iiss.org/en/publications/adelphi/by%20year/2006-4d94/libya-and-nuclear-proliferation--stepping-back-from-the-brink-8955>

[9] See "Report of the Panel of Experts Established Pursuant to resolution 1874 (2009)," enclosed under UN Security Council document S/2015/131), February 23, 2015.

[10] On Iranian illicit procurement, see Albright et al, "Iran Admits Illegally Acquiring Goods for its Nuclear Programs,' Institute for International Science and Security, September 2014. See also Ian Stewart and Nick Gillard, "Sabotage? Iranian Exhibition Gives Insights into Illicit Procurement Methods and Challenges," Project Alpha, King's College London, September 2014, <https://projectalpha.eu/proliferation/item/347-sabotage-iranian-exhibition-gives-insights-into-illicit-procurement-methods-and-challenges>.

[11] "Iran President Rouhani Hits out at U.S. Sanctions," *BBC News*, August 30 2014.

[12] Louis Charbonneau, "UN Experts' Report Shows Iran's Deceptive Procurement Tactics," *Reuters*, May 12, 2014.

In exploring the 'point of deception,' a three-part process is hypothesised. The first phase relates to understanding the targets from whom goods can be obtained. The second relates to the ways by which goods can be acquired from the target – i.e. the provider of goods, normally a commercial company in the business of manufacturing or supplying the goods concerned. The third relates to the techniques that proliferators can use to avoid raising the attention of the government under whose export jurisdiction the provider sits, and to avoid interruption by international counter-proliferation actors such as foreign intelligence services.

The paper argues that gaining an insight into the various 'points of deception' presents nonproliferation opportunities. In fact, it may be that a 'point of deception' is one of the places in which an illicit procurement network is most vulnerable. If the party being deceived can see through the ruse then they would be strongly positioned to gain insights into the network, and may be motivated to work with nonproliferation authorities to exploit these insights in order to thwart the proliferator's procurement objectives. It may also result in the existence of a hitherto unknown illicit programme being uncovered.

This paper proceeds as follows. First, the point of deception framework is set out and its elements developed. Next, the paper examines the points of deception routinely used in procurement for the nuclear and missile programs of Pakistan, Iraq and North Korea. Finally, consideration is given to what insights the points of deception framework gives to improve nonproliferation controls.

Nonproliferation Controls

Since the beginning of the nuclear age, efforts have been made to prevent proliferation through international trade. The early efforts were introduced alongside the Atoms for Peace initiative which was announced in 1953. This principally involved IAEA safeguards intended to prevent the supplied technologies being misused. The nature and scope of Atoms for Peace era controls was insufficient to prevent the misuse of nuclear technology, however, as was vividly demonstrated by India's "peaceful nuclear explosion" in 1974. India, a country that had not signed the Nuclear Nonproliferation Treaty, had accepted only basic safeguards to ensure that nuclear materials supplied from overseas could not be used in a nuclear weapon: these measures did not prohibit India from utilising foreign-supplied facilities to produce its own fissile material for use in the nuclear explosion or from conducting the explosion for peaceful as opposed to military ends.[13]

In parallel to the efforts of states like India to advance their nuclear programmes for military ends, supplier states were beginning to take measures to curb proliferation based upon imported materials and technologies. The first effort in this regard was that of the "Western Suppliers Group" in the 1960s.[14] A second initiative was the Nuclear Nonproliferation Treaty which was negotiated after China's nuclear test in 1964 and which eventually came into force in 1972. The next major initiative was the creation of the Nuclear Suppliers Group (NSG) in 1975-1978 which sought to produce even more detailed lists of technology and agreement on more stringent rules for their transfer.

By the late 1970s, then, the key elements of the nonproliferation toolset, as viewed today, were in place. However, there were still limitations that would be exploited. These included the failure of the NSG to agree to controls on "dual-use" technologies (which were referred to as "grey areas") during negotiations in the 1970s.[15] These challenges were gradually addressed in the decades that followed, particularly after the discovery of Iraq's substantial clandestine nuclear infrastructure following the first Gulf War.[16] However,

---

[13] Andrew Koch, Christopher Derrick, Shelby McNichols, "Selected Indian Nuclear Facilities," Monterey Institute of International Studies, July 1999.

[14] K.D Kapur, "Nuclear Nonproliferation Regime and the Soviet Union," *India Quarterly: A Journal of International Affairs* 44:3 (July 1988), pp. 188-225.

[15] A file on the subject of "grey areas" left over from the NSG discussions in the 1970s was found in UK national archives. FCO96/991: Nonproliferation "Grey Areas," UK National Archives, Kew Gardens.

[16] See, for example, "Press Statement of Nuclear Suppliers Meeting: Meeting of States Adhering to the Nuclear Suppliers

one substantial gap that remained was related to coverage of controls: the Nuclear Suppliers Group had seven original participants which quickly increased to fourteen in the 1970s. By the time Iraq's programme was uncovered in 1991, this had risen to twenty-six. However, there were still numerous states that had no controls in place at all. The proliferation ring of A Q Khan, which sold enrichment capabilities to several states, exploited this loophole and also procured from countries with weak export controls to facilitate its illicit activities. However, it also succeeded in procuring illicitly from countries with stronger controls.[17] The adoption of United Nations Security Council resolution 1540 in 2004 provided the final substantial addition to the nonproliferation toolset, making implementation of nonproliferation controls a requirement of all states under Chapter VII of the UN Charter.[18]

Evasion of Controls

Despite the increasing coverage of controls, it is apparent that several states have been able to advance clandestine nuclear programmes over the past 30 years. Individual procurements will be examined further in the next section, but for now it is useful to highlight the extent to which illicit procurement methods have been utilised to forward such programmes.

Table I: Illicit Procurement Programmes

Country	Dates
Pakistan	Mid-1970s – present decade
Iraq	Mid-1970s - 1991
Iran	Mid-1970s – present decade
Libya	1969 - 2003
North Korea	1960s – present decade

The scale of the materiel need for a nuclear programme is immense, meaning that it is typically not one but hundreds of procurements that are required.[19] For example, a centrifuge cascade, which typically consists of 164 or more centrifuges, likely requires several hundred or more individual components – from metal tubes to precision electronics. Evidently, the technique used for each individual procurement will vary depending on a variety of factors. These may include the control status, sensitivity, and commercial availability of the goods being sought – some goods are more closely watched by international authorities than others. The timescale in which the item is required is also a factor. Another is whether a programme is already viewed as being of concern across the international community, or whether detection of the procurement is likely to result in it becoming so.[20,21]

Guidelines," Warsaw, Poland, April 3, 1992, <http://www.nuclearsuppliersgroup.org/images/Files/Documents-page/Public_Statements/1992-Press.pdf>.

[17] An example of how the Khan network benefitted from such a lack of controls is given by the Malaysian police report which concluded that no Malaysian laws were broken when large numbers of centrifuge components designed for uranium enrichment were manufactured in Malaysia by private company SCOMI **and** shipped secretly to Libya (Polis Diraja Malaysia, "Press Release by Inspector General of Police in Relation to Investigation on the Alleged Production of Component's for Libya's Uranium Enrichment Programme," 20 February 2004).

[18] United Nations Security Council 1540, S/RES/1540, New York, April 2004.

[19] The Libya case differs from the other cases mentioned in Table I as Libya procured an entire infrastructure from the Khan network. It was the Khan network, rather than the Libyan state, that sought the materials and components through hundreds of individual transactions.

[20] Pakistan and Iraq at various times have apparently not been of high concern in real terms to senior Western policymakers (at least in the US) because of geopolitical issues that trumped proliferation concerns. See Catherine Scott-Clark and Adrian Levy, *Deception: Pakistan, the United States, and the Secret Trade in Nuclear Weapons* (London: Atlantic Books, 2007).

[21] For example, given the nominally peaceful nature of the Iranian nuclear programme and the high degree of scrutiny the

Clandestine Procurement Techniques: The Points of Deception

In the absence of an ability to procure goods overtly, proliferators must procure goods illicitly. In illicit procurement, a party – be it the exporter, the licensing authority, or some other party, must be deceived. Conceptually, there appear to be three tasks for a proliferator when designing a point of deception. The first concerns where to procure the goods – herein called 'targeting.' The second is how to approach the supplier. The third, assuming that the exporting state is not complicit in the transaction (else the procurement would be overt rather than clandestine) is that of evading the export authority.[22] Additionally, there will be on-going enabling activity involving development and maintenance of procurement networks and their associated infrastructure, and protecting them from detection/disruption by national and international authorities. These four elements make up the "points of deception" framework and are explored in turn below.

Targeting

The first step in the process of setting a point of deception is to identify from where the items can be sourced. As the goods required can usually be procured via ordinary transactions with commercial suppliers, for the most part, this activity often amounts to the same market research that a licit procurer would carry out, using standard commercial information sources and contacts in the trade. In practice, there is a relatively small manufacturing base for most proliferation-sensitive goods, although some of these goods can be sourced through global supply chains.[23] In some instances the procurer might be able to identify opportunities to obtain certain goods from non-conventional sources of supply, such as black marketeers or illegal counterfeit manufacturing operations.[24] Another possibility is to identify companies or individuals who have the ability to manufacture the items, even though they would not normally appear to be suppliers for these goods.[25] An additional possibility is to identify an organisation that is a user of the goods being sought, that might be prevailed upon to sell those goods to the procurer. This may be particularly likely to succeed if the goods have been legitimately exported from their country of origin to a customer located in another country, where export controls are less developed and there is a generally lower risk to the illicit procurer. Re-export to the end destination, possibly via one or more intermediary countries to reduce the chances of detection, can then be carried out. Of course, an alternative would be to proactively seek out someone with a credible legitimate end use for the goods in question in such a third party country, and persuade them to purchase the goods from a supplier country with the ultimate (hidden) objective of selling them on.

Traditionally, targeting may have included the use of trade directories and cold calling in the absence of specific knowledge of potential suppliers.[26] In the era of the internet, this task is changing: online trading platforms such as alibaba.com have often made the process of finding a vendor for desired items much simpler and have facilitated speedy transactions. To some extent, industry and market knowledge, and access to relatively expensive reference resources (such as the hardcopy directories of equipment and

---

programme faces, officials would likely proceed very cautiously if they were procuring a technology with a specific application to nuclear weapons design.

[22] Overt to the involved elements of the government in the supplier country, that is. The procurement could still be clandestine with respect to the rest of the world.

[23] 'The Global Manufacturing Base for Proliferation-Sensitive Items: Interim Findings," unpublished paper, Project Alpha, Centre for Science and Security Studies, King's College London, August 11, 2015.

[24] As an example of the potential issue, an examination of the increasing problem of counterfeit parts in the aerospace industry is given in "Counterfeit Parts: Increasing Awareness and Developing Countermeasures," Aerospace Industries Association of America, 2011.< http://www.aia-aerospace.org/assets/counterfeit-web11.pdf>

[25] For example the manufacturing of centrifuge rotors for Iraq in the 1980s by the German company Rosch, whose usual line of business was carbon fibre products for the automobile, aircraft and computer industries. Rosch was owned by Karl Heinz Schaab. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

[26] An associate of A Q Khan's, Abdus Salam, reportedly connected with businessman Peter Griffin when misdialling a cold-call to a firm. See Catherine Scott-Clark and Adrian Levy, *Deception: Pakistan, the United States, and the Secret Trade in Nuclear Weapons* (London: Atlantic Books, 2007).

suppliers that once featured prominently) are now of significantly less importance, and a greater number of individuals can attempt to conduct procurement for technical items in an economical fashion with a reasonable chance for success, although this is probably less the case when it comes to acquisition of the most specialist and distinctive items with nuclear applications.[27]

The perceived strength of nonproliferation controls in each supplier's country and the risk that any specific transaction is a sting operation could affect the choice of target. In this context, it is notable that countries such as Iran prefer US and European-origin goods but often seek to procure them via countries such as China, which is perceived to have a less robust export control system.[28,29]

Approaching the Supplier

The proliferator must carefully consider how to approach a supplier as, depending on the nature of the procurement, it could result in the programme being detected (if it has remained hidden up to that point) or the procurement channel being compromised. For example, it was an approach to the UK company Emerson Industrial Controls for frequency inverters by the Special Works Organisation in Rawalpindi, followed by a subsequent message from the purchaser asking for technical modifications, which resulted in the UK concluding that Pakistan was pursuing uranium enrichment by centrifuge, likely in support of a nuclear weapons programme.[30] In general, in any illicit transaction, the supplier can either consent from the outset, be suborned or be manipulated. These scenarios are explained below.

An additional possibility is theft from the supplier. Although cases of theft of goods from suppliers appear to be relatively rare for proliferation purposes, there have been a number of cases where a mixed methods approach is used: an insider is co-opted who then, in effect, commits an act of theft against his employer. One example of this is the case of Sihai Cheng. Cheng was indicted by the United States in 2013 and charged with facilitating the diversion of MKS-brand pressure transducers from the company's Chinese subsidiary to Iran's nuclear programme. It is alleged that Cheng worked with sales staff of the subsidiary to have the goods shipped to intermediary counties for onward export to Iran while the sales staff declared the sales to be for existing and new customers.[31]

Consent (Whether Informed or Given in Ignorance)

Informed consent: In some instances, the procurer may turn to a provider who he already knows (or has good reason to expect) can be made aware from the outset of the true nature of the proposed deal. This situation may arise because the provider has been used before by the procurement network, they have information that the provider has been used by another illicit procurement network in the past and the situation is comparable, or because the provider has been 'scouted' by someone who has established their

[27] See for example Nick Gillard, "Online Marketplaces and Proliferation," Project Alpha, King's College London, October 31, 2014. < https://projectalpha.eu/proliferation/item/368-online-marketplaces-and-proliferation-project-alpha-in-the-bulletin-of-the-atomic-scientists>.

[28] See, for example, Nick Gillard, "The United States Just might be Iran's Favourite New Nuclear Supplier," The Bulletin of the Atomic Scientists, April 28, 2015. <http://thebulletin.org/united-states-just-might-be-iran%E2%80%99s-favorite-new-nuclear-supplier8257>.

[29] See Ian Stewart and Nick Gillard, "Iran's Illicit Procurement Activities: Past, Present and Future," Project Alpha, King's College London), July 24, 2015. < http://www.projectalpha.eu/proliferation/item/428-iran-s-illicit-procurement-past-present-and-future>.

[30] Letter from R J Alston to Mr Moberly, "Pakistan: Inverters," FCO37/214: 'The Nuclear Policy of Pakistan," December 12, 1978.

[31] "United States District Court in the District of Massachusetts, Grand Jury Indictment: United States of America v. Sihai Cheng et al., Crim. No. 13cr10332, Filed November 21, 2013.'

willingness to provide goods illicitly, prior to any specific request.[32]

Ignorance: The possibility that a supplier is simply ignorant of export controls and/or proliferation risks (be it true ignorance or wilful blindness) should not be discounted. In such circumstances, a proliferator could approach a supplier without subterfuge, or using only a very small amount of subterfuge and obtain the goods.

Working with consenting suppliers may be attractive to proliferators as in some respects it reduces the need for subterfuge. However, deception would still be necessary to evade national controls, as explored below. Additionally, a consenting partner may increase their prices because of the increased risks involved.

Subornment of Supplier

At times, the procurement network may try to suborn an individual, or individuals, outside the existing network.[33] For instance the buyer may not believe that the supplier can be put at ease with deception about the end-use of the goods. This may occur for a number of reasons, for example if the procurement requirement demands particular specifications that will give clues as to the real end-use.[34] In such a case the procurers may try to suborn the appropriate person or persons in the supplier company into conspiring with them.

As well as enabling the procurement of goods from any supplier organisations they may belong to, subornees may be invaluable in approaching other suppliers (particularly when these can then appear to be unremarkable domestic enquiries from fellow nationals or the suborned individual or their company is well known in the industry), in the evasion of export controls, avoiding the attentions of investigative/intelligence agencies, etc. and arranging financing and other services. Subornees may also help in obtaining training, maintenance, technical information, and the benefits of empirical experience in a particular field including hard-to-capture tacit knowledge.[35]

There are a variety of ways in which an individual can be suborned. Generally, these align with the motivations through which an intelligence service may persuade an individual to give them access to information. These are often held to be chiefly financial reward, ideological reasons, self-esteem and/or excitement, and revenge (although a number of other factors, including some subtle aspects of interpersonal relations, can often play a key role, and are arguably sometimes the decisive factor).[36] A key ability for the procurer will be to identify who might be suborned to meet their ends, and identify what characteristics, objectives, desires and vulnerabilities a target for subornment may have, which can be exploited.[37] Thus the first part

---

[32] An example of this is the use of a French businessman, alias 'Jaques Rough', to help acquire maraging steel for the Iraqi centrifuge project in the 1980s. Rough was already involved in less clandestine procurement for Iraq's conventional arms industry. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

[33] Subornment is an activity in which an illicit procurer persuades or induces a person (or persons) outside the illicit procurement network to become complicit in illicit activity in order to help achieve the procurement goals.

[34] For example in the procurement of 350-grade maraging steel by the Iraqi gas centrifuge project in 1988, the procurers were unable to come up with a credible cover story regarding the use the steel would be put to, and so went directly to a black market dealer. This dealer ('Malik') had been located for them by an intermediary that had been working with the Iraqi government for some time and who was aware from the outset that the deal would be illicit. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

[35] The contribution to overcoming Iraqi problems in balancing developmental centrifuges made by Karl Heinz Schaab illustrates the importance of the tacit knowledge that key subornees may contribute. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

[36] Michael J. Schulick, "Seminar on Intelligence, Command and Control – Human Intelligence," Program on Information Resources Policy, Harvard University, September 2007 and Randy Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCLS," *Studies in Intelligence* 57:1 (Extracts March 2013).

[37] For example the co-opting of German engineer Bruno Stemmler by the network procuring for Iraq's clandestine gas centrifuge programme in the 1980s. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

of the subornment task overlaps with areas within the Targeting activity discussed above.

Once the target has been identified, the next hurdle will be the actual act of subornment, which may rely heavily on the abilities (such as interpersonal skills) of the individual tasked to undertake it. Once a target has been successfully suborned, managing that relationship and getting the results desired, whether for a one-off deal or on an on-going basis, presents additional challenges.

Subornment can be a high risk operation: if it goes wrong, the suborner's cover can be compromised and, in some cases, criminal prosecutions could result.[38] Even if subornment is successful, there remains a risk that at a later stage a suborned individual will have second thoughts, or be uncovered by uncorrupted colleagues, business contacts or the authorities, leading to them either being exposed or secretly 'turned' to work for the authorities.[39] There is also the risk that those targeted have already been enlisted to assist the authorities, and have in fact been working against the procurement network from the outset.

Another potential disadvantage of using subornment is cost. Those suborned are likely to want financial inducements in exchange for cooperation.[40] There is also the issue of the time and effort put into the initial subornment and subsequently handling that contact. This could be substantial, particularly if a suborned individual proved to be malicious, unstable or incompetent, or began to have worries over their illicit dealings.

Nevertheless, there are circumstances where it is likely to be very difficult, if not impossible, to meet specific procurement requirements without some degree of subornment.[41] In addition, a successful subornment can provide great benefits to an illicit procurement effort, particularly if the individual or individuals concerned are reliable and stable, discreet, capable, knowledgeable in their field, well-connected and have initiative.[42]

Supplier Manipulation[43]

For the majority of illicit transactions, the provider will probably neither knowingly consent nor be suborned. Instead, they will be manipulated through the provision of false information, or misled with incomplete information.[44]

---

[38] Examples include the operations by US Homeland Security Investigations against Iranian procurer Amir Ardebili in 2007 (see John Shiffman, *Operation Shakespeare* (New York: Simon & Schuster, 2014) and by US Customs against Iraqi procurers in 1990, which involved the UK-based front company Euromac, ostensibly a 'food exporter' (see Burrows and Windrem, *Critical Mass* (New York: Simon & Schuster, 1994), pp. 204-206.

[39] For example, the reported recruitment of members of the Tinner family, part of A.Q. Khan's procurement network, by the CIA. See Collins and Franz, *Fallout*' (New York: Free Press, Simon & Schuster, Inc, 2011).

[40] Financial motivations were key to the assistance provided by the owners of H&H Metalform to Iraq (see Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

[41] Subornment may be required in situations where the specifications of materials or equipment required are so particular that they strongly indicate that the items are desired for an illicit end-use, particularly where there are few (if any) credible legitimate end-users for such items, and the buyer cannot convincingly present themselves as representing one of these possible end-users. Quantities required may also make it difficult to mislead any supplier over the actual end-use intended for the items. In such situations attempting to deceive or manipulate a supplier is unlikely to be feasible, and their witting assistance of illicit acquisition will be needed. An example of a situation where a credible cover story could not be manufactured and reliably maintained, and the procurers instead had to identify a supplier who would be willing to engage in illicitly supplying material while effectively conscious of the real end use, is given in Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

[42] One example of such a high value individual is Peter Hinze, of German company H & H Metalform, who accepted an offer of a 'silent partnership' and funding from Safa Habobi, a senior figure in Iraq's clandestine procurement efforts, in the 1980s. Hinze went on to facilitate cooperation by many companies with whom he had relationships and Iraq's illicit procurement campaign. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

[43] I.e. where the provider of the goods is manipulated, including the use of deception aimed at the provider.

[44] There are many examples where goods ostensibly destined for a civil purpose have been diverted to proliferation-related uses. In 2003, the Australian government prohibited an Australian firm, GBC, from exporting a dual-use mass spectrometer to Iran.

The two key areas in which a law-abiding supplier is typically deceived relates to the real end-use for the goods and the identity of the real end-user. In some circumstances, deception about either one or the other may suffice, but usually the procurer will need to deceive the supplier on both scores. The declared end use for the goods would usually have to be consistent with the nature of the business that purports to be the true end user.[45]

This type of deception is a common tactic.[46] It can be an inexpensive option as there is no need to suborn suppliers or pay a risk premium for their products or services. However, the cost and complexity of establishing credible *bona fides* can be substantial, particularly if they are to deceive the national authority too.

One particular strategy that has been seen in practice has involved manipulation of suppliers into thinking that a sale is not for export when in fact it was. This technique often involves a third entity in the country, be it a credible customer or a freight forwarder that is abetting the illicit procurement network. This technique, while potentially very effective, also has costs and risks. It requires a complicit buyer based in the target territory and a way must still be found to get the goods out of the territory.

Buying, or Buying Into, a Supplier

Another strategy that procurers have been known to pursue involves buying into commercial companies that are either manufacturers/suppliers of goods of interest in their own right, or due to the nature of their overt business are legitimate customers for such goods. In some cases such buying in has been conducted by individuals or commercial entities quite overtly and through normal commercial channels. Cases often involve producers of high technology goods that are in financial difficulty.

In other instances the act of buying into the target company was conducted through straightforward channels without the use of false identities or nationalities, but done in a discreet fashion that might escape attention by any parties with a nonproliferation interest. In some cases proliferators acquired a stake in target companies by means of a 'silent partnership,' whereby the proliferator had no official/ legal stake in the target company, but behind the scenes and 'off the books' personal deals had been done with the target company owners/ managers that gave the proliferator a de facto stake in, and ability to leverage/exploit, the target company.[47]

The IAEA had previously found that another spectrometer made by GBC and originally exported to an Iranian university had been diverted for use in Iran's clandestine laser enrichment program, without the knowledge of GBC or the Australian government. See Mark Fitzpatrick, "Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks," International Institute for Strategic Studies, 2007, p.53. < https://www.iiss.org/en/publications/strategic%20dossiers/issues/nuclear-black-markets--pakistan--a-q--khan-and-the-rise-of-proliferation-networks---a-net-assessmen-23e1A>.

[45] For example, an Iranian procurer, Hossein Tanideh, introduced himself to clients as a 'refinery manager' while deceptively obtaining valves for Iran's UN-proscribed heavy water reactor at Arak. Valves frequently have applications in petrochemical industries, and referring to himself in this fashion may have served to inspire confidence as a legitimate trading partner. See Daniel Salisbury and Ian J. Stewart, "Valves for Arak," Proliferation Case Study Series, Project Alpha, August 22, 2014. < http://www.projectalpha.eu/proliferation/item/342-valves-for-arak>.

[46] See "Proliferation Financing Report," Financial Action Task Force, 18 June 2008, pp.5-6. < http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>.

[47] An example of the 'silent partnership' approach has been given earlier, at footnote 40, concerning German company H & H Metalform's relationship with Iraqi procurement figures in the 1980s. Purchasing a formal interest in companies in supplier countries was a method practiced by Iraq in the 1980s, with procurers acting for the Iraqi government involved in manufacturing companies in the UK and elsewhere: see Mark Fitzpatrick, ed., *Nuclear Black Markets: Pakistan, A Q Khan and the Rise of Proliferation Networks – a Net Assessment* (London: International Institute for Strategic Studies, 2007), pp.45-46. More recently, in 2013, the *Washington Post* suggested that Iranian entities may have attempted to purchase a bankrupt composite material component factory, located in Germany, in order to obtain the company's specialised equipment and use it for nuclear- or missile-related purposes. See Michael Birnbaum and Joby Warrick, "A Mysterious Iranian-run Factory in Germany," *The Washington Post*, April 15, 2013, <https://www.washingtonpost.com/world/europe/a-mysterious-iranian-run-factory-in-germany/2013/04/15/92259d7a-a29f-11e2-82bc-511538ae90a4_story.html>. See also Cristina Rotaru, 'The case of MCS Technologies – Did Iran Use a German Factory for Illicit Procurement?," Project Alpha, King's College London, August 19, 2015, < http://www.projectalpha.eu/proliferation/item/434-mcs-technologies-germany-iran>.

This strategy may be attractive as most countries do not have in place strong controls on foreign investment and company ownership. However, the cost of buying a controlling stake in a company is evidently still high.

Synergy of Methods for Approaching the Supplier

Interestingly, there are examples where all three mechanisms can be seen in cases of illicit procurement involving one company (subornment, deception and theft), such as the MKS case referred to above. This indicates that there can be numerous points of deception in a complex supply chain.

Evading the Authorities

The next step for the illicit procurer is to take measures to evade counter proliferation authorities. The majority of cases of illicit procurement appear to involve purchasing by conventional transactions from commercial suppliers, and subsequently export via normal commercial channels (whether this is performed immediately, or at a later date if goods have been purchased by a domestic customer acting for the illicit network).[48] In such cases, the problem with regard to evading the authorities in the supplier country is threefold: firstly the export control authorities, secondly the border/Customs authorities at sea- and air ports and land border crossing points plus authorities acting within customs areas where trans-shipment can be carried out without the usual Customs controls, and thirdly those investigative agencies that are proactively seeking out intelligence on illicit procurement operations.[49]

Firstly, illicit procurers must deal with the problem posed by export control authorities either by arranging for the goods to be exported without anyone contacting the export control authorities, or by having those authorities contacted and them granting an export license (or responding that no license is required). The procurers need to avoid a situation in which the supplier or any of the other parties to the deal (e.g. freight forwarders, financiers, shippers, insurers and so on) contacts the authorities because their suspicions have been raised or because of some automated alerting system.

Secondly, procurers must evade border controls and Customs. This primarily involves either having paperwork from export control authorities that grants an export license (or attests that no license is required), or by having the consignment appear to be one that doesn't require any such permission. Alternatively the procurers might be able to arrange for border/Customs authorities at the relevant locations to be suborned into allowing the consignment to proceed.

Thirdly, the illicit procurers need to evade the attentions of those investigative agencies (whether they are intelligence services, law enforcement agencies, regulatory organisations including auditors, or other) that are specifically and proactively trying to discover illicit procurement, related activities and persons and organisations involved on an on-going basis.[50] As a point of interest, it may be the case that for most of the time no-one really knows how effective illicit procurers' evasion efforts are, until and unless some watershed event arises that reveals the historical activities of a particular programme in detail, such as the

[48] Financial and operational drivers that incline illicit procurers towards working through normal commercial channels in order to transport goods are discussed in Justin V. Hastings, "The Geography of Nuclear Proliferation Networks," Nonproliferation Review 19:3 (November 2012), pp. 429-450.

[49] Such 'customs areas', surrounded by a 'customs border,' are usually designated within ordinary air- and sea ports, and at land border crossings, and allow easy transhipment of goods in transit to another country without the necessity of clearing customs. Free ports or free zones, sometimes termed bonded areas, may also have no customs controls for goods being transhipped, or have more relaxed customs regulations than normal.

[50] See Thomas Graham Jr. and Keith Hansen, *Preventing Catastrophe: The Use and Misuse of Intelligence in Efforts to Halt the Proliferation of Weapons of Mass Destruction* (Palo Alto: Stanford Security Studies, Stanford University Press, 2009).

coalition military campaign against Iraq in 1991 and subsequent UN inspection efforts.

Dealing With Export Control Authorities

Options for dealing with export control authorities vary. A key factor is whether or not the goods are of a type and specification which is listed under one of the control regimes (such as the NSG list) that are relevant in the country where the goods are being bought. If so, then there will be a legal obligation on suppliers to inform the export control authorities, and ask for an export license to be granted. Similarly, if the given end-destination is one that is subject to sanctions and embargoes then there may be a legal requirement to contact the authorities for export permission even if the goods are not on the usual control lists (in some cases certain sanctions regimes may simply ban all exports to that destination. Finally, in a particular country there may be obligations in some circumstances for those involved in an export deal to report the deal to the authorities even where the nature of the goods or the end-destination are not listed. In some countries with so-called 'catch-all legislation', a legal obligation may exist in any case where a party has reasonable suspicion that the goods will go to illicit use.

Cases where the Authorities Are Contacted

If the authorities are contacted the procurer will have to supply details to the supplier to pass on to the authorities, that will satisfy the scrutiny of those authorities. This presents a certain element of risk for the illicit procurer. The authorities may have information which will allow them to spot something untoward. For example, they may have access to intelligence information which gives identities or contact details for some illicit procurers, or may have information about particular requirements for proliferation programmes which dovetail with the goods being sought.[51]

The authorities may have greater ability to carry out probing due diligence checks than commercial companies, possibly including pre- and /or post-delivery verification visits to the claimed end-user. Furthermore, in some circumstances it may be possible to repeat post-delivery verification after the initial post-delivery check, which can be a means of preventing, or at least detecting, subsequent further export of the goods to another country. Post-delivery inspection can also help guard against the movement from a legitimate user to another, illegitimate, user in the same country. Another contingency is the diversion of goods in place, where they are used for legitimate purposes that can be declared to the supplier and that supplier's government, but are at times used in the same location for illicit purposes.

In general government authorities in an exporting country may have greater abilities to carry out in-depth due diligence, possibly with the assistance of classified intelligence information. In some situations the authorities may be easier to deceive than an alert non-complicit supplier with a more detailed understanding of the market for their own goods, whereas in other cases the greater hurdle may be to deceive the authorities.[52] In cases where the procurer has suborned the supplier, both parties can conspire together to produce a

[51] In 2003, a joint US-UK-Germany-Italy operation intercepted a shipment of centrifuge parts that were being shipped by the A.Q. Khan network to Libya. The operation was clearly based on intelligence penetration of Khan's network. See Mark Fitzpatrick, "Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks," International Institute for Strategic Studies, 2007, < https://www.iiss.org/en/publications/strategic%20dossiers/issues/nuclear-black-markets--pakistan--a-q--khan-and-the-rise-of-proliferation-networks---a-net-assessmen-23e1 >, p. 76. See also the discussion regarding the case of the BBC China in Gordon Correra, *Shopping for Bombs* (Oxford: Oxford University Press, 2006).

[52] A case where an alert and conscientious supplier company became suspicious of an order based on its product and market knowledge is given in the following paper: David Albright, Paul Brannan and Andrea Scheel, "A Company's Discretion Detects Large Iranian Valve Orders by Scrutinizing Items and End-Users Instead of Lists," Institute for Science and International Security, January 28, 2009, <http://www.isis-online.org/uploads/isis-reports/documents/Iran_Valves_28January2009.pdf>.

submission to the authorities that is most likely to survive scrutiny.[53]

The illicit procurer could contemplate attempting to suborn the export authorities. However, in general this is likely to be a difficult proposition, unless corruption is very widespread in the country concerned. Identifying which officials will be involved in the scrutiny of a particular export case may be challenging, and ensuring that the case is not reviewed by others is another problem. Some of those involved in reviewing license applications may have security clearances which allow them to see intelligence material and therefore should, in general, be individuals who are more difficult to suborn.[54]

Cases Where Authorities Are Not Contacted Involving Listed Dual-Use Goods

If an illicit procurer has suborned a supplier the co-conspirators may decide not to contact the authorities, and attempt to export the goods anyway. This might involve using an anodyne description of the goods that made it appear that they were not relevant to export controls. There might be some residual risk that the goods would be stopped by Customs and questions asked regarding the details of the consignment.

However, if the in question goods were not of a type or specification that appeared in export control lists then, unless there was evidence that the supplier knew, or (in some jurisdictions) had reasonable grounds for suspicion, that the consignment was headed to a proliferator's programme, it is unlikely, in the absence of some specific evidence, that it could be proven that the supplier had transgressed (unless they had contravened any relevant sanctions or embargoes).

Dealing With Border/Customs Authorities

In general, if the export licensing authorities have been contacted regarding a particular consignment, and have given approval for its export, then the border and/or Customs authorities at ports and borders will not present an obstacle. However, if goods are being exported without approval, a possible point of failure may occur when they pass through Customs and border checks. At this point an official (or automated risk management system) may hold up the shipment for further investigation.[55]

Consideration might also be given to other methods of smuggling which avoid the goods concerned being moved through normal commercial channels, such as hand carrying of items on aircraft – a technique that has been used in the past.[56] Other possibilities involve the use of private aircraft and the use of sailing boats.

---

[53] A reported case where both the supplier and procurer conspired to submit false details to authorities occurred in 2015, when US authorities disrupted an alleged procurement ring involving a US manufacturer of electronic systems, Smart Power Systems, with an Iranian sister company, Faratel. The two companies allegedly conspired to procure electronic components for Iranian military or missile-related end-users. See Christopher Coughlin and Andrea Stricker, "Case Study: Skilled Procurement Ring Charged in Illegally Obtaining Goods for Iran," Institute for Science and International Security, May 5, 2015, <http://www.isisnucleariran.org/assets/pdf/Skilled_Procurement_Ring_Faratel_5May2015.pdf>.

[54] As an example of subornment amongst government figures and others of influence, a Philippines-based conspirator of an Iranian illicit procurer claimed to have the support of "politicians or bigtime [sic] businessmen" in Manila who would purportedly help smooth illicit transactions. See Daniel Salisbury, "Khaki-Yi, Project Alpha Case Study in Illicit Procurement," Project Alpha, King's College, 2013, <https://www.acsss.info/proliferation/item/download/19_fccf93c94c0d060b52f205af729f6ff1>.

[55] Events such as these, e.g. 'Customs stops', may be prompted by a number of things. There may be something about the consignment, the details provided, those handling it, and so on, that arouses suspicion. Alternatively, a consignment may be stopped without any suspicion having been aroused, simply as a part of 'spot checks'. The task for the illicit procurer is to try to ensure that nothing about the consignment appears suspicious enough to warrant a stop. Providing the details of the goods, consignee, etc. appear benign, and none of the identities and contact details on the accompanying paperwork match with identities on any 'watch-lists' held by the border authorities, then in most cases there will be no reason to hold the consignment up.

[56] In 2009, Iranian procurers reportedly had plans to send a shipment of gyroscopes and accelerometers to Iran's missile programme by having a visiting Iranian government delegation carry them in travel bags on their return to Iran. See "Informing Beijing of Chinese Firm Limmt's Continued Proliferation to Iranian Ballistic Missile Program (S)," Wikileaks, March 18, 2009, <https://wikileaks.org/plusd/cables/09STATE25689_a.html>.

Developing and Maintaining Assets and Infrastructure

Another important feature of illicit, nuclear related trade across the programmes mentioned above is the existence of transnational networks which, to a greater or lesser degree, share methods and tactics. The networks themselves appear to vary substantially in size, shape, and durability. While it is the A.Q. Khan proliferation ring that may spring to mind when thinking of networks, in reality most networks are likely much more transient and ad hoc in nature, and the degree to which individuals in the 'downstream' elements of the procurement chain (i.e. those closest to the supplier) may be fully witting to the real intended final destination and end-use may vary considerably.[57]

To a greater or lesser extent, depending on the specifics of a particular procurement effort, there may be a need to develop assets and infrastructure for the network. These include 'front companies', commercial premises, warehouses, 'safe houses', communications equipment, and so on. Some networks may contain individuals, commercial entities and infrastructure that are significantly 'tethered' in countries that are opposed to the illicit procurement effort (or would be if aware of it) or neutral (and could possibly become hostile). To varying degrees, some procurement networks operate with assets 'at risk' in hostile or potentially hostile territory. This presents a potential vulnerability but such assets may often present the network with valuable capabilities (for example an apparently reputable company in the same country as significant potential supplier companies, may be able to make sales enquiries and purchase goods).

Other networks may be set up in a much more light-footed and less 'forward-deployed' fashion, foregoing some useful capabilities for a less vulnerable and often less expensive set-up.[58] Illicit procurement can often be performed almost 'from the bedroom' these days. This is illustrated by cases of illicit procurers such as the Austrian Daniel Frosch, who operated from home, without warehouse or any significant overheads, and likely just a computer.[59] At a minimum, an instance of illicit procurement is likely to require arrangements for a 'front entity' of some sort to be available that can be declared as the customer. This entity will need to appear be a credible customer with a legitimate use, at least when subject to whatever level of scrutiny is going to be forthcoming from the authorities.

The front entity might be a purely fictitious creation, whose name is simply given by the illicit buyer to the supplier along with a delivery address and contact details where the procurement network can take messages and pick up the goods. Alternatively the procurement network might create a real organisation, but one which does not actually carry out any real business in its declared line, and instead is used purely to enable illicit trade. Another option is to use a real entity carrying out legitimate activities but use it to enable illicit activity. Setting up and maintaining any of these arrangements in a way that passes scrutiny by any potentially hostile authorities, and meets all the requirements of the illicit procurement network (which may include being economically viable as well as successfully enabling illicit trade), requires certain skills and knowledge which go beyond regular legitimate commercial practice.[60]

---

[57] Some indication in the transient nature of procurement networks is of the sheer number of entities – some several hundred – that have been subject to designation by the US government and European Union for their involvement in illicit procurement. New procurers apparently emerge on a regular basis, and others cease activity for a variety of reasons, including due to law enforcement action.

[58] A discussion of Iran's frequent use of 'disposable' middlemen overseas is given in David Albright, Andrea Stricker and Houston Wood, "Future World of Illicit Nuclear Trade," Institute for Science and International Security, July 29, 2013, < http://isis-online.org/uploads/isis-reports/documents/Full_Report_DTRA-PASCC_29July2013-FINAL.pdf>.

[59] Nick Gillard, "The Illicit Trade Network of Daniel Frosch," Proliferation Case Study Series, Project Alpha, King's College London, 5 January 5, 2015, < https://projectalpha.eu/proliferation/item/380-new-alpha-case-study-the-illicit-trade-network-of-daniel-frosch>.

[60] Some indication of this is given by the case of Karl Lee (aka Li Fangwei), a China-based businessman who has been reportedly supplying Iran's missile programme for the last decade, despite repeated efforts by US authorities to stop him. Lee's survival suggests a certain level of savvy and adaptability. See Ian J. Stewart and Daniel B. Salisbury, "Wanted: Karl Lee," *The Diplomat*, May 22, 2014, <http://thediplomat.com/2014/05/wanted-karl-lee/>.

At the other end of the spectrum, an illicit procurement network may do business in such a way that as well as a 'front' entity to pose as a legitimate customer, its operations involve a more extensive clandestine infrastructure, possibly involving setting up additional front organisations to act as the buyer or other intermediaries, some of which may be based in the same countries as the supplier entities are located in. Depending on the specific nature of the operation, there may be a need for provision of facilities such as safe houses, clandestine communications arrangements, falsified documents, special financial arrangements, alias identities for some individuals involved, transport and other logistics facilities under the control of the procurement network, and so on. Setting up and maintaining such a clandestine infrastructure while faced with the potential threat posed by hostile authorities requires a range of skills and resources that may be very challenging. More complex clandestine infrastructure for illicit procurement has often been set up and maintained by, or with the aid of, the proliferator state's intelligence service.[61]

Network Communication

An important aspect of proliferation networks relates to communications. Communications are vital for such networks but are also a source of risk. Should authorities be able to intercept the network's communication, the network's operations would be compromised. The Snowden revelations may have helped networks develop communication methods that are less susceptible to intercept by authorities. However, even if so, proliferation networks must still communicate 'in the clear' with suppliers and authorities, leaving open an opportunity to gain insight into their activities. Great care and skill is therefore required in such networks if their communication is not to be compromised.

As in many other areas, there is a trade-off involved for networks that wish to practise more clandestine and secure communications, in terms of generally decreasing speed, increased expense, and increased man-hours required. There is also the possibility that sometimes the use of such techniques will not evade attention but will actually highlight that the network is engaged in illicit activity. Judgement of whether and when to use enhanced techniques or to stick more closely to normal commercially-confidential business practice may be a key skill for successful illicit procurement campaigns.[62]

Use of Diplomatic Cover and Premises

International diplomatic conventions furnish nation-states with the ability to overtly set up relatively secure facilities on the territory of any country with which they have diplomatic relations. The confines of an embassy are only relatively secure because of the common employment of local nationals in some roles and the high possibility that parts of an embassy building and grounds have been compromised by planted listening devices and the like. However within an embassy a capable nation can install secure meeting rooms and communications facilities that have a high degree of security.[63] A diplomatic post thus furnishes a country with a multi-purpose facility which its nationals (and other guests) can overtly visit for all manner of potential purposes, and where confidential meetings can be conducted, records stored, and secure messages sent and received using encrypted communications. The frequent secure sending and receiving of encrypted communications via a range of telecommunications channels is routine, and of itself tells the host country

[61] Iraq's procurement activities under Saddam Hussein provide a clear case. As the CIA has noted, 'the Iraqi Intelligence Service (IIS) and the Military Industrialization Commission (MIC), however, were directly responsible for skirting UN monitoring and importing prohibited items for Saddam.' See "Comprehensive Report of the Special Advisor on Iraq's WMD," CIA, December 30, 2004, <https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004/chap2.html>.

[62] However, in practice considerations of the potential for personal profit-making may often be an important factor in determining the extent to which different methods are selected.

[63] The procurement network of Karl Lee, a Chinese businessman who has purportedly supplied Iran's ballistic missile programme with dual-use goods, has been facilitated by Iranian operatives working from the country's embassy in Beijing. See for example, "Informing Beijing of Chinese Firm Limmt's Continued Proliferation to Iranian Ballistic Missile Program (S)," March 18, 2009, <https://wikileaks.org/plusd/cables/09STATE25689_a.html>.

little of significance (although increased levels of message traffic on occasion can be of interest).[64]

Furthermore, the diplomatic immunity conferred upon those members of an embassy's staff who are accredited diplomats recognised by the host country allows such personnel to carry out activities which if exposed would normally lead to criminal prosecution in the country concerned, but would only subject a diplomat to expulsion from the country and being made *persona non grata*.[65]

A diplomatic post can thus provide a convenient and easily accessed base of operations for illicit procurement activity, and a useful meeting location and short-term support facility for visiting members of an illicit procurement network, or in some circumstances for network members permanently based in the country concerned.[66, 67, 68]

One particular feature of international diplomatic conventions that is particularly interesting when examining illicit procurement is the diplomatic bag (aka diplomatic pouch) service operated by diplomatic posts. This allows posts to send and receive packages marked as diplomatic correspondence, sent between diplomatic posts of a particular country and their home government, which should not be opened by anyone other than that country's authorised officials. Security of diplomatic pouches, and immunity from having their passage obstructed, is guaranteed under the Vienna Convention of 1961 and appears to be generally respected in most countries around the world.[69] Given the wide parameters acceptable with regard to type of package/container, size and weight, many items that have been procured and taken to diplomatic premises can in principle be placed in a diplomatic pouch which is then sealed and sent out of the country. For example, it is reported that in the late 1980s Iraqi procurers obtained a sample of maraging steel from a black market supplier (actually a British national) while in France, and that the sample was taken by one of the procurement team to the Iraqi Embassy in Paris. It was then sent by diplomatic pouch to Germany,

---

[64] For a discussion of diplomatic premises' communications, see Kishan S. Rana, *The Contemporary Embassy: Paths to Diplomatic Excellence*, (New York: Palgrave MacMillian, 2013), pp. 17-18.

[65] In the 1980s and 1990s, a North Korean diplomat named Yun Ho Jin, based at the DPRK's mission in Vienna, was responsible for illicit procurement of nuclear technology. He was designated by the UN Security Council in 2009, effectively making him persona non grata. See David Albright and Paul Brannan, "Taking Stock: North Korea's Uranium Enrichment Program," Institute for Science and International Security, October 8, 2010, <http://isis-online.org/uploads/isis-reports/documents/ISIS_DPRK_UEP.pdf>.

[66] See David Armstrong and Joseph Trento, *America and the Islamic Bomb* (Hanover: Steerforth, 2007), p. 74; Shahid-Ur-Rehman, *Long Road to Chaghai* (Islamabad: Print Wise Productions, 1999), p. 63; Egmont Koch, *Wanted…Bomb Business: Nuclear Aid for Pakistan and India*' (Cologne: West German Broadcasting, 1986); Steve Weissman and Herbert Krosnev, *The Islamic Bomb* (New York: New Work Times Books, 1981); David Albright, *Peddling Peril* (New York: Simon and Schuster, 2010), p. 22.

[67] The case of Karim Ali Sobhani, Iranian intelligence officer and procurer, is also worth noting. Sobhani was active in illicit procurement activities during the 1980s while serving under diplomatic cover in Germany. Indicted for export-related offences by the US, he was declared persona non grata by the German government. However he subsequently resumed procurement activities in Europe while acting under non-official cover, and during this time visited the Iranian Embassy in Bonn on business. See New York Times News Service, "US Fights Germans' Aid to Iran," *Chicago Tribune*, June 27, 1989.

[68] Within reason, all manner of objects can be packaged and placed in a diplomatic 'pouch,' as the physical form of 'pouches' can vary considerably, and can range from a brief case, sack, crate or even potentially a shipping container. The Vienna Convention sets no limits on the physical size of a designated diplomatic pouch, nor its weight. Similarly, there is no generally agreed convention formally recognised by most nations regarding form, size or weight. In practice there have been occasions when a nation has challenged the validity of a particular diplomatic pouch on the grounds of size and weight, for example in 1984 the Swiss authorities challenged the Soviet Union's attempt to have a 9 ton trailer truck regarded as a diplomatic pouch, and stated that they regarded 450 lbs. to be the maximum acceptable weight for a legitimate diplomatic pouch. However such opinions on reasonable size limits for diplomatic pouches are by no means generally accepted. See Charles Ashman and Pamela Trescott, *Diplomatic Crime: Killings, Thefts, Rapes, Slavery & Other Outrageous Crimes* (Washington DC: Acropolis Books Inc., 1987) and "Pouch Without a Home," *Time Magazine*, July 30, 1984, < http://content.time.com/time/magazine/article/0,9171,926723,00.html>.

[69] For a discussion of the obligations and immunities adherence to the Convention involves concerning diplomatic bags, see Michael Hardy, *Modern Diplomatic Law* (Manchester: Manchester University Press, 1968), pp. 39-40.

where it was taken to a commercial company for testing.[70,71]

Protecting the Network: Secrecy, Security and Counter Intelligence

A proliferation programme with an illicit procurement component is likely to be the target of intelligence-gathering efforts by a number of investigative agencies from a range of countries. This might be expected to cause some of those involved with illicit procurement to consider the risks they run in having their procurement network penetrated by one or more of these hostile agencies.[72] Security measures might be taken such as 'vetting' those who will be involved in illicit procurement activity, to the extent possible, and restricting information according to 'need-to-know' principles. A proliferation programme might also consider carrying out some clandestine investigation of people within its procurement network or their key business contacts, where practicable. These activities might require significant effort if undertaken, however this would need to be set against consideration of the risks to the illicit procurement effort and the proliferation programme if the procurement network was penetrated, and its efforts impeded or sabotaged.

Another potential security activity is organising network activities so that individuals with access to sensitive information are less able to either deliberately betray the network on their own initiative, or be targeted by hostile intelligence/investigatory services. An example of this might be some situations involving technical experts from the proliferation programme who do not routinely travel abroad, but might sometimes be needed to accompany procurers who for a particular mission do not have sufficient technical expertise.[73] In such cases specialists, particularly if they are traveling under their own names (which may often be more practical) and have become known overseas in the past (for example if they have studied abroad) may attract attention from hostile agencies.[74] Sophisticated procurement networks may consider using measures to reduce the risks, such as placing their specialists under some form of counter-surveillance and monitoring open source and social media about the project and its staff.

Counter-Intelligence Activity

If someone is trying to do the utmost to preserve the security of a an illicit nuclear programme and its procurement efforts then one important task is the collection, collation and analysis of information that provides indications to what counter-proliferation authorities know about that programme. Apart from material gained through intelligence sources and methods, information can come from a variety of more easily accessible sources, including court reports of prosecutions for export control violations, information provided to the defence in the course of a prosecution, press reporting of public statements by officials and politicians, open political debates (e.g. parliamentary proceedings) and from both informal diplomatic warnings and formal protests such as demarches to the proliferator government concerned.

There might also be the option to attempt to feed in misinformation to investigative agencies using any intelligence channels available. Effective deception operations of this sort might require a relatively high degree of skill from the agency performing them, but some of the countries who have engaged in nuclear proliferation in recent history have possessed foreign intelligence arms with a significant capability to

---

[70] The use of the diplomatic pouch by Iraqi procurer Obeidi has been mentioned earlier. For the use of diplomatic pouches by Pakistan, see Gordon Correra, *Shopping for Bombs* (Oxord: Oxford University Press, 2006), p. 22.

[71] A further example of the use of the diplomatic pouch by proliferators is given in Armstrong and Trento, *America and the Islamic Bomb* (Hanover: Steerforth Press, 2007), p. 68.

[72] By 2003, the CIA had reportedly recruited three Swiss-based members of the A.Q. Khan network who provided highly-detailed knowledge of the network's activity. See Catherine Collins and Douglas Frantz, *Fallout: The True Story of the CIA's Secret War on Nuclear Trafficking* (New York: Free Press, Simon & Schuster, 2011).

[73] See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

[74] For an account of travels by Iraqi technical specialists on illicit procurement missions to Europe in the 1980s, see Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

conduct clandestine operations with considerable international reach.[75]

Points of Deception

The previous sections have highlighted that for proliferation to occur, a point of deception must normally exist (except in a situation where the country from which the goods are supplied is uninterested in nonproliferation, at least where the particular country of destination is concerned, or is bereft of export controls). From the examination of proliferation techniques and proliferation networks above, it is apparent that points of deception could rest almost anywhere in the supply chain. For example, if the supplier has been co-opted into illicit procurement then the supplier would have to deceive the licensing and/or Customs authorities, and the primary point of deception in such a case could be considered to lie at the juncture between the complicit supplier and the authorities. In general, someone upstream of the point of deception would engage in the deception of parties downstream, be it to deceive the supplier, the supplier's licensing authority, Customs, etc. The list of those who may be deceived is also not limited to supplier and government authorities: shippers, insurers and financiers could also have a role to play.[76]

It was also suggested that several programs had utilised these techniques in support of their clandestine nuclear and missile programs. In this context, it is useful to briefly review the use of these techniques in the cases of certain nations. For this review, Pakistan, Iraq and Iran were selected. The reason for selecting these cases relates primarily to the substantial amount that is known about how the nuclear and missile programs of these countries have procured goods. Libya was discounted as it was the A.Q. Khan network rather than the Libyan government that had responsibility for procuring most of the items.

Pakistan

Pakistan's nuclear program started in earnest in the early 1970s and accelerated after the Indian peaceful nuclear explosion in 1974. Pakistan turned to illicit procurement after its efforts to procure reprocessing capability from France were frustrated. In the 1970s, much of Pakistan's illicit procurement was coordinated from diplomatic missions overseas. In particular, individuals based in Pakistan's mission to Germany played a key role. By the late 1970s and 1980s, Pakistan relied on networks of complicit and ignorant European suppliers, often taking advantage of lax export controls and profit-motivated businessmen. Since the 1990s, the bulk of Pakistan's illicit procurement seems to have been through entities in Pakistan acting as front companies.

Interestingly, there have been few known instances of Pakistan buying into overseas firms. However, Pakistan has utilised nearly every other procurement technique available.

Iraq

Iraq's illicit procurement began after the destruction of the OSIRAK reactor in 1981. Saddam placed high importance on the county's nuclear program, resulting in use of the entire state machinery to move it forward. For example, in the CIA's comprehensive assessment of Iran which was conducted after the 2003 invasion and which drew upon Iraqi documents, it was noted that:[77]

Saddam used the [Iraqi Intelligence Service] to undertake the most sensitive procurement

[75] For example, Iran's Ministry of Intelligence and Security has a sophisticated international presence including in European capitals. See Federal Research Division, Library of Congress, "Iran's Ministry of Intelligence and Security: A Profile,' December 2012, <http://fas.org:8080/irp/world/iran/mois-loc.pdf>.

[76] On the role of the finance and shipping industry, see: United Nations Security Council, "Sanctions Compliance in the Maritime Transport Sector," S/2015/28, New York, January 16, 2015.

[77] "Comprehensive Report of the Special Adviser to the DCI on Iraq's WMD (Regime Finance and Procurement)," Central Intelligence Agency, September 30, 2004, < https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004>.

missions. Consequently, the IIS facilitated the import of UN sanctioned and dual-use goods into Iraq through countries like Syria, Jordan, Belarus and Turkey. The IIS had representatives in most of Iraq's embassies in these foreign countries using a variety of official covers. One type of cover was the "commercial attaches" that were sent to make contacts with foreign businesses. The attaches set up front companies, facilitated the banking process and transfers of funds as determined, and approved by the senior officials within the Government.

The MFA played a critical role in facilitating Iraq's procurement of military goods, dual-use goods pertaining to WMD, transporting cash and other valuable goods earned by illicit oil revenue, and forming and implementing a diplomatic strategy to end UN sanctions and the subsequent UN OFF program by nefarious means.

Saddam used the Ministry of Higher Education and Scientific Research (MHESR) through its universities and research programs to maintain, develop, and acquire expertise, to advance or preserve existent research projects and developments, and to procure goods prohibited by UN SC sanctions.

Iraq under Saddam successfully devised various methods to acquire and import items prohibited under UN sanctions. Numerous Iraqi and foreign trade intermediaries disguised illicit items, hid the identity of the end user, and/or changed the final destination of the commodity to get it to the region. For a cut of the profits, these trade intermediaries moved, and in many cases smuggled, the prohibited items through land, sea, and air entry points along the Iraqi border.

Iraq also made extensive use of the technique of buying out overseas manufacturers. The entities that Iraq targeted for takeover were often in financial difficulty.[78]

Iran

Iran's nuclear program paused after the fall of the Shah but resumed during the Iran-Iraq war, during which Iran was approached by A.Q. Khan. Iran bought designs for Pakistan's basic P-1 centrifuge and a limited number of parts, and later designs for the more advanced P-2 centrifuge. However, Iran did not procure wholesale the capability to enrich uranium as Libya did. Instead, Iran set about making and buying what was needed. Iranian illicit procurement has been largely commercial in nature, with Iranian nationals securing the support of intermediaries via financial inducement. Iran has also made extensive use of front companies.[79]

There are some signs that Iran has used diplomatic cover in pursuit of components and expertise. Iranian diplomatic officials in China have reportedly assisted procurement of missile components, although known cases are dated from more than five years ago.[80] Officials from an Iranian state agency known as the President's Technology Cooperation Office have also reportedly been involved in procurement of WMD-related expertise.[81]

---

[78] For some insights into Iraq's approach in the 1980s, see Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

[79] Ian Stewart and Nick Gillard, "Iran's Illicit Procurement: Past, Present and Future," Project Alpha, King's College, July 24, 2015, < http://www.projectalpha.eu/proliferation/item/428-iran-s-illicit-procurement-past-present-and-future>.

[80] See "Informing Beijing of Chinese firm Limmt's Continued Proliferation to Iranian Ballistic Missile Program (S)," March 18, 2009, <https://wikileaks.org/plusd/cables/09STATE25689_a.html>.

[81] An Iranian dissident group has alleged that the Technology Cooperation Office was responsible for recruiting a former Soviet nuclear weapons scientist who has reportedly provided nuclear weapon-related expertise to Iran. See "Exposing the Parchin

There are a few reported examples of Iran having bought out foreign manufacturers for the purposes of obtaining controlled technology. Examining these three cases highlights several trends. First, use of illicit procurement was generally similar in all three cases, albeit with some variations. Second, use of diplomatic premises appears to have declined (or has been detected less frequently). This may be due to proliferators judging that, given the amount of past reporting of activity by diplomatic staff, use of such personnel as procurement agents may simply attract the attention of national authorities. However this would not necessarily affect the utility of using diplomatic bag arrangements to get some goods, procured by other parties, out of the originating country. If the use of diplomatic bags has actually declined then the reasons for this are not clear. Additionally, the buying out of manufacturers also seems to have declined. Again, the reasons for this (if a genuine trend) are unclear.

Points of Deception and Nonproliferation Controls

This paper has examined illicit trade supplying dual-use goods to proliferators' nuclear programmes and to some extent has considered such supply to associated missile delivery system programmes. The examination of this trade through the points of deception framework has highlighted several challenges to the effectiveness of nonproliferation controls, as well as some opportunities.

It is clear that illicit procurement techniques undermine the effectiveness of nuclear nonproliferation controls. Supply-side controls, generally aimed at controlling exports of relevant dual-use goods and, to a lesser but growing extent, broader aspects of strategic trade controls, have been expanded since the 1970s and have served to create increasing obstacles.[82] However, through the use of increasingly indirect and deceptive methods, procurers have continued to acquire goods, albeit with increasing financial outlay required and delays incurred.

Situations in which a supplier or an element thereof is complicit, and an end user has provided credible false end use information, appear to be particularly difficult to thwart. There are certainly steps that states can take to reduce the likelihood of complicity. This includes awareness raising to remove ignorance and enforcement action to change cost/benefit calculus.

There are additional steps that companies could take to mitigate supply chain issues. For example, MKS Instruments Ltd., which was mentioned above, has implemented a "controlled delivery model" in which distributors are not used and all customers are subject to end use verification.[83] In some sectors, this supply-chain model presents a credible opportunity to mitigate supply-chain risks. It should be recognised, however, that for most sectors such a model would not be suitable as it would substantially disrupt usual commercial practise.

However, use of similar models including end-use verification, whether carried out by the supplier company, the state of origin, or both, would appear to be a particularly valuable tool. It seems desirable that, as far as is feasible, similar practices are instituted internationally to cover the most critical industry sectors. It may be useful to identify where any arrangements are currently in place with regard to the various commercial sources of supply most directly relevant, starting with items identified in the Nuclear Suppliers Group (NSG) list of controlled dual-use goods.[84]

Mystery – Key Figures, Officials, Organizations, Staff, and Foreign Advisers," National Council for Resistance in Iran, November 7, 2014, <http://www.ncrius.org/press-conference.html>.

[82] For suggested definitions of strategic trade controls vis-a-vis strategic trade controls, and what these entail, see Catherine B. Dill and Ian J. Stewart, "Defining Effective Strategic Trade Controls at the National Level," Strategic Trade Review 1:1 (Autumn 2015).

[83] For further details regarding MKS's approach, see Ian Stewart and John McGovern, "Beyond Compliance: Preventing the Diversion of Sensitive Vacuum Measuring Equipment – The "Controlled Delivery Model," Project Alpha, King's College London, September 2013.

[84] The various known commercial suppliers for these goods were identified in "Commercial Producers of NSG Controlled

It is also apparent that national export controls cannot be expected to prevent shipment via diplomatic pouch, domestic sales of sensitive items, or foreign investment in domestic industry. In this context, the importance of other methods is key. Intelligence activities appear to present a particular opportunity to counter illicit procurement. Another area where it might be prudent to make more efforts relates to scrutiny of foreign investments in manufacturing firms.

This paper has focused on nuclear proliferation and has only briefly touched upon associated missile delivery systems. However the foregoing has given no reason to believe that the methods used to procure for such missile programmes are essentially different. While the specific problems involved in areas such as inventing plausible benign end uses to declare for goods being sought may differ, the essential problem appears to be the same. In addition, although this paper has not examined any instances of procurement for an illicit chemical or biological weapons programme, the techniques general necessity for the procurer to successfully establish at least one point of deception would appear to be applicable, even though the sheer scale and diversity of the chemical, biotechnology and related industries worldwide may offer more opportunities to hide illicit activity.

Conclusions

The growing scope and coverage of supply-side nonproliferation controls focused chiefly on strategic export controls, and to a broader extent strategic trade controls (such as controls on brokering in some countries' legislation) has changed rather than prevented procurement for nuclear and missile programs. Several states have relied upon similar techniques over the course of the last four decades suggesting that current nonproliferation controls can be poorly suited to preventing such behaviour. Current controls rely heavily on export control regulations which can be difficult and resource-intensive to enforce.

The paper has presented a model – "points of deception" - through which such illicit trade can be understood. It is notable that according to information available through open sources proliferators have been reported to utilise nearly every technique that was identified through the model.

Examination of illicit trade through the model provides certain insights into what measures could be taken to disrupt proliferation networks. These include awareness raising and enforcement and the use of advanced supply-chain techniques to prevent complicity. It includes improving physical security and vetting in companies to prevent theft and insider threats.

The examination also highlighted the utility of scrutiny programs on inward investment to mitigate the risks of foreign buy-out, particularly for producers of sensitive goods that are in financial difficulty.

For certain risks that were identified through the application of the framework, such as the use of diplomatic bags to ship goods, there are no clear solutions. Instead, consideration should be given to how best to monitor domestic sales of proliferation-sensitive technologies.

This paper has examined a wide range of techniques and activities that fall within the tradecraft of illicit procurers. Although the sophistication, complexity, degree of direction and centralised organisation used in illicit procurement activities can vary greatly, in general in a particular procurement attempt an individual procurer or a wider network will have to successfully manage at least one 'point of deception' and may draw upon a range of other particular skills practised whilst carrying out procurement for ultimately clandestine means.

Dual-Use Goods," Project Alpha, King's College London, August 26, 2015. < https://projectalpha.eu/visualisations/commercial-producers-of-nsg-controlled-dual-use-goods>.

Illicit procurement can thus be viewed in part as a contest between the due diligence efforts of commercial suppliers and governments opposing proliferation together with those government's counter-proliferation intelligence activities on one side, and on the other side the procurers' ability to deceive, suborn, manipulate and generally manage the clandestine elements of their business, combined with proliferator government's counterintelligence and security. This may be a useful viewpoint to take when devising or scrutinising nonproliferation controls, measures and postures, where some degree of war gaming or 'red teaming' the countermeasures that proliferators may use may be helpful to ensure that counter-procurement is made as effective as possible.

The use of illicit procurement techniques has been endemic since the 1970s. There are few reasons to suspect that use of the practices will end any time soon. Nonproliferation controls and efforts to prevent illicit trade can only slow down or frustrate illicit procurement. Ultimately, therefore, the international community must also look to other solutions in order to prevent proliferation. To that end, it will remain important to work continuously to ensure to that illicit procurement is countered as effectively as possible in order to buy time for other solutions to be developed.

Proliferation Financing: The Potential Impact of the Nuclear Agreement with Iran on International Controls

JONATHAN BREWER[1]

Abstract

The UN framework of controls on financing of proliferation included, until 16 January 2016, Implementation Day of the JCPOA, financial provisions of resolution 1540 (2004) and financial sanctions on DPRK and on Iran. To implement financial sanctions effectively, States were required to put in place appropriate legislation, structures and procedures that could also serve, at least in part, to implement financial requirements under resolution 1540. Following Implementation Day, sanctions on Iran have been removed or replaced by "specific restrictions" under UN resolution 2231 (2015), and in consequence the UN framework of controls on financing of proliferation has been loosened. Even before Implementation Day, assessments published by the Financial Action Task Force (FATF) suggested that few States properly implemented one of the key controls on proliferation - targeted financial sanctions. Following Implementation Day, and despite the looser UN framework of controls, it will be important that States maintain in place effective legislation, structures and procedures to ensure they can identify and disrupt financing of proliferation.

Keywords

Proliferation financing, resolution 1540, Iran, DPRK, resolution 2231, financial sanctions, Joint Comprehensive Plan of Action (JCPOA)

Introduction

The financing of proliferation of weapons of mass destruction (WMD) is prohibited by international sanctions and controls, including a framework of United Nations (UN) Security Council resolutions. Detecting and disrupting circumvention of these sanctions and controls is an important element of the international community's efforts to combat proliferation.[2] Financial transactions connected with proliferation usually take place at least in part through the global financial system, so detection and disruption is usually focused on that system.[3]

[1]Jonathan Brewer is a Visiting Professor at King's College, London, Centre for Science and Security Studies. From 2010 to 2015 he served as the financial expert on the UN Panel on Iran created pursuant to resolution 1929 (2010).

[2] Council of the European Union, "Council Conclusions and New Lines for Action by the European Union in Combating the Proliferation of Weapons of Mass Destruction and their Delivery Systems," 17172/08, Brussels, December 17, 2008.

[3] FATF, "FATF Typologies Report on Proliferation Financing," June 18, 2008, < http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>; United Nations, "Final Report of the Panel of Experts

The UN framework has been modified following the successful start of the Joint Comprehensive Plan of Action (JCPOA). On 16 January 2016, Implementation Day of the JCPOA, UN sanctions resolutions (four in total) on Iran were terminated.[4] Their financial provisions were either removed altogether or replaced by financial restrictions under UN resolution 2231 (2015). This is not a sanctions resolution.

The purpose of this paper is to highlight the possibility that states may be tempted to divert the resources previously devoted to financial sanctions on Iran and use them to bolster work taking place against other priorities. The paper outlines the UN framework of controls before Implementation Day and examines available evidence, albeit limited, of how well UN Member States implemented them. The paper makes the case that resources devoted to implementation of UN financial sanctions may also assist in implementation of financial measures under resolution 1540 (2004).

The paper concludes that diversion of resources following Implementation Day, if any, must be done with great care. There is a continuing need to implement financial controls on Iran under resolution 2231 (2015), even though these are time-limited.[5] There is a need to monitor the JCPOA and ensure no cheating. States are obliged to implement UN sanctions on proliferation and proliferation financing by the DPRK. A recent successful prosecution of financing of proliferation is a timely reminder to states and the private sector that identifying and disrupting such activity should remain a high priority.[6]

Background

There is no universally-recognised definition of financing of proliferation. The definition used in this paper follows that adopted by the Financial Action Task Force (FATF), i.e. "the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."[7]

The current UN framework of controls against proliferation financing includes measures in resolution 1540 (2004) and subsequent resolutions, the five sanctions resolutions on the Democratic Peoples Republic of Korea (DPRK) and restrictions on the Islamic Republic of Iran.[8,9,10]

The UN Framework to Combat the Financing of Proliferation: Before Implementation Day

The UN framework to combat the financing of proliferation rests on two pillars. One pillar was (and still

---

Submitted Pursuant to Resolution 2141, S/2015/131, 2014.

[4] UN Security Council Resolution 1737, S/Res/1737, 2006; UN Security Council Resolution 1747, S/Res/1747, 2007; UN Security Council Resolution 1803, S/Res/1803, 2008; UN Security Council Resolution 1929, S/Res/1929, 2010.

[5] UN Security Council Resolution 1737, S/Res/1737, 2006; UN Security Council Resolution 2231, S/Res/2231, 2015 contains provisions for the re-imposition of UN sanctions in the even of "significant non-performance" of the JCPOA.

[6] Andrea Berger, "Thanks to the Banks: Counter-Proliferation Finance and the Chinpo Shipping Case," 38 North, 16 December 2015, < http://38north.org/2015/12/aberger121615/>.

[7] FATF, "Combatting Proliferation Financing: A Status Report on Policy Development and Consultation," February 2010, < http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf>. FATF's methodology for assessing technical compliance with FATF Standards, and effectiveness of their implementation, is described in the FATF publication: Methodology for Assessing Technical Compliance with FATF Recommendations and the Effectiveness of AML/CFT Systems, February 2013.

[8] UN Security Council Resolution 1673, S/Res/1673, 2006; UN Security Council Resolution 1810, S/Res/1810, 2008, UN Security Council Resolution 1977, S/Res/1977, 2011.

[9] UN Security Council Resolution 1718, S/Res/1718, 2006; UN Security Council Resolution 1874, S/Res/1874, 2009; UN Security Council Resolution 2087, S/Res/2087, 2013, UN Security Council Resolution 2094, S/Res/2094, 2013 and the most recent, UN Security Counci Resolution 2270, S/Res/2270, March 2016.

[10] UN Security Council Resolution 2231, S/Res/2231, 2015.

is) resolution 1540 (2004). This resolution requires States to adopt and enforce legislation which prohibits financing of activities prohibited under the resolution. Prohibitions include WMD-related activities by non-State actors and their financing. The term "non-State actors" is not defined, but could include any entity or individual that is not acting under control of the State.[11] In addition, States are required to maintain effective export controls, including controls on provision of related funds and financial services.[12]

The second pillar for combatting proliferation financing is comprised of UN Security Council Chapter VII resolutions on Iran and DPRK.[13] Implementation of such resolutions is mandatory for all UN Member States although it is for States to determine how they do so. The resolutions included (and in the case of DPRK still include) a variety of provisions intended to halt or slow Iran's or DPRK's proliferation-related activities, including four categories of financial sanctions:[14,15]

Targeted Financial Sanctions (TFS)

TFS require the freezing of funds, other financial assets and economic resources of designated entities and individuals, as well as those of persons or entities acting on their behalf or at their direction, or of entities owned or controlled by them.[16] Designated individuals and entities were listed on the websites of the Security Council Committees established pursuant to resolution 1737 (2006) for Iran, and resolution 1718 (2006) for DPRK. Forty-three individuals and 78 entities were designated for Iran, and 12 individuals and 20 entities for DPRK. They included five financial institutions: Bank Sepah and Bank Sepah International, and First East Export Bank (in the case of Iran) and Amroggang Development Banking Corporation, Bank of East Land and Tanchon Commercial Bank (for DPRK).[17] The numbers of designated banks were not large by comparison with the numbers designated under unilateral sanctions (such as those of the European Union or United States), but UN sanctions were obligatory on all Member States and their implementation effectively blocked these banks from accessing the international financial system.

---

[11] Definitions of non-State actors include a variety of organisations. For example, the Report of the International Law Association Hague Conference (2010) on Non State Actors included the private sector as well as armed groups in the term.

[12] Two paragraphs of resolution 1540 (2004) make explicit reference of financing. Under paragraph 2 of resolution 1540 (2015) States "… in accordance with their national procedures, shall adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or *finance* them"; and under paragraph 3(d), States are required to "Establish, develop, review and maintain appropriate effective national export and trans-shipment controls over such items, including appropriate laws and regulations to control export, transit, trans-shipment and re-export and controls on providing funds and services related to such export and trans-shipment such as *financing*, and transporting that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations" (italics are mine). Paragraph 9, without making a specific reference, clearly extends, financing: "… States [are called upon] to promote dialogue and cooperation on non- proliferation so as to address the threat posed by proliferation of nuclear, chemical, or biological weapons, and their means of delivery."

[13] UN Security Council Resolution 1718, S/Res/1718, 2006; UN Security Council Resolution 1874, S/Res/1874, 2009; UN Security Council Resolution 2087, S/Res/2087, 2013, UN Security Council Resolution 2094.

[14] Financial measures included in a further Security Council resolution imposed on DPRK on 3 March 2016, UN Security Council Resolution 2270, S/Res/2270, 2016, are described in footnotes 35, 36 and 37 below.

[15] These categories are further defined in FATF's Guidance: FATF, "The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction," June 2013, < http://www.fatf-gafi.org/documents/documents/unscr-proliferation-wmd.html>.

[16] For Iran: Paragraphs 12 to 15 of resolution 1737 (2006), paragraph 6 of resolution 1747 (2007), paragraph 7 of resolution 1803 (2008) and paragraphs 11, 12 and 19 of resolution 1929 (2010); for DPRK, paragraph 8(d) of resolution 1718 (2006), paragraph 7 of resolution 1874 (2009), paragraph 5(a) of resolution 2087 (2013) and paragraph 8 of resolution 2094 (2013).

[17] Although under UN sanctions on Iran only two banks were designated, under unilateral sanctions regimes, in particular those of the US and EU, most of Iran's other major banks were also designated. The UN Panel on Iran created pursuant to resolution 1929 (2010) noted instances of trading companies established by Iranians overseas apparently being used to facilitate financial transactions, perhaps in attempts to circumvent these sanctions (paragraph 194 (c) of the 2012 Report, and Annex V of the 2014 Report, of the Panel of Experts created pursuant to resolution 1929 (2010).

Activity-based Sanctions

These prevented the transfer of financial resources or services related to the supply, sale, transfer, manufacture and use of proliferation-sensitive items that were prohibited for transfer to Iran or DPRK. They also prevented the provision of financial services and transfer of financial assets or resources which could contribute to prohibited activities by Iran or DPRK.[18,19]

Vigilance Requirements:[20]

In the case of Iran, States were obliged to ensure individuals and entities were vigilant when doing business with Iran. States were also called upon to exercise vigilance in the provision of any financial assistance or services to Iran, and vigilance over the banking sector's interaction with Iran's banks (in particular with Bank Melli and Bank Saderat, and also the Central Bank of Iran). In the case of DPRK, States are called upon to exercise vigilance and monitoring over business conducted with DPRK financial institutions, and also over DPRK diplomatic personnel (in connection with cash smuggling). In practice, many States exercised vigilance by requiring transactions with individuals or entities in Iran for example, if over a certain limit, to be licensed.[21]

Other Financial Provisions:[22]

In the case of Iran these included a prohibition on initiating new business between Member States banks and Iranian banks if related to prohibited activities. In the case of DPRK, States are called upon not to provide grants and loans, or support for trade and new business with banks if connected with prohibited activities.

Prior to Implementation Day, how well in fact were the two pillars of the UN framework being implemented? On the basis of available information it is difficult to answer this question with more than general, qualitative statements. Resolution 1540 (2004) for example makes no provision for formal assessment of its implementation by Member States. A few clues can be found in reports published by the Committee established pursuant to resolution 1540 (2004), in particular the Committee Report of 2011, summarized in the table below.[23] The Committee noted in this report that, rather than implementing legislation directed specifically at financing of proliferation, in many of the cases in this table States had used existing anti-terrorism and anti-money-laundering enforcement legislation to criminalize the financing of illicit activities relating to nuclear, chemical and biological weapons and their means of delivery. Legislation directed specifically at financing of proliferation is rare.

---

[18] For Iran, paragraph 6 of UN Security Council Resolution 1737, S/Res/1737, 2006, paragraphs 8, 13 and 21 of UN Security Council Resolution 1929, S/Res/1929, 2010; for DPRK, paragraph 8(c) of UN Security Council Resolution 1718, S/Res/1718, 2006, paragraphs 9, 10 and 18 of UN Security Council Resolution 1874, S/Res/1874, 2009, paragraph 5(b) of UN Security Council Resolution 2087, S/Res/2087, 2013, and paragraphs 7, 11, 14 and 20 of UN Security Council Resolution 2094, S/Res/2094, 2013.

[19] In the case of Iran, prohibited activities included proliferation-sensitive nuclear activities or the development of nuclear weapon delivery systems. In the case of DPRK they included nuclear-related, ballistic missile-related and other WMD-related programmes.

[20] For Iran: Paragraph 6 of UN Security Council Resolution 1747, S/Res/1747, 2007, paragraphs 9 and 10 of UN Security Council Resolution 1803, S/Res/1803, 2008, paragraph 22 of UN Security Council Resolution 1929, S/Res/1929, 2010; For DPRK, paragraph 18 of UN Security Council Resolution 1874, S/Res/1874, 2009, paragraph 6 of UN Security Council Resolution 2087, S/Res/2087, 2013, and paragraph 24 of UN Security Council Resolution 2094, S/Res/2094, 2013.

[21] E.g. Council Regulation (EU), No 961/2010 of 25 October 2010 on Restrictive Measures against Iran, 2010.

[22] For Iran: Paragraph 7 of UN Security Council Resolution 1747, S/Res/1747, 2007, paragraph 7, 23 and 24 of UN Security Council Resolution 1929, S/Res/1929, 2010; for DPRK, paragraphs 19 and 20 of UN Security Council Resolution 1874, S/Res/1874, 2009 and paragraphs 12 and 13 of UN Security Council Resolution 2094, S/Res/2094, 2013.

[23] UN, "Report of the Committee Established Pursuant to Resolution 1540 (2004)," September 12, 2011, paragraphs 54 and 74.

	2008	Dec 2010	
Legislative measures to prevent financing of:	Nuclear weapons	66	125
	Chemical weapons	71	128
	Biological weapons	64	121
Enforcement measures to prevent financing of:	Nuclear weapons	78	120
	Chemical weapons	87	122
	Biological weapons	75	114
States with measures in place against the financing of illicit trade transactions related to nuclear, chemical and biological weapons, their means of delivery and related materials	29	49	

Compared to the total number of UN Member States (193) these numbers are low. However, they increased significantly between 2008 and December 2011 and if the trend continued it can be assumed that many UN Member States have some sort of framework for implementing financial aspects of resolution 1540 (2004), even if this framework is not set out specifically in terms of financing of proliferation.

UN sanctions resolutions, and resolution 2231 (2015), similarly make no formal provision for assessment of their implementation by Member States. The best available information can be found in reports of relevant UN Panels.[24] Qualitative assessments by these Panels suggest most States were implementing financial sanctions reasonably well. For example, the Panel on Iran found in 2012 "…a high level of awareness among Member States and the private sector of United Nations financial sanctions. Many Member States are implementing sanctions through their financial regulatory bodies with rigour."[25] The Panel on DPRK assessed in 2014 that "Financial measures in the resolutions, along with the strengthening of standards governing international finance, have combined to change fundamentally the financial environment in which the Democratic People's Republic of Korea operates."[26]

However, when implementation is looked at in more detail, this conclusion looks overly-positive, as demonstrated by reviews published by FATF and FATF-style regional bodies (FSRBs). As part of FATF's review of Member States under the mutual evaluation process, a formal assessment is made of implementation of one specific element of UN controls on proliferation, TFS, under Recommendation VII.[27] Assessments published to date of performance against Recommendation VII provide insights into the challenges of UN TFS implementation, and the legislation, structures and procedures set up by individual countries to meet them.[28] The results of these assessments are summarized in Table I below. The data all pre-date Implementation Day.

---

[24] In the case of DPRK these are: UN document S/2010/517 of 5 November 2010, S/2012/422 of 14 June 2012, S/2013/337 of 11 June 2013, S/2014/147 of 6 March 2014 and S/2015/131 of 23 February 2015. In the case of Iran they are S/2012/395 of 12 June 2012, S/2013/331 of 5 June 2013, S/2014/393 of 5 June 2014 and S/2015/401 of 2 June 2015.

[25] UN, "Report of 12 June 2012 of the UN Panel Created Pursuant to 1929 (2010)," June 2012, Paragraph 208.

[26] UN, "Report of 6 March 2014 of the UN Panel established pursuant to resolution 1874 (2009)," March 2014, Paragraph 164.

[27] Recommendation 7 of the FATF Standards of 2012 states that «Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.», <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>.

[28] See for example Chapter IV of the Mutual Evaluation Report of Spain of December 2014, the first such report to evaluate a country's implementation of Recommendation 7.

Table 1: Assessments Published to Date of Performance against Recommendation VII[29]

Country and Date of Publication of FATF/FSRB Review	Technical Compliance[1] with Recommendation VII	Effectiveness of Implementation[2] of Recommendation VII (Measured by Immediate Outcome 11)
Spain (Dec 2014)	Partially Compliant	Moderate
Norway (Dec 2014)	Partially Compliant	Moderate
Belgium (Apr 2015)	Partially Compliant	Moderate
Australia (Apr 2015)	Compliant	Substantial
Ethiopia (Jun 2015)	Non-Compliant	Low
Malaysia (Sep 2015)	Partially Compliant	Substantial
Sri Lanka (Oct 2015)	Non-Compliant	Low
Vanuatu (Oct 2015)	Non-Compliant	Low
Samoa (Oct 2015)	Non-Compliant	Low
Cuba (Dec 2015)	Largely Compliant	Moderate
Costa Rica (Dec 2015)	Non-Compliant	Low
Armenia (Jan 2016)	Partially Compliant	Substantial
Italy (Feb 2016)	Partially Compliant	Substantial
FATF Technical Compliance Ratings		
Compliant	There are no shortcomings	
Largely Compliant	There are only minor shortcomings.	
Partially Compliant	There are moderate shortcomings.	
Non-Compliant	There are major shortcomings.	
FATF Effectiveness Ratings		
High level of effectiveness	The Immediate Outcome is achieved to a very large extent. Minor improvements needed.	
Substantial level of effectiveness	The Immediate Outcome is achieved to a large extent. Moderate improvements needed.	
Moderate level of effectiveness	The Immediate Outcome is achieved to some extent. Major improvements needed.	
Low level of effectiveness	The Immediate Outcome is not achieved or achieved to a negligible extent. Fundamental improvements are needed.	

The data set is as yet very limited (there will probably be in total more than 180 reviews of FATF or FSRB jurisdictions assessed in due course against Recommendation VII) and may not be representative of FATF/FSRB States in total.[30] However, it can be seen immediately from Table 1 that with the exception

[29] The information in this table is taken from the FATF website <fatf-gafi.org>.

[30] According to a statement on FATF's website "Over 180 jurisdictions around the world have committed to the FATF

of Australia, no country has been assessed by FATF or by a FSRB as meeting the requirements to be rated at the top of the scale ("Compliant") with the technical requirements of Recommendation VII. The scores against technical requirements of the majority of States cluster in lower parts of the scale, in the "Partially Compliant" or "Non-Compliant" categories. Against FATF measures for effectiveness of compliance with Recommendation VII, no country has been assessed at the top of the scale ("Highly Effective") although the majority of States cluster towards the middle of this scale ("Substantial" or "Moderate").

In summary, the data, albeit limited, show that the majority of States were not implementing FATF Recommendation VII to a satisfactory standard before Implementation Day. It seems reasonable to conclude, therefore, that the majority of UN Member States were probably not implementing UN TFS to a satisfactory standard, and, likely, were not implementing the full range UN financial sanctions to a satisfactory standard.

There are a number of reasons why this may have been the case. Transactions associated with financing of proliferation may be difficult to distinguish from legitimate transactions. The goods or materials involved may not be distinctive and the sums involved may not stand out.[31] Iran and DPRK practice deception to try to hide their involvement in the transactions. The channels used for financing may be separate, possibly in foreign jurisdictions, and so difficult to match with related goods and materials. Financial authorities or institutions may not have access to relevant information. Finally, there is relatively little work publicly available about typical typologies (the most recent compilation was published by FATF in 2008).[32]

The UN Framework to Combat the Financing of Proliferation: After Implementation Day

The provisions of resolution 1540 (2004) remain of course unchanged. The four UN sanctions resolutions on DPRK also remain unchanged but in addition the Security Council has subsequently imposed a fifth resolution, 2270 (2016). This contains additional TFS (two more financial institutions are designated: Daedong Credit Bank (also known as Taedong Credit Bank) and the Korea Kwangson Banking Corporation), activity-based sanctions, and other financial provisions.[33,34,35] However, in the case of Iran, the Security Council has terminated all sanctions, and in their place resolution 2231 (2015) imposes a variety of new controls (referred to as "specific restrictions").[36] These are mandatory and time-limited, as follows:

Procurement by Iran that was previously prohibited under UN sanctions, together with provision of related financial assistance and transfer of financial resources and services, is now permitted so long as the Security Council approves each transaction on a case-by-case basis:

1. For nuclear goods and materials, procurement must take place through a "procurement channel,"with ultimate approval by the Security Council.[37] This requirement ceases ten years after 18 October 2015;[38]

Recommendations through the global network of FSRBs and FATF memberships," <fatf-gafi.org>.

[31] UN, "UN Panel on Iran Report of June 2013", Paragraph 143, < http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2013_331.pdf>.

[32] FATF, "FATF Report on Typologies of Proliferation Financing," 2008, < http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html>.

[33] UN Security Council Resolution 2270, S/Res/2270, 2016, paragraph 32.

[34] UN Security Council Resolution 2270, S/Res/2270, 2016, paragraph 37.

[35] UN Security Council Resolution 2270, S/Res/2270, 2016, paragraphs 33, 34, 35 and 36.

[36] UN Security Council Resolution 2231, S/Res/2231, 2015, paragraph 18.1 of Annex V of Annex A.

[37] See Annex IV to Annex A (the JCPOA) of UN Security Council Resolution 2231, S/Res/2231, 2015.

[38] Or sooner if the IAEA reaches a "Broader Conclusion" regarding Iran's nuclear programme. A "Broader Conclusion" that "all nuclear material remains in peaceful activities" requires IAEA to conclude both that no indication exists of diversion of declared nuclear materials and that no indication exists of undeclared nuclear material or activities. See IAEA Safeguards, "Staying Ahead of the Game," 2007, p.18, <https://www.iaea.org/sites/default/files/safeguards0707.pdf>.

2. For procurement related to missile technologies, the requirement for approval by the Security Council ceases eight years after 18 October 2015;[39]

3. For procurement of certain categories of conventional arms, the need for approval ceases five years after 18 October 2015.[40]

States must continue to freeze funds, other financial assets and economic resources that are owned or controlled by individuals or entities listed by the UN. Although in many respects this requirement is identical to requirements under UN sanctions TFS, some differences exist:

1. The provision expires eight years after 18 October 2015;[41]

2. Only 23 individuals and 62 entities, connected with Iran's ballistic missile activities, conventional arms transfers or the IRGC, are listed.[42] They comprise those remaining on the list maintained by the 1737 Sanctions Committee after entities and individuals directly connected with Iran's nuclear programme, and Bank Sepah, were removed on or following Implementation Day;[43]

3. The 23 individuals and 62 entities are not included in the UN's consolidated sanctions list of designations under all UN sanctions regimes, but listed separately.[44,45] This is consistent with resolution 2231 (2015) not being a sanctions resolution;

4. Under UN sanctions prior to Implementation Day, requirements to freeze funds, other financial assets and economic resources of listed individuals and entities extended also to entities owned or controlled by listed individuals or entities, and to individuals or entities acting on their behalf or at their direction. Resolution 2231 (2015) contains no language requiring such extension;

5. Exemptions in place under UN sanctions remain in their same general form under resolution 2231 (2015) but are also extended.[46]

Additional asset freezes must be imposed by States on individuals and entities that may be designated by the Security Council for involvement in activities contrary to Iran's commitments under the JCPoA, for assisting designated individuals or entities evading or acting inconsistently with the JCPoA or resolution 2231 (2015), for acting on behalf or at the direction of designated individuals or entities, or for being owned or controlled by designated individuals or entities.

Following Implementation Day all activity-based financial sanctions, requirements for vigilance and other financial measures are terminated.

---

[39] Ibid.

[40] Ibid.

[41] Or sooner if the IAEA reaches a "Broader Conclusion" regarding Iran's nuclear programme.

[42] United Nations Security Council, "Resolution 2231 List," <http://www.un.org/en/sc/2231/list.shtml>.

[43] UN, "Security Council Removes Bank Sepah and Bank Sepah International from 2231 List," January 17, 2016, <http://www.un.org/press/en/2016/sc12209.doc.htm>. Bank Sepah was listed because of its connections to Iran's ballistic missile programmes.

[44] United Nations Security Council, "Consolidated United Nations Security Council Sanctions List," <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>.

[45] United Nations Security Council, "Resolution 2231 List," <http://www.un.org/en/sc/2231/list.shtml>.

[46] These exceptions include basic expenses (subject to notification to the Security Council); extraordinary expenses (subject to approval by the Security Council); if subject to judicial lien etc (subject to notification to the Security Council), in connection with civil nuclear cooperation and activities required for implementation of the JCPoA (both also subject to approval by the Security Council).

The Changes to the Framework of UN Controls on Financing of Proliferation

UN sanctions were imposed on Iran in response to prohibited proliferation activities, so it is logical that these sanctions, including financial sanctions, should be modified under resolution 2231 (2015). The JCPoA and resolution 2231 (2015) comprise a series of steps which, if successfully implemented, will enable a determination by the IAEA and the international community that Iran's nuclear programme is exclusively peaceful in nature and of no proliferation concern.

Furthermore, although financial sanctions on Iran have formally been removed, resolution 2231 (2015) has in effect created a new type of control on proliferation and the financing of proliferation: the need for Security Council approval of procurement and related financial assistance or transfer of financial resources or services, on a case-by-case basis. Financing of any relevant procurement that takes place outside this framework could be considered not only a violation of resolution 2231 (2015) but also financing of proliferation.

However, in other respects resolution 2231 (2015) loosens the UN framework of controls on financing of proliferation following Implementation Day. First, consistent with resolution 2231 (2015) not being a sanctions resolution, the specific restrictions are scheduled to terminate after set periods of time. Iran is not reliant on their termination by a Security Council decision. Termination could take place even if Iran fails to comply with the resolution, so long as any such failure does not constitute "significant non-performance" with the JCPOA and a trigger of "snap-back" provisions.[47] Furthermore, even though "snap-back" provisions apply to the JCPOA, no such provisions exist in respect of non-compliance by Iran with other controls on proliferation or its financing under resolution 2231 (2015), such as ballistic missile activities. A Security Council resolution would be necessary to penalize Iran for any such non-compliance.

Second, Resolution 2231 (2015), not being a sanctions resolution, includes no provision for the creation of a Security Council Committee or an independent Panel of Experts to provide guidance or advice to Security Council or Member States regarding implementation of the resolution, or to investigate reports of possible violations. Although the UN Secretariat will take on some of these tasks, it may not have the expertise nor independence of a Panel of Experts. Furthermore its terms of reference include no requirement to investigate allegations of non-compliance.[48] In summary therefore not only are financial restrictions under Resolution 2231 (2015) weaker than under UN sanctions, but it is possible that the resolution itself may not be as well policed as were UN sanctions.

Potential Impact of these Changes on Implementation of Controls on Financing of Proliferation

In addition to loosening the global framework of controls on financing of proliferation, resolution 2231 (2015) may weaken the commitment of individual States to maintain in place appropriate structures and procedures to control it. It is too soon after Implementation Day to test whether this has happened, but the relevant UN structures, and FATF, will need to be vigilant for any indications.[49] There are two potential dangers: first, to financial sanctions on DPRK that States must continue to implement; and second, because structures and procedures to implement sanctions can also contribute to the capacity of Member States to implement effectively financial measures under resolution 1540 (2004).

Examples of structures and procedures are described in annual reports of the UN Panels on Iran and on DPRK

---

[47] See Annex A (the JCPOA) of UN Security Council Resolution 2231, S/Res/2231, 2015.

[48] UN, "Note by President of the Security Council: Security Council Tasks under Security Council resolution 2231 (2015)," S/2016/44, January 16, 2016, < http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/44&referer=http://www.un.org/en/sc/2231/note.shtml&Lang=E>.

[49] In the case of UN sanctions on DPRK, the Panel, and in the case of resolution 2231 (2015) the UN Secretariat structures set up under the note referenced in footnote 41.

published by the Security Council.[50] They include, for example, effective inter-departmental coordination of policy, and of operational responses (such as disruption), in response to information about attempts to circumvent financial sanctions and financing of proliferation. Fundamental is effective inter-departmental communication: in the case of TFS, for example, the need to identify assets of designated individuals or entities requires mechanisms for exchange of relevant information which might be sensitive or classified. Mechanisms for exchanging sensitive or classified information with overseas partners are also vital.

Crucial, in addition, are effective procedures and channels for communication between authorities and the private sector. These should be capable of handling information that may be commercially sensitive or classified intelligence, including regarding policy issues as well as specific information about suspicious individuals or entities.[51] Financial institutions in turn must be required to submit relevant Suspicious Activity Reports. These should be investigated and, if appropriate, action taken to disrupt proliferation activity.[52]

Successful implementation of UN sanctions on financing of proliferation requires significant investment of resources and effort in these structures and procedures. States may be tempted, in the light of the successful start to the JCPOA, to assume that the need to implement such sanctions is less pressing, and so be tempted to divert resources elsewhere. This they must do, if at all, with extreme care. There is a continuing need to implement financial controls on Iran under resolution 2231 (2015) and a need to monitor the JCPOA and ensure no cheating. In addition, States remain obliged to implement UN sanctions to counter the financing of proliferation by the DPRK.

The importance of ensuring that existing structures and procedures are not permitted to wither is demonstrated by the very small number of reports, even to date, of identification and disruption of financing of proliferation. A recent case (December 2015) in which a defendant was found guilty by a Singaporean court of providing financial services or transferring financial assets or resources "that may reasonably be used to contribute to the nuclear-related, ballistic missile-related, or other weapons of mass destruction-related programs or activities of the Democratic People's Republic of Korea," simply demonstrates that cases are rarely brought to trial.[53] Even in the cases of suspicious transactions reports submitted by banks on the basis of proliferation, subsequent prosecutions are almost always based on other grounds (for example, export control violations). Prosecutions of related financial activity, on the rare occasions these take place, are usually based on money-laundering or other offences.[54]

The second area of potential danger is the undermining of the capacity of Member States to implement financial measures effectively under resolution 1540 (2004). These measures (see footnote 9 above) are set out in only in general terms. The resolution mandates no standards or procedures. There are no specific requirements, for example, to freeze assets, conduct vigilance or implement activity-based financial sanctions. Member States must decide for themselves what measures to take, and the resources to devote to the task.

In the absence of mandated standards or procedures, some guidance can be found in certain of the financial provisions of UN sanctions on Iran and on DPRK. These in some respects resemble the financial provisions

[50] See footnote 20.

[51] Paragraph 188 of UN, "Report of 2012 of UN Panel of Experts pursuant to resolution 1929 (2010)," 2012.

[52] See example described in paragraph 23 of UN, "Final report of the UN Panel on Iran," S/2013/331, 2013.

[53] Under Regulation 12b of Singapore's United Nations Regulations, 2010.

[54] For example, Karl Lee (aka Li Fang Wei), indicted on a series of charges related to procurement of WMD-related goods and materials that included money-laundering and wire fraud. Funds have been seized in the US in connection with alleged violations of US sanctions law by overseas companies owned by Lee, see US Department of Justice, ""Karl Lee" Charged in Manhattan Federal Court with Using a Web of Front Companies to Evade U.S. Sanctions," April 29, 2014, <http://www.justice.gov/opa/pr/karl-lee-charged-manhattan-federal-court-using-web-front-companies-evade-us-sanctions>.

of resolution 1540 (2004). For example, language in UN resolutions regarding activity-based financial sanctions is similar to that in paragraph 2 of resolution 1540 (2004) under which States are required to "…adopt …laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery …as well as attempts to engage in any of the foregoing activities … or finance them."[55]

Similar language, relating to "manufacture, transfer and use" of items, and references to "activities", can also be found in the former UN sanctions resolutions on Iran: States were a) required to "…take the necessary measures to prevent the provision … of … financial assistance, investment … and the transfer of financial resources or services, related to the supply, sale, transfer, manufacture or use of… items, materials, equipment, goods and technology…" which could contribute to prohibited nuclear activities or to the development of nuclear weapon delivery systems; and b) called upon to prevent the provision of financial services…or the transfer … of any financial or other assets or resources … that … could contribute to Iran's proliferation-sensitive nuclear activities."[56]

Similarly under UN resolutions relating to DPRK states are required to a) "…prevent any transfers … of services…related to the provision, manufacture, maintenance or use…" of items prohibited for "direct or indirect transfer" to DPRK"; and b) "…prevent the provision of financial services or the transfer of any financial or other assets or resources... that could contribute to [DPRK's prohibited WMD programmes] … or other activities prohibited by [UN sanctions resolutions] …". [57]

Separately, under paragraph 3(d) of resolution 1540 (2004), States are required to implement "…export and trans-shipment controls over nuclear, chemical or biological weapons and their means of delivery including appropriate laws and regulations to control … funds and services … such as financing... that would contribute to proliferation." Effective implementation of this requirement requires states, in order to control "funds and services such as financing", to determine precisely what items fall into the category of "nuclear, chemical or biological weapons and their means of delivery."

Provisions of UN sanctions resolutions on Iran and DPRK relating to funding and financing of items subject to export controls contain similar language, but in addition they reference specific lists of items that fall into the category of "nuclear, chemical or biological weapons and their means of delivery". For example, with regards to Iran, states were required to "take the necessary measures to prevent the provision to Iran of … financial assistance … and the transfer of financial resources or services, related to the supply, … transfer … of the prohibited items …".[58] Resolutions on DPRK require states to prevent "…services … related to provision …" of prohibited items.[59] In the case of both Iran and of DPRK, the resolutions state that the prohibited items referred to are those on relevant versions of lists published by the Nuclear Suppliers Group and by the Missile Technology Control Regime.[60,61]

It is very likely therefore that despite the absence of mandated standards or procedures under resolution 1540 (2004), and the difficulties of many Member States in determining what constitutes implementation to

---

[55] United Nations Security Council Resolution 1540, S/Res/1540, 2004, paragraph 2.

[56] Paragraph 6 of United Nations Security Council Resolution Resolution 1737, S/Res/1737, 2006 and paragraph 13 and 21 of United Nations Security Council Resolution 1929, S/Res/1929, 2010.

[57] Paragraphs 8(a) and 8(c) of United Nations Security Council Resolution 1718, S/Res/1718, 2006, paragraph 11 of United Nations Security Council Resolution 2094, S/Res/2094, 2013.

[58] Paragraph 6 of United Nations Security Council Resolution Resolution 1737, S/Res/1737, 2006.

[59] Paragraph 8 of United Nations Security Council Resolution 1718, S/Res/1718, 2006.

[60] See current version at: "NSG Guidelines Dual Use List," Nuclear Suppliers Group, <http://www.nuclearsuppliersgroup.org/en/news/148-update-of-nsg-control-lists>.

[61] See current version at: "MTCR Equipment, Software, Technology Annex," Missile Technology Control Regime, <http://www.mtcr.info/english/annex.html>.

a satisfactory standard, those states that already possess legislation, structures and procedures to implement sanctions on Iran and on DPRK are also in a position to implement effectively, at least in part, financial measures of resolution 1540 (2004). Hence, any diversion of resources and or dilution of procedures related to financial monitoring and control, following Implementation Day, could impact on the ability of states to combat effectively financing of proliferation under resolution 1540 (2004). This might matter less if states were already implementing UN controls on financing of proliferation satisfactorily, but as described above, most are probably not.

FATF's Role in Assessing Implementation of UN Resolutions on Financing of Proliferation

Asset freezes under the specific restrictions of resolution 2231 (2015) are similar to TFS on Iran that existed prior to Implementation Day, so FATF could presumably assess their implementation in future, in some form. Recommendation 7 and FATF's mutual evaluation procedures would need to be modified. It will be important that FATF does so in order to provide an independent assessment of States' implementation of resolution 2231 (2015), and to continue to contribute fully to international efforts to ensure that UN controls on proliferation are effectively implemented.

Other elements of UN sanctions on financing of proliferation, such as activity-based sanctions and vigilance, are not covered by FATF Recommendations. FATF has published a number of other papers on proliferation financing and guidance regarding their implementation.[62,63] The latter in particular will also need to be updated following Implementation Day.

Conclusion

The framework of UN controls on financing of proliferation has been loosened following Implementation Day. UN sanctions on Iran, including financial sanctions, are substituted by specific restrictions of varying timescales culminating, after ten years, with lifting of sanctions[64]. The financial requirements of UN sanctions on DPRK, recently extended, and resolution 1540 (2004) must continue to be implemented. It remains as important as ever that states have in place effective measures to identify and disrupt financing of proliferation.

The mechanisms and procedures put in place by states to implement Iran and DPRK sanctions can be used to implement resolution 1540 (2004), at least in part. States need to ensure that such mechanisms and procedures are not allowed to wither following Implementation Day. It is too early to say whether this is happening, but the relevant UN structures, and FATF, need to be vigilant for any signs that it is. FATF will in particular need to consider how to incorporate asset freezing elements of resolution 2231 (2015) into Recommendation 7. FATF assessments of how well FATF countries are implementing financial measures under this resolution will contribute to ensuring that the UN framework of controls on financing of proliferation is maintained effectively.

Acknowledgements

This paper benefitted significantly from comments by Raphael Prenat, financial expert of the Group of Experts supporting the 1540 Committee, and by referees' comments.

[62] FATF, "FATF Report on Typologies of Proliferation Financing," 2008, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html>; FATF, "Combatting Proliferation Financing: A Status Report on Policy Development and Consultation," February 2010, < http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf>.

[63] FATF, "The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction," 2013, < http://www.fatf-gafi.org/documents/documents/unscr-proliferation-wmd.html>.

[64] "….provided that the provisions of previous resolutions have not been reinstated.", paragraph 23 of the JCPOA, Annex A (the JCPOA) of UN Security Council Resolution 2231, S/Res/2231, 2015.

ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns

MARK BROMLEY, KEES JAN STEENHOEK, SIMONE HALINK AND EVELIEN WIJKSTRA[1]

Abstract

In recent years, sections of the European Union (EU), EU Member States, non-government organizations (NGOs) and Members of European Parliament (MEPs) have sought to use dual-use export controls to restrict exports of Information Communication Technology (ICT) surveillance systems. This process was driven by revelations in 2011 about the role of EU-based companies in the supply of security, surveillance and censorship technologies and services to states in the Middle East and North Africa and their use in violations of human rights. In response, the Wassenaar Arrangement and the EU have expanded controls on exports of dual-use goods to capture certain ICT surveillance systems and is discussing the adoption of additional measures as part of the ongoing review of the Dual-Use Regulation. This has included discussion about the application of export licensing criteria based on 'human security' considerations in order to better capture the range of concerns raised by the export of these technologies. This article explores the motivations behind these actions, the impact they have had to date, and the ongoing discussion about the adoption of additional measures. It concludes by arguing in favour of a holistic approach which combines export controls with other areas of trade policy, particularly improved standards in corporate social responsibility (CSR). This approach carries the greatest chance for success in restricting the supply of ICT-surveillance systems in situations where they are likely to be used in human rights violations.

Keywords

ICT surveillance systems, human rights, export controls, corporate social responsibility, holistic approach.

Introduction

In recent years, many cases showed that repressive regimes used Information Communication Technology (ICT) surveillance systems to identify and intimidate dissidents and in the commission of other violations of

[1] Mark Bromley is Co-Director of the Dual-Use and Arms Trade Control Programme at the Stockholm International Peace Research Institute (SIPRI) and PhD candidate at the Department of Economic History, Stockholm University; Kees Jan Steenhoek acted as head of the dual-use export control division until July 2015 and is currently deputy head of the nonproliferation and disarmament division, both at the Netherlands Ministry of Foreign Affairs; Simone Halink is Deputy Head of International Cyber Policies at the Netherlands Ministry of Foreign Affairs; Evelien Wijkstra is senior policy officer at the Taskforce International Cyber Policies at the Netherlands Ministry of Foreign Affairs.

international human rights law.[2] These systems have greatly enhanced the surveillance capacities of these regimes allowing them to target people in ways and on a scale not previously possible. Instead of citizens having technology on their side, advanced digital technology has been turned into a tool for surveillance.[3]

Subsequent investigations by NGOs and media organisations have shown that many of the ICT surveillance systems used by these regimes were supplied by companies based in Europe and North America. Prior to 2011, certain ICT surveillance systems were covered by dual-use export controls due to the level of encryption they employed.[4] However, in many instances, existing export controls did not apply. This led to calls from NGOs and Parliamentarians for export controls to be expanded in order to apply greater restrictions on the supply of ICT surveillance systems.

The most coordinated campaign in this regard is the Coalition Against Unlawful Surveillance Exports (CAUSE) which was set up by several leading NGOs.[5] CAUSE called for an effective export control policy to prevent human rights violations by developing regulations requiring export control authorities to take into account human rights implications when making licensing decisions. Other measures promoted by CAUSE include subjecting all relevant ICT surveillance systems to licensing, addressing disparities between national policies, and for security researchers, industry and civil society to be involved in policy processes regarding this issue.[6] In addition, civil society actors have advocated for more transparency from governments about licenses granted and denied in order to develop a clearer overview of relevant actors involved.

In 2012 and 2013, some of these export control gaps were closed through the addition of new categories in the Wassenaar Arrangement's dual-use control list. In particular, 'mobile telecommunications interception or jamming equipment', 'Internet Protocol (IP) network surveillance systems' and 'intrusion software' were added to the Wassenaar Arrangement's dual-use control list.[7] However, NGOs, Parliamentarians and national governments have argued that gaps continue to exist and that a wide range of ICT surveillance systems remain outside the scope of export controls.[8] They have also argued that the issue is not only about

---

[2] E.g. an Iranian women's rights activist turned to using pay phones when she found out that all her communications were under watch. On her way to meetings with other activists she would be called by police who would tell her they knew where she was headed. Interrogators at Tehran's notorious Evin Prison asked Shojaee about her acquaintances and displayed call records and transcripts going back several months. Ben Elginvand, Vernon Silver, and Alan Katz, "Iranian Police Seizing Dissidents Get Aid Of Western Companies," *Bloomberg Business*, October 31, 2011, <http://www.bloomberg.com/news/articles/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies>. For another example from Libya, see FIDH, "Surveillance Technologies Made in Europe: Regulation Needed to Prevent Human Rights Abuses," Position Paper Presented through FIDH Website, December 2014, <http://fr.scribd.com/doc/251396002/Surveillance-Technologies-Made-in-Europe> .

[3] James Bamford, "The Espionage Economy," *Foreign Policy* (Jan/Feb 2016), pp. 70-72.

[4] The range of activities that states seek to control through national licensing procedures has been expanded beyond exports to include brokering, transit, trans-shipment. Following existing practice within the EU and among EU member states, the terms 'export control' is used here in the broader sense as refering to controls on exports and these other related activities.

[5] CAUSE is made up of the following NGOs: Amnesty International, Digitale Gesellschaft, FIDH, Human Rights Watch, Open Technology Institute, Privacy International, Reporters Without Borders and Access, <http://www.globalcause.net/>.

[6] Coalition Against Unlawful Surveillance (CAUSE), "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

[7] Sibylle Bauer et al., "Dual-use and Arms Trade Controls," *SIPRI Yearbook* (Oxford: Oxford University Press, 2013); and Sibylle Bauer et al., "Dual-use and Arms Trade Controls," *SIPRI Yearbook* (Oxford: Oxford University Press, 2014). The Wassenaar Arrangement seeks to prevent 'destabilizing accumulations' by states of conventional arms and related dual-use goods and technologies and to prevent the acquisition of such items by terrorist groups, organizations and individuals. See <www.wassenaar.org/>.

[8] See Coalition Against Unlawful Surveillance (CAUSE), "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>, European Parliament, "Resolution on 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," September 8, 2015, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0288+0+DOC+XML+V0//EN>, and Catherine Strupp, "Germany Leaves Brussels Behind on

the items that are subject to control, but also the mechanisms through which controls are exercised. In particular, they have argued that states need to develop better criteria for assessing licences for the export of ICT surveillance systems.[9]

Discussions about additional control list categories have taken place within the Wassenaar Arrangement and the EU. However, discussions about the development of improved criteria for assessing export licences have exclusively taken place at the EU-level. Since 2011, the EU has made a number of commitments to restrict exports of ICT surveillance systems that might be used in human rights violations.[10] A range of different policy options have been discussed, including developing improved guidelines for supplier companies and providing dissidents with technologies that would enable them to evade detection. However, most of the concrete steps and substantive discussions have focused on the use of export controls.

In 2011 and 2012, the EU added a broad range of ICT surveillance to its sanctions on Iran and Syria. The main focus of debate since has been about how the EU Dual-Use Regulation can be used as a means of further expanding controls on transfers of ICT surveillance systems. The EU Dual-Use Regulation is currently undergoing a review and the issue of expanding controls on ICT surveillance systems has become a central part of the process.[11] In November 2014 Cecilia Malmström, the EU Commissioner for Trade, stated that 'the export of surveillance technologies is an element—and a very important element—of our export control policy review.'[12]

As part of the review process, the Commission is examining the possibility of controlling ICT surveillance systems that are not included in the Wassenaar Arrangement's controls list. The EU maintains its own list of dual-use goods and in the 2014 update, Wassenaar Arrangement control list categories in the field of ICT surveillance systems were added. As of now, the EU list is drawn exclusively from the Wassenaar Arrangement and other multilateral control regimes. The EU is also discussing the development of new criteria for assessing exports of ICT surveillance technologies, including the possible application of concepts from the human security field.

A number of commentators have argued that the application of export controls to the field of ICT surveillance systems is at best insufficient and at worst counter-productive. In particular, they have argued that the expansion of controls in this area risks creating unnecessary regulatory burden for the ICT sector, particularly for companies and individuals working in the field of IT security.[13] Others have argued that more work needs to be devoted to exploring other mechanisms besides export controls through which the supply of ICT surveillance systems can be regulated. This includes the application of other tools in the field of trade controls, particularly the development and implementation of improved standards in Corporate Social Responsibility (CSR).[14]

Surveillance Tech Export Controls," Euractiv.Com, July 10, 2015, <http://www.euractiv.com/section/digital/news/germany-leaves-brussels-behind-on-surveillance-tech-export-controls/>.

[9] Ibid.

[10] Council of the European Union, "EU Strategic Framework and Action Plan on Human Rights and Democracy," June 25, 2012, <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf> and Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline," May 12, 2014, < http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf>.

[11] "Joint statement by the European Parliament, the Council and the Commission on the Review of the Dual-use Export Control System," April 16, 2014, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.173.01.0079.01.ENG&toc=OJ:L:2014:173:TOC>.

[12] Malmström, Cecilia, EU Commissioner for Trade, "Debate at European Parliament in Strasbourg," November 24, 2014, <http://www. europarl.europa.eu/sides/getDoc.do?pubRef=-//ep//text+cre+20141124+item-018+doc+xml+v0//en>.

[13] Joe Uchill, "Industry Warns Proposed Arms Export Rule Will Thwart Basic Cyberdefenses," *Christian Science Monito*r, June 26, 2015, <http://www.csmonitor.com/World/Passcode/2015/0626/Industry-warns-proposed-arms-export-rule-will-thwart-basic-cyberdefenses>; and Dennis Fisher, "Coalition of Security Companies Forms to Oppose Wassenaar Rules," *Threat Post*, n.d., <https://threatpost.com/coalition-of-security-companies-forms-to-oppose-wassenaar-rules/113794>.

[14] See Centre for Internet and Human Rights (CIHR), "Export Controls of Surveillance Technologies," 2015, <https://www.

During the Global Conference on CyberSpace (GCCS 2015) on the 16th and 17th of April 2015 in The Hague, one session brought together experts in the field of ICT surveillance systems from the European Parliament, the European Commission, NGO's, the OECD and national governments.[15] The panellists compared notes on latest policy developments and agreed that unlawful interception and subsequent human rights infringements are 'a problem worth solving'. They highlighted several options for improvement of export control policy from different angles, ranging from the provision of more transparency by States about licenses granted and denied, to creating more awareness about the issue and the need for smart regulation. The panel concluded that a flexible, effective and comprehensive solution could be found through a balanced approach, which might include a list-based regime, end-user controls and vendor due diligence (as required, for example, by the OECD Guidelines for Multinational Enterprises and the UN Guiding Principles on Business and Human Rights).[16]

This article presents an overview of recent debates about the use of both export controls and CSR standards in order to exert greater control over exports of ICT surveillance systems Section II presents an overview of the range of ICT surveillance systems that have been the subject of debate because of their use in alleged human rights violations and highlights the factors that speak for and against the application of export controls as a means of exerting control on their use. Sections III and IV discuss the way in which existing export controls apply to these systems, how these powers have expanded in recent years, and debates about widening them further, looking at developments at both the Wassenaar Arrangement and EU level. In particular, Section III focuses on debates about expansions in the range of ICT surveillance systems that should be subject to control while Section IV focuses on debates about the criteria states should use when assessing licences for their export. Section V highlights the important role that other tools in field of trade controls can play in controlling transfers of ICT surveillance systems, particularly improved standards in CSR. It lays out the range of existing CSR mechanisms that already exist and the gaps and challenges that remain. Section VI presents conclusions, arguing that export controls and improved standards in CSR are both necessary elements of an effective policy response to the challenges posed by the export and use of ICT surveillance systems.

ICT Surveillance Systems: Different Risks, Different Challenges

The debate about controls on exports of ICT surveillance systems encompasses a wide range of systems and technologies. Its boundaries and sub-categories are often unclear and subject to different views and interpretations. In particular, it is difficult to clearly mark the technological boundaries of the various technologies. Not only because it is a rapidly developing field, but also because it's not always possible to define when the items are "used" and when they are "abused".

This article defines 'ICT surveillance systems' as systems that enable the monitoring and exploitation of data or content that is stored, processed or transferred via ICTs, including computers, mobiles phones and telecommunications networks. It pays particular attention to systems that were subject to export controls prior to 2011, that have since become subject to export controls, or have been the subject of debate in this area. This includes, but is not limited to: mobile telecommunications interception equipment; intrusion software; IP network surveillance systems; monitoring centres; lawful interception (LI) systems; data retention systems; digital forensics; probes; and deep packet inspection (DPI) (see box 1).

---

gccs2015.com/sites/default/files/documents/Export%20Controls%20of%20Surveillance%20Technologies_DEF_BW.pdf>.

[15] Global Conference on Cyberspace 2015 programme (link also directs to a video registration of the panel discussion and a background document): <https://www.gccs2015.com/programme?programme=2>.

[16] Global Conference on Cyberspace 2015, "Chair's Statement," April 2015, <https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf>.

Box 1 – Different Types of ICT Surveillance Systems

Mobile telecommunications interception equipment – Also known as 'IMSI Catchers,' mobile telecommunications interception equipment are used to remotely track, identify, intercept and record mobiles phones.

Intrusion software – A type of malware that can be inserted on computers and mobile phones without detection and used to remotely monitor and in certain cases control them.[17]

IP Network Surveillance - Used to intercept, collect and, some cases analyse data as it passes through an Internet Protocol (IP) network.

Monitoring centres – Monitoring centres are used by law enforcement and intelligence agencies to collect, store and analyse difference forms of communications data from various surveillance sources.[18]

Lawful Interception (LI) systems – Used by network operators to enable them to comply with requests from law enforcement or intelligence agencies for the provision of their users' communications data.[19]

Data retention systems - Used by network operators to comply with legal requirement for 'meta data' storage of their users for potential later use by law enforcement or intelligence agencies.

Digital forensics – Enable law enforcement or intelligence agencies to retrieve and analyse data stored on networks, computers and mobile devices.[20]

Probes – Used to collect data as it passes through a communications network.[21] They are used in several ICT surveillance systems but also have a range of non-surveillance applications.

Deep Packet Inspection (DPI) – Used to examine the content of data as it passes through a communications network.[22] They are used in several ICT surveillance systems but also have a range of non-surveillance applications.

A 'network operator' is a company that manages a communications network, such as Vodafone or TeliaSonera. 'Communications data' can be: (a) 'meta data,' meaning information about the use of a network or the calls that a subscriber has made; (b) 'content data,' meaning what is said in a phone call or the content of a text

[17] "The Little Black Book of Electronic Surveillance: 2015," *Insider Surveillance*, January 30, 2015, < https://insidersurveillance.com/the-little-black-book-of-electronic-surveillance-2015/>.

[18] Edin Omanovic and Matthew Rice, "Monitoring Centers: Force Multiplier From the Surveillance Industry," Privacy International, April 29, 2014, <https://www.privacyinternational.org/?q=node/439>.

[19] See Frost and Sullivan, "Lawful Interception: A Mounting Challenge for Service Providers and Governments," 2011, < https://www.wikileaks.org/spyfiles/docs/FROSTSULLIVAN-LawfInteA-en.pdf>; and Vodaphone, "Law Enforcement Disclosure Report," February 2015, <http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html>.

[20] UK Government, "Assessing Cyber Security Export Risks," TeckUK, 2014, p. 15, <https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf>.

[21] Passive probes collect data indiscriminately as it moves through the communications network. Actives probes collect data from specific individuals using their identifiers (e.g. IP address) or based on specific signatures (e.g. specific semantic content). See "Catalyst 6500 Series Switches Lawful Intercept Configuration Guide," CISCO, August 2007, <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/lawful/intercept/book.pdf>.

[22] Duncan Geere, "How Deep Packet Inspection Works," *Wired*, April 27, 2012, <http://www.wired.co.uk/news/archive/2012-04/27/how-deep-packet-inspection-works>.

message; or (c) 'location data,' meaning information about the movements of a subscriber to a mobile phone network.

ICT surveillance systems differ significantly in many ways. These differences include the type, size and location of the companies engaged in their production. Some of the producers are large defence contractors such as Thales and BAE Systems that produce a range of ICT surveillance systems for law enforcement and intelligence agencies as part of a broad portfolio of defence and security products and solutions. Others are large ICT companies, particularly Nokia and Ericsson, that produce telecommunications networks and are legally required to have LI systems 'built in' to their products or to enable their inclusion.

Other companies are smaller ICT firms such as Gamma International and Hacking Team that specialize exclusively in the production of certain types of surveillance technologies, such as IMSI catchers or intrusion software.

There are also differences with regards to the types of human rights abuses that have been connected to the use of different ICT surveillance systems and the nature of that connection. In certain cases, the connection is fairly direct. For example, by analysing the content of malware found on the target's computer, Citizen Lab have shown how Hacking Team intrusion software has been used by the UAE authorities to monitor the communications of a human rights activist.[23] Moreover, documents found in the Libyan intelligence files following the overthrow of Colonel Gadaffi show that, prior to 2012, the Libyan authorities used Amesys' Eagle IP Network Surveillance system to monitor phone and email conversations of government opponents on a 'massive scale.'[24]

In other cases, a clear connection between a particular ICT surveillance system and abuses of human rights is less clear or harder to establish. For example, digital forensics systems can potentially be used by law enforcement agencies to recover personal data from individuals who are under investigation for political reasons.[25] However, there are no clearly documented cases where this has happened. Meanwhile, certain ICT surveillance systems raise both human rights and security concerns. For example, IMSI catchers and intrusion software can be used in the theft of commercial and government secrets.[26]

Certain aspects of the production and supply of ICT surveillance systems make them a suitable target for export controls. For instance, ICT surveillance systems, particularly intrusion software, require regular software updates in order to remain undetected and to function effectively, meaning that they can be effectively 'switched off' by the supplier.[27] Moreover, existing regulations mean that many ICT surveillance systems are sold exclusively to national governments, making it possible to target end-user based controls effectively.[28]

At the same time, there is a significant level of internationalization in the industry, which creates challenges for nationally implemented, list-based export control systems. Many of the companies involved maintain

---

[23] Citizen Lab, "Backdoors are Forever: Hacking Team and the Targeting of Dissent?," October 10, 2012, <https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/>.

[24] Mattieu Aikins, "Jamming Tripoli, Inside Moammar Gadhafi's Secret Surveillance Network," *Wired*, May 18 2012, <http://www.wired.com/2012/05/ff_libya/all/>.

[25] Ibid.

[26] Jeff, Stein, "New Eavesdropping Equipment Sucks All Data Off Your Phone," *Newsweek*, June 22, 2014, <http://www.newsweek.com/2014/07/04/your-phone-just-got-sucked-255790.html> and James Clapper, Director of National Intelligence, "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence," US Government, March 23, 2013.

[27] Kenneth Page, "Six Things We Know from the Latest FinFisher Documents," Privacy International, August 15, 2014, <https://www.privacyinternational.org/?q=node/371>.

[28] Privacy International, "Privacy International BIS Submission," [N/D], <https://www.privacyinternational.org/sites/default/files/Privacy%20International%20BIS%20submission.pdf>.

offices in different countries, including ones that are inside and outside of the Wassenaar Arrangement, and can move production from one country to the other.[29] In addition, many of the technologies involved have legitimate non-surveillance applications, meaning that there is significant potential for creating unintended consequences for other parts of the ICT sector. Probes and DPI systems have a wide range of non-surveillance applications, including in quality of service, network diagnostics and IT security.[30]

There is also significant overlap between the techniques used in certain areas of ICT surveillance and IT security, which risks unintended consequences when crafting list-based control systems. For example, there are concerns that the attempts to place controls on intrusion software have inadvertently captured, and will have a chilling effect upon, the processes of 'responsible disclosure' through which software vulnerabilities are identified and reported. Finally, many of the ICT surveillance systems states use are composites of several different sub-systems provided by different suppliers.[31] Concerns have been raised that the controls created on IP surveillance systems could be effectively bypassed by sourcing different elements of the system from different vendors and assembling it in the recipient country.[32]

Export Controls: Expansions in Coverage

To date, debate on how to restrict transfers of ICT surveillance systems through the application of export controls has centered on two sets of issues. First, there has been a debate about which systems and technologies should be made subject to controls. This debate has taken place at the Wassenaar Arrangement and the EU levels and within different national capitals in Europe and North America. It has focused on where and how controls should be implemented and the best way to avoid generating unintended consequences for the IT security sector and the telecommunications industry. Second, there has been a debate about what standards national export licensing authorities should use when assessing licences for the export of ICT surveillance systems. This debate has largely been confined to the EU level and has focused on the application of existing human rights standards and the potential development of new standards based around notions of 'human security.' Both debates are ongoing and in some cases expand to involve other issue areas.

Certain ICT surveillance systems were already covered by export controls prior to 2011. For example, exports of IMSI Catchers were controlled by certain states on the grounds that they were covered by '5A001 - Telecommunications systems, equipment, components' or '5D002 - Software', while exports of certain types of intrusion software and digital forensics were covered by '5A002 - Cryptography'.[33] However, these controls were largely indirect in nature and not intentionally targeted on ICT surveillance systems. In late 2011 and early 2012, the EU arms embargoes on Iran and Syria were updated to include prohibitions on the sale of ICT surveillance systems.[34] The language used in both cases was broad in scope, covering any

---

[29] Henry Habegger, "Bund Verscheucht Hersteller von Spionagesoftware Aus Der Schweiz [Bund Chases manufacturer of spy software from Switzerland]," *Schweiz Am Sonntag*, August 1, 2015, <http://www.schweizamsonntag.ch/ressort/politik/bund_verscheucht_hersteller_von_spionagesoftware_aus_der_schweiz/>.

[30] Hewlett Packard manufactures several types of probes and DPI systems that can be used for both surveillance and non-surveillance purposes. "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," Coalition Against Unlawful Surveillance (CAUSE), June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

[31] Collin, Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies," *Access*, March 13, 2015, <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

[32] Adam Weber, et al, "IP Network Communications Surveillance Systems: Deciphering Wassenaar Arrangement Controls," *World ECR*, April 2015.

[33] Privacy International, "British Government Admits it has Already Started Controlling Exports of Gamma International's FinSpy," September 9, 2012, <https://www.privacyinternational.org/news/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma>.

[34] Council of the European Union, "Council Decision 2011/782/CFSP of 1 December 2011 Concerning Restrictive Measures against Syria and Repealing Decision 2011/273/CFSP," Official Journal of the European Union, December 2, 2011; Council of the European Union, "Council Decision 2012/168/CFSP of 23 March 2012 Amending Decision 2011/235/CFSP Concerning

'equipment or software intended primarily for use in the monitoring or interception […] of the Internet and of telephone communications on mobile or fixed networks,' as well as associated services.[35] The sanctions cover the export of a wide range of ICT surveillance systems but have also had implications for the supply of telecommunications networks and services from EU-based companies. Since their implementation, Ericsson and Nokia have reduced sales of communications networks to Iran.[36]

In 2012 and 2013 certain types of 'mobile telecommunications interception or jamming equipment,' 'IP network surveillance systems' and 'intrusion software' were added to the Wassenaar Arrangement's dual-use control list. In all cases, these additions were justified, at least in part, on the national security concerns associated with their use. For example, the controls on intrusion software were justified on the grounds that they 'may be detrimental to international and regional security and stability.'[37] In December 2014, these items were added to the EU's Dual-Use control list. In 2015, Germany imposed national controls on the export of certain types of data retention systems and monitoring centres and is seeking to promote their adoption at the EU and Wassenaar Arrangement.[38]

Since 2014, an ongoing discussion has taken place within both the EU and the Wassenaar Arrangement about if and how additional ICT surveillance systems should be made subject to dual-use export controls. In particular, a number of Members of European Parliament (MEPs) and NGOs have called for existing controls to be expanded and additional ICT surveillance systems to be included.[39] One EU-level option under discussion is the adoption of a dedicated 'catch-all' control for exports of unlisted ICT surveillance systems that might play a role in human rights abuses. The proposal for such a control was made by the European Parliament in October 2012 but was not adopted.[40] At the time, the Council Working Group on Dual-use Goods - the EU level body where EU Member States discuss the legal and political aspects of Dual-use export controls through the Dual-use Regulation - was of the opinion that the new procedures for amending the control lists should be implemented as quickly as possible. Some delegations were concerned that a policy debate on substantive matters would postpone European implementation of the changes to the control lists agreed in the export control regimes in 2010 and 2011.[41]

Making further expansions in the range of ICT surveillance systems that are subject to control is likely to involve focusing on systems that are mainly of interest because of their human rights concerns, given that most of the systems that have been made subject to control on national security grounds are already covered. This is likely to be more achievable at the EU rather than at the Wassenaar Arrangement level.

Restrictive Measures Directed against Certain Persons and Entities in View of the Situation in Iran," Official Journal of the European Union, March 25, 2012, p. 85.

[35] Ibid.

[36] Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," *Reuters*, March 22, 2012, <http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322>.

[37] Wassenaar Arrangement, "Public Statement 2013. Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," December 4, 2013, <http://www.wassenaar.org/publicdocuments/index_PS_PS.html/>.

[38] BMWI, "Anlage AL zur Außenwirtschaftverordnung [Annex AL to the German Foreign Trade Regulations]," July 2015, <http://www.bmwi.de/BMWi/Redaktion/PDF/A/anlage-al-zur-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>.

[39] Coalition Against Unlawful Surveillance (CAUSE), "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

[40] European Parliament, «Legislative Resolution on the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) no. 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, (COM(2011)0704 – C7-0395/2011 – 2011/0310(COD)), October 23, 2012.

[41] Tweede Kamer, vergaderjaar 2012–2013, 33 400 V, nr. 152 [Proceedings of Dutch Parliament, 33 400 V: approval of the budget of the Ministry of Foreign Affairs (V) and the budget for Foreign Trade and Development Cooperation for the year 2013, no. 152: letter from the Minister for Foreign Trade and Development Cooperation.], <https://zoek.officielebekendmakingen.nl/kst-33400-V-152.html>.

Adding technologies to the Wassenaar Arrangement list on purely human rights grounds would likely be opposed by other participating states, and all list additions have to be made by consensus. However, adopting EU-level controls on items that are not included in the control lists of the various multilateral export controls regimes is something that industry and EU member states seek to avoid. This is due both to the impact it might have on the competitiveness of EU-based companies and the confusion it may generate for non-EU states who value the EU dual-use control list as a synthesis of the multilateral regime's control lists and implement it nationally.

The expansion of controls on ICT surveillance systems has generated concerns about unintended side-effects. This has been particularly apparent in relation to the controls on 'intrusion software' adopted by the Wassenaar Arrangement in 2013.[42] Specifically, significant concerns have been raised about the impact of the controls on intrusion software on 'vulnerability coordination' or 'vulnerability disclosure', the process by which individuals or organizations make ICT companies aware of software vulnerabilities and exploits. A number of papers have argued that the control list language effectively describes a software exploit and thereby makes the process of identifying and reporting them subject to control.[43] A number of articles have argued that the controls, if properly applied, should not have an effect in these areas.[44] Guidance language released by the UK government , who originally proposed the control language at the Wassenaar Arrangement, has also sought to make this point.[45]

However, concerns have persisted, fed largely by the US Bureau of Industry and Security (BIS) language on its proposed national implementation of the intrusion software controls, published in May 2015.[46] The language included a number of phrases that alarmed academics and individuals working in IT security, implying, in particular, that vulnerability disclosures would be covered by the controls.[47] The debate in the United States has since grown particularly heated. A coalition of IT security companies and researchers have successfully delayed the US adoption of the intrusion software controls and sought to press the US government to propose revisions to the control list language at the Wassenaar Arrangement.[48]

Regardless of whether the concerns raised in relation to the intrusion software controls are justified, they highlight the need for clarity when drafting control list language and the potential risks when export controls are expanded into a new areas and engage with communities that do not have experience of being subject to their coverage.

Export Controls: New Criteria and the EU Dual-Use Regulation

Much of the debate about how to assess licences for the export of ICT surveillance systems has been confined to the EU. Under the EU Dual-Use regulation, member states already have an obligation to take

---

[42] Uchill, Joe, "Industry Warns Proposed Arms Export Rule Will Thwart Basic Cyberdefenses," *Christian Science Monitor*, June 26, 2015, <http://www.csmonitor.com/World/Passcode/2015/0626/Industry-warns-proposed-arms-export-rule-will-thwart-basic-cyberdefenses>.

[43] Sergey Bratus, D.J. Capelis, Michael Locasto, and Anna Shubina, "Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It," October 9, 2014, <http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf>.

[44] See Collin Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies," *Access*, March 13, 2015, <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

[45] UK Department for Business Innovation & Skills, "Intrusion Software Tools and Export Control," August 10, 2015, <http://blogs.bis.gov.uk/exportcontrol/uncategorized/eco-issues-guidance-on-intrusion-software-controls/>.

[46] Uchill, Joe, "Industry Warns Proposed Arms Export Rule Will Thwart Basic Cyberdefenses," *Christian Science Monitor*, June 26, 2015, <http://www.csmonitor.com/World/Passcode/2015/0626/Industry-warns-proposed-arms-export-rule-will-thwart-basic-cyberdefenses> and Dennis Fisher, "Coalition of Security Companies Forms to Oppose Wassenaar Rules," *Threat Post*, n.d., <https://threatpost.com/coalition-of-security-companies-forms-to-oppose-wassenaar-rules/113794>.

[47] For example, see "Google, the Wassenaar Arrangement, and Vulnerability Research," Google Online Security Blog, July 20, 2015, <http://googleonlinesecurity.blogspot.se/2015/07/google-wassenaar-arrangement-and.html>.

[48] Kevin Carty, "Lawmakers Assail Cybersecurity Provisions in International Treaty," *Morning Consult*, January 12, 2016, <https://morningconsult.com/alert/lawmakers-assail-cybersecurity-provisions-in-international-treaty/>.

into account human rights considerations when considering exports of certain ICT surveillance systems.

For example, the EU general export authorisation (GEA) for telecommunications equipment (EU 005) allows the export of a range of dual-use items covered under category 5 of the control list to nine countries, including China, Russia and Turkey. This authorisation cannot be used if the exporter has been told by the licensing authority or is otherwise aware that the export will be used 'in connection with a violation of human rights, democratic principles or freedom of speech' through the use of 'interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of Internet use.'[49]

More broadly, Article 12 of the EU Dual-use Regulation requires member states to take into account 'all relevant considerations' when assessing export and brokering licences for dual-use goods, including those covered by Council Common Position 2008/944/CFSP defining common rules governing control of exports of military technology and equipment (EU Common Position).[50] The Council Common Position lays down eight criteria that EU Member States should apply when assessing license applications for the exports of conventional arms. Many of the human rights and security concerns associated with the export and use of ICT surveillance systems are addressed in the eight criteria of the EU Common Position and the accompanying User's Guide which provides guidance on how the Common Position should be implemented.[51]

In particular, criterion 2 of the Common Position requires member states to deny an export licence if there is a 'clear risk' that the goods 'might be used 'for internal repression' or 'in the commission of serious violations of international humanitarian law.'[52] The guidelines for criterion 2 in the User's Guide note that 'communications/surveillance equipment can have a strong role in facilitating repression.'[53] Meanwhile, criterion 5 requires member states to take into account the impact of the potential export on their own and other member states' defence and security interests.[54] A number of EU Member States have denied licences for the export of ICT surveillance systems on human rights grounds. For example, in 2009 it was reported that the UK denied a licence for the export of IMSI Catchers to a country in the Asia Pacific region because of the risk that the goods would be used to commit human rights abuses.[55]

However, other human rights concerns relating to the export and use of ICT surveillance systems are not referenced in the EU Common Position. For example, potential threats to the right to privacy and freedom of expression are not mentioned. Also not mentioned is the need for recipient states to have effective regulatory and oversight mechanisms that regulate the performance of investigative and surveillance duties and the powers of law enforcement and intelligence agencies and their use of ICT surveillance systems. There are also no references to the specific security threats associated with the use of ICT surveillance systems, such as the theft of government and commercial information and attacks on critical infrastructure.

---

[49] Regulation (EU) No. 1232/2011 of the European Parliament and of the Council of 16 November 2011 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, Official Journal of the European Union, 8 December 2011, pp. 37-38.

[50] Council of the European Union, "User's Guide to Council Common Position 2008/944/CFSP Defining Common Rules Governing the Control of Exports of Military Technology and Equipment," Brussels, April 29, 2009, <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209241%202009%20INIT>.

[51] Ibid.

[52] Council of the European Union, Council Common Position 2008/944/CFSP of 8 Dec. 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment, Official Journal of the European Union, L335.

[53] Council of the European Union, User's Guide to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment., Brussels, 20 July 2015, p. 38.

[54] Council of the European Union, Council Common Position 2008/944/CFSP of 8 Dec. 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment, Official Journal of the European Union, L335.

[55] Matthew Rice, "Collaborating Companies: Shady Moves in a Secretive Sector," Privacy International, May 27, 2015, <https://www.privacyinternational.org/node/587>.

The European Commission has raised the prospect of filling this gap by applying a 'human security approach' to exports of dual-use goods. This forms one of a range of potential policy proposals that the Commission is considering proposing in order to expand the application of export controls on ICT surveillance systems within the context of the ongoing review of the Dual-Use Regulation. The European Commission has announced that it will put forward proposed amendments to the Dual-Use Regulation in the first half of 2016. This legislative step is the last in a series that started with the publication of the Green Paper on dual-use exports in 2011.[56]

It is widely expected that the proposals will include measures aimed at preventing the misuse of European cyber systems for human rights infringements as various communications of the European Commission, the European Parliament and the Council have flagged the importance of addressing this issue. Upon amending the Dual-Use Regulation on 16 April 2014 to accelerate the procedure to update the list of dual-use items, the European Parliament, the Council and the Commission jointly acknowledged that the export of certain ICT systems can be used in connection with human rights violations and have the potential to undermine the EU's security. They also noted that options would be explored to address this issue in the context of the ongoing review of EU dual-use export control policy.

On 24 April 2014, the European Commission published a communication on the export control policy review. It laid out a range of 'concrete policy options' for the review with regards to export controls of ICT surveillance systems, such as adopting an EU-level control list, adopting an EU-level catch-all mechanism, making joint proposals for additions to the Wassenaar Arrangement control list, and developing new export assessment criteria. The communication also included potentially evolving towards a 'human security' approach to take into account broader security implications, including human rights violations.[57]

Under the Italian Presidency in the second half of 2014, the Council adopted conclusions that reconfirmed the April 2014 statement.[58] On 8 September 2015, the European Parliament adopted a non-binding resolution urging the Commission to put forward a proposal to regulate the export of dual-use technologies, addressing potentially harmful exports of ICT products and services to third countries.[59]

The next stage in the review of the Dual-Use Regulation will arrive in early 2016 when the Commission presents an impact assessment. This will be followed by a legislative proposal. As part of its preparation for the impact assessment, the Commission funded the production of a data collection project, conducted by SIPRI and ECORYS, to examine the current and potential economic, social and security costs and benefits of the Dual-Use Regulation. The study included a section focusing on the recent expansion of controls on ICT surveillance technologies and the potential for further action in this area.[60]

According to the European Commission, the adoption of a 'human security' approach would potentially involve 'a clarification of control criteria to take into consideration broader security implications, including

---

[56] European Commission, "Green Paper: The Dual-Use Export Control System of the European Union: Enduring Security and Competitiveness in a Changing World," COM(2011)393 final, June 30, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>.

[57] European Commission, "Communication for the Commission to the Council and the European Parliament: The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World," COM(2014)244 final, <http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf>.

[58] Council of the European Union, "Outcome of the Council Meeting, 21 November 2014, 15792/14," <http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/145922.pdf>.

[59] European Parliament, "Report on Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," 2014/2232(INI), <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2015-0178&language=EN>.

[60] SIPRI and Ecorys, "Data and Information Collection for EU Dual-use Export Control Policy Review," November 6, 2015, <http://www.egadd.org.uk/wp-content/uploads/sites/25/2015/12/FINAL-REPORT.pdf, pp. 219-221>.

the potential effect on the security of persons e.g. through terrorism or human rights violations.'[61] Industry associations and NGOs have both voiced concerns about its application to export licensing decision-making.[62] Unlike human rights and international humanitarian law (IHL), 'human security' has never been integrated into regional or international legal instruments and lacks any kind of universally agreed upon definition.[63]

While the discussion regarding the adoption of human security criteria for assessing exports of dual-use goods has taken place largely in response to the recent debate about exports of ICT surveillance systems, it can be assumed that any standards developed would be applicable to all exports of other controlled items as well. This has generated concerns about the potential unintended effects of such a move. In particular, an attempt to create a set of human security considerations for states to take into account when assessing dual-use exports may have implications for other areas of the 'dual-use industry' and generate calls for further additions in the range of items that are subject to control.

It will be up to European legislators and regulators to strike the balance between the commercial interests of European cyber companies and their commitments to address this issue and adopt effective measures.

CSR and the Potential Benefits of a More Holistic Approach

The development and implementation of improved standards in CSR has always been part of the EU's discussion about the range of policy responses to the challenges posed by the export of ICT surveillance technologies. In May 2012 the European Parliament adopted a non-legislative resolution calling on the European Commission to 'produce guidelines for EU companies to act in a manner consistent with the Union's fundamental principles in such situations.'[64] The Commission has requested information on stakeholders' views regarding the creation of standards on 'due diligence and self-regulation by industry' within the context of a possible adoption of a 'human security approach' under the review of the Dual-Use Regulation.[65]

However, this aspect of the potential policy response to exports of ICT surveillance systems has been largely set to one side in the discussion about the application of export controls. Indeed, in the heat of the European debate about whether or not to amend export control regulations to include restrictions for ICT surveillance systems, it is easy to forget that CSR is a trade policy objective that already seeks to deal with the issues at hand.

CSR is a policy objective that, like export control policy, aims at mitigating the risks of international trade in an increasingly globalised world economy. Where export controls are aimed at non-proliferation and security objectives, CSR focuses on the impact of business operations on people, the environment and society. In addition, the role of government in these policies differs; where export controls are mainly driven by internationally developed legal obligations (hard law), like authorization requirements and end-

[61] European Commission, "The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World," April 2014.

[62] "ASD Position Paper on the Review of the Dual-Use Export Control System of the European Union," ASD, 22 Oct. 2014; and "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," Coalition Against Unlawful Surveillance (CAUSE), June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

[63] Oscar A. Gomez and Des Gasper, "Human Security: A Thematic Guidance Note for Regional and National Human Development Report Teams," UNDP, n.d., <http://hdr.undp.org/sites/default/files/human_security_guidance_note_r-nhdrs.pdf.>.

[64] European Parliament, "Trade for Change: The EU Trade and Investment Strategy for the Southern Mediterranean following the Arab Spring Revolutions, 2011/2113(INI) Resolution, May 19, 2012, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0201+0+DOC+XML+V0//EN>.

[65] See European Commission, "Consultation on the Export Control Policy Review (Regulation (EC) No 428/2009)," July 2015, <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153629.pdf>.

user verification, CSR is a responsibility of enterprises and merely promoted by the government (soft law).

In 1976 the Organisation for Economic Co-operation and Development (OECD) first adopted the Guidelines for Multinational Enterprises. The Guidelines are recommendations by governments covering all major areas of business ethics, including corporate steps to obey the law, observe internationally-recognised standards and respond to other societal expectations.[66]

In 2011, the Guidelines were amended to include a chapter on human rights. This amendment anticipated the endorsement by the UN General Assembly of the UN Guiding Principles on Business and Human Rights that were proposed by UN Special Representative on business & human rights John Ruggie.[67,68] Both the UN Guiding Principles and the OECD Guidelines prescribe that enterprises should respect human rights, avoid causing or contributing to and seek ways to mitigate human rights infringements and provide remediation in case of 'causing' or 'contributing.' Although these instruments are non-binding in nature, non-observance of the guidelines can have serious consequences for enterprises. The OECD guidelines have a built-in grievance mechanism through National Contact Points (NCP). Adherent governments are required to set up an NCP, whose main role is to further the effectiveness of the Guidelines by undertaking promotional activities, handling enquiries, and contributing to the resolution of issues that arise from the alleged non-observance of the guidelines in specific instances (case law in a soft-law system).

In February 2013 a group of NGOs led by Privacy International submitted a complaint to the UK NCP against Gamma International. It alleged that the company had supplied an intrusion software product, Finfisher, to agencies of the Bahrain government that had used it to target pro-democracy activists. In December 2014, the UK NCP concluded that Gamma had not acted consistently with the provisions of the OECD Guidelines and made a number of recommendations, including that the company become more transparent and cooperate to remedy the misuse of its products.[69]

After the GCCS 2015, Professor Roel Nieuwenkamp, one of the panellists and chair of the OECD working group on responsible business conduct, commented on the developments in this area, including the UK NCP ruling.[70] He argued that although the NCP rulings represent "soft" law, their conclusions and recommendations might have "hard" consequences, as they may cause significant reputational damage to involved companies. Companies might lose government contracts, no longer receive export credit insurance or lose their governments' commercial diplomatic support. In addition, commercial investors might withdraw from companies that do not comply with OECD guidelines.

Implementing CSR in enterprises can be challenging, especially when it comes to understanding the impact of operations by suppliers or subcontractors. Luckily for exporters, there is guidance available with recommended measures companies can take to mitigate the risk that their products will be used to abuse human rights. These include the 'Guiding Principles on Business and Human Rights' produced by

---

[66] Organisation for Economic Co-operation and Development, "OECD Guidelines for Multinational Enterprises," May 25, 2011, <http://www.oecd.org/daf/inv/mne/48004323.pdf>.

[67] United Nations General Assembly, "Human Rights and Transnational Corporations and Other Business Enterprises," A/HRC/RES/17/4, July 6, 2011.

[68] UN Human Rights Council, "Guiding Principles on Business and Human Rights," June 2011, <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

[69] UK National Contact Point for the OECD Guidelines for Multinational Enterprises, "Privacy International & Gamma International UK Ltd: Final Statement after Examination of Complaint," December 2014, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf>.

[70] Roel Nieuwenkamp, "Responsible Business Conduct in Cyberspace," April 30, 2015, <https://friendsoftheoecdguidelines.wordpress.com/2015/05/05/responsible-business-conduct-in-cyberspace/>.

the UN; the 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights' produced by the European Commission; and the "Know Your Customer" Standards for Sales of Surveillance Equipment' produced by the Electronic Frontiers Foundation.[71,72,73] Several ICT companies have also developed their own due diligence policies. For example, Ericsson and Nokia have systems for vetting potential sales that include a range of potential human rights risks.[74]

In 2014, the UK industry association TechUK published a set of guidelines about the risks associated with the export and use of 'cyber security' systems that included detailed guidance on the particular concerns associated with ICT surveillance systems.[75] This guide identifies specific human rights, such as the right to privacy and freedom of expression that could be affected by these systems. It provides examples of non-intended consequences of technology exports illustrated with real life examples and highlights specific actions companies can take to address human rights risks. These actions include pre-sale and post-sale scrutiny to identify customers of concern as well as potential technical and contractual options to mitigate potential risks if the company wants to go ahead with a specific transaction.

Improved CSR standards can act as an effective complement to export controls by strengthening the human rights policy objective without introducing a large licensing burden for the companies involved. However, like export controls, industry self-regulation alone is unlikely to solve the challenges related to the export of ICT surveillance systems. As noted, a wide range of companies produce these systems. These companies are likely to differ significantly in terms of their willingness and ability to develop and implement effective self-regulation processes. In addition, unlike in other sectors such as nuclear, chemical or defence, no EU or national industry associations exist that represent all companies producing ICT surveillance technologies and which could act as a coordinator for the development self-regulation standards.[76]

Moreover, companies that have publicly stated that they have developed systems of self-regulation have been faulted for the way they have been applied in practice. Since 2013, Hacking Team has taken steps to develop and implement a system of self-regulation for assessing its exports of intrusion software. However, following the theft and release of Hacking Team's internal emails, the content of their ICP was criticised on the grounds that it did not appear to be preventing the company from doing business with governments with 'controversial human rights records.'[77]

Conclusions

Efforts to apply export controls to ICT surveillance systems highlight an expansion in the range of policy objectives that states and NGOs seek to pursue through the use of these tools. Traditionally, dual-use

---

[71] UN Human Rights Council, "Guiding Principles on Business and Human Rights," June 2011, <http://shiftproject.org/sites/default/files/GuidingPrinciplesBusinessHR_EN.pdf>.

[72] European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights," June 2013, <http://shiftproject.org/sites/default/files/ECHRSG.ICT_.pdf>.

[73] Cindy Cohn and Jillian York, "Know Your Customer' Standards for Sales of Surveillance Equipment," Electronic Frontier Foundation, October 24, 2011, <https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment>.

[74] Nokia, "Nokia Human Rights Policy," February 25, 2015, <http://company.nokia.com/sites/default/files/download/nokia_human_rights_policy_1.pdf>; and Ericsson, "ICT and Human Rights: An Eco-System Approach," 2013, <http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/2012/human_rights0521_final_web.pdf>.

[75] Cyber Growth Partnership Industry Guidance, "Assessing Cyber Security Export Risks," November 26, 2014, <http://www.ihrb.org/publications/reports/human-rights-guidance-for-cyber-security-companies.html>.

[76] Some companies are members of ICT-focussed associations (e.g. Digital Europe), IT-focussed associations (e.g. BitKom), and/or defence industry associations (e.g. ASD), while others are not members of any association.

[77] James Lee, "Hacking Team Leak Highlights the Need to Implement Human Rights Due Diligence," *Tech UK*, July 14, 2015, <https://www.techuk.org/insights/news/item/5123-hacking-team-leak>.

goods have been understood as goods and technologies that have both military and civilian applications.[78] Expanding controls to encompass ICT surveillance systems where the end-user may be a law enforcement or intelligence agency indicates an expansion of this notion. Meanwhile, states have sought to control exports that pose a threat to national or regional security or that may be used in violations of human rights or international humanitarian law. Adopting criteria based on notions of human security would represent an expansion in the range of concerns that states take into account when assessing export licences.

The subsequent debate about the implementation of these controls reflects the challenges facing export controls as they are applied to a sector that is rapidly evolving, international, and highly mobile. At least one of the companies that was the intended target for controls, Gamma Group, moved its work on FinFisher intrusion software to offices in countries that are outside of the Wassenaar Arrangement.[79] Moreover, questions have been raised about the ability of list-based control systems to keep pace in a field where new systems are developed on a regular basis. At the same time, there is concern that the adoption of catch-all controls will generate confusion for ICT companies about whether their systems and technologies are covered.[80]

That said, these issues are not unique to the field of ICT surveillance systems but confront many areas of export controls. Many of the goods and technologies subject to export controls are rapidly evolving and produced by mobile companies. Moreover, the vast majority of the companies that produce ICT surveillance systems have chosen to remain in place and make themselves subject to controls.

In most of the areas where it applies, export controls are never a silver bullet that can solve a particular challenge but rather present one of a range of different policy tools that can affect change. Export controls may not prevent questionable exports of ICT surveillance technologies from taking place. However, in states where information is published about the granting of export licences, they can help to shed light on the secretive trade in ICT surveillance systems and generate debate about the best way to respond effectively.[81] As this article argues, industry self-regulation and the application of CSR guidelines forms a useful complement to export controls in the effort to create improved standards in the export of ICT surveillance systems. Indeed, as European legislators and regulators continue their legislative process to amend the Dual-Use Regulation to include legal measures aimed at preventing human rights abuse through the use of ICT surveillance systems, they should bear in mind that multinational enterprises have the responsibility to respect human rights. Legal measures should be aimed at clarifyng these responsibilities. At the same time, widely accepted principles can be adopted into legislation to create a level playing field while creating and maintaining a high ethical standard.

One challenge facing the effective implementation of CSR guidelines and export controls is the lack of clear standards for how ICT surveillance systems should be effectively governed. Almost all of the ICT surveillance systems that have been the focus of debate in recent years – including IMSI Catchers and intrusion software - are also widely used by EU and other Western law enforcement and intelligence agencies.[82] However, there

---

[78] The term 'dual-use' is also used to refer to items that have nuclear and non-nuclear applications as well as items that have WMD and non-WMD applications. See Quentin Michel, "Dual-use Exports Require a Common Definition," Dual-use Technologies in the European Union - Prospects for the Future, Friends of Europe, 2015, < http://www.friendsofeurope.org/security-europe/dual-use-exports-require-common-definition/>.

[79] Edin Omanovic, "Surveillance Companies Ditch Switzerland, but Further Action Needed," March 5, 2014, <https://www.privacyinternational.org/?q=node/377>; and Henry Habegger, "Bund Verscheucht Hersteller von Spionagesoftware Aus Der Schweiz [Bund Chases manufacturer of spy software from Switzerland]," *Schweiz Am Sonntag*, August 1, 2015, <http://www.schweizamsonntag.ch/ressort/politik/bund_verscheucht_hersteller_von_spionagesoftware_aus_der_schweiz/>.

[80] SIPRI and Ecorys, "Data and Information Collection for EU Dual-use Export Control Policy Review," November 6, 2015, <http://www.egadd.org.uk/wp-content/uploads/sites/25/2015/12/FINAL-REPORT.pdf, pp. 219-221>.

[81] Griffin, Andre, "Government has been Allowing UK Firms to Sell Invasive Spying Equipment to Countries Including Saudi Arabia, Records Show," *The Independent*, January 27, 2016, <http://www.independent.co.uk/life-style/gadgets-and-tech/news/government-has-been-allowing-uk-firms-to-sell-invasive-spying-equipment-to-countries-including-saudi-a6836651.html>.

[82] Eric King and Matthew Rice, "Behind the Curve: When Will the UK Stop Pretending IMSI Catchers Don't Exist," Privacy

is nothing in the way of agreed standards either at the EU level or elsewhere for how these systems should be used or how this use should be effectively governed and controlled.

Standards have been developed for LI systems and data retention systems.[83] However, these are primarily technical standards that do not stipulate the mechanisms that should govern the use of these powers, the government agencies that should be able to utilize them, or the way they should be employed in practice. Moreover, nothing has been developed for other ICT surveillance systems, such as IMSI Catchers, intrusion software and monitoring centres. Several EU member states do have legislation in place that governs the use of these systems or are currently putting legislation in place.[84] However, this is the exception rather than the rule and the standards that do exist vary significantly. Moreover, these discussions have not yet 'moved upwards' to the EU level.

The measures discussed in this article can contribute to preventing cases where exported ICT surveillance systems are used in human rights violations. However, when taking steps in this area, legislators and regulators should be careful to not introduce measures that form a disproportionate burden for the companies involved. A holistic approach, which combines export controls with improved standards for industry self-regulation and the application of CSR principles, carries the greatest chance of success for promoting change. List-based trade controls allow for legal certainty and transparency, end-use controls allow for flexibility and adaptability and industry self-regulation, and CSR allows companies to take initiative and demonstrate responsibility to their shareholders and customers.

International, November 5, 2014, <https://www.privacyinternational.org/?q=node/454>.

[83] See "Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture," ETSI TR 101 943 V2.2.1, ETSI, November 2006, < http://www.etsi.org/deliver/etsi_tr/101900_101999/101943/02.01.01_60/tr_101943v020101p.pdf>.

[84] Eric King and Matthew Rice, "Behind the Curve: When Will the UK Stop Pretending IMSI Catchers Don't Exist," Privacy International, November 5, 2014, <https://www.privacyinternational.org/?q=node/454>.

Mass Surveillance Technology: Trading Trojan Horses?

LIA CAPONETTI[1]

Abstract

This paper challenges the effectiveness and necessity of "mass surveillance technology"(MST) on two dimensions: (a) states' internal use of MST and the subsequent issue of violation of fundamental freedoms, and (b) surveillance technology export control, especially to third countries likely to use such technology to violate human rights. Following the Snowden Datagate scandal, many States undertook inquiries and adopted measures that, in some cases, were meant to regulate the use of mass surveillance technology. The paper will: a) assess and evaluate current regulations on mass surveillance technology and its place in democratic societies, including what is at stake in terms of technology, threats, reactions to threats, and geographic extension, b) the risks linked to the use of MST on the national level by questioning the validity of counter-terrorism measures as a justification for MST use c) analyze international trade control regimes and legislation to highlighting their inadequacy in the face of the threats posed by MST, and d) map the evolution of the EU dual-use trade control system towards a human security approach with regard to human rights protection, in order to assess the capability of the system to avoid the misuse of MST.

Keywords

Mass surveillance technology, trade controls, cyber-security, human security, human rights, EU Dual-use Regulation

Introduction

> *Whether we like it or not, the international norms of tomorrow are being constructed today, right now, by the work of bodies like this Committee. If liberal States decide that the convenience of spies is more valuable than the rights of their citizens, the inevitable result will be States that are both less liberal and less safe.*

With these words, Edward Snowden concluded his testimony to the European Parliament (EP) as part of the EP's inquiry on Electronic Mass Surveillance of EU Citizens.[2,] Since Snowden's disclosures on

[1] Lia Caponetti is a junior researcher and assistant at the European Studies Unit (ESU) of the University of Liège (Belgium), where she has worked since October 2013.

[2] Edward Snowden is a former contractor for the CIA. He left the US in late May 2013 after leaking to the media details of extensive Internet and phone surveillance by American intelligence. Mr Snowden, who has been granted temporary asylum in Russia, faces espionage charges. The scandal broke in early June 2013, when The Guardian newspaper reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans. The paper published the secret court order directing telecommunications company Verizon to hand over all of its telephone data to the NSA on an "ongoing daily basis." That report was followed by revelations in both The Washington Post and The Guardian that the NSA tapped directly into the servers of nine internet firms including Facebook, Google, Microsoft and Yahoo to track online communication in a surveillance programme known as Prism. See "Edward Snowden: Leaks that Exposed US Spy Programme,"

controversial mass surveillance programmes by intelligence and national security agencies, MST has been in the spotlight of public debate and political inquiries.[3,4]

The EP was particularly active on this front, conducting a series of studies and inquiries. For instance, through the Committee on Civil Liberties, Justice and Home Affairs (LIBE) in collaboration with national Parliaments and the EU-US expert group, the EP published a report and a resolution on 21 February 2014 and 12 March 2014, respectively.[5,6,7] A study was also conducted via the Directorate General for Internal Policies entitled National Programs of Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law, examining mass surveillance practices in five EU countries: France, Germany, Sweden, Netherlands, and the United Kingdom. The study found that a network called "Five Eyes," dating back to 1946, gathered the intelligence services of five countries (US, UK, Canada, Australia and New Zealand) and cooperated on signals intelligence and other activities extended over time (Echelon and now Fornsat).[8] Finally, the report 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries' (2014/2232(INI)) was published, on 3 June 2015, by Member of European Parliament (MEP) Marietje Schaake.[9] The report was followed by the adoption of a resolution, published on 8 September 2015.[10]

Three international developments took place in this regard. The first was the publication by the UN Special Rapporteur of a report, 'Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism,' denouncing the situation regarding mass surveillance and the lack of effective judicial control.[11] The second was another report, adopted by the Council of Europe Committee on Legal Affairs and Human Rights of the Parliamentary Assembly, on mass surveillance adopted unanimously on 26 January 2015.[12] The third was the implementation of export controls related to some "Intrusion Software" and "IP Network Surveillance Systems" within the Wassenaar Arrangement (WA) and within the EU via the entry into force, on 22 October 2014, of the Commission Delegated Regulation (EU) No 1382/2014

BBC News, January 14, 2014.

[3] Edward Snowden, "Edward Snowden' Testimony," European Parliament, March 7, 2014, <http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>.

[4] UK intelligence and security Committee inquiry, the Dutch CTIVD inquiry, the Brazilian Senate investigation fóf NSA spying in Brazil, the European Parliament Civil Liberties Committee investigation on electronic surveillance, the Australian Senate inquiry into revision of the Telecommunications Act, the German Bundestag launch of the NSA Investigation Committee, the Council of Europe reports on whistleblowing and mass surveillance.

[5] The LIBE Committee was instructed to conduct the inquiry in European Parliament resolution of 4 July 2013, see European Parliament, "The US National Security Agency Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Privacy," 2013/2682(RSP), July 4, 2013, < http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//ENZ.

[6] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur Claude Moraes, "Draft Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs," 2013/2188(INI), February 21, 2014, < http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0%2F%2FEN>.

[7] European Parliament resolution of 12 March 2014 on "The US NSA surveillance programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs," 2013/2188(INI), July 4, 2013.

[8] For more information on surveillance, including Echelon/Fornsat, see European Parliament, "Interception Capabilities, " 2014, <http://www.europarl.europa.eu/document/activities/cont/201309/20130916ATT71388/20130916ATT71388EN.pdf.>.

[9] European Parliament, Committee on Foreign Affairs, Rapporteur Marietje Schaake, "Report on Human Rights and Technology: the Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," 2014/2232(INI), June 3, 2015.

[10] European Parliament resolution of 8 September 2015, "Human Rights and Technology: the Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," 2014/2232(INI), September 8, 2015.

[11] United Nations Office of the High Commissioner for Human Rights, Report on Promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, September 23, 2014.

[12] Parliamentary Assembly, "Report on Mass Surveillance," Doc. 13734, March 18, 2015.

updating Annex I.[13,14]

The so-called "Snowden Datagate" brought into the spotlight not only intelligence and national security agencies but also suppliers of the "spyware industry." Scandals involving European industries providing mass surveillance technology to authoritarian States drew attention to companies such as the Italian Hacking Team or the British-German Gamma Group, also know as FinFisher. The Italian company, for example, has been accused by MEP Schaake of exporting spy tools to repressive regimes such as Russia and Sudan and violating European sanctions, in some cases. The MEP also blamed the Italian competent authority for having issued a global authorisation to Hacking Team, allowing the company to export its products freely in all countries of the WA.[15]

As new threats emerge and technology continues rapid development, States' capacity to regulate cyberspace, as well as their security approach, is questioned vis-à-vis the growing violation of citizens' privacy and, in some States, of human rights. On the one hand, some trade control regimes try to keep pace and evolve to control technologies that could violate human rights, shifting their paradigm from a purely strategic to a more human security approach. On the other hand, the fight against terrorism seems to be, still, a sound reason to scratch ground to fundamental freedoms.

Through the analysis of official documents, reports and legislation on the topic, this paper will assess the situation on the control and use of mass surveillance technology the national and international level. The paper will argue that because of the risks related to the use of MST on states' domestic systems (such as the violation of the right to privacy) and the inadequacy of international trade controls regimes and legislation to prevent these risks, MST not only is ineffective in its declared security purpose, but it is also dangerous for the very foundations of democratic societies. The European Union dual-use trade control system will serve as an example to show incompatibilities between fundamental freedoms and MST. An analysis of the evolution of the EU system towards a "human security" approach when dealing with trade controls will show loopholes and limits of the system.

Targeted Surveillance vs. Mass Surveillance: National-Level Mass Surveillance Technology Risks

This section deals with the dangers posed by mass surveillance technology on the national level. To understand the dangers of this technology, it is first important to understand the difference between mass surveillance and targeted surveillance. While the latter is a valuable instrument for countering terrorism and preventing other delinquent acts, the former is a violation of fundamental freedoms, especially the right to privacy and to data protection. While targeted surveillance is subject to prior judicial authorisation and respects the criteria of proportionality and legal necessity, mass surveillance represents a permanent delegation to dodge the law.

The issue is being particularly debated at the UN and European level under the lead of the European Parliament. The UN report 'Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism' makes the distinction between targeted surveillance and mass surveillance, identifying the former as a valuable means to counter terrorism. In fact, targeted surveillance of suspected individuals and organizations allows intelligence and law enforcement agencies "to intercept and monitor

[13] It seems that the WA' s decision to implement export controls on some "Intrusion Software" and "IP Network Surveillance Systems" came after an open letter sent by a coalition of human rights organisations (led by the Coalition Against Unlawful Surveillance Exports - CAUSE) to the WA, in order to push the international regime to implement such controls.

[14] Wassenaar Arrangement, "Public Statement 2013 Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," Vienna, December 4, 2013, <www.wassenaar.org>.

[15] Marietje Schaake, "Hacking Team Company at Receiving End of Hacks," Marietje Schaake's Blog, posted on July 7, 2015, <www.marietjeschaake.eu>.

calls made on a landline or mobile telephone, enabling an individual's location to be determined, his or her movements to be tracked through cell site analysis and his or her text messages to be read and recorded. Targeted surveillance also enables (…) to monitor the online activity of particular individuals, to penetrate databases and cloud facilities, and to capture the information stored on them."[16]

The main feature of targeted surveillance is that it depends upon the existence of prior suspicion of the targeted individual/organisation. From a procedural and legal point of view, it also means that a prior authorisation for surveillance is required, whether judicial or executive, to assess the legality and proportionality of surveillance measures by reference to the facts of the specific case. In other words, targeted surveillance is a preventive security measure, applied by intelligence and enforcement agencies following a judicial or executive authorisation, which is issued on a case-by-case basis assessing the necessity and the proportionality of the measures to apply.

Several States secured bulk access to communications and content data without prior suspicion. As explained in the UN report:

> *Relevant authorities in these States are now able to apply automated "data mining" algorithms to dragnet a potentially limitless universe of communications traffic. By placing taps on fibre-optic cables through which the majority of digital communications travel, relevant States have thus been able to conduct mass surveillance of communications content and metadata, providing intelligence and law enforcement agencies with the opportunity to monitor and record not only their own citizens' communications, but also the communications of individuals located in other States.*[17]

The study on mass surveillance realised in December 2014 by the EP Research Service Science and Technology Options Assessment (STOA) also makes the distinction between "mass unwarranted and indiscriminate interception" and "targeted lawful interception of Internet and telephony data for the purpose of law enforcement and crime investigation."[18] While this latter is considered a necessary and legitimate instrument, the former is seen as a threat to civil liberties such as the right to freedom of opinion and expression.

The STOA study also explains the difference between communication data and meta-data and focuses on practices of interception and analysis of end-user meta-data. This latter is defined as data that is produced when electronic communication channels are used and provides information about the time, origin, destination, location, duration and frequency of the communications carried out. However, meta-data does not contain the content of communications.[19] This distinction is particularly important since while meta-data is considered personal data under UE legislation, it is not the case for all foreign legislation and notably, it is not the case for US legislation.

Both the UN report and the STOA study explain how telecommunications and Internet service providers cooperate, although not always in a "spontaneous" way, regarding the collection of data and meta-data for mass surveillance purposes. For example, the EP Working Document on the Follow-up of the LIBE Inquiry

---

[16] United Nations, "Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism," A/69/397, September 23, 2014, < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf>, pp. 3-4.

[17] Ibid, p. 4.

[18] European Parliament, European Parliamentary Research Service Science and Technology Options Assessment (STOA), "Mass Surveillance: What are the Risks for the Citizens and the Opportunities for the European Information Society? What are the Possible Mitigation Strategies?," Study IP/G/STOA/FWC-2013-1/LOT9/C5/SC1, December 2014.

[19] Another distinction, within meta-data, is between meta-data of the communication (e.g. sender, receiver, communication duration, communication channel, etc.) and meta-data on the content (e.g. read/write/modify, attributes of the file, author of the document, GPS location of a picture, etc.) and within communication meta-data, two further subcategories are Telephony meta-data and Internet meta-data (also-called Internet Protocol (IP) meta-data).

on Electronic Mass Surveillance of EU Citizens reports that three of the major phone networks in the UK including EE, Vodafone and Three, gave police mobile call records without requiring staff to initiate a review of all police information requests.[20] In addition, in the UK telecommunications company Cable and Wireless was bought by Vodafone in July 2012, provided UK GCHQ with access to Internet traffic.[21] The company was part of a programme called "Mastering the Internet" operated under the pseudonym "Gerontic."[22]

It is worthwhile noticing that States' capacity to collect citizens' data is reinforced by mandatory data retention laws that require telecommunications and Internet service providers to preserve communications data for inspection analysis. However, as reported by the STOA study, methodologies to obtain this kind of data from telecommunications and Internet service providers can also be less "orthodox" than on the basis of a lawful request. Threats of fines or "undeclared" capabilities to break system protections and to infiltrate systems and networks by applying advanced hard and software technology seem to be additional ways to access citizens' data. For example, in September 2013, Belgacom denounced to the criminal judicial authorities a hacking incident affecting the company. Press coverage and IT security company Symantec reported that Belgacom had been the victim of a complex malware called REGIN that allegedly originated in US or UK intelligence agencies.[23]

Going back to the criteria for lawful targeted surveillance, the UN report points out three main criteria to assess whether surveillance is lawful or not. The starting point for the assessment is Article 17 of the International Covenant on Civil and Political Rights, considered the most important legally binding treaty provision guaranteeing the right to privacy at the universal level.[24] The article provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation;

2. Everyone has the right to the protection of the law against such interference or attacks.[25]

It is acknowledged that, although the article does not contain a clause specifying the conditions in which such a right could be limited, the UN report delineates three conditions allowing for the restriction of the right to privacy:[26]

1. Restrictions/interference/surveillance measures are authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant;

2. Such measures pursue a legitimate aim;

3. They meet the test of necessity and proportionality.

---

[20] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Claude Moraes, "Working Document on the Follow-up of the LIBE Inquiry on Electronic Mass Surveillance of EU Citizens," January 19, 2015.

[21] GCHQ, which stands for Government Communications Headquarters, is UK' security and intelligence organisation (the equivalent of US' NSA).

[22] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Claude Moraes, "Working Document on the Follow-up of the LIBE Inquiry on Electronic Mass Surveillance of EU Citizens," January 19, 2015.

[23] Ibid.

[24] All EU Member States are States Parties to the Covenant, as well as the United States (which, however, are not State Party as regard to the Optional Protocol to the International Covenant on Civil and Political Rights of 1976), New Zealand, Australia and Canada. To check the status of a specific State, use the following link: <http://indicators.ohchr.org>.

[25] United Nations, International Covenant on Civil and Political Rights, General Assembly resolution 2200A, March 23, 1976.

[26] United Nations, "Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism," A/69/397, September 23, 2014, < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf>, p.12.

Still, at the supra-national level, EU Member States are even more engaged to the right to privacy and protection of personal data by the Charter of Fundamental Rights (CFR) of the European Union, annexed to the Lisbon treaty and which acquired legally binding status on 1 December 2009. Article 7 of the Charter states that, "everyone has the right to respect for his or her private and family life, home and communications."[27]

Article 8 of the Charter lays down provisions for the protection of personal data.[28] However, the rights may be restricted, as established by Article 52(1), on the basis of some preconditions. Notably, the restrictions must be done lawfully, respecting the principle of proportionality and necessity as well as genuinely meeting objectives of the general interest recognised by the Union.[29]

These conditions/criteria listed in the UN report and established in the CFR of the EU are not met by mass surveillance programmes, first of all because of the lack of proportionality and of a case-by-case analysis. The use of bulk access to all digital communications traffic eliminates *a priori* any possibility of individualized proportionality analysis. Since there is no target-specific justification for mass surveillance, states seek to justify the general practice of bulk access and "data-mining" to and of digital communications, shifting, in this way, the proportionality analysis "from the micro level (assessing the justification for invading a particular individual's or organisation's privacy) to the macro level (assessing the justification for adopting a system that involves wholesale interference with the individual and collective privacy rights of all Internet users)."[30]

As for the necessity of mass surveillance programmes, states engaged in the activity have so far failed to provide a detailed and evidence-based public justification for its necessity and almost no state has enacted explicit domestic legislation to authorise its use. The threat of terrorism can provide a justification for mass surveillance but evidence should be shown as to the real utility of such technologies in countering it.[31]

The final UN Report, led by UN Rapporteur Claude Moraes on the EU inquiry conducted by the LIBE Committee on the US NSA surveillance programme, arrives to the same conclusion when, in the main findings, it notes that the claim that mass surveillance programmes are necessary to combat terrorism cannot be a justification for untargeted, secret or even illegal mass surveillance programmes because they are incompatible with the principles of necessity and proportionality in a democratic society. Finally, the report considers that "data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens."[32]

On the issue of proportionality, the European Court of Justice, in the judgement of 8 April 2014, in joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, declared the EU Data Retention Directive 2006/24/EC to be invalid.[33] In fact, the CJEU is of the opinion that, by adopting this Directive, the EU legislature exceeded the limits imposed by compliance with the principle of proportionality. The

---

[27] European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Union (C 364/1), December 18, 2000.

[28] Ibid.

[29] Ibid.

[30] United Nations, "Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism," A/69/397, September 23, 2014, < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf>, p.5.

[31] [31] Edward Snowden, "Edward Snowden' Testimony," European Parliament, March 7, 2014, <http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>, pp. 1-2.

[32] European Parliament, "Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs," 2013/2188(INI), February 21, 2014, pp. 20-21.

[33] European Court of Justice, "Judgement of the Court (Grand Chamber) of 8 April 2014, in Joint Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others," Official Journal of the European Union, (C 175/6), June 10, 2014.

objective of the Directive was to harmonise Member States' provisions concerning the retention of certain data generated or processed by providers of publicly available electronic communications services or of public communications networks. The general aim of the Directive, therefore, was to make this data available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as, in particular, organised crime and terrorism. With this aim, the Directive obliged providers to retain traffic and location data as well as related data necessary to identify subscribers or users, although it did not permit the retention of the content of the communication or of information consulted. Despite this exclusion, the Court judged that the retention of the data allowed by the Directive was more than sufficient to provide very precise information on the private lives of the persons whose data was retained. By consequence, the Directive interfered in a serious manner with fundamental rights to respect for private life and to protection of personal data, especially since data could be used without the subscriber or user being informed. The Court considered that, although the retention of data required by the Directive could be appropriate to attain the objective of the Directive, namely the fight against serious crime and, ultimately, public security, the wide-ranging and serious interference of the Directive with fundamental rights at stake is not sufficiently circumscribed to ensure that the interference is actually limited to what is strictly necessary. In fact, the Directive covers in an overly generalised way all individuals, all means of electronic communication, and all traffic data without any differentiation, limitation or exception. Furthermore, it does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and use them and, above all, the access to the data is not subject to a prior review by a court or an independent administrative body. In other words, the Court identified a risk of abuse, aggravated by the vague definition of the data retention period identified in a timeframe between six months and twenty-four months, without any further specifications.

On the issue of surveillance and, in particular mass surveillance, some states' legislation displays several loopholes and, above all, lack of transparency. While several states are filling these loopholes by strengthening individuals' rights in cyber-space, other states are going in the opposite direction by "legalising" practices of mass surveillance. The UK and the Netherlands are examples of this latter category of states. On 18 July 2014, the UK Parliament adopted the Data Retention and Investigatory Powers Act which expands surveillance powers by empowering the UK Secretary of State for the Home Department to issue interception warrants for communications content that is stored outside of UK territorial jurisdiction and gives UK authorities broad powers to obtain, access and store communications meta-data. Legislative proposals were also made in the Netherlands to introduce an amendment to the Dutch Intelligence and Security Act 2002 allowing for intelligence services to also intercept cable-bound communications.[34]

Mass Surveillance Technologies and Suppliers: Who Exports What and Why?

This section explores the international dimension of the risks linked to the export of mass surveillance technology, in particular in the field of human rights protection. It is useful first to identify the scope of this kind of technology in terms of the object (what it is), in terms of subject (who provides it) and in terms of location (where is it/where is it exported).

Once identified, the "traffic" of mass surveillance technology in international trade and the relationships between suppliers and end-users will be considered with a particular focus on the relation between suppliers and national authorities as end-users. The objective is to "raise a red flag" on the conflict of interest that exists between the State as legislator of trade controls and guarantor of fundamental freedoms, and its role as end-user of mass surveillance technology. The risk of such a close relationship, in fact, could result in "permissive" legislation or policy implementation and/or in a degree of "blind" policy implementation leaving legislative loopholes in the system.

Mass surveillance technology is part of the wider ICT sector (information and telecommunication

[34] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Claude Moraes, "Working Document on the Follow-up of the LIBE Inquiry on Electronic Mass Surveillance of EU Citizens," January 19, 2015.

technologies). The ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights divides the ICT sector in five main segments (for more technical details, please see the table in Annex I):[35]

- Telecommunications services;
- Web-based (and cloud-based) services/platforms;
- Manufacture of consumer and business end-user devices ("device manufacturer");
- Manufacture of telecommunications components, device components and network equipment ("component manufacturers");
- Software.

The Wall Street Journal (WSJ) reported in 2011 that "a retail market for surveillance tools has sprung up from 'nearly zero' in 2001 to about $5 billion a year."[36] More precisely, the WSJ reported that "a new global market for the off-the-shelf surveillance technology has arisen in the decade since the terrorist attacks of September 11, 2001," linking the "war on terror" and the spread of surveillance technology.[37] According to the paper *Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age*, the 9/11 terrorist attacks, as well as other terrorist attacks in Bali, Madrid, London and Mumbai, were perceived as intelligence failures, and generated the "need" for better intelligence-gathering capabilities.[38]

In addition, the market for surveillance technology grew due to the existence of legislative and regulatory loopholes allowing intelligence and law enforcement agencies to profit from systemic gaps to use data not subject to regulation. The increasing dependency of governments on the private sector, which seems more capable of keeping the pace with technological changes and demands, also contributes to to growth in the sector.

However, surveillance technology leading companies, mainly European and US-based companies, did not limit themselves to serve their own governments, but went international. It emerged due to the release of many former regimes' documents following the Arab Spring that several Western companies exported surveillance technology to authoritarian governments, such as Assad in Syria and Gadhafi in Libya (see Annex II).[39]

A report published on September 2014 suggests that between 2003 and 2013, German companies alone exported "surveillance technologies to Albania, Argentina, Chile, India, Indonesia, Qatar, Kosovo, Kuwait, Lebanon, Malaysia, Morocco, Mexico, Norway, Oman, Pakistan, Russia, Saudi Arabia, Switzerland, Singapore, Taiwan, Turkey, Turkmenistan, USA, and the UAE."[40] Two of the companies in the surveillance technology sector are the Italian Hacking Team and the British-German Gamma Group. Hacking Team's flagship program, Remote Control System (RCS) "Galileo," installs malicious software on a target phone or computer that can be used to remotely monitor audio or video data. As described on the company's website:

---

[35] In December 2011, the European Commission (DG for Enterprise and Industry) instructed IHRB and Shift to develop sector-specific guidance on the corporate responsibility to respect human rights. This initiative is part of the Commission's policy on corporate social responsibility, adopted in October 2011. European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights," <http://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf>.

[36] "Document Trove Exposes Surveillance Methods," *The Wall Street Journal*, November 19, 2011.

[37] Ibid.

[38] Tim Maurer, Edin Omanovic, and Ben Wagner, "Uncontrolled Global Surveillance Updating Export Controls to the Digital Age," *Digitale Gesellschaft*, March 2014, <www.digitalegesellschaft.de>.

[39] https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe-1-2.pdf

[40] Ben Wagner and Claudio Guarnieri, "German Companies Are Selling Unlicensed Surveillance Technologies to Human Rights Violators – and Making Millions," *Global Voices*, September 2014.

Take control of your targets and monitor them regardless of encryption and mobility. It doesn't matter if you are after an Android phone or a Windows computer: you can monitor all the devices.
Remote Control System is invisible to the user, evades antivirus and firewalls, and doesn't affect the devices' performance or battery life.
Hack into your targets with the most advanced infection vectors available. Enter his wireless network and tackle tactical operations with ad-hoc equipment designed to operate while on the move.
Keep an eye on all your targets and manage them remotely, all from a single screen. Be alerted on incoming relevant data and have meaningful events automatically highlighted.[41]

In July 2015, Hacking Team found itself the victim of hacking on a grand scale. Gamma International, suffered a similar hack in 2014, revealing the company's clients, capabilities and pricing.[42] Hacking Team's Twitter account was hijacked and used by hackers to release what is alleged to be more than 400 gigabytes of the company's internal documents, email correspondence, employee passwords and the underlying source code of its products. Among the documents published was the list of the company's active and inactive clients at the end of 2014. Among the company's clients, there were police agencies in several European countries, the US Drug Enforcement Administration and police and State security organisations in countries with records of human rights abuses such as Egypt, Ethiopia, Kazakhstan, Morocco, Nigeria, Saudi Arabia and Sudan. Sudan's National Intelligence Security Service was a customer given a special designation of "not officially supported." However, in a second document, an invoice for 480,000 euros to the same security service calls into question repeated denials by Hacking Team that it never did business with Sudan, which is subject to heavy trade restrictions.[43,44]

In response to concerns that Hacking Team supplied tools to repressive States, the founder of the Italian company declared to the Italian newspaper La Stampa, "We did [sell tools to Libya] when suddenly it seemed that the Libyans had become our best friends." He also admitted providing tools to Egypt, Ethiopia, Morocco and Sudan (though denied dealing with Syria). He added that "the geopolitics changes rapidly, and sometimes situations evolve. But we do not trade in weapons, we do not sell guns that can be used for years." He said that without regular updates, its tools are rapidly blocked by cyber security countermeasures.

La Stampa reports that in June 2014, the Security Council Committee, overseeing the implementation of sanctions against Sudan (established pursuant to UN Security Council resolution 1591/2005), asked the Hacking Team if the company was still selling to Sudan or if it did so in the past. The answer came following three requests on the side of the Security Council Committee, after the company stopped, in December 2014, supplying to Sudan. Hacking Team answered that, at the moment, the company was not supplying Sudan.

Since UN/EU sanctions against Sudan do not target dual-use goods and technology, the UN insisted on considering Hacking Team's products as belonging to the category "military assistance" covered by the sanctions. The debate on the legality of Hacking Team's exports was ended with the entry into force in January 2015 of Commission Delegated Regulation (EU) No 1382/2014 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.[45] The delegated act, in fact, updating the list of items subject to export authorisation,

---

[41] Hacking Team, "Remote Control System Galileo, Overview," <www.hackingteam.it>.

[42] "Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim," *The Guardian*, July 6, 2015.

[43] "Hacking Team Surveillance Technology Firm Hacked," *CBC News*, July 7, 2015.

[44] As regards to UN embargoes, see: UNSCR 1556/2004, 1591/2005, 1945/2010, 035/2012 and 2200/2015. As regard to EU embargoes, see: Council Decision 2014/450/CFSP (OJ L 203, 11.7.2014, p. 106) and Council Regulation (EC) No 747/2014 (OJ L 203, 11.7.2014, p. 1).

[45] Commission Delegated Regulation (EU) No 1382/2014 of 22 October 2014 amending Council Regulation (EC) No 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal

included the updates established by the Wassenaar Arrangement in December 2013, among which was intrusion software.[46] However, before the European regulation, the Italian competent authority, the Ministry of Economic Development (MED), imposed a catch-all clause on Hacking Team' product, on the basis of Article 4 of Regulation 428/2009 in order to control the company's exports. The catch-all clause was established on 30 October 2014 but, already on 27 November 2014, the measure was suspended (with a validity of six months) by MED.[47] According to some Italian newspapers, the decision to revoke the MED's measure came almost without surprise considering the pressure put on the competent authority by the Italian Government and the Aise (Italian External Information and Security Agency), both clients of Hacking Team.[48] Also, one day before the publication of the MED' decision to suspend the catch-all clause, a meeting between MED and Hacking Team was held following the company's request to withdraw the catch-all clause for the reason of self-defence. The document, released the following day, with MED's decision to suspend the measure, explains the constraints that Hacking Team would encounter with the catch-all clause in force. The most important reasons were stated as the following:

> *The company has very tight delivery deadlines, incompatible with the timing of administrative procedures required by the implementation of the catch-all clause;*
> *End-users are mainly governmental security and law enforcement agencies having specific needs in terms of secrecy and quick delivery;*
> *The exported product needs not to be "detected" by third parties, requiring, to this end, constant updates (camouflage software) in order to be operative and to not be neutralised by an antivirus software;*
> *Delay in deliveries (with deadlines already agreed with clients) would cause the company the payment of penalties, threatening the company's liquidity with subsequent possible failure.*

The MED' document, before stating the decision to suspend the catch-all clause, highlights Hacking Team's cooperative attitude with the MED, following the adoption of the catch-all clause, promptly presenting all required documents necessary for issuing the export authorisations.

Despite the EU Delegated Regulation No 1382/2014, which *de facto* subjected Hacking Team's product to trade controls, questions and doubts persist on the relationship between these kind of companies and their governments. It seems quite logical to raise questions about transparency and scrutiny on the supply and use of this kind of technology. It is legitimate to ask if it is acceptable that the authority that is supposed to control and verify the exports of a company is, in a way or partially, a client of the company itself. How can the government (in this specific case the MED) ensure proper trade control implementation or impose sanctions in case of violation on the company that supplies the government itself (here, in particular, the Ministry of Defence, the Aise, etc.)? What are the guarantees against the misuse of such technology by the government against its citizens? The answer given by Hacking Team's CEO, David Vincenzetti, that his company works with governments to ensure citizens' security seems inadequate in light of recent disclosures of states' mass surveillance programmes and authoritarian regimes' violation of human rights. More transparency and judiciary control are necessary.

The EU Trade Control Regime: Evolution Regarding Human Rights Protection

This section seeks to give a practical example of the difficulty of controlling MST due to three main

---

of the European Union (L 371/1), December 30, 2014.

[46] "Così il Sudan ha Messo in Crisi Hacking Team," *La Stampa*, Tecnologia, July 9, 2015.

[47] Ministero dello Sviluppo Economico, Direzione Generale per la Politica Commerciale Internazionale, Divisione IV, "Registro Ufficiale, Prot. N. 0211026 – 27/11/2014 – Uscita," November 27, 2014.

[48] "La Tecnologia di Sorveglianza Hacking Team Offerta Anche alla Gendarmeria Vaticana," *L'espresso,* July 13, 2015. See also "Hacking Team, Pansa: Gravi Danni alle Inchieste," *La Stampa*, July 30, 2015.

reasons: the rapid evolution of this technology, some systemic constrains (e.g. update of control lists) and lack of political will. The case of the EU dual-use trade control system has been chosen because it is one of the most comprehensive and advanced systems for what concerns dual-use, its emphasis on human rights issues and the protection of fundamental freedoms, and the large involvement of EU-based enterprises in the trade of MST. Despite the evolution of the EU dual-use trade control system toward a human security approach, expanding the scope of trade controls also in case of human rights concerns, the system is inadequate to prevent the misuse of mass surveillance technology.

The EU has been engaged in the protection of human rights in the field of ICTs since 2011, when the European Commission adopted the No Disconnect Strategy (NDS) to address restrictions and disruptions through ICTs, including the Internet, employed by authorities during the Arab Spring to control and repress citizens.[49] This first attempt at addressing the issues of human rights defenders facing surveillance and censorship in third countries was followed, in June 2012, by a new strategic framework and an action plan on human rights and democracy.[50] One of the main goals of this framework was to promote human rights in all EU external policies, including trade, technology and the Internet. Point 24 of the Action Plan addresses the issue of "Freedom of expression online and offline" and points out four strategies to pursue this main objective, among which: "to ensure that a clear human rights perspective and impact assessment is present in the development of policies and programmes relating to cyber security, the fight against cyber crime, Internet governance and other EU policies in this regard" and to "include human rights violations as one of the reasons following which non-listed items may be subject to export restrictions by Member States."[51]

These two strategies are particularly relevant because they relate to trade controls and in particular to the "evolution" of the EU Dual-use Regulation with regard to human rights protection. No further developments on the side of NDS have been registered.[52] Particularly useful for the protection of human rights, through trade controls, is Article 8(1) of Regulation 428/2009.[53] The Article establishes the possibility for national competent authorities to deny or require prior authorisation for export of dual-use items not listed in Annex I for reasons of public security or human rights considerations. It is quite curious to notice that, despite this provision already existing in the previous EU dual-use legislation, it has been used only in 2012 by Italy (published on September 19 (C 283/4, 19.9.2012)), when the Italian competent authority adopted a catch-all clause against Syria for public security and human rights considerations.[54] The measures aimed at controlling Public LAN database centralised monitoring system, Internet and 2G/3G services to be exported to Syrian Telecommunication Establishment (STE) in Syria.[55]

Although some Member States have mechanisms to require prior authorisations for items not listed in Annex I and some of them require systematically an authorisation for items not listed in Annex I in application of Article 8, none of the Member States has implemented Article 8 to impose an export prohibition of non-listed items.[56]

---

[49] European Commission, DG Information Society and Media Unit A3 (Internet; Network and Information Security), No Disconnect Strategy. More information on <http://europa.eu/rapid/press-release_IP-11-1525_en.htm?locale=en>.

[50] Council of the European Union, "EU Strategic Framework on Human Rights and Democracy," Luxembourg, June 25, 2012.

[51] Ibid.

[52] European Parliament, Marietje Schaake, Member of the European Parliament, Alliance of Liberals and Democrats for Europe, "Written Questions on the Follow-up on the No Disconnect Strategy," E-011923/2015, July 27, 2015.

[53] Council Regulation (EC) No 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 134/1) of May 29, 2009. It is worth to notice that Council Regulation 428/2009, compared to the previous dual-use Regulation, is much more comprehensive in terms of operations covered and items listed.

[54] Information note: Council Regulation (EC) No 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items: Information on Measures adopted by Member States in Conformity with Articles 5, 6, 8, 9, 10, 17 and 22, Official Journal of the European Union (C 283/4), September 19, 2012.

[55] "Italy has Adopted a Catch-all Clause against Syria for Public Security and Human Rights Considerations," University of Liege, European Studies Unit (ESU), Nonproliferation News, September 19, 2012, <www.esu.ulg.ac.be>.

[56] Quentin Michel. "The European Union Dual-Use Items Control Regime: Comment of the Legislation Article-by-Article,"

Regulation 428/2009 has been subject to review since 2011. On 30 June 2011, the Commission issued a Green Paper, as established by Art. 25 of Regulation 428/2009 requiring the Commission to prepare a report on the implementation of the EU trade control system and possible area of reform.[57] The aim of the paper was to launch a broad debate concerning the EU trade control system, calling stakeholders to raise the main issues and express their views on possible evolution.

Among the challenges that the EU trade control system has to face, the Green Paper recognises new threats to security coupled with technological progress leading to increased availability of sensitive items. It also acknowledges that "technological development and the increasing number of transactions taking place put a constantly growing burden on the limited resources of export control authorities."[58] On 17 January 2013, a report on the 2011 Green Paper results was published which confirmed and developed the challenges raised by new technologies and technological development.[59] Among the new technologies, transformational technologies and cloud computing are cited, while the term "cyber-tools" appears for the first time in the Commission's documents on dual-use trade control.[60] The connection between international political events, such as the Arab Spring, and the need to prevent human rights abuses through the export control of telecommunications surveillance and internet monitoring systems are, for the first time, brought to the attention of the Commission by some Member States, some MEPs, civil society organisations and researchers. Still, in relation to computers and information security in general, some Member States, industry associations and exporters call for the introduction of new EU general authorisations in order to resolve the difficulties surrounding export of encryption technology.[61] On the issue of encryption, the document highlights that some Member States have introduced additional regulations that require advance declaration or authorisation for imports, intra EU-transfers and in-country supply, while the same items would not require any authorisation in other Member States.[62] Finally, the document points out that Member States report only few cases of additional controls introduced for reasons of security policy or human rights considerations (in application of Art.8 of Regulation 428/2009).[63]

A second step in the review process was marked by a report to the EP and the Council on the implementation of the Regulation. On the human rights issue, the report does not add much compared to the January 2013 document except for a note on national implementing measures, announcing that Italy notified the imposition of a specific national authorisation requirement on the export to Syria of certain telecommunication items not listed in Annex I for reasons of public security and human rights considerations.[64]

The Commission Communication of 24 April 2014, «The Review of export control policy: ensuring security and competitiveness in a changing world» can be considered a watershed in the EU approach to trade controls.[65] In fact, contrary to previous Commission documents, new cyber-tools and their connection

University of Liege, European Studies Unit (ESU), DUV5Rev4, August 2015, <www.esu.ulg.ac.be>.

[57] European Commission, "Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," COM(2011) 393 final, Brussels, June 30, 2011.

[58] Ibid, p. 12.

[59] European Commission, "Commission Staff Working Document, Strategic Export Controls: Ensuring Security and Competitiveness in a Changing World - A Report on the Public Consultation Launched under the Green Paper," COM(2011) 393, SWD(2013) 7 final, Brussels, January 17, 2013.

[60] Ibid, p. 5.

[61] Ibid, p. 17.

[62] Ibid, p. 9.

[63] Ibid, p. 12.

[64] European Commission, "Report from the Commission to the Council and the European Parliament on the Implementation of Regulation (EC) No 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items," COM(2013) 710 final, Brussels, October 16, 2013, p. 5.

[65] European Commission, "Communication from the Commission to the Council and the European Parliament: The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World," COM(2014) 244 final, Brussels, April

with human rights abuses constitutes one of the main topic of focus, at the point of changing the EU approach to trade controls from military/WMD proliferation risks-based towards a "human security" approach. This new approach implies a widening of the scope of the term "strategic" as to include items and, above all technologies, which could be used for human rights abuses, although not having any direct relations with WMD proliferation concerns. As stated in the Commission Communication:

> *The Commission will consider evolving towards a "human security" approach recognising that security and human rights are inextricably interlinked. This may involve evolving towards a notion of "strategic" items addressing not only and strictly, items with possible military and WMD proliferation end-uses, but taking a wider security approach. This may also imply a clarification of control criteria to take into consideration broader security implications, including the potential effect on the security of persons e.g. through terrorism or human rights violations (…).*[66]

The Communication makes reference also to a "smart security" approach to "adjust to the transformations of dual-use items and the proliferation of new technologies."[67] Part of this approach is the development of an "EU technological reaction capacity" to ensure rapid reaction to the challenges posed by emerging technologies such as cloud computing, additive manufacturing (3-D printing), nanotechnology and to de-control items that have become obsolete or widely available commercially. In addition, to face the use of cyber-space for proliferation activities and clarification of controls of cyber-tools, the Commission considers taking actions at the multilateral level or "alternative options such as the introduction of EU autonomous lists or a dedicated catch-all mechanism."[68]

On the issue of autonomous lists, several human rights organisations asked for this solution as a possible way out from multilateral mechanisms presenting several shortcomings. In particular, a report published by CAUSE in 2014 highlights two reasons for which the EU should adopt autonomous control lists.[69] The first reason lies in the nature of the Wassenaar Arrangement, which "was established at the end of the Cold War and functions similarly to its Cold War predecessor, it focuses on risks to regional and international security and stability related to the spread of conventional weapons and dual-use goods and technologies."[70] In this sense, the WA could have a minor interest in controlling goods and technology that could be used for human rights violations or internal repression. It is more plausible that the WA places under control some surveillance technology (in particular Intrusion Software and IP Network Surveillance) because it could significantly increase the military capabilities of a State.[71] The second reason lies in the decision-making process which is time-consuming, with consensus difficult to reach due to political and technical issues.[72] In other words, the interest in including human rights issues in trade controls could not be the same at the international level, especially in a multilateral regime grouping together different countries with varying records as regards human rights.

The Commission Communication employs for the first time the term "cyber-proliferation" and makes reference to the emergence of specific cyber-tools for mass surveillance, monitoring, tracking and interception,

---

24, 2014.

[66] Ibid, p. 6.

[67] Ibid.

[68] Ibid.

[69] The Coalition Against Unlawful Surveillance Exports (CAUSE) includes: Amnesty International, Fidh, Open Technology Institute, Reporters without Borders, Digitale Gesellschaft, Human Rights Watch, Privacy International and Access.

[70] Wasseenaar Arrangement, "Introduction," <www.wassenaar.org>.

[71] Tim Maurer, Edin Omanovic, and Ben Wagner, March 2014.

[72] For example, in 2013, the WA agreed to add trojans to its list through the articulation of a control on "intrusion software," something which has proved problematic because the agreed language risks inadvertently catching too many items.

recognising that they are becoming an important dimension of export controls.[73] Finally, a relevant novelty as regards ICT control is the proposal to introduce additional EUGEAs such as for encryption to allow the export of ICT items widely used in industrial processes and operating in a highly competitive environment and for intra-company technology transfers for research and development purposes.

The European Parliament, in its legislative resolution of 23 October 2012 proposed two amendments to the Commission's proposal as regards the introduction of provisions to control unlisted items for human rights considerations.[74] One of the amendments proposed concerned the wording of Article 8(1) and precisely, the EP proposed to replace the word "may" with the word "shall":

> *A Member State may prohibit or impose an authorisation requirement on the export of dual-use items not listed in Annex I for reasons of public security or human rights considerations.*

It is reasonable to think that the EP, by introducing the modal verb "shall" instead of "may" wanted to give a more mandatory tone to the provision, reducing Member States' marging of appreciation.

The second major amendment proposed by the EP and not introduced in the Regulation was the insertion of a paragraph to Article 4, which establishes the possibility of catch-all clauses. The amendment proposed by the EP was that the following paragraph be inserted:

> *An authorisation shall also be required for the export of dual-use items not listed in Annex I if the exporter has been informed by the authorities referred to in paragraphs 1 and 2, or by the Commission, that the items in question are or may be intended, in their entirety or in part, for use in connection with a violation of human rights, democratic principles or freedom of speech as defined in the Charter of Fundamental Rights of the European Union, by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use, such as via monitoring centres or lawful interception gateways.*[75]

It is evident that the EP, already in 2012, recognised the importance of covering the control of items and technologies that could be used in violation of human rights and, going even further, the EP tried to insert a mechanism also for the protection of democratic principles and freedom of speech as defined by the Charter of Fundamental Rights of the EU- a human rights/democratic principle catch-all clause identifying the type of items and technologies that could be included in such a provision (interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use, such as via monitoring centres or lawful interception gateways). A pending question is why the Commission only made reference to such risks and related measures in its Communication in 2014 and why the EP's proposals for amendment were not inserted in the final Regulation.

Proceeding with the evolutionary process of the EU Dual-use Regulation as regards human rights protection, on 30 December 2014, Commission Delegated Regulation (EU) No 1382/2014 entered into force updating Annex I as to include modifications adopted by export control regimes in 2011, 2012 and 2013.[76] This

[73] European Commission, COM(2014) 244 final, Brussels, April 24, 2014, p. 3.

[74] European Parliament legislative resolution of 23 October 2012 on "the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, COM(2011)0704 – C7-0395/2011 – 2011/0310(COD), October 23, 2012.

[75] Ibid.

[76] European Commission, "Commission Delegated Regulation (EU) No 1382/2014 of 22 October 2014.

delegated Regulation has particular importance as regards human rights protection and mass surveillance technology control because it inserts the Wassenaar Arrangement's December 2013 updates, including some "Intrusion Software" and "IP Network Surveillance Systems."

As for Annex I of the EU Dual-Use Regulation, "Intrusion software" falls within Category 4, (Computers Systems, Equipment and Components), control entry 4A005, while "IP Network Surveillance Systems" fall within Category 5 (Telecommunications systems, equipment, components and accessories), control entry 5A001. A white paper released by Access in March 2015 makes a technical analysis of these two categories of items included in the WA Control list and raises some important points, especially at the level of language used in the definition and the scope covered.[77]

The main concerns emerging from the analysis are the following:

As regards "Intrusion software,"the control is not designed to solve the totality of threats to information security and privacy[78] (for example, it does not regulate the ample market for commercial malware that is sold to the general public and it does not attempt to holistically control the broad range of software that may be used to compromise user data); and "the definition of control is too broad as to create fear that the controls regulate commonplace research, instead of concerns about missed technologies."

As regards IP Network Surveillance, the paper states that "there is no indication that the Wassenaar Arrangement language would apply to the deep packet inspection (DPI) equipment or lawful interception systems that have routinely evoked controversy when exported to countries that violate human rights.... The definition of the IP Network Surveillance is too narrow and may be reflective of the uncertainty that export control authorities face in asserting administrative burden on the sale of dual-use network equipment (frequently used for censorship, but also commonplace in networks for caching of content, mitigating security threats and other purposes, even in countries with human rights challenges)."[79]

However, the paper underlines that:

> *The exemptions under both Intrusion Software (for debuggers, software reverse engineering, digital rights management, and asset recovery) and IP Network Surveillance (marketing and network management) appear to be narrowly-defined and are unlikely to present significant short-term risk of re-labelling by companies that may want to apply avoid scrutiny*[80].

It seems that the 2013 WA updates on surveillance technology are the results of two different proposals: a UK proposal focused on "advanced persistent threat software and related equipment (offensive cyber tools) and a French proposal for the control of IP network surveillance systems.[81]

The term used "intrusion software" (language finally adopted by the WA plenary in December 2013) is defined as:

---

[77] Collin Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies", March 9, 2015, available at: http://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf.

[78] Ibid. p. 11.

[79] Ibid. p. 5.

[80] Ibid. p. 7.

[81] Tim Maurer, Edin Omanovic, and Ben Wagner, "Uncontrolled Global Surveillance Updating Export Controls to the Digital Age," *Digitale Gesellschaft*, March 2014, <www.digitalegesellschaft.de>.

Software specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network capable device, and performing any of the following:
a. The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or
b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.
Points (a) and (b) captures two different aspects of the technology that will be subject to control. Point (a) covers the exfiltration of data from the victim's system such as microphone or camera streams and it also includes software that changes files on the victim's machine. Point « b » defines the mechanism by which commercial malware typically infects its victim's devices (this is the exploit mechanism that the surveillance product takes advantage of).

The actual controls are defined as:

4. A. 5. Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".
4. D. 4. "Software" specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".
[4. E. 1.] c. "Technology" for the "development" of "intrusion software."

Two main considerations (strictly related) can be done on the definition of controls. The first is that intrusion software per se is not subject to controls; the second consideration is that controls target the components that stay under direct control of the purchaser, leaving outside any component that would end up on a victim's end-user device. The logic behind this definition of control is clear and it is to target those who purchase intrusion software and seek to target others, not those who are infected with it. Without this logic, the risk would be a violation of export controls by the targeted user carrying an infected device, especially if travelling to another country. As a consequence, software to achieve these activities must reside off the victim's device, while the intrusion software itself must reside on the device.[82]

Regarding IP network surveillance systems, these are defined as:

5. A. 1. j. IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:
1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
Indexing of extracted data; and
2. Being specially designed to carry out all of the following:
Execution of searches on the basis of 'hard selectors'; and
Mapping of the relational network of an individual or of a group of people.

The concern here is that the definition of controls targets a very narrow category of products, risking to fail to cover some of the systems of greatest concern, as already stressed above.[83] As explained, surveillance technology remains an issue for several reasons. The first is that not all states are members of the WA and,

[82] Ibid.
[83] Ibid.

even if this was the case, there is no legally-binding obligation for states to implement decisions taken in the multilateral forum. Second, although all WA members are willing to implement trade controls established at the international level (as it is the case for EU Member States implementing WA updates through the EU Dual-use Regulation, legally-binding and directly applicable to/in all EU Member States), competent national authorities in each state do not necessarily have the same interpretation of the provisions, as stressed by MEP Schaake in her oral question on export controls and Hacking Team, debated in the European Parliament on 5 October 2015.[84] The result is a very fragmented regulatory system leaving too much space for violations and abuses.

In June 2015, a report was published by the EP Committee on Foreign Affairs.[85] The Rapporteur highlights the dual-use nature of information technology, especially software, which plays an increasingly important role in enabling and ensuring the fulfilment and full respect for human rights and fundamental freedoms by expanding the scope of freedom of expression, of association and assembly and access to information. But, at the same time, the same tools can be used for the violation of human rights and fundamental freedoms through surveillance, censorship, unauthorised access to devices, jamming, interception and tracing and tracking of information and individuals. The report also points out the increasing role assumed by private actors in assessing the legality of content and in developing cyber-security systems and surveillance systems in the absence of a legal basis that rests on the precepts of necessity, proportionality, and democratic and judicial oversight. The role of EU-based companies is also recognised as having an important share of global market in ICTs, in particular in the field of surveillance, tracking, intrusion and monitoring technology exports. At the same time, the responsibilities of some EU-based companies is clearly recognised as having contributed to human rights violations worldwide through the export of such technology. Member States are also called into question as far as their complicity in the NSA's mass surveillance programmes "as revealed by Edward Snowden, has caused serious damage to the credibility of the EU's human rights policy and has undermined global trust in the benefits of ICTs."[86] The EP report, as many other documents and articles, establishes a direct link between violation of human rights and fundamental freedoms counter-terrorism measures used as pretexts for such violations. To this end, the EP insists that such measures be pursued strictly in line with the rule of law and human rights standards.

To react against such a negative trend, the report asks for several actions to be taken. One is the inclusion of clauses in agreements with third countries that would promote, guarantee and respect digital freedoms, net neutrality, uncensored and unrestricted access to the Internet, privacy rights and the protection of data."[87] Other actions are, for example, to ensure greater transparency in the relationship between internet service providers and governments; the implementation and monitoring of EU regulations and sanctions relating to ICTs; the public exclusion of companies engaging in ICTs exports with detrimental effects on human rights, and the introduction of "end to end" encryption standards. In the specific framework of the dual-use policy review, the EP, however, calls on the Commission to pay attention to avoid any measures that could inhibit legitimate research or access to and exchange of information and that could have a "chilling effect" on individuals or SMEs. To avoid this side effect, the EP proposes, for example, the use of EU General Export Authorisations for dual-use research. Finally, the report calls for an end to mass surveillance, considering that the issue must be addressed and stopped.

The EP resolution of 8 September 2015, which transposes word by word the report, addresses the mass surveillance issue on two dimensions: the internal dimension involving the surveillance of EU citizens and

---

[84] European Parliament, Marietje Schaake, Member of the European Parliament, Alliance of Liberals and Democrats for Europe, "Oral Questions on Export Controls and Hacking Team," (O-000094/2015), September 3, 2015.

[85] European Parliament, "Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," 2014/2232(INI), June 6, 2015.

[86] Ibid, p. 8.

[87] Ibid, p. 10.

the subsequent issue of violation of fundamental freedoms and on the external dimension, by addressing the problem of surveillance technology export controls.

This EP resolution, during the dual-use policy review period, can be considered a reminder of the challenges posed by information and digital technology. But it is also a warning, on the side of the democratically elected institution, to governments and to public opinion in general to pay attention to the kind of society being built. In fact, although the EP resolution is meant to address the issue of the impact of intrusion and surveillance systems on human rights in third countries, half of the report focuses on the impact of surveillance technology inside the EU, on EU citizens "attacked" not by terrorists but by their governments.

Conclusion

This paper analysed the issue of mass surveillance technology on two dimensions: states' internal dimension involving the surveillance of citizens and the subsequent issue of violation of fundamental freedoms (such as the right to privacy and data protection), and the external dimension, by addressing the problem of surveillance technology export control, especially to countries likely to use such technology to violate human rights. It emerged that following the "Snowden's datagate scandal" on mass surveillance programmes, many states undertook inquiries and adopted measures that, in some cases, were meant to regulate the use of mass surveillance technology. It appeared, in fact, that surveillance technology used by security and law enforcement agencies, in order to fight terrorism, was not always used following the principle of proportionality and necessity, giving birth to the phenomenon of mass surveillance to the detriment of targeted surveillance subject to prior judiciary control.

On the external level, rapid technological development and a certain dose of inertia on the side of political élites left the legal framework deprived of adequate instruments to control the export of surveillance technology. The consequence has been a rapid development of private industry in supplying such technology to governments all over the world, sometimes regardless of any human rights implications.

In this intricate context, the EU started to develop a trade control policy more inclusive of a "human security" approach. Especially through the review of the Dual-use Regulation, since 2011 the EU widened the scope of its trade control system to include goods and technologies that could be used in violation of human rights. This is the aim and raison d'être of article 8(1) of EU Regulation 428/2009 establishing the possibility for national competent authorities to deny or require prior authorisation for export of dual-use items not listed in Annex I for reasons of public security or human rights considerations. Another step forward has been the entry into force of Commission Delegated Regulation (EU) No 1382/2014 of 22 October 2014, which updated Annex I to include modifications adopted by export control regimes in 2011, 2012 and 2013 and, in particular, December 2013 Wassenaar Arrangement's updates, including some "Intrusion Software" and "IP Network Surveillance Systems." Despite this progress, several issues remain that raise questions about the effectiveness of trade controls in preventing the violation of human rights and, in general, the capacity of trade control systems to adopt the human security approach.

The first issue concerns the nature of existing multilateral export control regimes, especially the WA, which does not take into account the control of goods and technologies for human rights concerns. This reality is particularly problematic for implementation of the EU dual-use control list, which being an implementer of multilateral export control regimes' lists, is "limited" to control items decided on the international level. Until present, the idea of an EU independent list is not being considered. The catch-all clause mechanism has been the only way include the possibility of controlling items on the grounds of human rights concerns

but is just a possibility and the implementation is up to Member States.[88]

A second issue regards suppliers of surveillance technology that, given their role as governments' suppliers, sometimes seem to consider themselves (or are allowed to consider themselves as) "above the law," invoking their role of "security providers." In fact, whether they have been operating in a grey zone where surveillance technology has not always been clearly subject to trade controls, or under strict and transparent legislation on surveillance technology trade controls, the privileged relationship that some companies have with their own governments (in the form of of technology suppliers) may not be a warranty of fairness and legality. Would a government sanction the a company for trade controls violations, when the same firm is that governments' supplier?

There is still hope that the current dual-use Regulation review period will take into account recent EP resolutions and human rights defenders' requests to strengthen the EU trade control system in a way to be more in line with EU values and principles that, from the very beginning, inspired its construction and integration. One last wish is that democratic societies all over the world will remember Benjamin Franklin's famous quote, "Those who desire to give up freedom in order to gain security will not have, nor do they deserve, either one."

[88] It is worth noting that the implementation of catch-all clauses in the EU could be problematic and create problems at the level of fair competition. The issue of competition, but at the international level, was raised also by the Italian company Hacking Team affirming that if it was hindered by the competent authority to export, one of its main competitor (the Israeli company Maglan) would have won, adding that there is a lot of difference between a technology developed by an Italian company under the supervision of the MED and an Israeli one that could be designed with multiple and obscure purposes.

Special Section: Trade Controls in Southeast Asia

INTRODUCTION BY DAVID SANTORO AND CARL BAKER

Southeast Asia is one of the world's fastest growing economic centers – and also one of the least understood. While China remains the dominant economic power in East Asia, investors and multinational corporations are increasingly turning to the 10 countries that make the Association of Southeast Asian Nations (ASEAN) for new opportunities. Founded in 1967, ASEAN today includes Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam, economies at significantly different stages of development. While some are rapidly moving into high-end technology, others remain largely dependent on agriculture and basic commodities. As this economic transition occurs, countries in the region increasingly recognize the value of an effective strategic trade management system to attract investments in high technology manufacturing and ensuring goods transiting the region are properly controlled.

This issue of *Strategic Trade Review* provides several articles on the implementation of strategic trade controls in this dynamic region. It opens with an overview of potential nonproliferation challenges in the region by Stephanie Lieggi, a senior research associate from the James Martin Center for Nonproliferation Studies at the Middlebury Institute. Her analysis focuses on the key industries that will be most affected by the shifting economic landscape in the region. This is followed by four case studies: Singapore, Malaysia, the Philippines, and Indonesia. Authored by George Tan, president of Global Trade Security Consulting, the article on Singapore walks the reader through the country's journey toward its adoption and implementation of strategic trade controls, which took place in the early 2000s and was the region's first. Mohamed Shahabar Abdul Kareem, an independent consultant and former strategic trade controller of Malaysia, then gives an account of why and how Malaysia decided to implement strategic trade controls, which started with the adoption of the 2010 Strategic Trade Act. Next, an article on the Philippines by Karla Mae Pabelina, a foreign affairs researcher at the Center for International Relations and Strategic Studies, lays out the history of her country's decision to implement strategic trade controls, focusing on the dynamics associated with recent enactment of strategic trade legislation. The final article, authored by Andy Rachmianto, director for international security and disarmament at Indonesia's Ministry of Foreign Affairs, explores Jakarta's unique approach to nonproliferation and strategic trade controls. All five authors write in their personal capacity; their opinions do not necessarily reflect the views of their respective organizations.

We hope that this introductory scholarship on strategic trade controls implementation in Southeast Asia will stimulate additional work on this important topic.

Dual-Use Technology in Southeast Asia: Nonproliferation Challenges for the Next Decade

STEPHANIE LIEGGI[1]

Abstract

As industrial growth and technological progress continues in Southeast Asia, the region is rapidly becoming the next big provider of proliferation sensitive dual-use commodities. Unlike most traditional suppliers, many countries in Southeast Asia do not have strong strategic trade management systems, a fact that will leave the region open to becoming a hub for WMD proliferation. Based on a review of export statistics, industry projections, and discussions with regional industry experts, a number of key sectors can be identified as particularly challenging: oil and gas, chemicals, aerospace, nuclear energy, electronics, and automobile manufacturing. Other emerging trends like additive manufacturing and the growth of online marketplaces will also impact the ability of the region to manage dual-use commodities. Having a better understanding of how growth in dual-use commodities will progress in the near-term can assist regional leaders and international partners in focusing their attention and limited resources most effectively. Improving regulations and control lists is only one part of the way forward. Creating outreach strategies that fully engage key industries will also play an important role in stemming the illicit spread of sensitive dual-use items from the growing economies of the region.

Keywords

Nonproliferation, export control, strategic trade control, Southeast Asia, weapons of mass destruction

Introduction

Southeast Asian nations are already an essential part of the global trade system. The Association of Southeast Asian Nations (ASEAN) members have a total trade volume of $2.5 trillion in 2014, and about 80 million twenty-foot equivalent units (TEUs)—or 15 percent of total ocean-going containers—pass through ASEAN

[1] Stephanie Lieggi is a research associate at Middlebury Institute's James Martin Center for Nonproliferation Studies. This article results from research supported by the Naval Postgraduate School's Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC) via Assistance Grant/Agreement No. N00244-15-1-0002 awarded by the NAVSUP Fleet Logistics Center San Diego (NAVSUP FLC San Diego). However, the views expressed in this article are those of the author and do not necessarily reflect the official policies of the Naval Postgraduate School. The author would like to thank PASCC for their support for this research as well as Ms. Catherine Dill, CNS Research Associate, for her indispensable assistance with compiling and analyzing the trade statistics used for this article, and Ms Diana Lee, former CNS Graduate Research Assistance, for early assistance with compiling industry projections.

ports annually.[2] The growth rates for the fastest developing economies in the region are expected to average about five percent a year into the next decade. As the economies in the region grow and increase in complexity, Southeast Asian states will play a larger role in the development and trade of sensitive, high-tech commodities—both as customers and manufacturers. The increased prominence of these dual-use commodities in the region points to a need for a strengthened security framework to prevent possible proliferation of sensitive materials to programs, by both state and non-state actors, aimed at developing weapons of mass destruction (WMD).

Concerns about Southeast Asia's place in WMD-related trafficking efforts are not new. Countries in ASEAN have previously been used as both transshipment conduits and manufacturing hubs for WMD trafficking networks. Most notoriously, the nuclear smuggling network of A.Q. Khan employed Southeast Asia-based firms to manufacture centrifuge parts for Libya's nuclear weapons program and utilized ports in the region to transship sensitive commodities. Apart from the Khan network, illicit procurement efforts by Iran and North Korea have used Southeast Asian entities and ports to obtain sensitive dual-use commodities. In many of these transfers, manufacturing firms specializing in sectors such as oil and gas have inadvertently sold dual-use materials to suspect end-users. As the region's capacity to manufacture and export dual-use commodities increases in the coming years, it is more likely that incidents like these will grow in frequency and that the harm they inflict on international security will be more severe. Until very recently, many governments in Southeast Asia did not see a need to focus much attention on the management of dual-use commodities. For many officials, proliferation sensitive technologies were not seen as widely available in the region and controls on trade would therefore be an unnecessary burden on economic development. This notion is now being challenged by the known cases of proliferation activity and the increased manufacturing of dual-use commodities by ASEAN-based firms.

In the last few years, a growing number of countries in ASEAN have paid more attention to the issue of proliferation of dual-use commodities. Singapore was the earliest adopter of a strategic trade management system, followed by Malaysia in 2010. In the Philippines, President Benigno Aquino signed into law the Strategic Trade Management Act (STMA) in November 2015.[3] Thailand is also on the path to having its first regulation of dual-use exports, although the timeline remains unclear. However, many countries in the region—even those noted above—still lack a full understanding of the number and types of domestic industries likely to be using or manufacturing dual-use commodities.

Both regulatory authorities and domestic industries in ASEAN remain unaware of the extent to which locally-based firms can contribute to the proliferation of WMD-related programs. In part this is due to the rapid growth in industries new to the region where proliferation sensitive items are major components for manufacturing and production. These industries include the oil and gas sector, chemical, aerospace, energy (particularly nuclear), electronics, and automobile manufacturing. The management of proliferation sensitive technologies in Southeast Asia is likely to be further challenged by the recent advent of disruptive technologies that traditional supplier countries are still grappling with controlling, like additive manufacturing. All this is made more complicated by the growing popularity of online marketplaces in the region, and the extent to which these portals are able to quickly facilitate exports of proliferation sensitive dual-use commodities from smaller firms less cognizant of the need to control these items.

Using industry projections and export statistics, as well as discussions with regional experts, it is possible to identify likely industries and high-tech sectors in the region that will pose a challenge to strategic trade

[2] Total numbers based on data from: "Table 17 ASEAN Trade, 2013-2014," ASEAN External Trade Statistics, <http://www.asean.org/images/2015/July/external_trade_statistic/table17_asof17June15.pdf>; and "Container Port Traffic," World Bank, <http://data.worldbank.org/indicator/IS.SHP.GOOD.TU>.

[3] Charmie Joy Pagulong, "Noy Signs Law vs. Weapons of Mass Destruction," *Philippine Star,* November 18, 2015. For the full text of the law, see <http://www.gov.ph/2015/11/13/republic-act-no-10697/>.

management and nonproliferation efforts in the next five to ten years. For this research, the author looked mainly at trade and industry data pertaining to the five fastest growing ASEAN economies (based on GDP growth rates)—Indonesia, Malaysia, the Philippines, Thailand, and Vietnam. Singapore, with a GDP per capita significantly higher than its neighbors, has the most mature trade management system. Considering Singapore's unique status in the region—having both established industry sectors with significant dual-use capabilities as well as a relatively advanced trade control system—the author excluded it from the review of projections and export data. Likewise, although Brunei Darussalam has the second highest GDP per capita in ASEAN, its economic complexity ranking falls well below that of its ASEAN neighbors.[4] Brunei's lack of economic complexity is largely due to its complete reliance on oil exports to support its economy.[5] Although the development of dual-use technology in Brunei remains a possibility, its prospects are more akin to the slower growing countries—Cambodia, Lao DPR, and Myanmar—over the next decade.

As is true in traditional supplier countries, including the US, Japan and the EU, Southeast Asian states have to meet the challenge of managing the trade of dual-use commodities with limited resources shared between competing interests. With an improved understanding of how dual-use growth will progress in the near-term, regional leaders and their international partners should be able to focus these limited resources on the most critical sector. With the key industries identified, regional authorities can structure their systems to meet the challenges created by these new and developing sectors. Improving regulations and control lists should be only one part of the way forward. Creating outreach strategies that fully engage the most relevant industries will also play an important role in stemming the illicit spread of sensitive dual-use commodities in the region.

Prospects for ASEAN's Economic and Technological Development

Although growth in ASEAN's top economies can fluctuate from year to year, the overall growth predicted over the next decade is expected to be positive. ASEAN as whole has been the second fastest growing economy in Asia (after China), having seen GDP growth of 300 percent between 2001 and 2013.[6] The ASEAN-6—Singapore, Malaysia, Indonesia, Thailand, the Philippines, Vietnam—have had an average rate of six percent growth over the last five years; similar rates are expected to continue into at least the next five years. This consistent growth is expected to foster technological expansion and sophistication. Based on recent export statistics and discussions with regional experts, it is clear that as these countries develop technologically, the volume of dual-use commodities available in the region will likewise increase.[7]

The entry of more multinational corporations and expansion of foreign direct investment have already increased the level of sophistication in many industrial sectors. ASEAN, particularly the top growth economies, is attractive to many foreign firms due to the presence of a strong manufacturing base and a labor market that is more affordable than other developed Asian countries. Increased interest from outside investors will only speed up the dual-use capabilities throughout the region. Although specific data on the introduction of dual-use technology is hard to identify, anecdotal evidence based on discussion with regional experts indicates that large multinational firms have already created manufacturing hubs in the region for controlled dual-use commodities.[8]

---

[4] The economic complexity index (ECI) measures the diversity of a country's exports – which is typically an indicator of positive economic development in the near future. According to *The Atlas on Economic Complexity,* <http://atlas.cid.harvard.edu/>, Brunei's ECI is -2.543563, whereas in comparison Myanmar's ECI is -1.167571, Thailand's is 0.9931926, and Singapore's is 1.613748.

[5] In 2013, 96 percent of Brunei's exports were petroleum products. See *The Atlas on Economic Complexity,* <http://atlas.cid.harvard.edu/>.

[6] GDP growth rates as calculated by the East-West Center's "Asia Matters For America" site, <http://www.asiamattersforamerica.org/asean/data/gdppercapita>.

[7] Discussions with regional experts at CNS sponsored roundtable discussion "Forecasting Industrial Development & Dual-Use Capabilities in Southeast Asia," September 29, 2015; report forthcoming.

[8] For example, a representative of General Electric working on trade compliance issues in the region noted that GE had facilities

The expansion of both domestic and export markets help explain the strength of ASEAN's economic development, and both will likely promote similar growth in the future. ASEAN is the world's third largest market, based on total population, and the fourth largest exporting region. The economic focus of regional leaders continues to be the full establishment of the ASEAN Economic Community, and related efforts like creation of the ASEAN Single Window, which aims to integrate regional customs agencies and further streamline intra-ASEAN trade.[9] If ASEAN economic integration continues smoothly, the increased ability to trade, invest and move technology across the region is expected to further improve growth throughout the region. Although including the concept of dual-use trade management into these integration efforts has been discussed, it remains a minor part of the overall integration efforts in the region.

It should be noted that many analysts remain skeptical about how much integration will actually occur over the next decade.[10] The wide disparity in development between the ten ASEAN states remains a major challenge for creating a true open market, and institutional weakness is likely to continue to slow economic progress for many countries. However, the fastest growing economies are likely to meet integration goals sooner, spurring further development of high-tech industries in the ASEAN-6 countries in the near to mid-term.

Projected Growth in Dual-Use Sectors

Based on current industry projections and discussions with regional experts, proliferation sensitive sectors expected to grow over the next decade include: oil and gas, chemical, aerospace, nuclear energy, automotive manufacturing, defense products and electronics. In reviewing existing trade data—specifically export statistics from the UN Comtrade database—the growth in many of these sectors over the last five years is clear. Although this data can fluctuate in reliability, and therefore cannot be taken by itself as proof of potential growth, the generally positive correlation with industry projections and the views of regional experts helps provide some validation of the author's forecasts with regard to these dual-use industries.

Another area of proliferation concern is the expected rapid adoption of additive manufacturing technology—commonly referred to as 3-D printing. Although Singapore is currently the main regional driver for this type of disruptive technology, the relevant know-how and equipment is expected to spread relatively quickly throughout the region. The increasing popularity of online marketplaces in the top growing economies in the region is also likely to have an impact on the ability to manage dual-use trade in ASEAN states.[11] The potential influence of these two emerging issues will be reviewed separately at the end of this section.

In order to reconfirm whether these growth industries could produce sensitive dual-use commodities in the region, CNS analyzed available UN Comtrade data on exports of certain categories of items frequently used in these industries. To get a rough estimate of the volume of currently traded proliferation sensitive goods, we analyzed the export of certain categories of items based on their Harmonized System (HS) Code from the selected five countries over the last five years of available data (2009-2014) to chart the overall growth in production. The HS Code system was developed by the World Customs Organization (WCO) and its member states to uniformly categorize commodities traded internationally. HS Code include 5,000

---

in both Singapore and Indonesia for the manufacture of controlled nickel-alloy clad valves. These valves were specifically intended for oil and gas drilling operations. Discussions at CNS sponsored roundtable discussion "Forecasting Industrial Development & Dual-Use Capabilities in Southeast Asia," September 29, 2015; report forthcoming.

[9] For more on the ASEAN Economic Community, see "ASEAN Economic Community: 12 Things to Know," on the Asian Development Bank website <http://www.adb.org/features/asean-economic-community-12-things-know>. For details on the ASEAN Single Window, see the ASW's official website at <http://asw.asean.org/>.

[10] See D. Pilling, "The Fiction of a Unified South-East Asia," *Australian Financial Review*, December 11, 2015; and Sanchita Basu Das, "The ASEAN Economic Community: A Work in Progress," *The Diplomat*, May 23, 2015, <http://thediplomat.com/2015/05/the-asean-economic-community-a-work-in-progress/>.

[11] Discussions at CNS sponsored roundtable discussion "Forecasting Industrial Development & Dual-Use Capabilities in Southeast Asia," September 29, 2015; report forthcoming.

commodity groups organized in a hierarchy of chapters (two digits), headings (four digits), and subheadings (six digits). Some countries have gone beyond the six digits, having codes that might go to eight or ten digits in order to describe commodities in more detail.[12]

*Table: HS Codes With Likely Dual-Use Implications**

Chapters	Description of Categories of Items
28	Inorganic chemicals; organic or inorganic compounds of precious metals, of rare-earth metals, of radioactive elements or isotopes
29	Organic Chemicals
38	Miscellaneous chemical products
70	Glass and glassware
73	Articles of iron and steel
75	Nickel and articles thereof
76	Aluminum and articles thereof
84	Nuclear reactors, boilers, machinery and mechanical appliances; parts thereof
85	Electrical machinery and equipment and parts thereof; sound recorders and reproducers, television image and sound recorders and reproducers, and parts and accessories of such articles
88	Aircraft, spacecraft, and parts thereof
90	Optical, photographic, cinematographic, measuring, checking, precision, medical or surgical instruments and apparatus; parts and accessories thereof
96	Miscellaneous manufactured articles

*The survey included numerous headings and subheading under each chapter listed that are likely to include dual-use items. Full list of headings and subheadings can be found in the appendix of this article.

The analysis of the data saw a steady, if not always rapid, growth in many categories with potentially proliferation sensitive commodities. Although this result appears to bolster the validity of the analysis based on other data used in our forecasts, it is important to note a number of caveats on the data set we used. Firstly, Comtrade data can be unreliable as countries use different levels of quality control when preparing these statistics and dependability of reporting varies from country to country. Sometimes adjustments need to be made to deal with discrepancies or anomalies. For instance, as this data was being compiled, Vietnam had not yet published statistics for 2014. To deal with this discrepancy, we used Vietnam's 2013 numbers as a proxy for 2014 to get a reasonable estimate of overall growth in the different sectors reviewed.

A second problem with the data set is that the use of HS Codes to identify likely dual-use commodities being traded is still more art than science. Our judgement on which HS headings (four digits) and subheadings (six digits) to analyze in this research was based on previous work done by CNS experts, as well as experts at King's College London, in correlating HS codes with dual-use control lists. The EU's Joint Research Center has also published work on the correlation of HS codes to dual-use controls, which were very helpful for this analysis.[13] Although the four and six digit specifications do allow for some refinement identifying possible dual-use commodities, none of the correlations to proliferation sensitive commodities are perfect and much work is needed to improve the predictive nature of HS codes when looking for controlled commodities. Keeping in mind both the issue of reliability of the Comtrade data and the unprecise nature of the HS code correlation, the ultimate results of this data analysis are an approximation of growth and a proxy of expected

[12] A useful breakdown of the structure of the HS Codes and relevant nomenclature can be found in Appendix 2 of C. Versino, "Dual-use Trade Figures and How they Combine, 2015," European Commission Joint Research Centre, <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97664/2015.11.19.economicrelevancedualuse_online_version.pdf>.

[13] C. Versino, "Dual-use Trade Figures and How they Combine, 2015," European Commission Joint Research Centre, <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97664/2015.11.19.economicrelevancedualuse_online_version.pdf>.

progress in the future.

Oil and Gas Sector:

Industries in Southeast Asia related to the oil and gas sector—such as drilling, production, refining, and petrochemicals—are expected to grow, albeit at slower rates than the previous decade, and gain market share over the next decade. While earlier growth was largely tied to investment from foreign companies and joint ventures, growth in the near future is likely to be centered on investments and technical development of local oil companies.[14]

The commodities required for the oil and gas sector can have significant dual-use implications and industries manufacturing for this sector have been previously duped by traffickers' claims that the items would be used for oil and gas production. Categories of commodities that industry experts see as being proliferation sensitive are numerous and include items like:

- Pumps and valves (usable in chemical weapons and nuclear weapons development)
- Specialized lubricants and other chemicals (relevant to chemical weapons development);
- Gyros and guidance systems (used installing pipelines, for instance, but can also be useful in missile development); and
- Drilling equipment including piping (usable in various WMD, particularly nuclear and missile development.)

In the case of the A.Q. Khan network, the Malaysian company Scomi Precision Engineering (SCOPE) manufactured numerous different components including casings, molecular pumps, crash rings, stationary tubes, clamp holders, and flanges. The employees of SCOPE believed the items they were producing were for oil & gas production.[15] Instead, they were used to finish the assembly of centrifuges meant for Libya's uranium enrichment program.

Of the top five growth economies, Malaysia had the most significant increase in the oil and gas sector over the last few years, with foreign investment playing a major role in this growth. Malaysian companies are focusing significant attention on developing liquefied natural gas (LNG) resources. In 2015, Malaysia was the world's second largest exporter of LNG.[16] Petroleum related business accounts for about 20 percent of all government revenue, meaning fluctuations in oil prices can be particularly troubling for country's national budget.[17]

Indonesia is the region's largest oil producer, ranking 20th in the world.[18] However, the country's oil production has slowed over the past few years and some projections point to a decline beginning in 2017. The decline is in part linked to the lack of regulatory reform in the oil and gas sector, which is heavily controlled by Indonesian state entities, as well as a lack of infrastructure improvements that hinder improvements in production capacity. Despite this less than positive outlook, industry analysts note that Indonesia has significant "below-ground potential" which could lead to increase in production if the "business environment

---

[14] Business Monitor International, "Industry Trend Analysis - Weak Oil Prices Will Hit Region's Long-Term O&G Production," September 23, 2015, <https://bmo.bmiresearch.com/article/view?article=1101613&iso=%2BA>.

[15] Kenley Butler, "How the Abdul Qadeer Khan Network Circumvented Export Controls," *Asian Export Control Observer*, April/May 2005, <https://www.nonproliferation.org/wp-content/themes/pitch_premium/pdfs/aeco_0504.pdf>.

[16] Business Monitor International, "Industry Trend Analysis - Australian LNG To Erode Malaysia's Market Share," August 27, 2015.

[17] Economist Intelligence Unit, "Country Report: Malaysia," August 2015, <www.eiu.com>.

[18] "Oil and Gas in Indonesia," PwC Indonesia, May 2014, <http://www.pwc.com/id/en/publications/assets/oil_and_gas_guide_2014.pdf>.

improves."[19]

Thailand is the primary oil refiner in the region and is investing heavily in domestic exploration as well as exploration in other countries like Myanmar.[20] However, foreign investment, which is likely needed to expand domestic capacity further, has been hampered by regulatory delays and an uncertain political situation. Gas production has been on the decline over the last few years is likely to continue in that direction in the near future.[21]

Of the five countries surveyed, the Vietnam and the Philippines had the least active oil and gas sectors. The Philippines is a major consumer of oil and gas from its neighbors, receiving almost its entire supply of refined petroleum products from Asia – including about 25 percent from other ASEAN countries.[22] Likewise, Vietnam's oil and gas production has been on the decline in recent years in spite of marked increases in domestic consumption. Vietnam's oil and gas sector is dominated by state-owned Petro Vietnam, which has been seen as a barrier to foreign investment. On the upside, Vietnam is pushing forward with off-shore exploration efforts, despite maritime disputes in the South China Sea.

Although the prospects for consistent growth in this sector are tenuous for ASEAN's top growth economies, most analysts see it remaining as a major area of investment and economic productivity in the region. While production may slow, it is not expected to decline rapidly in the next decade. Additionally, the level of domestic investment placed by all five states surveyed into the oil and gas sector means that the sector will likely continue to play a major role in increasing the presence of dual-use commodities in the year to come, particularly in the manufacturing firms aimed at servicing this sector. This growth in manufacturing will further increase prevalence, as well as indigenous development, of dual-use equipment such as precision machine tools that are also crucial for development of WMD and missile programs.

Chemical Industry

The growth of the chemical industry in the region is in part associated with the growth of the oil and gas sector, as much of the chemical manufacturing taking place is related to petrochemicals. However manufacturing in other sectors, including plastics and basic chemicals, is also on the rise.[23] When looking at export statistics from UN Comtrade, the HS chapters related to controlled and other sensitive chemicals have grown at a relatively steady rate since 2008. These HS chapters include commodities—both chemicals and related equipment—that are controlled for nonproliferation purposes either by the Chemical Weapons Convention or the Australia Group.[24]

Of the five economies surveyed, regional expert saw Malaysia and Thailand as the fastest growing chemical industries, although Indonesia was also expanding rapidly.[25] As the production of the most proliferation

---

[19] Business Monitor International, "BMI Industry View - Indonesia - Q4 2015," August 15, 2015, <https://bmo.bmiresearch.com/article/view?article=1086719&iso=ID>.

[20] "Thailand Economy: Thai Businesses Spread their Wings," Economist Intelligence Unit, 2015.

[21] "BMI Industry View - Thailand - Q1 2016," November 20 2015, <https://bmo.bmiresearch.com.proxy.miis.edu/sar/reports/view?issue=20160101&productid=148>.

[22] See "Where did the Philippines Import Petroleum Oils, Refined from in 2013?," <http://atlas.cid.harvard.edu/explore/tree_map/import/phl/show/2710/2013/>.

[23] "Basic chemicals" are produced in large quantities for industrial needs and are traded within the chemical industry before becoming a final product for the general consumer. See definition at *The Essential Chemical Industry Online*, <http://www.essentialchemicalindustry.org/chemicals.html>. Some basic chemicals are controlled under the Australia Group and/or the Chemical Weapons Convention (CWC) Schedule 3.

[24] The CWC is the multilateral treaty which bans the development and use of chemical weapons. The Australia Group is the multilateral export control regime that focuses on chemical and biological related materials. Both the CWC and AG have lists of items that should be subject to trade controls for nonproliferation reasons. All ASEAN members are also parties to the CWC; a number of ASEAN members, particularly Singapore and Malaysia, also include AG lists in their controls.

[25] Discussions at CNS sponsored roundtable discussion "Forecasting Industrial Development & Dual-Use Capabilities in

sensitive chemicals are controlled by the Chemical Weapons Convention (CWC), of which all ASEAN states are members, a number of industries in the region are already aware of the need to control those commodities. However, many small and medium size enterprises (SMEs) in the region, including in the top growing countries, are less cognizant of the potential security impact of their products. Additionally, many companies remain unfamiliar with controls on dual-use equipment, which although covered by the Australia Group is not covered by the more universally accepted CWC.

For Malaysia, the largest chemical producer in ASEAN, chemicals and related commodities comprise the second largest share of manufactured exports. As noted by Malaysia's trade promotion agency, the chemical industry is directly linked to other key sectors in the economy, including automotive, electronics, pharmaceutical and construction.[26] The petrochemical industry in Malaysia in particular is expanding with new facilities being added by both domestic and international chemical firms.[27] Other parts of Malaysia's chemical industry are also expanding, including in the manufacture of plastics, industrial gases, and specialty chemicals.[28] All of these sectors include not only chemicals that are dual-use in nature, like phosgene or perfluoroisobutene (PFIB), but also require use of specialized equipment needed for CW and other WMD programs, including reaction vessels and distillation columns.[29]

As the primary oil refiner in the region along with an extensive petrochemical industry, Thailand is the second largest chemical producer in ASEAN. The country has increased the export of chemicals and the petrochemical industry has increased the capacity to produce polymers and olefins. Domestic consumption of polymers, which have potential dual-use characteristics, are also expected to increase over the next five years.[30]

Indonesia's chemical industry ranks third behind Malaysia and Thailand in size. However, the government sees the chemical industry as an important area for increased investment. To attract foreign and domestic investment in this sector, it has offered tax incentives and strengthening the chemical manufacturing sector is part of the government's overall industrialization strategy. Indonesia's domestic chemical industry currently includes manufacturers of petrochemical, inorganics, and agrochemicals. As with Malaysia and Thailand, Indonesia's manufacturing is dominated by petrochemicals, although industry experts expect other sectors to grow in the near term. Indonesian experts specifically noted agrochemicals as an area of growth where dual-use chemicals were likely to be used or produced.[31]

Chemical-related commodities make up about three percent of exports from the Philippines, a significantly smaller share than ASEAN's top chemical producers.[32] Philippine manufacturing of basic chemicals is on the increase, however, as is output of chemicals related to plastic and rubber production.[33] Recent production of polymers is also on the increase, spurred on by industries like automotive parts manufacturing. However,

---

Southeast Asia," September 29, 2015; report forthcoming.

[26] "Chemicals & Chemical Products," Chemical Unit, Trade and Services Promotion Division, MATRADE website, <http://www.matrade.gov.my/en/foriegn-buyers-section/69-industry-write-up--products/519-chemicals-a-chemical-products>.

[27] Business Monitor International, "BMI Industry View - Malaysia – 2016," November 24, 2015.

[28] Foo, Dominic C Y, P.E., Ceng, "The Malaysian Chemicals Industry: From Commodities to Manufacturing," *Chemical Engineering Progress*, November 2015.

[29] Phosgene is used to make plastics and pesticides, but is also a precursor for chemical weapons and controlled under the CWC and the Australia Group. The industrial gas PFIB is similarly controlled as it is a choking agent; in industry it is widely used in semi-conductor manufacturing and is a byproduct in the production of Teflon. Equipment like reaction vessels and distillations columns is critical to development of these and many other chemicals. Many of them are also controlled under the Australia Group due to their use in the development of chemical weapons.

[30] Business Monitor International, "Industry Trends And Developments - Thailand - Q1 2016 – Petrochemicals," November 25, 2015.

[31] Discussions at CNS sponsored roundtable discussion "Forecasting Industrial Development & Dual-Use Capabilities in Southeast Asia," September 29, 2015; report forthcoming.

[32] Based on 2013 statistics available from *The Atlas of Economic Complexity,* <http://atlas.cid.harvard.edu/>.

[33] Business Monitor International, "Industry Forecast - Philippines - Q4 2015," September 11, 2015.

analysts feel that Philippine capabilities in polymers are underutilized, which may slow growth in the industry overall.[34]

Vietnam's chemical industry remains small in comparison to other sectors in the country, but recent projections show a potential annual growth rate of six percent. With a new refinery coming online by 2017, operated by Nghi Son Refinery & Petrochemical and Vung Ro Petroleum, Vietnam's petrochemical capacity is expected to significantly increase. With this increase, Vietnam could become a self-sufficient producer of many basic chemicals, although there are also fears that Vietnam's progress might result in an overproduction in the region.[35] Although chemical-related commodities hover about six percent of the total exports, the government recently approved restructuring plans for the industry that aims specifically at increasing exports in this sector and modernizing Vietnam's chemical manufacturing.[36]

Aerospace

Beginning in the late 2000s, leading multinational companies began working with aircraft maintenance and aerospace-related manufacturing industries in a number of Southeast Asian states. Boeing, for instance, began sourcing some of its spare parts, assembly and maintenance services from manufacturing centers in the ASEAN-6 economies. The Asia Pacific region is set to be the largest market for new commercial aircraft with orders expected to reach 12,820 units by 2032.[37] Much of that production will likely be sourced locally by multinational firms relying on regionally based suppliers.

Dual-use commodities are ubiquitous in the aerospace industry. Common components from civilian aircraft manufacturing can also be used in military programs, particularly missile related development. The precision equipment needed for manufacturing is also dual-use in nature, and can be used for both missile and nuclear programs. Even maintenance and assembly services, the least specialized of the sub-sectors found in ASEAN, require equipment and engineering capabilities that could contribute to ballistic missile development. As domestic firms become more integrated into the global aerospace supply chain, they will require more precision equipment that until recently has been largely in the hands of traditional suppliers.

Thailand has offered significant incentives to help foster its aerospace industry, including exemptions on import duties and corporate tax exemptions.[38] Rolls Royce works with a number of Thai companies to supply parts and according to a recent interview with a top Rolls Royce executive, Thailand's "strong industrial foundation, good airports and skilled labor" play a major role in the country's success.[39] The draw of Thailand for aerospace related production is also based on its long-standing reputation as a central airplane maintenance center.

Similar to Thailand, Malaysia has offered incentives and provided a good infrastructure for aerospace firms to invest. Malaysia's aerospace manufacturing capabilities are also likely to benefit from its investment in military aircraft from Boeing. As part of that deal, Malaysia expects to be able to "spin-off" technologies to the civilian aviation sector. Malaysia expects these types of projects to allow them to gain access to

---

[34] Business Monitor International, "Philippines Petrochemicals Report," *Philippines Petrochemicals Quarterly*, January 2016.

[35] Business Monitor International, "Industry Forecast - Refining - Vietnam - Q1 2016," November 24, 2015, <https://bmo.bmiresearch.com/article/view?article=1071170&advanced_search=1&matches=6983&page=2&position=4&keyword=southeast%20asia>.

[36] "Vietnam: Chemical Sector Restructuring to Boost Exports," *Asia News Monitor*, October 7, 2015.

[37] "Aerospace," Malaysian Investment Development Authority, <http://www.mida.gov.my/home/aerospace/posts/>.

[38] "Aerospace Industry," Thailand Board of Investment North America, <http://www.thinkasiainvestthailand.com/web/en-investment-opportunity.php?id=2>.

[39] See "ASEAN Aerospace gets Global & National Level Push; Boeing & Rolls Royce Spur Know How," <https://aseaneconomist.wordpress.com/2013/01/03/asean-aerospace-gets-global-national-level-push-boeing-rolls-royce-spurs-development-of-local-knowhow/>.

specialized aerospace technologies.[40] Malaysia is already a hub for assembling aerospace components and includes manufacturing repair and overhaul (MRO) activities, as well as design and development.[41]

The Indonesia's aerospace industry received a significant boost when PT Dirgantara Indonesia (PTDI) won an Airbus contract to supply wing parts for the A380 airliner.[42] More recently, in early 2015, Airbus announced plans to shift its production and assembly of the C295 military transport aircraft to West Java capital Bandung from its existing factory in Spain. A recent deal with Indonesian based RAI, which has ties to the family of former President Habibie, will see PTDI design and build an indigenous aircraft.

Vietnam has a number of projects with Boeing and Airbus aimed at increasing their capacity in aerospace manufacturing but the progress is slower than many of its neighbors. The Philippines has so far been the least successful in the aerospace sector in comparison with the other top five growing states in ASEAN; however, Manila is expecting some growth in the aerospace sector over the next decade. Aerospace accounted for just 0.15 percent of Philippine GDP in 2013 but the government expects a modest rise to 0.57 percent by 2020.[43]

Nuclear Energy

The top growing economies in ASEAN have all shown some interest in nuclear energy, although the plans and capabilities of Vietnam and Indonesia are more concrete than the other three countries reviewed here. The ASEAN states most interested in nuclear power are working closely with international nuclear suppliers and any transfer of equipment and technology will likely require IAEA safeguards, making diversion less likely. However, as these projects develop, the components and equipment that are needed to service the construction and operation of the imported reactors will require some level of indigenous industry involvement. As such, companies in the region may begin to manufacture components and parts for nuclear facilities in the near to mid-term, including dual-use components such as valves, pumps and piping. These firms could therefore potentially become suppliers of dual-use nuclear materials to illicit WMD networks outside the region.

Within ASEAN, Vietnam appears to be the fastest growing with four reactors planned, the first expected to go on line by 2025. Vietnam is working with numerous nuclear suppliers to complete its planned reactors, particularly with firms in Japan and Russia.[44] In early 2014, the Vietnam-based Doosan Vina was certified by the American Society of Mechanical Engineers (ASME) to manufacture certain equipment for nuclear power plants. Doosan Vina, the Vietnamese arm of a large South Korean manufacturing company, was the first firm in Southeast Asia to get this type of accreditation which signifies that the company's quality assurance programs meet the high levels required for products used by nuclear industry.[45]

In Indonesia, domestic interest in nuclear energy is mixed, but even with some popular push back based on environmental, safety and security concerns, nuclear authorities are intent on development of civilian nuclear capabilities. The National Nuclear Energy Agency of Indonesia, generally referred to by its Indonesian acronym BATAN, operates three research reactors. These facilities are used to support the development of

---

[40] Mikhail Raj Abdullah, "Boeing's Partnership In Malaysia To Have Substantial Spin-offs In Transforming Aerospace Sector," *Bernama*, October 12, 2012, <http://aviation.bernama.com/news.php?id=701412&lang=en>.

[41] "Aerospace," Malaysian Investment Development Authority (MIDA), 2015, <http://www.mida.gov.my/home/aerospace/posts/>.

[42] "On a Wing and a Prayer," *Economist,* February 15, 2014, <http://www.economist.com/news/business/21596589-state-aerospace-firm-risks-forgetting-lessons-asian-crisis-wing-and-prayer>.

[43] "Aerospace," Philippine Department of Trade and Industry website, <http://industry.gov.ph/industry/aerospace/>.

[44] "Nuclear Power in Vietnam," World Nuclear Association website, October 2015, <http://www.world-nuclear.org/info/Country-Profiles/Countries-T-Z/Vietnam/>.

[45] "Doosan Vina Celebrates N-Stamp," *World Nuclear News*, April 3, 2014, <http://www.world-nuclear-news.org/C-Doosan-Vina-celebrates-N-stamp-0304147.html>.

nuclear energy in the country as well as the production of medical and industrial radioisotopes. Indonesia's nuclear authorities also have facilities focusing on fuel fabrication at a laboratory scale.

Malaysia appears interested in nuclear energy, but its efforts remain in the planning stages. In 2014, Malaysia announced its desire to develop nuclear energy by 2025 and have three to four reactors providing about 15 percent of the nation's electricity by 2030. Although that timeline is likely to slip, the Malaysia Nuclear Power Corporation (MNPC) appears to be moving forward with plans, including having discussions with foreign reactor suppliers, despite continuing public concerns about the safety of nuclear power.[46]

Thailand is not strongly committed to developing nuclear power in the near term, although officials have stated that nuclear energy needs to be considered in the long run if the country is going to move away from fossil fuels. Thailand's interest in nuclear energy was significantly impacted by the Fukushima crisis; the government reacted by delaying the potential start date of construction of a nuclear power plant until 2026.[47] The Philippines has also shown little consistent interest in renewing a nuclear power program, although the country's Department of Energy noted a plan to look into reinstating the mothballed Bataan nuclear plant that was built in the 1980s but never went online.

Defense Products

The global "Revolution in Military Affairs" that began in the early 1990s has also influenced defense and economic developments in ASEAN. The purposeful merging of military and industrial applications within defense development has become increasingly common within ASEAN, particularly in Singapore, Malaysia and Indonesia where indigenous investment in military technology is significant. This method is seen as increasing efficiencies and assuring that investments in defense industries payoff on the commercial side as well. The "spinning off" of military into commercial sectors is prominent in aviation and electronic sectors in particular, however, numerous other high-tech sectors benefit from investment in the defense sector. Many actors in the region see investment in indigenous capabilities as more lucrative and sustainable if military technologies can be directly spun off to commercial projects.[48]

Of the five economies reviewed here, Indonesia has shown the most interest in spinning off defense developments into the commercial sector. In an effort to modernize its military, Indonesia is expected to double its defense budget in the next year, with some of the increased procurement focusing on local industries, although imports and foreign partnerships will still be required to further modernization efforts. Indonesia's three domestic defense producers have been developing products for export to other countries in the region.[49] Although much of the current effort remains strictly focused on military products, defense firms like PT Dirgantara Indonesia—which focuses on aerospace manufacturing—develops and manufactures both civilian and military aircraft.

While the defense manufacturing sector in Malaysia remains small, it is showing signs of growth. Local firms are increasing their technological capacities under cooperative arrangements and joint ventures with foreign firms which have resulted in increased indigenous production of various defense items including unmanned aerial vehicles (UAVs). Slow growth is expected through the end of this decade as the defense industrial base remains nascent. However, the Malaysian government is looking to invest heavily in its defense industry, partially in hopes of improving overall manufacturing and product development

[46] Sheridan Mahavera, "Malaysia's Nuclear Power Plant Not a Done Deal, Says Atomic Power Body," *Malaysian Insider,* May 19, 2015, <http://www.themalaysianinsider.com/malaysia/article/malaysias-nuclear-power-plant-not-a-done-deal-says-atomic-power-body>.

[47] Business Monitor International, "Industry Forecast - Energy & Utilities Infrastructure - Q1 2016," November 2015.

[48] Presentation by Ms. Curie Maharanie, BINUS University, Jakarta, September 2015, at CNS sponsored roundtable discussion "Forecasting Industrial Development & Dual-Use Capabilities in Southeast Asia," September 29, 2015.

[49] Business Monitor International, "Indonesia Defence & Security Report 2015," October 2015.

capabilities.[50]

Electronics

Regional experts point to the electronics sector as a significant area of expected growth in the years to come.[51] The electronics industry is already quite substantial in the fastest growing economies in ASEAN, but their growth and sophistication is expected to increase over the next decade. ASEAN manufactures a significant amount of the world's consumer electronics including 80 percent of the world's hard drives.[52] The strength of ASEAN in this sector is largely due to the region's relatively lower manufacturing costs and positive financial incentives offered by governments.[53] Throughout the region, multinationals have set-up manufacturing facilities for a number of consumer electronics. The transfer of technology occurring in this process is improving overall manufacturing capacity in the region. Local firms are likely to acquire more dual-use commodities to further advance the region's electronics sector, including production equipment, like isostatic presses, and testing equipment, like oscilloscopes, frequency changers and mass spectrometers. Likewise as local firms take on more advanced manufacturing, the electronics they produce will have increased dual-use implications, particularly commodities like microprocessors, capacitors, and spark gaps.

In Malaysia, the electronics industry accounts for about 25 percent of manufacturing output and 33 percent of total exports. Malaysia has shown particular strength in the hardware and semiconductor sector, although appears to be slipping in strength in the electronics and electrical services sector.[54] The Malaysian government has identified the electronics sector as one of the National Key Economic Areas (NKEAs) "to help the country to attain high-income status by 2020."

Thailand is a major electronics exporter and is an important global source of components for hard drives and circuit boards. Numerous multinational companies, including Samsung, LG, Toshiba and Sharp, have a manufacturing presence in Thailand, lured by the lower average wages and government tax incentives. Although multinationals have dominated until now, domestic companies, like Hana Microelectronics, are beginning to have a foothold.[55] The electronics sector currently accounts for about 15 percent of Thailand's export market. Some analysts fear that the Thai electronics market is losing market share to even lower wage countries in the region. In an effort to maintain the lucrative export market, Thailand-based firms are looking at producing more advanced electronics like converters for hybrid cars.[56]

As noted above, the lower wage countries of Indonesia, Vietnam and the Philippines are seeing increased opportunities to grow in this sector as manufacturing and assembly plants are relocated from China and elsewhere.[57] Industry analysts predict a five percent annual growth rate in electronics manufacturing in Indonesia, while Vietnam and the Philippines will see even faster growth at 7.5 percent.[58]
Although Thailand and Malaysia are expected to be priced out of some of the consumer electronics market,

---

[50] Business Monitor International, "Market Overview - Malaysia – 2015," November 2015.

[51] Discussion with regional experts at CNS sponsored roundtable discussion "Forecasting Industrial Development & Dual-Use Capabilities in Southeast Asia," September 29, 2015.

[52] "Electronics," Invest in ASEAN website, <http://investasean.asean.org/index.php/page/view/electronics>.

[53] Kan Matsuzaki, "Electronics Industry, Organizing and Fighting Against Precarious Work," IndustriALL website, May 19, 2015, <http://www.industriall-union.org/report-electronics-industry-organizing-and-fighting-against-precarious-work>.

[54] "Malaysia Economy: Electronics Industry in Need of Reboot," *EIU ViewsWire*, November 27, 2015.

[55] Business Monitor International, "Thailand Consumer Electronics Report," January 2016.

[56] Orathai Sriring & Pairat Temphairojana, "Thailand's Outdated Tech Sector Casts Cloud Over Economy," *Reuters*, March 18, 2015, <http://www.reuters.com/article/us-thailand-economy-electronics-idUSKBN0ME2S620150318>.

[57] "ASEAN: Electronics industry competition will grow," Oxford Analytica Daily Brief, April 02, 2015, <https://www.oxan.com/display.aspx?ItemID=DB198734>.

[58] See Business Monitor International, "Indonesia Consumer Electronics Report - Q3 2015," and Global industry forecasts, "Electronics and Computers: Industry Forecasts," Oxford Economics Ltd. (2015).

their focus on higher-end and advanced products will likely continue to foster some growth in the sector overall. As alluded to above, the more advanced the electronics industry becomes in these countries, the more likely they are to require proliferation sensitive commodities for production and be able to produce items that can assist in the development WMD and missiles programs.

Automotive Manufacturing

The automotive industry, and the auxiliary industries supporting this sector, has improved engineering and technological capabilities in a number of ASEAN countries. Manufacturing facilities for automobiles, particularly cars with advanced systems, require numerous pieces of dual-use equipment and commodities. These dual-use products include items like precision machine tools and isostatic presses that can also be used to manufacture components for missile or nuclear programs, or sensitive chemicals products like polymers which have components that can be used for production of chemical weapons. Materials required for automotive production, particularly carbon fiber and high strength steel, are also dual-use commodities that are particularly useful in WMD programs.[59]

Malaysia's national car brands—Proton and Perodua—have been relatively successful, in part due to government efforts to bolster the industry by imposing tariffs against imported vehicles. These two brands, although now threatened by competition as Malaysia's protectionist policies loosen, helped create a strong local production base for Malaysia's manufacturing sector.[60] In 2014, Malaysia introduced the National Automotive Policy (NAP) which included targeted incentives aimed at promoting the expansion of the country's automotive industry, particularly in the production of energy efficient vehicles. Malaysia has also consistently encouraged domestic and foreign investment in the manufacturing of critical components (engines, transmissions, and chassis), auto electronic components (engine management system and vehicle intelligence system), modular manufacture/system integration, and research and development aimed at enhancing domestic technical skills and engineering capabilities.[61]

Indonesia's automotive industry is primarily focused on the manufacturing of budget passenger vehicles and motorcycles for domestic sale.[62] However, more sophisticated product lines, including high-end manufactures like Mercedes, are now assembled fully in Indonesia. Japanese carmakers like Toyota and Suzuki have recently increased their investments in the manufacturing capacity of their Indonesian facilities. Analysts believe the increased output will result in higher automotive exports from Indonesia, particularly to other parts of Southeast Asia. Malaysia's carmaker Proton is currently in discussions with Indonesia's PT Adiperkasa Citra Lestari (ACL) to create a joint venture aimed at developing Indonesia's first indigenous car brand. If this deal were to go through and development were to be successful, Indonesia's auto sector would increase in sophistication and capability.[63]

Thailand is also considered a major auto manufacturing hub. Automotive related commodities, including vehicles and related parts, account for about 12 percent of Thailand's exports.[64] Most recently, the Thai government has looked toward electric vehicles as the next growth segment for this industry and some

---

[59] In one example illustrating the extent of the dual-use challenges from automotive manufacturing, an Iranian-connected firm took over an automotive production plant in Germany as an apparent front for obtaining number of sensitive items, including carbon fiber, precision machine tools and high strength steel, likely for ultimate use in building uranium centrifuges. See Michael Birnbaum and Joby Warrick, "A mysterious Iranian-run factory in Germany," *Washington Post,* April 15, 2013, <https://www.washingtonpost.com/world/europe/a-mysterious-iranian-run-factory-in-germany/2013/04/15/92259d7a-a29f-11e2-82bc-511538ae90a4_story.html>.

[60] Business Monitor International, *Malaysia Autos Report - Q1 2016*, (2016).

[61] "Business Opportunity: Malaysia Automotive Industry," *MIDA-Business Opportunity,* August 1, 2010.

[62] "ASEAN: Auto Sector Disunity Implies Competition Danger," OxResearch Daily Brief Service, October 26, 2015.

[63] Business Monitor International, "Indonesia Autos Report - Q4 2015," (2015).

[64] See statistics on Thai exports at <http://atlas.cid.harvard.edu/explore/tree_map/export/tha/all/show/2013/>.

Japanese manufactures appear interested in sharing their production technology and capacity with Thai counterparts.[65] Highlighting how support services for an industry can develop dual-use technologies, growth in Thailand's automotive industry is seen as one likely impetus to the ongoing growth in domestically manufactured machine tools. Automotive and auto parts firms are the customers for about 35 percent of the domestically produced machine tools, including advanced lathes.[66]

Vietnam's role in regional auto manufacturing supply chain is still small but appears to be growing. Vehicle production is on the rise, although not for export. Foreign firms are looking more favorably at Vietnam due to lower production costs than some of its neighbors. However, it is unlikely that Vietnam will transplant the other three big regional players—Malaysia, Indonesia and Thailand—in the near term. This is in part due to the smaller scale of production currently capable in Vietnam, the limited domestic demand and the lack of economic incentives offered by Hanoi.[67]

The Philippines auto industry is currently a relatively small but notable source of manufacturing output for the country—about five percent of the overall total. Industry experts see creating significant growth in this sector as a challenge because of the lack of raw materials, problems with maintaining key testing facilities, and the small domestic market.[68] However, recent government initiatives, including comprehensive automotive resurgence strategy (CARS) program announced by President Aquino earlier this year, aimed to help the industry overcome those challenges. An official from the Philippine Automotive Competitiveness Council noted that small and medium sized enterprises (SMEs) play a major role in the Philippine industry. The CARS program is aimed to further increase the growth of SMEs in this sector as means of creating more skilled jobs.[69]

Emerging Sectors

Aside from the sectors noted above, industry experts also raised concerns about a number of emerging technologies that have potential to grow in the region but are not necessarily being looked at carefully by industry analysts or being captured by trade data. In particular, additive manufacturing was highlighted as an area of growth in the region that could have significant implications on proliferation of sensitive materials.[70] Additive manufacturing (particularly 3D printing with highly specialized metal) can create sophisticated components for use in industry or in military systems. Although the technology is thought to be currently out of reach for many involved with illicit WMD networks, experts are concerned that the proliferation of this technology could be a major challenge to nonproliferation and export control efforts in the near future.[71] In September 2015, a Singapore-based firm Ultra Clean Asia Pacific opened the largest commercial additive manufacturing facility in Southeast Asia. The facility is meant to service a number of key growth sectors in the region, including aerospace.[72] Additive manufacturing is seen as a "disruptive" technology by analysts

---

[65] T. Pugliese, "Thailand targets EVs for future growth," *Auto Global News,* July 08, 2015.

[66] "Thailand: Machinery - High Demand Amidst Rapid Development," *Asia News Monitor,* September 23, 2015.

[67] Business Monitor International, "Vietnam Autos Report - Q1 2016," (2015).

[68] "Local Automotive Industry to Thrive Despite Challenges, Industry Player Says," *Philippines News Agency (PNA)*, April 24, 2015.

[69] "Aquino Issues Order to Develop Philippines as Regional Automotive Manufacturing Hub," *Xinhua News Agency*, June 2, 2015.

[70] Discussion with regional experts at CNS sponsored roundtable discussion "Forecasting Industrial Development & Dual-Use Capabilities in Southeast Asia," September 29, 2015.

[71] For an initial discussion of how AM can impact nonproliferation see: Matthew Kroenig and Tristan Volpe, "3-D Printing the Bomb? The Nuclear Nonproliferation Challenge," *Washington Quarterly* (Fall 2015), <https://twq.elliott.gwu.edu/sites/twq.elliott.gwu.edu/files/downloads/TWQ_Fall2015_Kroenig-Volpe.pdf>; and Amy Nelson, "The Truth About 3-D Printing and Nuclear Proliferation," WarOntheRocks.com, December 14, 2015, <http://warontherocks.com/2015/12/the-truth-about-3-d-printing-and-nuclear-proliferation/>

[72] "Singapore Opens Southeast Asia's Largest 3D Printing Facility," *IANS English,* September 28, 2015.

in the region, and as more sophisticated printers become affordable, other companies will likely adopt this form of manufacturing for their industries.[73] Although currently only prominent in Singapore, the speed at which additive manufacturing is being adopted globally means that it is likely the technology will become popular in the other top ASEAN economic performers.

The rising popularity of online marketplaces in bolstering exports from regional firms, particularly SMEs, is also as a potential challenge to nonproliferation efforts in ASEAN. SMEs in ASEAN have been moving rapidly to online sales as a means to increase both domestic and foreign markets.[74] The popularity of online marketplaces in ASEAN remains small in comparison to other regions, but the potential growth is significant as countries improve their IT infrastructure. As has occurred in other parts of Asia, including China, Japan and South Korea, as online marketplaces rise in popularity, the level of sophistication of the products being sold on these platforms also increases. Recent analysis of the sale of dual-use materials via global sites like Alibaba and eBay illustrate the challenge these sites can pose to nonproliferation efforts. In the Southeast Asian context, SMEs are using local online platforms to sell their commodities; as the majority of SMEs are unlikely to be aware that products they develop or trade in may be dual-use, this trend can have significant security implications.

Addressing the Security Implications of Dual-Use Commodities in ASEAN

The prevalence of dual-use commodities in ASEAN will grow over the next decade, particularly in the top five growth countries. Although current industry projections may fluctuate in the sectors reviewed, those fluctuations are not likely to severely impede overall technological advancement in the relevant industries. As these industries advance, a framework for managing the resulting growth in dual-use technologies needs to be constructed. As mentioned in the first section of this paper, the initial steps of that framework have been taken by a number of countries, but significant work is still to be done.

While recognizing the need for greater controls as technical capacity grows, some regional experts from industry and academia have raised concerns that increased regulation would not necessarily create more effective systems. At the moment, regional governments are trying to *de-regulate* in an effort to spur development and growth; additional regulations for trade controls at a time when governments are attempting to keep GDP growth steady will continue to be a hard sell in the region.[75] That said, there is also a growing recognition that countries without established trade management systems might be penalized as they try to move up the technological ladder. Domestic companies will be less appealing to foreign high-tech firms if their national trade management systems are not effective in preventing diversion. Companies in the region that are not cognizant of the dual-use implications of the commodities they work with are less likely to attract foreign partners willing to provide, or cooperate on developing, sensitive technologies.

Ultimately, the sooner countries in the region begin creating an effective system and working with the domestic industries that pose the most pressing dual-use challenges, the more likely they will avoid unwanted diversion of their technologies. As trade control authorities in Southeast Asia (and elsewhere) are burdened by competing economic interest and limited resources, they can significantly benefit a greater understanding of what sectors will pose the most challenges domestically. Focusing attention on these sectors will help authorities build and sustain systems in a more efficient and, hopefully, cost effective way.

Below are recommendations for regional authorities and international partners that can further strengthen the existing strategic trade management framework within the region and develop systems better able

[73] "Outlook 2014: Asia Equities," *Asian Investor*, February 2014.

[74] Discussion with regional experts at CNS sponsored roundtable discussion "Forecasting Industrial Development & Dual-Use Capabilities in Southeast Asia," September 29, 2015.

[75] Ibid.

to stem potential proliferation activities in the near to mid-term. These recommendations stem from the projections reviewed above and are specific to dealing with growing dual-use challenges over the next decade, particularly in the top performing countries in ASEAN. These recommendations are not meant to supersede current efforts aimed at fortifying nascent systems in the region. For ASEAN members that do not yet have fully functioning systems with control lists and established procedures, regional and international partners should continue to focus on essentials such as establishing a legal framework, and creating licensing and enforcement authorities. For systems where these essential aspects are still missing, the recommendations below can be integrated into capacity building efforts as the role of dual-use commodities in a given system becomes more prevalent.

- *Regular Monitoring and Analyzing of Trade Data and Independent Industry Projections*

As the outlook on growth in different industries will changes, the needs of strategic trade management systems must change accordingly. Although the projections above are a good basis for policy decisions in the near term, remaining vigilant for shifts in industry that might affect dual-use capacities in Southeast Asia is important to maintaining effective controls in the longer term. Assuring that strategic trade management authorities can obtain and properly utilize detailed analysis of up-to-date trade data would be highly beneficial to assuring their systems stays a step ahead of proliferators. Likewise, assuring their access to unbiased industry projections that highlight emerging industries and technologies will greatly assist strategic trade management officials' ability to steer resources correctly.

International partners, such as the US, EU and others, can support further efforts to improve collection and reporting of trade data in growing economies to assure the data provided is accurate. This could be done in a number of ways, including providing more training on data collection, and better hardware and software for collection and analysis for officials in the growing economies. More attention should also be given to improving the correlation between the HS Codes and dual-use controls, particularly the EU's dual-use control list which many ASEAN states look to when creating their own trade management system.

Regional trade control officials might already have access to government growth projections, and this analysis can be helpful as a basis for policies on industry outreach and licensing. However, government projections can sometimes be impacted by political or bureaucratic pressures and suffer from forecast bias. Internal government forecasts, particularly in many developing economies, might also lack data related to the outlook of trade partners and likely foreign investors. In order to develop a more accurate picture of future industry growth, regional authorities need access to independent and unbiased industry forecasts. Combining improved trade data and independent forecasting would assist regional authorities in creating policies better able to cope with coming challenges

- *Developing Effective Outreach to Most Prevalent Dual-Use Industries*

To establish an effective strategic trade management system, government should strive to have an inclusive and cooperative relationship with the industries most involved with dual-use commodities as early as possible. To balance both the security and economic needs of ASEAN economies, regional authorities and international partners should focus attention on the education of industry, in particularly those noted above, about the security concerns related to dual-use commodities specific to their industries. The use of current trade data and projections can inform these outreach efforts, help identify the sectors of most concern, and tailor outreach for those sectors.

Industry outreach is a vital part of any strategic trade management system and the improvement of these efforts will go far to build up trade compliance in regional companies. Outreach can include: creation of curriculum aimed at creating a compliance culture in domestic firms, publishing clear guidelines to help industry determine their compliance responsibility, and establishment of formal or informal lines of

communication where industry can reach out to licensing officials for questions and clarifications. These outreach methodologies and others that might be seen as beneficial to regional authorities should also highlight the idea that strategic trade management is not just about controlling and stopping trade; complying with international norms on trade in controlled commodities will benefit overall economic growth as foreign firms view more companies in the region as "trusted" trade partners.

- *Engaging Industry Early and Often*

One area that has not been fully developed in ASEAN, even in countries with relatively well established systems like Singapore and Malaysia, is the cooperation between domestic authorities and relevant industry groups. These groups can play a key role in raising awareness on the security challenges posed by the increased prevalence of dual-use commodities. This work could go further than standard industry engagement, which can often be one-way discussions, with governments talking and industry listening. Industry groups can help act as an effective intermediary between companies and the government, and create an effective conduit for relaying industry concerns to government about scope of controls while at the same time giving strategic trade management authorities an avenue for building awareness about the issue. This method would be particularly helpful for reaching small and medium sized enterprises who often look to these industry associations for guidance on regulatory requirements and changing business environments.

Some efforts are already taking place at a nascent level in a number of ASEAN countries, and increased focus on the industries of most concern, such as those noted above, would likely carry numerous benefits. Domestic Chambers of Commerce as well as sector-specific associations are well suited to take a more active role and begin to build understanding within industry for the economic imperative of creating effective trade management systems. By identifying the most vulnerable sectors now, regional governments and international partners can begin outreach to key industries before proliferating entities begin identifying these regional firms as suppliers for their WMD programs.

- *Staying Ahead of Proliferators*

The growing economies of Southeast Asian need to prioritize the management of their dual-use capabilities in order to prevent the region becoming the next major threat to nonproliferation and international security. In order to balance these efforts with competing economic and political interests, regional authorities need to have a comprehensive understanding of which commodities and industries will pose the greatest challenges. The research reviewed here was meant to assist with the prioritization of trade management efforts and look at tools that will help regional officials and their international partners to most effectively use limited resources.

Getting those industries most affected by controls involved early in the process can be critical to removing possible roadblocks to the development of an effective trade managements system. Close collaboration with industry, especially through industry associations or Chambers of Commerce, can allow regional authorities and their international partners to cooperatively develop standards and guidelines for domestic firms that can be practically implemented while at the same time meet domestic and international security needs. As industry will be quick to point out, additional controls and stricter regulation should not be the only answer; cooperative activities combined with controls that target the most sensitive technologies will go far in establishing systems that are sustainable and effective in the decades to come.

Singapore's Journey Towards its Implementation of Strategic Trade Controls

GEORGE TAN[1]

Absract

This paper provides an overview of Singapore's economic transformation through the decades and the parallel evolution of its strategic trade controls. It examines the strategic reasons behind the establishment of the Strategic Goods (Control) Act, its salient features and the revision of its various components - the Strategic Goods (Control) Act licensing regime, the Strategic Trade Scheme, as well as the TradeFIRST Programme. Finally, the paper looks at the future of Singapore's strategic trade controls.

Keywords

Export control, strategic trade control, Singapore, Strategic Goods (Control) Act, Southeast Asia

Introduction

Singapore's journey from a developing country to one of the world's richest is an economic miracle, especially given its short 50 years of history. From the start, Singapore was handicapped – limited land mass, an ethnically and religiously diverse population, and an acute lack of natural resources. Despite these disadvantages, it had one crucial advantage – an excellent geographical location at the crossroads of global trading lanes, making it a natural port of call. That was why the British colonised Singapore back in 1819 and made it one of the crown jewels of the British Empire in East Asia.

The new government earmarked entrepot trade as one of the key drivers of growth in Singapore's early years. At the same time, the government also focused its effort on attracting foreign direct investment (FDI) from multinational companies. To grow and develop these two areas, Singapore needed to keep its business environment conducive. Policies and legislation had to be trade facilitative and applied in a consistent and fair manner. As a result, Singapore gradually became the location of choice for multinational companies to base their Asian headquarters.

Singapore initially opposed to the idea of implementing strategic trade controls due to the perception that they would "hinder" trade and increase the cost of doing business. Singapore has been conspicuously missing from the list of countries participating in the four multilateral export control regimes, namely the Australia Group, Nuclear Suppliers Group, Missile Technology Control Regime and the Wassenaar Arrangement, which are the basis of almost every national strategic trade control regime.

In its formative stage through the 1980s, Singapore's neutral stance towards strategic trade controls worked. The government was able to withstand international pressure to implement such controls. However, this

stance was increasingly untenable from the 1990s for three reasons. First, there was a significant increase in international pressure from developed countries, namely the United States, Europe, and Japan, which were concerned with national security threats from rogue countries and non-state actors (terrorist networks). Growing international concerns were mounting about the possible leak of technological capabilities and intellectual property to unwanted parties. Second, by the 1990s, Singapore's focus had shifted from low-end manufacturing to higher value-added manufacturing and services due to increasing labour wages and business costs. Local businesses and foreign multinational companies also started to develop technological and intellectual properties. There was more at stake for the Singapore government to protect such enterprises and continue to maintain a conducive business environment. Third, by the 1990s, Singapore had become one of the world's busiest transhipment hubs and it was therefore increasingly difficult for its government not to contribute to international efforts curbing the proliferation of weapons of mass destruction (WMDs). The urge to act became particularly strong when other emerging Asian economies, such as South Korea, Taiwan, and Hong Kong, implemented or started to implement their respective national strategic trade control regimes.

Singapore's Decision to Go Ahead

In 1998, the Singapore government decided to collaborate with countries with established regimes to implement its own regime. The Ministry of Foreign Affairs was initially the lead agency, closely supported by the Ministry of Trade and Industry. Singapore adopted important aspects of the other national strategic trade controls regimes, stripping or scaling down those not facilitative to businesses, and developing new aspects customised for Singapore. The government was careful to avoid developing an overtly cumbersome regime. The Ministry of Trade and Industry subsequently took over from the Ministry of Foreign Affairs as the lead government body. This was motivated by a realization that the regime would have a direct impact on cross-border trade and the increasing concern that the local business community placed on maintaining the ease of cross border transactions and compliance costs.

These efforts bore fruit when the Parliament started hearings and readings from 2001 to 2002. The main legislation – the Strategic Goods (Control) Act (SGCA) – was passed in 2002 and ratified on January 1, 2003.[1] The SGCA is supported by the Strategic Goods (Control) Regulations and the Strategic Goods (Control) Brokering Order, which seek to control the transfer and brokering of strategic goods, strategic goods technology capable of being used to develop, product, operate, stockpile or acquire weapons capable of causing mass destruction, and related purposes.[2]

The product coding system of the various strategic goods and technologies was fully adopted from the EU. The EU system was (and still is) considered as the world's lead, with the United States also taking guidance from its product coding system. Given the large US and European presence in Singapore, the EU system was adopted to minimize complexities and duplication of classification efforts.

In terms of number of strategic goods and technologies, the SGCA initially only covered about 600 (mainly nuclear-related materials and equipment) items and technologies from the EU Control List, covering the more sensitive products and technologies. The Singapore government was mindful of the impact on locally based business and the economy. Singapore's product control list was incorporated into the SGCA.The

[1] Singapore Strategic Goods Control Act, July 31, 2003, < http://statutes.agc.gov.sg/>.

[2] Singapore Strategic Goods (Control) Regulations, November 30, 2006, < http://statutes.agc.gov.sg/aol/search/display/view.w3p;ident=65f18a11-e8c9-4165-bf7e-826c9df17b9c;page=0;query=DocId%3Aa2975918-88db-459b-a1c4-a1dd63f94594%20Depth%3A0%20Status%3Ainforce;rec=0 >, Singapore Strategic Goods (Control) Brokering Order, November 2, 2015, < http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A3f75011a-20f0-4d4a-99b1-58b7685455df%20Depth%3A0%20Status%3Ainforce;rec=0;whole=yes>.

SGCA also allowed amendments without requiring parliamentary approval, maximizing flexibility.

Singapore Customs was appointed as the sole governing agency to administer all strategic trade control-related matters, enforce the SGCA, and conduct public outreach programs. To build and retain technical knowledge, the team from the Ministry of Trade and Industry involved in the development of the SGCA was later transferred to Customs. In addition, Customs put together a dedicated Strategic Trade Control Branch, which serves as a one-stop centre to facilitate application of strategic trade control permits. Singapore Customs' role as the sole governing agency differs from that of other countries in which two or more government agencies (separate licensing and enforcement agencies) are involved. Using a single agency helps to avoid delays in licensing approvals, conflicting implementation messages between government agencies to companies, or insufficient sharing of intelligence between government agencies.

One initial challenge for companies was the requirement for individual strategic trade permits for every transfer of strategic goods or technologies. Given that the application process took an average of 5 working days, this increased turnaround time, especially for companies with high volumes of strategic goods and technologies. As a result, six years after ratifying the SGCA, Singapore Customs decided to pilot a bulk licensing regime for companies proven to have met a certain standard of strategic trade controls. The bulk licensing regime was called the Approved Company Scheme (ACS), enabling companies to apply for a bulk permit for export of multiple strategic goods to a single country destination or export of a single strategic good to multiple country destinations.

Regardless of the type of bulk permit, companies must have strategic goods and country destinations pre-approved by Singapore Customs. The two qualifying criteria are a good track record with customs and an effective internal compliance program (ICP). ICP requirements must be in line with international requirements and standard good practices, including:

- Company's commitment statement in implementing strategic trade controls;
- Designating responsible company's personnel to implement strategic trade controls;
- Product classification to determine whether its good/technology is subject to controls and if so, determine the product control code;
- Order screening to determine if a proposed transaction is subject to strategic trade controls (apart from the product in question);
- Training program for all company personnel and business partners that have touch points to ensure compliance of strategic trade controls;
- Regular internal audits of company's operations to ensure continued compliance; and
- Comprehensive recordkeeping of all transactions (such as invoices, export declarations, or airway bills).

Any country embarking on establishing a national strategic trade control regime faces a steep learning curve. This is true for all parties involved – the governing agency, their management team and enforcement officers, as well as the local business community. To raise awareness of the SGCA, its rationale, and how businesses should comply, there was a series of public outreach programmes conducted by Singapore Customs. Internally, Singapore Customs had to train a team of customs officers to educate the local business community. This effort also involved sending officers overseas to undergo training with other government agencies such as the US Commerce Department's Bureau of Industry and Security. Officers received training on how to identify non-compliance by companies, assess the effectiveness of companies' ICPs, conduct investigations or audits, use various product classification techniques, and understand industry good practices consistent with government requirements.

Balancing Compliance and Trade Facilitation

After the SGCA was implemented in 2003, it created a buzz within the local business community. Most

companies appreciated its need but were unsure how to implement its requirements. As a result, many companies developed a laissez-faire and ad-hoc approach to handling potential transactions requiring strategic trade permits from Singapore Customs. They would only apply if suppliers or customers flagged them as part of their ICP procedures or if Customs identified them based on intelligence assessments. Some companies also adopted a wait-and-see approach, letting their competitors establish relevant industry practices to copy them. Companies targeted by the SCGA typically failed to appreciate its applicability to their operations, especially those only indirectly involved in the trade of dual-use strategic goods.

Singapore Customs recognised the obstacles that the local business community was facing and worked to raise awareness of the SGCA and provide assistance to help them comply. In seeking to balance the need to comply with the SGCA and to facilitate trade, the government applied a soft touch in terms of enforcing the SGCA to the extent possible, especially for bona fide companies that unwittingly found themselves non-compliant with the SGCA. This treatment extended to local branches of multinational corporations (MNCs) as well. Singapore Customs, however, did share such intelligence with MNC's home countries, requesting them to impose their own penalties on headquarters, depending on the extent of extra-territorial reach of their strategic trade control legislation. This is the case of the United States because its Export Administration Regulations (EAR) system permits the US Government to impose heavy penalties on US companies if their overseas subsidiaries are found to be non-compliant with the EAR. This approach by Singapore Customs helped Singapore retain its image as a trade facilitator, while implementing strategic trade controls.

Companies or parties that knowingly circumvented the SGCA with fraudulent/malicious intent were prosecuted. Singapore Customs published the details of the cases and penalties for the general public to portray the image that it was serious in its enforcement of the SGCA.

Singapore Customs has always placed importance on striking the right balance between compliance and trade facilitation throughout its implementation journey of the SGCA since 2003. It has therefore consistently and continuously revised/enhanced its regulations along the way to preserve its own interests and that of the local business community. A summary of these revisions is presented below with subsequent details explaining the rationale behind these decisions.

Revamp of the SGCA Licensing Regime

The ACS licensing system was an effective trade facilitative initiative for the first few formative years of the SCGA, especially for companies with high volumes of controlled transactions involving either repeated controlled products to a single country destination or a single controlled product to multiple repeated destination countries. The ACS, however, had limitations for companies that sent a large number of controlled products to several countries. For such companies, they had to apply repeatedly to Singapore Customs, which was cumbersome for both the companies applying and Singapore Customs. This was even more cumbersome when companies had regularly new controlled products or new country destinations not previously applied and pre-approved by Customs.

To ease and streamline this process, Singapore Customs planned to grant further trade facilitation by allowing them a new type of bulk permit covering multiple controlled products to multiple country destinations. That would reduce administrative efforts for the companies and Singapore Customs. It was a novel concept with a high degree of trade facilitation and Singapore Customs wanted to do its due diligence to ensure that the new bulk permit framework would work for companies while preserving compliance standards for the SGCA.

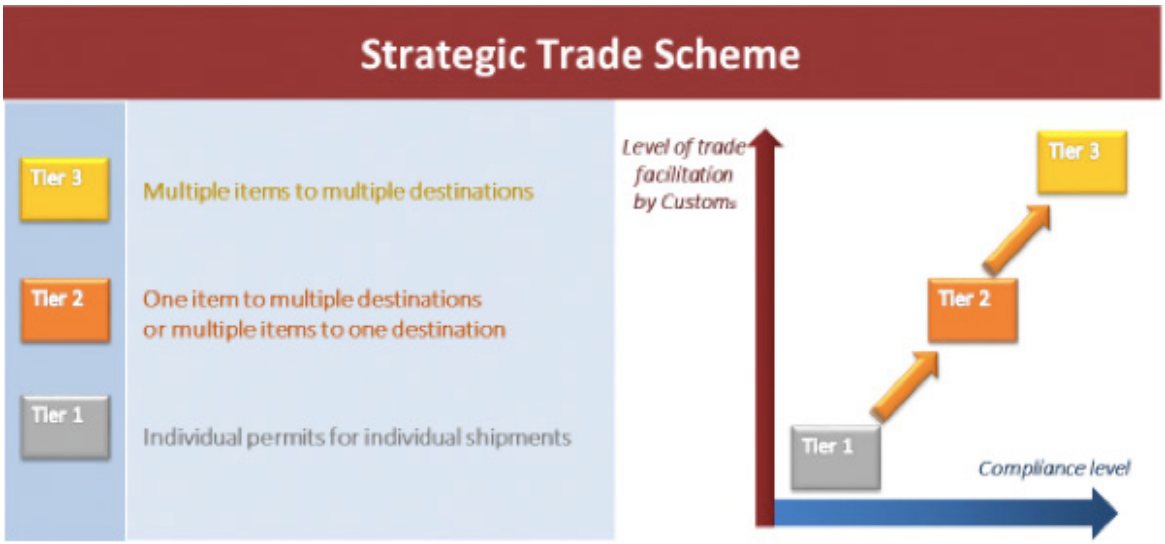
Subsequently, in early 2006, it conducted a pilot program for selected companies with this type of operating profile and a proven robust ICP for its local operations that were beyond its standards of the ICP required

for the ACS. It was a classic case of a successful collaboration between the public and private sector. The pilot program provided further insight to Singapore Customs as to how best to tweak its national licensing regulations for enhanced trade facilitation without compromising effective compliance and enforcement.

Launch of the Strategic Trade Scheme

In 2007, Singapore Customs decided to launch a new type of bulk permit in a revamp of its strategic trade control licensing framework, naming it the Strategic Trade Scheme (STS). The STS was designed as a 3-tiered licensing framework, as follows:

Figure 1: Singapore Strategic Trade Scheme (3-tiers Licensing System from 2007-2014)



Tier 2 permits are similar to the previous ACS in terms of the of the bulk permit, while the underlying requirements for an effective ICP are relatively easier as compared to the Tier 3 permit bulk permits.

Figure 2: ICP Elements Required for Tier 2 and Tier 3 Bulk Permit

Tier 2	Tier 3	Elements of Internal Compliance Program
Not required, but beneficial	Required	1. Company's Commitment
		2. Nomination of Strategic Goods Control Officer
		3. Regular in-house training program
Required		4. Regular internal compliance audit
		5. Proper record keeping
		6. End user screening
		7. Product screening

The revamp was an important milestone in Singapore Customs' journey toward an innovative licensing framework that could meet the objectives of both Customs and the individual companies. The revamp also sparked another round of public outreach programs for the business community and further raised the level

of awareness of the SGCA.

Expansion and Update of the Singapore Product Control List

Given technological developments, in 2007, Singapore Customs adopted the new EU Dual-Use List and WA Munitions List, which came into force on January 1, 2008. Since Singapore has always followed the EU's cue, Singapore's control list also underwent regular changes, albeit with a few months of delay because Singapore Customs had to study the changes and decide whether to adopt them fully or only partially. Since the inception of the SGCA in 2008, Singapore Customs has alerted and educated companies of impending changes.

The original SGCA had the product control list embedded within the Act as a Schedule that was regularly updated as the control list was changed. Mindful that regular amendments to the Act would confuse companies, Singapore Customs decided to separate the control list from the Act as Subsidiary Legislation – the Strategic Goods (Control) Order (SGCO).

To the layman, the SGCO was overwhelming. Singapore Customs recognised the problems faced by companies and accepted classification requests. This has allowed companies to operate with greater certainty, thus facilitating supply chain planning improving turnaround time.

Brokering Activities of Selected Munition Items Controlled

Singapore has had the Arms and Explosives Act and the Arms Offence Act in place to prevent the illegitimate proliferation of weapons and the related activities. Yet the Act was limiting and sometimes vague in its product coverage, omitting references to the four multilateral export control regimes despite the passing of the SGCA. Singapore Customs came to realize through its intelligence and enforcement cases that there were brokering activities being conducted through Singapore relating to certain munition items that were controlled in other countries' national strategic trade control regimes.

To further tighten and clarify the scope of control specifically for brokering activities, Singapore Customs added the Strategic Goods (Control) Brokering Order 2007 under the SGCA. It came into effect on January 1, 2008 and controlled broker registration and application of permits on an individual basis (i.e. no bulk permits).

Evolution of the Voluntary Disclosure Program

Another area of concern for some companies to comply with the SGCA was the initial lack of a formal voluntary disclosure program to cover strategic trade control violations. In 2003, when the SGCA was implemented, Singapore Customs had a voluntary disclosure program (VDP) in place, but its focus was mainly on incorrect payments of the Goods and Services Tax (GST). During the first few years of implementation, it was inevitable that some companies would unwittingly violate the SGCA. Customs has always encouraged companies to share their historical violations. The process was initially informal and flexible as long as the disclosure was complete and substantiated with explanation and proposed corrective actions. Customs then extended the process to cover SGCA violations, a move well received by the business community.

TradeFirst Program - Complementing Supply Chain Security Measures with the STS[3]

After the September 11, 2001 terrorist attacks in the United States, perceptions of the threats posed by international terrorist networks and ancillary illegitimate dealers have steadily increased. This has extended

[3] TradeFirst (Trade Facilitation & Integrated Risk-based SysTem), an integration of STS with AEO (Singapore version is known as Strategic Trade Partnership; STP).

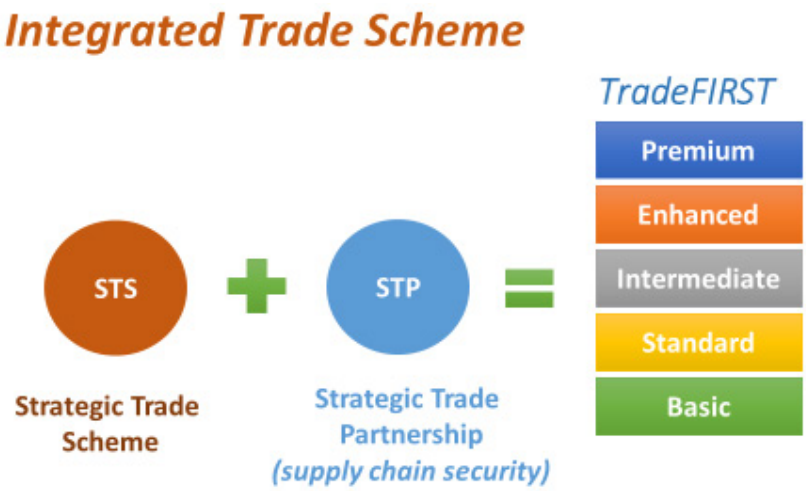
to their usually complex supply chains of illegitimate trade of controlled goods. Alongside strategic trade controls, concerns over supply chain security have likewise grown on the international stage.

Singapore Customs, as a major global transhipment and transit hub, had to conform to the new security environment by increasing focus on supply chain security and strengthening supply chain security measures. Given its high level of trade facilitation with multiple schemes such as the STS designed to assist companies in their Singapore based supply chains, it had to ensure that the overall level of trade compliance for business communities was of a high standard and granted trade facilitation benefits. Singapore Customs also recognised that many prerequisites/conditions of trade facilitative schemes were overlapping and repetitive for companies that were on more than one such schemes, resulting in increased compliance costs.

Customs decided to launch the TradeFirst Program in January 2011, which is still in place today. It is intended to be a one-stop risk assessment framework for Customs to holistically assess a company based on a single set of criteria applied across all trade facilitative schemes granted by Customs to the company. That includes the STS. The TradeFirst program requires the companies to first conduct their own self-assessment of the robustness of supply chain security against the explicit guidelines set by Singapore Customs. The guidelines are wide-ranging, including a company's strong commitment communicated to its employees and business partners, the designation of knowledgeable in-house personnel responsible for supply chain security, implementation of standard operating procedures around inventory management, warehousing, cargo transportation, storage site security measures, and import and export processes.

Once a company is ready, Customs assigns it a dedicated account manager and decides on the banding that serves as prerequisite to qualify for trade facilitative schemes. For the STS in particular, the applying company would be required to attain at least the Enhanced Band under the TradeFirst Program. An overview of the TradeFirst compliance bands and the respective schemes available is shown below:

Figure 3: Singapore Integrated STS and AEO in 2011



The assessment requires the applicant to work closely with the account manager with the latter advising the company about the various industry good practices in supply chain security. Upon successful attainment of the applied band, the account manager remains with the company, thereby further strengthening the relationship.

Restructuring of Customs Departments to Enhance Effectiveness

Prior to the actual implementation of the TradeFirst Program and with increased focus on both supply chain security and trade facilitation, Singapore Customs decided to restructure in July 2010 to better align itself with these two objectives. In relation to strategic trade control administration, licensing, and enforcement matters, the officers within the original Strategic Trade Control Branch were split into the following:

Table 1: Singapore Customs Branches

Customs Branch	Main Responsibilities in Relation to Strategic Trade Controls
Procedures and Systems Branch	Application for all strategic goods permits submitted Registration to Broker Goods under the Strategic Goods (Control) (Brokering) Order 2007; Application for permit to broker goods under the SGCA Application for permit to transmit or hand carry strategic good related software and technology; Application for preliminary advice on strategic goods transactions Application for Import Certificate delivery verification National Authority (Chemical Weapons Convention) license application and declaration related matters.
Schemes & Licensing Branch	Application for STS Tier 2 and 3 bulk permits
Tariffs & Trade Services Branch	Application for Classification of Strategic Goods

The re-organisation sought to grow a nucleus of customs officers with enhanced knowledge of industry practices and realities both in brevity and depth through closer partnerships with companies applying for trade facilitation schemes and individual licenses. Feedback from companies was also positive as they realised operational efficiencies when dealing with dedicated customs officers without always having to explain the nature of their businesses and specific circumstances that they operate under.

License Exemptions for Certain Transhipment and Transit Activities

Singapore Customs are open to feedback to maintain the country's competitive edge. Singapore took into account difficulties faced by trading companies and logistics providers in meeting SCGA requirements by granting license exemptions for transhipment and transit activities that satisfy the following conditions:

- The goods remain constantly within one or more free trade zones; and
- The total time period of the goods being in Singapore is no more than 45 days (for goods brought in via the sea) or 21 days (for goods brought in via air)

The license exemptions apply to all goods except for selected controlled products such as actual arms under the munition control list and nuclear related items under the dual-use list. These items are typically controlled because they are deemed to be so critical and sensitive that the risk of exempting the license requirement for them is too high. The specific lists of products not covered by these license exemptions were revised and took effect in January 2015 as part of Customs' continuous efforts to maintain the relevancy of the license exemptions with technological developments over time.

These license exemptions are in place today. To date, they have been well received by the local business community, especially those in the logistics industry.

Implementation of the Advance Export Declaration

The increasing international emphasis on supply chain security globally has led various countries to implement regulations for companies to be more stringent in business operations within their organisations and their trading operations to prevent illegitimate proliferation of WMDs and related items. Singapore is no exception in this regards and has to be in line with the World Customs Organization (WCO) SAFE framework of standards as a responsible country to secure and facilitate trade for exporters.[4] Compliance with the WCO SAFE framework also enables Singapore to negotiate mutual recognition arrangements with other countries to allow its importers and exporters easier processes to declare their goods in these countries to optimise turnaround time and business costs.

Singapore found itself having to modify an administrative arrangement made in 1976 under its Regulation of Imports and Exports Regulations (RIER) that previously allowed exporters to submit export declarations within 3 days of the goods' export for non-controlled and non-dutiable goods exported by sea and air. The new arrangement, called the Advance Export Declaration (AED), came into effect from April 1, 2013 and continues to apply today. The AED requires exporters to lodge their export declaration to Singapore Customs before the goods physically leave Singapore.

The AED had a significant and potentially adverse impact on companies that had previously lodged their export declarations of non-controlled and non-dutiable within 3 days after the physical export had taken place. The impact of the AED on controlled exports under the STS is limited to those under bulk permits of the STS, where the exports were treated the same as non-controlled exports, enjoying administrative leeway to lodge the export declarations within three days of the goods being physically exported.

Singapore Customs again was careful not to be overtly draconian in its approach in implementing this requirement. It conducted extensive public consultation with companies and gathered feedback prior to implementation. The feedback included insufficient time or supply chain operational limitations to obtain the necessary information for export declarations prior to the physical exports, lack of resources for this additional operational requirement, or increased costs of conducting the exports. Singapore Customs was facilitative by offering assistance/leeway to the extent possible to allow these companies to comply without compromising the AED's requirements. That could be seen from the lead time of more than a year from the initial announcement of the AED to its actual full implementation.

The Second Major Revision of the Strategic Trade Scheme

The first revamp of the national strategic trade control licensing regime to a three tiered licensing framework took place from 2007 until April 2014, when Singapore Customs further revised the STS. More specifically, the bulk permit licensing coverage to either multiple products to multiple country destinations or multiple products to multiple specific entities (i.e. end users) was modified. The revisions are summarised below:

[4] The World Customs Organisation (WCO) had released the SAFE framework to Secure and Facilitate Global Trade (SAFE Framework) in 2005. It is a set of recommendations to national customs authorities which includes:

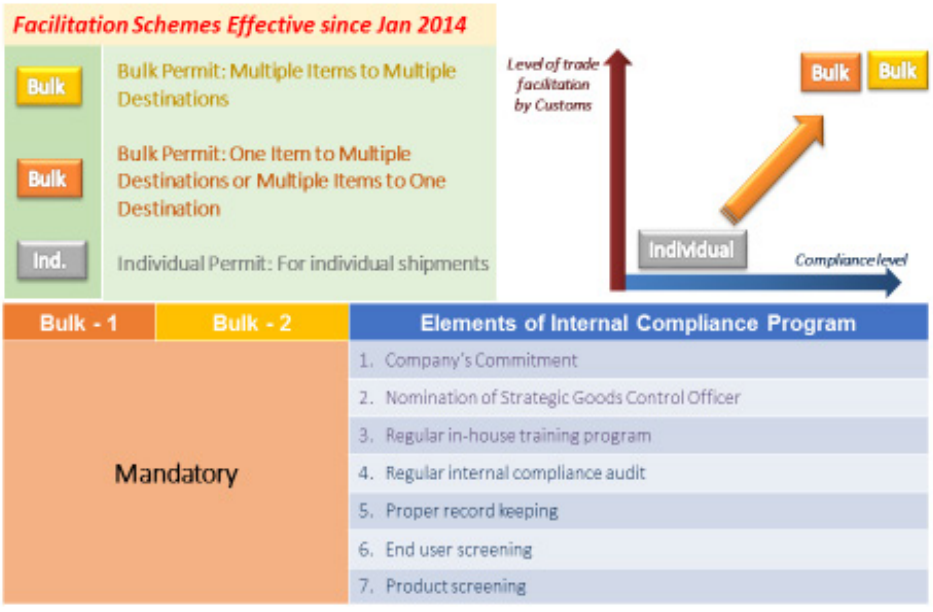
- Integrated customs control procedures for integrated supply chain management;
- Authority to inspect cargo and use modern technology in doing so;
- Risk-management system to identify potentially high-risk shipments;
- identification of high-risk cargo and container shipments;
- advance electronic information on cargo and container shipments;
- Joint targeting and screening.

Though non-binding, it is widely accepted by national customs authorities to be the standard bearer and basis for various national supply chain security related programs and mutual recognition arrangements.

Table 2: Changes in Revised STS

STS in 2007	Revised STS from April 2014 onwards
3-tiered licensing framework: Tier 3 bulk permit for multiple products to multiple country destinations Tier 2 permit for either single product to multiple country destination or multiple product to single country destination Tier 1 permit for each individual controlled transaction Note: The coverage of the bulk permit has to be pre-approved.	2-tiered licensing framework. Bulk permit to cover either list of multiple products to multiple country destinations or multiple products to multiple specific entities (i.e. end users). The various lists continue to be on a pre-approved basis with Customs. Individual permit for each controlled transaction.
Companies applying for the bulk permit are able to specifically list their intention to obtain the type of Tier 2 permit or Tier 3 permit.	Companies applying are unable to list their preference as to what kind of bulk permit will be granted to them. Customs will have the flexibility to decide the specific coverage of the bulk permit, depending on their assessment of the company profiles, business operations and compliance records with the SGCA.
Fulfilment of additional ICP elements for issuance of a companywide commitment to complying with the SGCA, appointment of dedicated in-house strategic goods control officer(s) and training programs for company stakeholders of strategic trade controls was only required for Tier 3 permit but not for Tier 2.	Regardless of the coverage of the bulk permit granted to the companies applying, they are to fulfil all 7 ICP elements.
For each export declaration under a bulk permit (i.e. Tier 2 or 3), it was optional for companies to indicate the details of consignees and end users.	For each export declaration under a bulk permit, it is compulsory going forward for companies to indicate the details of consignees and end users.

Figure IV: New Bulk Permit Launched in 2014 with Complete ICP 7 Elements



The key underlying reasons for the revisions were that, first, compliance standards for continued effective strategic trade controls and supply chain security had overall risen and/or evolved since the inception of the SGCA in 2003. There had been an increasing global focus and additional complexities associated with illegitimate diversions of shipments and proliferation of WMDs along with the related items (including those of dual-use). Second, it was observed that several companies that obtained the original Tier 2 or Tier 3 permit in the first few years of the original STS did not necessarily continue to meet the new compliance standards required when their bulk permits were due for reassessment and renewal. Their business models might also be no longer suitable for the bulk permit that they had initially applied for.

The Next Stage of Singapore's Strategic Trade Control Journey

Based on industry experience and feedback obtained through consulting work and years in industry, the author assesses that there are several challenges/issues that Singapore Customs may wish to address:

1. *Misuse of Companies' Unique Entity Number[5] (UEN) for Customs Declarations of Controlled Strategic Trade Shipments*

Singapore is one of the easiest trading places in the world. This is because companies are able to correspond with the Singapore government through online platforms that are transparent, quick, and straightforward. Companies can lodge customs declarations in Singapore through the TradeNet system.[6] As a result, it might sometimes be hard for Customs to identify misuses of companies' UEN, specifically when it is used to declare goods that do not belong to companies, and if so, whether it is done in a fraudulent or negligent manner. Some companies with existing strategic good bulk permits may be exporting goods on behalf of other companies that do not have adequate internal controls in place. In such instances, the bulk permit holders may not be conducting sufficient due diligence given the high volume of additional goods and/or a lack of knowledge about these transactions (e.g. product nature or end users), which they do not have access to.

Singapore Customs, through the designated account manager program for all its trade facilitative schemes, such as the STS, should constantly pay attention to business operations beyond the initial TradeFirst and STS bulk permit assessment stage to see if there are activities that do not seem to fit with the specific business profile or operations. More sampling checks of daily shipments and transactions can also be done to increase the chances of identifying illegitimate trade practices. Singapore Customs should also second more of its officers to businesses to better understand each industry from a trade compliance standpoint and increase their level of savviness to spot non-compliant activities in other companies.

As a complement to gathering better intelligence about potential malpractices, stronger enforcement and penalties are also required to prevent such activities.

2. *Stronger Enforcement to Drive Home the Compliance Message*

There is a possibility that some companies would misinterpret Customs' soft stance described above as an implicit message that enforcement of the SGCA might not be as strong as in other countries. As a result, companies, especially rogue ones, may decide not to take compliance with the SGCA seriously. For the majority of bona fide companies, however, this is not likely to be an issue.

[5] The UEN is the Singapore registered company's standard and unique identification number used for all of its business transactions with the Singapore Government.

[6] The TradeNet system is Singapore's national electronic data interchange platform for all declarants to lodge their customs declarations directly to Singapore Customs and Controlling Agencies (if relevant).

While Customs have penalised rogue companies with fines or imprisonments of key individuals (and disclosed their identities to the general public), these penalties may not be severe enough in comparison to the potential profits and/or adverse impacts that these activities would generate should they go undetected. The severity of penalties should be reexamined.

As for repeat offenders, Customs should consider imposing denial of export privileges. This is by far the most effective deterrent because it would prevent companies from conducting their businesses and generating income. This typically trumps fines and even imprisonment since these penalities may only impact specific individuals, allowing errant companies to continue their operations, sometimes under new guises (e.g. different UEN to lodge customs declarations).

Enforcement efforts can also be further intensified on two fronts. One is broader and deeper analysis of intelligence of potential non-compliant practices through trading data such as customs declarations and closer attention to industry players that are more likely to deal with strategic goods, software and/or technology. Second, implementation of a more comprehensive risk assessment approach to identify and investigate companies with potential non-compliant operations would improve coverage. This may include more spot checks of such companies' operations to assess the level of internal controls and help ensure companies conduct these checks on the same industries. These enforcement efforts, of course, have to be consistent with the resources available to Customs. The goal is to gain more effective results from enforcement efforts and enhance impact and coverage for more effective policing.

3. The Coming of the ASEAN Economic Community (AEC)

There has been much hype among government agencies and the media in recent years about the coming of the AEC and the various benefits that businesses can reap. The AEC is the realization of the goal of regional economic integration amongst the ASEAN countries by the end of 2015. The AEC espouses the key objectives to achieve:

- A single market and production base;
- A highly competitive economic region;
- A region of equitable economic development;
- A region fully integrated into the global economy.

Though strategic trade control is not specifically covered within the AEC Blueprint, its essence can be covered under the main objective of a single market and production base.[7] More specifically, the relevant work related to strategic trade controls involves the development of trade facilitative work programs, integration of customs functions, and the ASEAN single window.

The common misconception that ASEAN would become an economic community similar to the European Union has been dispelled through a series of public outreach programs by ASEAN countries. More businesses are aware of the limitations of the AEC and that a longer time period is required to implement the various initiatives. Their expectations about the AEC have likewise been scaled back, with businesses treating the end 2015 deadline as another work-in-progress milestone rather than a "big bang moment" that would result in immediate benefits for their businesses.

Likewise, companies looking for a unified set of strategic trade controls and licensing framework through the various ASEAN countries will have to wait longer. The ASEAN countries are still in varying stages of development for their respective national strategic trade control regimes with no immediate plans to

[7] The AEC Blueprint is a schedule breaking down the various objectives of the AEC into actionable steps and initiatives with specific timeline of completion. See AEC Blueprint, 2008, < http://www.asean.org/wp-content/uploads/archive/5187-10.pdf>.

standardize these efforts.

What it means for companies is that post-2015 they are still required to adhere to specific national strategic trade control regimes and lodge separate customs declarations to each national customs authority involved. This applies to not just control cross-border strategic trade shipments but also for all other non-strategic trade shipments as well.

Despite the current developments, Singapore Customs cannot act to reduce differences in other countries' national strategic trade control regimes. Singapore Customs may wish to share other countries' journey toward implementing their national strategic trade control regimes, especially with those countries that are in the process of developing one. An example was the positive collaboration between Malaysia and Singapore when Malaysia launched its national strategic trade control regime (i.e., Strategic Trade Act) in 2010. Common points such as having a common product control list should be established to reduce the efforts required for companies to comply without too much compromise on trade facilitation.

Another area to explore is the signing of mutual recognition arrangements (MRAs) to grant companies based in country A with proven compliance records and robust internal controls to manage their strategic items in country B. A possible example is for companies with a regional strategic trade compliance team and proven set of controls in country A covering all cross border transactions including those from country B in a sufficiently robust manner could be granted a waiver or simplified assessment process in a shorter time period to obtain strategic trade permits / licenses for their exports of strategic goods from country B. There are many potential synergies to explore between national Customs authorities, which in turn can translate to greater compliance cost savings and less cumbersome efforts for companies to set up their operations in their countries. Singapore, being the choice of most companies to set up their regional HQs, especially for the ASEAN region, should make strategic trade compliance easier for companies on a wider scale beyond Singapore. This is already done in the supply chain security landscape with increasing MRAs being signed. There should be an extension of such efforts in the strategic trade compliance space.

4. Capacity-Building for Businesses Playing Catch-up with Strategic Trade Controls

Singapore Customs has come a long way in a relatively short time period in designing its strategic trade licensing framework and the supporting regulations under the SGCA. Companies have spent substantial effort keeping up with various regulatory changes. But the reality is that companies will always have an endless list of diverse priorities to fulfil with finite resources, be it in capital, infrastructure or labour. This issue is perhaps most acute for the small and medium enterprises (SMEs) that often cannot afford to invest in a best-in-class internal compliance program/procedures. Difficulties in hiring qualified labour sufficiently versed in strategic trade controls and establishing a suitable internal infrastructure (e.g. IT systems, procedures, etc.) to manage the SGCA compliance process for their businesses is common feedback from businesses when they are asked about the challenges that they face in complying with the SGCA, especially when they apply for the bulk permit under the STS. The difficulties sometimes persist even in instances when the companies have the capital to hire personnel but are unable to find the personnel with the right knowledge and know-how to embed the compliance process through their business operations.

Singapore Customs recognise these operational realities and have embarked on various initiatives to resolve/minimise this capacity-building issue given the resources (e.g., number of customs officers) that they have at hand. As mentioned above, dedicated account managers have been designated to specific companies to assist them through the compliance process through the TradeFirst program framework. Additionally, Singapore Customs also launched its Singapore Academy to train and impart technical knowledge of various customs and trade related concepts, including strategic trade controls, to industry practitioners within the business community. This topic can be challenging and more so when the principles are practiced on a day-to-day basis in specific circumstances.

Companies invariably insist that more assistance is required, especially in terms of depth of assistance. One solution would be to set up a non-governmental organisation with the mandate to advise companies on the requirements associated with strategic trade controls on a much deeper level and over a prolonged period. This is already done in several countries with established national strategic trade control regimes including South Korea, Japan, the United States, and the European Union. The underlying idea is to pool the expertise of industry practitioners, retired customs officers/government officials, and companies' resources to realize economies of both scale and scope and make such compliance support readily available to all companies needing it at nominal fees. The aim is to make the strategic trade control ecosystem in Singapore even more viable for companies to comply with strategic trade controls on a sustainable basis without having to overtly invest in this respect. At the same time, such an NGO can potentially free up some capacity for Singapore Customs to focus on other initiatives as well. There would be a richer exchange of ideas and insights between the business community and Singapore Customs as to how strategic trade controls are or can be practised in real cases. Through such channels, more insightful feedback can be gathered by the Singapore authorities, allowing them to be even more in sync with the business community and implement even more effective regulations for a win-win situation for all parties involved in the strategic trade control landscape.

Conclusions

Strategic trade controls and securing global supply chains have gathered global momentum in an increasingly connected world. As a city state with international status as a transhipment hub and preferred port of choice, Singapore must implement strategic trade controls. Singapore does have some leeway in how exactly it implements the controls. Since the inception of the SGCA in 2003, Singapore has continuously reviewed the effectiveness of its national strategic trade controls and the underlying licensing framework, seeking to strike a balance between sufficient trade compliance and trade facilitation.

Singapore has adopted aspects of other countries' system that it thinks works well for the city state together with the customisation and integration of novel aspects of its particular strategic trade control requirements. It even has had countries studying its unique licensing framework for their own national regimes. Efforts have been undertaken to engage the business community in navigating through the various regulatory changes and ultimately minimising the level of adjustments and investments required to comply with the SGCA on a sustainable basis while preserving their business competitiveness both locally and globally.

As with all frameworks and systems, there will always be room for further enhancements. This is a continuous process but the Singapore spirit of seeking to strike the right balance between effective compliance and sufficient trade facilitation through the dynamic global, regional and local political, economic and national security climates will position the country in good stead in its journey toward a world-class strategic trade control system.

Implementation and Enforcement of Strategic Trade Controls in Malaysia

MOHAMED SHAHABAR ABDUL KAREEM[1]

Abstract

The Strategic Trade Act 2010, intended to implement strategic trade controls in Malaysia, received royal assent on July 2, 2010 and was published in the official gazette on July 10, 2010, effectively making it national law. This article is a narrative on Malaysia's journey to implement and enforce strategic trade controls. It lays out the history of Malaysia's decision to adopt and implement strategic trade controls and how it was done; analyzes the current system, its main components, including the organizational structure; and draws general conclusions about its effectiveness and limitations.

Keywords

Export control, strategic trade control, Malaysia, Strategic Trade Act, Southeast Asia

Introduction

On April 5, 2010, just prior to the Nuclear Security Summit (NSS) of April 12-13, 2010 hosted by US President Barack Obama in Washington DC, Malaysian Prime Minister Datuk Seri Najib Tun Razak officially announced the Malaysian government's adoption of the Strategic Trade Act. The Act was intended to fulfill Malaysia's obligations under United Nations Security Council Resolution 1540 (UNSCR 1540).[2] The Act, which was adopted in a sitting of the House of Representatives on that very date, was aimed at establishing controls to curb the proliferation and trafficking of weapons of mass destruction (WMD)-related materials and associated delivery systems from and through Malaysia.

The journey to the adoption of the Act, however, goes back at least five years. A working version to introduce the Act was drafted in 2005 and had been floating about in the government, without any domestic champion or political will to push it to fruition.[3] The delay in tabling the Bill was also the result of a turf war among

[1] Mr. Mohamed Shahabar was the first head of the export control organisation in Malaysia, the Strategic Trade Secretariat. Had the responsibility to establish from scratch the Secretariat and implement a comprehensive system of strategic export controls in the country. Currently retired but is pursuing his interest in strategic export controls as an independent specialist, in particular sharing Malaysia's experience in establishing an innovative and effective system and infrastructure for the management of strategic controls.

[2] "Malaysia to strictly enforce nuclear trafficking law," *AFP*, April 15, 2010, <www.channelnewsasia.com>; and "Parliament: Strategic Trade Bill is Passed," *Bernama*, April 5, 2010, <www.bernama.com>.

[3] Stephanie Lieggi and Richard Sabatini, "Malaysia's Export Control Laws: A Step Forward, But How Big?," NTI Analysis, May

government agencies that were eager to become the custodian of the Act, preventing any single agency from taking the lead.

An unlikely but influential champion for strategic trade controls emerged in 2009. It was none other than the Malaysian Prime Minister himself. With Prime Minister's support and using the existing working draft, the Attorney General's Chambers (AG Chambers), in the later half 2009, started consultations with relevant ministries and agencies to finalize the Bill. As soon as the Bill was ready to be tabled in Parliament, swift actions were taken culminating in the publication of the law in the Official Gazette of the Federation of Malaysia on June 10, 2010. The impressive timeline for the adoption of the Strategic Trade Act 2010 is as follows:

March 27, 2010 - Discussed and approved by the Cabinet
April 5, 2010 - Approved by the Lower House of Parliament
May 6, 2010 - Approved by the Senate
June 2, 2010 - Received Royal assent
June 10, 2010 - Published in the Gazette

The first NSS provided an important impetus to the process. According to a report by the Institute for Science and International Security dated April 9, 2010,

> *The Malaysian Prime Minister, scheduled to attend the Nuclear Security Summit on April 12-13, likely did not want to show up in Washington empty-handed at a conference that aims in part to end nuclear smuggling and reduce the likelihood of nuclear proliferation.*[4]

The United States had been urging Malaysia to enact laws for strategic export controls for years. Bearing the gift of 'STA 2010' at the Summit, Mr. Najib assured an important economic partner and political ally that was aligned on security issues, particularly on the security of trade. Showing Washington's pleasure with the gift, President Obama at a bilateral meeting held on the sidelines of the NSS on April 12, 2010 with Prime Minister Najib, congratulated Malaysia for adopting the Strategic Trade Act.

The publication of the law in the national Gazette officially signaled to the world and domestic stakeholders that Malaysia had the legal provisions in place and was ready to tackle the problem of proliferation and trafficking of WMD-related goods and technology. The time necessary for Malaysia to adopt the STA 2010 was unprecedented. Typically it takes up to three or more years from the drafting stage of a Bill to its final adoption as a law. Including the time necessary for drafting, the STA 2010 was done in less than a year, demonstrating the urgency and commitment the government had placed on enacting this comprehensive and all-encompassing Act.

Drivers

Many countries, particularly in Southeast Asia, face difficulties in enacting laws on strategic trade controls. The primary focus in these countries is trade facilitation, and therefore controlling trade is often not on the radar of the legislators and the government. In Malaysia, for example, there were always more pressing domestic issues requiring urgent attention, and championing such causes provided more visibility for law makers. 'Strategic trade controls' is also not something that attracts votes or generates an increase in the popularity of the ruling government or the opposition. Furthermore, the poor understanding of both the

2010, <www.nti.org>.

[4] David Albright, Paul Brannam, and Christina Walrond, "Malaysia Finally Adopts National Export Controls," Institute for Science and International Security, April 2010, <www.isis-online.org>.

executive and legislative branches on the meaning of strategic export controls remained a hindrance.[5]

There are five primary drivers that led to Malaysia to adopt STA 2010.

1. Malaysia's Obligations under UNSCR 1540

UNSCR 1540 requires member states to:

> *...take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall …establish, develop, review and maintain appropriate effective national export and trans-shipment controls over such items, including appropriate laws and regulations to control export, transit, trans-shipment and re-export...*

As a UN Member State, Malaysia is bound by Articles 25 and 48 of the Charter of the United Nations to comply with and implement these obligations. While UNSCR 1540 was adopted in 2004, the requirements it contained took some time to gain support and traction within the country. A hindrance was the view held by many government agencies that exports were already adequately controlled in Malaysia and, therefore, that there was no need for an additional legal instrument to control strategic goods and technologies.[6] This is partly true as there was other legislation in place to control the exports of explosives, military related goods, radioactive, hazardous, chemical and biological materials and products; and nuclear-related items either due to concerns on public health and safety. Therefore, it took a while to raise awareness and convince skeptics of the specific requirements under UNSCR 1540.

To explain the need for strategic trade controls to hostile stakeholders in developing countries like Malaysia, both in the public and private sector, nothing was stronger than the authority and mandate provided by UNSCR 1540, a resolution that was aimed at preventing rogue states and non-state parties from illicitly obtaining WMD-related materials. Using the resolution as the justification was important as many critics within the country were not receptive to the adoption of the law. It was viewed with suspicion and was seen as interference by foreign countries with vested interest and a challenge to the country's sovereignty and interests.

2. The Economic Driver

The Malaysian Government in the mid-1960s started diversifying its economy by attracting foreign investments in manufacturing to provide employment to its citizens and to establish an additional base for its economic growth and exports. This was a success as foreign investments propelled a relatively backward agricultural country into an industrialized upper middle-income economy in less than twenty years. The Asian financial crisis of 1997-98, unfortunately, stopped this growth short and Malaysia has since struggled to break out of the so-called middle-income trap.

Upon taking over the post of Prime Minister in 2009, Mr. Najib introduced an ambitious economic plan commonly known as *The New Economic Model,* a plan to accelerate and sustain economic growth, provide high-quality employment and increase wage levels, with the chief objective of attaining developed country status by 2020.[7] Key to this success was to move up the international high-tech value and supply chain by

---

[5] Stephanie Lieggi and Richard Sabatini, "Malaysia's Export Control Laws: A Step Forward, But How Big?," NTI Analysis, May 2010, <www.nti.org>.

[6] George Tan, "Export Controls in the Asean Region," *1540 Compass*, <www.cits.uga.edu/index.php?/1540compass/issue_2>.

[7] Economic Planning Unit, Prime Minister Department, Malaysia, <www.epu.gov.my/epu-theme/pdf/nem.pdf>.

attracting high value added, technology and knowledge intensive investments that could translate into high value exports.[8]

While the key policies to attain developed-country status by 2020 were already in place in 2010, it soon became apparent that the targets under the *New Economic Policy* could not be realized if foreign investors and exporters were not provided adequate legal protection against proliferation threats from Malaysia.

Strategic trade controls had become an important consideration for investors particularly after the September 11 attacks in the United States. Sensitive high value added products, technology, and knowledge intensive investment source countries, such as the United States, the European Union, and Japan also required their multinational companies to invest in recipient countries with strong strategic trade controls.

Meanwhile, several domestic organizations representing foreign business and investors' interest in Malaysia spearheaded the drive for the country to adopt strategic trade controls. The Malaysian International Chamber of Commerce and Industry, the American Malaysian Chamber of Commerce, the EU-Malaysia Chamber of Commerce and Industry, and the Japanese Chamber of Trade and Industry leaded these efforts. Malaysian authorities could no longer ignore the call for strategic trade controls by investors. The country, otherwise, may have stood to lose out to other countries that were more compliant to international standards on strategic trade controls. Having in place strategic trade controls was seen as adding a competitive advantage to the nation's already impressive portfolio as an attractive investment destination.

In this regard, and according to a diplomatic source, the US President himself had projected substantial increase in bilateral trade with the United States and more investments by US companies in sensitive high-technology and knowledge intensive industries, if strategic trade control laws are implemented. This assurance stood as an enticing offer for Malaysia, giving it sufficient incentive to hasten the adoption of its Act.

3. The External Push

Proponents of strategic trade controls started being active after the September 11 attacks. Their primary motive was to universalize controls on items, products, and technology that can contribute to nuclear terrorism. The goal was the universalization of strategic trade controls, in particular in international proliferation hot spots and major international transport routes, including Malaysia.[9]

Of the ten Member States that comprise ASEAN, only Singapore had enacted and implemented laws on strategic items prior to 2010.[10] Including Malaysia into this list was an achievement as it is an important international trading and transport hub. Substantial efforts and resources were spent to peddle the merits of such controls in Malaysia. Chief among these proponents were the United States and the European Union. The sustained push for controls by these countries, despite the snail paced progress in many of the target countries, was significant, as otherwise countries like Malaysia may not have adopted laws so quickly. Significantly, the United States, European Union, Japan, Australia, and several other countries were already involved in outreach and capacity-building programs with the Malaysian Government and business community before the Strategic Trade Act was adopted.[11] These outreach initiatives paved the way for better understanding of the objectives and philosophy behind strategic trade controls.

---

[8] George Tan, "Export Controls in the Asean Region," *1540 Compass*, <www.cits.uga.edu/index.php?/1540compass/issue_2>.

[9] Stephanie Lieggi and Richard Sabatini, "Malaysia's Export Control Laws: A Step Forward, But How Big?," NTI Analysis, May 2010, <www.nti.org>.

[10] Singapore Customs, <http://www.customs.gov.sg/strategicgoodscontrols>.

[11] Stephanie Lieggi and Richard Sabatini, "Malaysia's Export Control Laws: A Step Forward, But How Big?," NTI Analysis, May 2010, <www.nti.org>.

4. Political Will

Malaysia also adopted strategic trade controls quickly because there was strong political will within the Malaysian Government. Prime Minister Najib was its number one champion. This stood as a significant advantage, so much so that the bill was passed without debate in the lower and upper houses of Parliament.

The role played by the Malaysian Ambassador to the United States, Tan Sri Jamaludin Jarjis, a sitting Member of Parliament and a close confident of the Prime Minister, also should not be understated. Jamaludin was a diplomat who had established close ties with the Obama administration and had access to many key policymakers in Washington. Jamaludin saw strategic export controls as a low hanging fruit that could be quickly plucked to strengthen US-Malaysia bilateral relations. The fact that the law was adopted a few days before a scheduled US-Malaysian bilateral meeting on April 12, 2010 in Washington is also significant.

The SCOMI Precision Engineering (SCOPE) Case

Prior to STA 2010, Malaysia and Malaysians had been identified as a source of proliferation of WMD related materials. Several Malaysians had also been charged in US Courts for offenses under US export control legislation, in particular for their participation in transshipment of sensitive US-made products to countries under US sanctions.[12] Yet these cases did not receive much publicity in Malaysia.

One particular incident involving a Malaysian company in the oil and gas industry did receive wide attention and interest and is often cited as an important driver of Malaysia's decision to implement STA 2010.[13] SCOMI Precision Engineering (SCOPE) was implicated in 2003 for supplying the now infamous A.Q. Khan illicit network with aluminum pipes, which are also used in the oil and gas industry. The pipes manufactured by Malaysia's SCOPE were found on a ship bound for Libya,a restricted country.

SCOPE denied being a knowing party to this transaction, as to its knowledge the pipes were meant for use in the oil and gas industry in the United Arab Emirates. Nevertheless, this did not absolve it from any wrongdoing as it ran afoul of US laws that have extra-territorial provisions and result in objective liability. In the Malaysian context, the company had not done anything wrong either. There were no laws in place yet requiring exporters to be vigilant on the end-use and end-user of their products. This incident received wide attention within the Malaysian official establishment especially after the company was blacklisted by the United States for working with the illegal network. It was also a red flag, indicating that Malaysia had the capability to produce WMD-related products.

Arising from the SCOPE incident, it also became necessary to protect the Malaysian business community from potential exploitation by proliferators.[14] The fact that a draft bill on strategic trade controls was already available in Malaysia in 2005, soon after the SCOPE incident and long before its actual adoption, indicates that the SCOPE incident did have an impact on Malaysia. In outreach programs held after the passage of the STA 2010, the mere mention of SCOPE elicited more interest in the STA 2010 and assisted in converting critics to the view that STA 2010 could be an effective tool to protect their own interest and the commercial interest of the nation.

---

[12] Stephanie Lieggi and Richard Sabatini, "Malaysia's Export Control Laws: A Step Forward, But How Big?," NTI Analysis, May 2010, <www.nti.org>.

[13] Mohamed Shahabar Abdul Kareeem and Muthafa Yusof, 'Issues and Challenges Implementing the Strategic Trade Act in Malaysia," *1540 Compass*, <http://cits.uga.edu/1540compass/issue_5>.

[14] Ibid.

The Strategic Trade Act 2010 and Related Regulations and Orders

Act 708, Strategic Trade Act 2010,[15] is a comprehensive law that had adopted almost all the requirements of UNSCR 1540. The short title of the Act states:

> *An Act to provide for control over the export, transshipment, transit and brokering of strategic items, including arms and related material, and other activities that will or may facilitate the design, development and production of weapons of mass destruction and their delivery systems and to provide for other matters connected therewith, consistent with Malaysia's national security and international obligations.*

The Act, which closely mirrors the Singapore Strategic Goods (Control) Act (STGC), has an extra-territorial application, a catch-all provision, and sections covering the appointment and powers of the implementing Secretariat, what constitutes control of strategic items, unlisted items and restricted activities; the application of the Act to permits and registration for the exports of strategic items and technology; application of the Act for enforcement; and other general provisions for the smooth implementation of the Act.

On July 10, 2010 the legal instruments and authority to implement strategic trade controls in Malaysia were already in place. However, the physical infrastructure to implement the Act had yet to be determined. What had already been predetermined was the date of implementation and enforcement of the Act, on January 1, 2011.

At the recommendation of the AG Chambers, implementation of STA 2010 was placed under the direct purview of the Minister of International Trade and Industry of Malaysia. This closed a sticky point as many other Government agencies had an interest in becoming the implementation body. With this decision, the Ministry quickly took steps to establish the Strategic Trade Secretariat (STS), a requirement under the law to implement and enforce strategic export controls. On August 15, 2010 the Ministry received the official consent from the Public Services Department to establish the Secretariat. The STA 2010 entrusts the implementation of the Strategic Trade controls to the Strategic Trade Controller who reports directly to the Minister.

It is of interest to note that the Act has provided vast powers to the "implementer" and "enforcer," including the ability to request international and domestic assistance to carry out the task, an avenue for inter-agency co-operation by specifying the agencies deemed as authorized officers for enforcement of the STA and the related laws covered under this Act; a division of power between the implementing Secretariat, enforcement agencies and prosecution for offenses. It addition, the Act gives sufficient protection to Government officials from being sued while carrying out their duty, which includes powers of investigation, interdiction, search and seizure without warrant, access to places or premises and computerized data, power to search conveyances, use of force, power to arrest and interception of communications; and the penalties involved in exporting strategic items without a permit or falsified documents.

To get the STA 2010 enacted was a major achievement itself. While STA 2010 had provided the general legal framework for the implementation of strategic trade controls in Malaysia, it did not, however, specify the implementation mechanism that had to be put into place to enforce the law. Detail on how the law would be implemented is of critical importance to the business community as they are the target group which needs to adjust and put sufficient resources in place to effectively comply with the legal requirements of the Act.

---

[15] Available (upon subscription) at the <http://www.lawnet.com.my/ lawnetPublic/> or it can be purchased from the Government Printers - Percetakan Nasional Berhad. It can also be viewed in the Parliament website: <http://www.parlimen.gov.my/ billindex/ pdf/ DR042010.pdf>.

Over the course of four months from August 2010, the Secretariat started intensive consultations with relevant Government Department and Agencies to develop the implementing mechanisms and procedures. The core members of the team included representatives from the AG Chambers, Ministry of Foreign Affairs, Customs and the Atomic Energy Licensing Board. Private sector consultations were also undertaken separately by the Secretariat. This included consultations with trade and industry organizations, Chambers of Commerce and Industry, large companies and in particular those which have an important stake in exports of strategic items, but also individuals with experience in strategic trade controls and who were willing to share their experience and views with the Secretariat. These consultations were made easier as there were already working drafts available to focus discussions and comments. These efforts finally culminated in the development of the following Regulations and Orders that were published in the Gazette on December 31, 2010, and which became effective on January 1, 2011:

Strategic Trade Regulation 2010, that prescribes the forms, procedures, payable fees and other matters including how the Act would be implemented and enforced.[16]

Strategic Trade (Strategic Items) Order 2010, the Malaysian control list. It reproduces the EU control lists and contains items controlled under all the five international control regimes.[17,16]

Strategic Trade (Restricted End-users and Prohibited End-users) Order 2010, lists the restricted and prohibited parties with which the Malaysian trading community should restrain from pursuing commercial deals.[18,17] The prohibited end-user list is based on relevant UN resolutions e.g.: Iran (UNSCR 1696, 1737, 1747, 1803, 1929); North Korea (UNSCR 1718, 1874); Libya (UNSCR 1970) that list the individuals and associated companies that are under sanctions. The Restricted end-user list names the countries restricted by the United Nations from obtaining arms and military equipment, namely North Korea, Iran, Congo, Ivory Coast, Lebanon, Sudan, Afghanistan, Iraq, Liberia, Rwanda, Somalia, Eritrea, and Libya.

Implementing the Act

Steps to implement the Act began following the establishment of the Secretariat. Yet the Act gained greater traction only when the Regulations and Orders were in place. Some of the more important actions taken to put into place the necessary infrastructure for the implementation and enforcement of the Act are as follows:

Organizational Set-up of the Implementing Body

The implementing Secretariat was first established on August 15, 2010 with a skeleton manpower of seconded officers and staff from other business units within the Ministry of International Trade and Industry. It took another two months for the powers-to-be to approve the permanent staffing for the Secretariat. Fortunately, the skeleton staff who were initially seconded to the Secretariat had some knowledge of strategic trade controls as they had participated in outreach programs organized by the United States and the European Union held even before the law was adopted in Malaysia. A number of these officers had also been incorporated into the team under the AG Chambers during the drafting phase of the STA. Their participation in the outreach programs and the drafting committee had also exposed them to personalities in other agencies whose cooperation would be essential for the successful implementation of the STA 2010, as well as contacts in friendly foreign countries and international organizations that could be harnessed for capacity-building programs and other forms of assistance.

---

[16]Available (upon subscription) at the <http://www.lawnet.com.my/ lawnetPublic/> or it can be purchased from the Government Printers - Percetakan Nasional Berhad.

[17] Mohamed Shahabar Abdul Kareeem, "Facilitating Trade in a Secure Trading Environment," *1540 Compass*, <http://cits.uga.edu/1540compass/issue_2>.

The permanent manpower of the Secretariat was small and lean, consisting of twelve officers (excluding five support staffs), which includes the Controller and a Deputy. These twelve officers were placed under three working Units, each doing a multitude of job functions: permit issuance, outreach, audit, advisory, policy formation, and information technology. Of note, the core function of licensing or permit issuance is shared by all three Units.

One of the innovations to the organizational structure was the creation of a unit to house seconded officers from three Government Agencies, namely from the AG Chambers (to provide legal advisory services for the Secretariat), the Royal Malaysia Customs Department (to act as the liaison between the said Department and the Secretariat) and an officer from the Science and Technology Research Institute for Defense (STRIDE) (to provide technical advisory services on strategic items for the Secretariat and other stakeholders). These seconded officials are an asset to the organization as they are available to provide first-hand advice immediately on request by either the Secretariat or the business community. In addition, they are used as resource persons in their area of expertise in outreach programs conducted with the business community.

Helping Hand from External Partners

Two foreign countries, Australia and Singapore receive credit for helping frame the thinking behind the final organizational structure adopted to implement the 2010 STA. In the case of Australia, an invitation was received from the Australian Embassy in Malaysia to visit Canberra to learn from the Australian experience in dealing with strategic trade controls. The briefing that took place at the Department of Foreign Affairs and Trade (DFAT) was attended by most of the Australian Agencies involved in strategic trade controls in Australia, including representatives from the Prime Minister's office, the Customs Department, Nuclear Agencies, the Australia Group (international control regime), and many others. The full day briefing covered issues such as organizational structure, inter-agency cooperation, how decisions are made to allow or deny exports, who is involved in the inter-agency process, who provides the technical inputs to determine whether an item is strategic or not, what are the procedures adhered to in order to resolve issues when Agencies cannot find solutions to a policy issue, and how controls are enforced.

Singapore also shared its experience in implementing strategic trade controls in a briefing on implementation of its Strategic Goods (Control) Act. The briefing, attended by representatives from the Ministry, the Customs Department and the liaison officer on strategic goods from the Singapore Ministry of Defense, was held at the Ministry of Trade in Singapore.

These two working visits were eye openers and provided an excellent foundation for implementation of the STA 2010 in Malaysia. While the eventual model adopted by Malaysia was adapted to suit the Malaysian environment and national interests, it provided a quick and effective lesson on strategic trade controls that allowed Malaysia to get onto the task of implementing the law within four and a half months.

Outreach to Stakeholders

Nobody had gauged the response of the business community on the enactment of the STA 2010 until the laws were passed. To rectify this, the Secretariat started outreach programs to its core stakeholders, the business community, as soon as the Secretariat was established. The initial reception was hostile. The business community had many questions. The Secretariat had no ready answers. Answers were not available as the Regulation and Orders had not even been adopted. The Secretariat also had to answer a barrage of accusations and criticisms, including claims that the private sector had not been consulted on the bill, that the STA 2010 was a product of an "arm-twisting strategy" by foreign countries with vested interest, and that by adopting the law the Malaysian government had compromised its national interests and sovereignty.

To obtain stakeholder buy-in, one of the first actions of the Secretariat was to coin a catchy caption to

promote the STA 2010. The Secretariat sought to convince the business community that the STA would facilitate trade without compromising the security of exports and wider national interests. The caption that was finally adopted to push this message was *"STA 2010: Facilitating Trade in a Secure Trading Environment"* and it was used by the Secretariat when it embarked on its first outreach program itself.[19,18]

In the first three years of the Secretariat's existence more than 200 outreach programs were held all over Malaysia.[20,19] Some were conducted with the assistance of foreign partners such as the United States, the European Union, Japan, and Australia, but most were done by the Secretariat itself. The outreach took place in many forms. In most cases, the Secretariat arranged for large briefings to the business community, sometimes on its own or in collaboration with foreign partners or with the Malaysian trade and industry associations. These events were attended by 50 to 200 participants each session. The briefings were mostly general in nature and were also used by the Secretariat to also get feedback from the business community on the plans to implement the Act.

Harnessing private sector support was critical for the successful implementation of the STA. The Secretariat soon found a way of dealing with the initial hostility toward the STA. While there were people who were not happy with the implementation of the law, there were also others, primarily individuals working in large multinational companies, who acknowledged that the law was necessary. These individuals realized early that it was in their own interests to collaborate with the Secretariat and ensure that the rules were consistent with their company's economic interest. A few of these individuals did in fact offer to be used as resource persons in the outreach programs. Using private sector resources to talk to their peers was an effective strategy to garner private sector support. Listening to and acknowledging the private sector's concerns on the implementation of the STA 2010 had the effect of calming most skeptics and also providing them the assurance that the Secretariat was willing to listen to their concerns and suggestions.

Outreach to the business community is by itself insufficient for the effective implementation of the STA. Other important stakeholders are the government agencies that should work in tandem with the Secretariat and provide support for the implementation and enforcement of the Act, such as the Customs Department, and the three other Agencies that are authorized to assist the Secretariat in the issuance of permits, namely, the Atomic Energy Licensing Board (AELB), the Malaysian Communications and Multimedia Commission (MCMC), and the Pharmaceutical Services Division of the Ministry of Health,.

Other targets for outreach in the Government included the agencies involved in the enforcement of the law and those involved in the prosecution of offenders, namely the Attorney General Chambers, the Customs Department, the Department of Police, the Malaysian Maritime Enforcement Agency, and the Malaysian Communications and Multimedia Commission. Outreach sessions in many of these Agencies such as the Customs and Police Departments have to be undertaken repetitively and frequently as there is a high turn-over rate and staff rotation. This is compounded further by the sheer number of personnel in these Departments who are front-liners involved in handling strategic items almost on a daily basis, necessitating them to have at least an elementary knowledge of strategic trade controls.

Among other outreach tools used were specific briefings to large and small exporters exporting strategic items, web-page information including the creation of a Frequently Asked Question and answers to these crucial questions, weekly "meet your client day" with the Secretariat, newspaper articles on the need for export controls, including strategic export controls in speeches given by the Minister, and site visits to brief leading companies involved in exporting strategic items.

---

[19] Mohamed Shahabar Abdul Kareeem, "Facilitating Trade in a Secure Trading Environment," *1540 Compass*, <http://cits.uga.edu/1540compass/issue_2>.

[20] Information on the Strategic Trade Secretariat and scheduled outreach programs are available in <www.miti.gov.my/sta>.

Harnessing the Benefits of Information Technology

The Secretariat, at the very outset, sought to employ the benefits of information technology to its fullest to implement the STA. The objective was to create a comprehensive electronics system to manage not only the trade control licensing process, but to directly link the three other partner licensing agencies and the enforcement agencies together for effective implementation and enforcement. Using information technology also facilitates trade by cutting down the time required for applying, processing, and approval of permits, and is costs effective due to the minimal payments for services rendered by the systems provider. It has the future potential to link the system to strengthen strategic trade controls at the regional or global level.

In April 2011, *the STA e-permit system* was launched officially by the Minister of International Trade and Industry.[21] At this launch, twelve selected multinational companies that are exporters of strategic items were handed *electronic keys* (USB tokens with encrypted electronics passwords and signatures embedded) that would provide them access to the STA e-permit system. At this launch, these companies were requested to use the system and report back on its weakness and make recommendations for further improvements. The idea was to open the system for wider use only when the system is deemed robust, reliable and effective.

The STA e-permit system requires the permit applicant to first open an account with the services provider. Once the account is opened, the company can move to the next phase, which is, fill in the electronics registration form in the e-permit system. The registration captures information such as company details, strategic items exported and details on end-users that the company currently deals with. It is mandated that the registration be undertaken by the person authorized by the management in the company as the export control manager.

Each company is also allowed to apply for a maximum of five electronic keys to facilitate application for permits through the system and these are assigned to individuals who the company has authorized to apply for permits. The idea to ensure that management bears full responsibility for any misuse of the e-permit system and also to contain the number of personals within a company that have access to the e-permit system.

When the Secretariat has evaluated and is satisfied with the information provided, the company is informed of the type of permit that is approved (single-use, multiple-use, bulk-use or special permit) and thereafter, for the next two years, the company can continue applying for permits and receive approvals using the system. The company will undergo an audit within these two years to determine whether the company is compliant with the STA 2010 and whether the e-permit facility can be extended for another two years.

The approval for the company to apply for permit through the e-permit system only applies to existing strategic items and known end-users that had been pre-approved by the Secretariat. Any change to product specifications or the addition of new strategic items or adding in new end-users would require the Secretariat's approval first. The system will block permit applications for unregistered strategic items and unknown/unrecognized end-users and would also reject any application for export permit for restricted or prohibited end-users who are listed in the Restricted and Prohibited End-Users Order of STA 2010.

The e-permit system is directly linked to the three partner licensing agencies and the system itself routes the permit application to the relevant licensing agency, in this case to the Atomic Energy Licensing Board for nuclear related items, multimedia items including software and intangible technology to the Malaysian Communication and Multimedia Commission and bacteria, viruses and pathogens to the Pharmaceutical Services Division under the Ministry of Health.

[21] Dagang Net, <www.dagangnet.com/index.php/products/epermit_sta>.

Linking the E-permit System with the Customs Department for Enforcement

When a permit is approved or rejected by any of the licensing agency, the company receives this information directly through the e-permit system. If approved, a permit is issued. The permit lists the name of the company to which the permit is granted, the items and quantities approved for exports and the end-user/ users concerned. The system also generates a unique license number for the permit. This information is then directly lodged electronically in the Customs Information System for enforcement purposes.

Since 2011, all exporters in Malaysia exporting any item, strategic or not, have had to make a declaration in a field created in the customs export form (amended to take care of requirements under the STA 2010) regarding whether the item exported is a strategic item under the STA. If the exporter acknowledges it is a strategic item, the system will prompt for a STA permit license number. Failure to provide the right permit number, exceeding the quantity of items approved for export or entering an unapproved end-user as the consignee leads to the Customs Information System to block the export declaration to be processed.

Linking the e-permit system with the Customs Information System is an effective enforcement tool as other than the risk management system of random checks conducted by the Customs Department, the exporter's own declaration at the point of export places extra trade controls on every export transaction from Malaysia. It doubles the layer of enforcement controls at the border. With the declaration made through the Customs export forms, the exporter takes full responsibility for whatever is exported. In the event of the exporter running afoul of export control laws, the authorities have several options to charge them - under the Customs Act for mild offences such as miss-declaration, or under the STA 2010 for more severe offenses where higher penalties can act as a more effective deterrent or punishment.

Effectiveness and Limitations of STA 2010

The implementation of the Strategic Trade Act in Malaysia can be used as a case study on how and what should be done or avoided by other countries in the process of adopting similar laws and regulations on strategic trade controls. Countries interested in developing strategic trade controls may want to avoid some of the pitfalls but look positively at some of the good practices that worked in Malaysia when it comes to enactment, implementation, and enforcement.

The elements that enabled Malaysia to implement and enforce the Act in record time are described below.

Comprehensive Legislation

The Strategic Trade Act

The drafters of the Strategic Trade Act produced comprehensive legislation that fulfills the requirements of UNSCR 1540. The law provides all-important controls over export, transit, transshipment, brokering and other restricted actives, including the provision of technical knowledge. It also ensures that all other relevant laws that traditionally control exports continue to remain relevant but with a proviso that if any of them are in conflict with the STA, the Strategic Trade Act shall prevail. This provides a hassle-free law to the implementer and prevents turf wars from derailing efforts to enforce the Act. This created tensions in the initial period of the implementation and enforcement of the law but active engagement with relevant agencies by the Secretariat in inter-agency consultations soothed the situation. The law also allowed three technical agencies that were already issuing export permits to continue issuing permits under their own legislation but also allowed them to issue permits for similar items that are deemed to be covered under the STA. They do this on behalf of the STA Secretariat and on terms and conditions established by the Secretariat.

Separating Legal Instruments into Laws and Regulations

One of the strength of the Strategic Trade legislation is that it separates the legal instruments that require the approval of the legislative assemblies and those that can routinely be amended by issuing a notice in the official gazette. In this regard, any amendment to the STA 2010 has to be tabled in Parliament but the Regulations and the Orders need not go through this process. Based on feedback from the business community, the Secretariat used the flexibility under the Customs Act to issue improved end-user and delivery verification statements only few months after the Secretariat was established. The Strategic Trade (Strategic Items) Order was also amended in 2013; a year after the European Union adopted a new list. Such flexibility afforded by the law is important, as the implementers need not wait many years to make changes that may be immediately required to more effectively implement and enforce the law.

Adequate Powers Given to Implementers and Enforcement Agencies

The STA 2010 provides a very strong mandate to the Secretariat and the Controller. The law has vested vast powers to act quickly to stop proliferation from occurring, seek assistance from any party - domestic or foreign - to implement and enforce the Act, make the final decision on whether the item is strategic, and in general provide adequate legal support and protection for those involved in the implementation and enforcement of strategic trade controls. Giving adequate powers to implementers and enforcement agencies under the strategic trade laws is important as quick actions may be required to stop proliferation threats. Similarly the powers provided should be used to facilitate legitimate trade.

The E-permit Infrastructure

On-line Registration of Exporters and Permit Issuance

The decision by the Secretariat from the outset to harness the Internet for the registration of exports and brokers of strategic items and the issuance of permits under the STA helped in the effective implementation of strategic export controls. A robust and versatile STA e-permit system was in fact operational within eight months of the Secretariat's establishment. In the interim, permits were issued manually.

Before using the e-permit system to apply for permits, all exporters were required to register their company particulars, the personnel in charge of exports, the strategic items exported and all their known end-users of the products into the system. The registration is approved by a committee which decides on the type of permit to be given to the company. Bulk and multiple use permits are only given to companies that have Internal Compliance Programs. The company is also required to have all end-user statements for verification by the Secretariat within six months after the company is first issued with a permit. Using information technology was of immense help in buying in stakeholders' support for the implementation of STA 2010.

Lean Staffing Requirements with the Use of IT

Using the Internet placed less pressure on the staffing of the Secretariat. With only fourteen people in the Secretariat, the fledgling organization could not afford delays in decision making on exports as it would affect the business community. The e-permit system was the savior. It allows registered end-users to be crossed checked against on-line restricted end-users lists from various sources, get technical advice from experts, allow security checks on authorized personnel in the company who are allowed to apply for permits, provides access to information on strategic exports by partner agencies and Customs, and allows companies to continuously include new end-users (the Secretariat has to approve the new end-user before a permit is issued).

Costs of Doing Business Did not Increase Substantially

While the Secretariat itself does not impose any charges for its services, the e-permit service provider charges a minimal fee of less than USD 1.50 per approved permit only. Those approved with bulk or multiple use permits however only pay once as the permit allows multiple time usage to approved end-users until its expiry in two years. The business community's initial fear that the implementation of the STA would increase their costs of doing business turned out to be unfounded. The business community quickly adapted to the requirements of STA 2010, including the upgrading of their computer systems and software to apply for STA permits for their strategic exports.

The Limitations

Implementation and enforcement of STA 2010, while smooth in most instances, had its limitations as well. Some of the limitations that were experienced in the initial stage of the implementation of the STA 2010 are:

Timeline Given for Implementation

It took Singapore four years from the enactment to the implementation/enforcement of the law. This provided the Singapore authorities time to educate the business community and buy in their commitment and support and put in place the required supporting infrastructure for the application and issuance of permits. In the case of Malaysia, the time taken to implement the law was only about four months, which was further complicated by publication on the Gazette of the Regulation and Orders at almost the eleventh hour. Malaysia could have avoided some of the initial headaches it experienced if some additional time had been left for the business community to take adequate preparations to meet the requirements of the law. It would have also given the Secretariat time to reach out to the business community, prepare the implementing infrastructure and improve the expertise and knowledge of implementing agencies.

A time period of at least one to two years between the passage of the law and its implementation would have been ideal. Several important foreign investors and exporters of strategic items in Malaysia, as a precautionary measure and wanting to ensure that their operations would not be affected by the uncertainty posed by the sudden implementation of the STA, did in fact move their distribution center for certain fast moving items to third countries as they were clueless about how the STA would be implemented on the implementation date. Such anxiety could have be avoided if a proper timeline for implementation and enforcement would have been communicated early to all stakeholders and carried out systematically according to schedule.

Inadequate Consultations with Private Sector

One of the main grievances expressed by the private sector as soon as the law was passed is that they had not been consulted. The private sector, especially the multinationals, had decades of dealing with export control and could have given valuable advice and direction on the law itself and how it could be implemented to suit local conditions. The Secretariat, once established, harnessed the vast knowledge available locally to implement the law in a business friendly manner. Consultations with the private sector led to several amendments, including to the end-user and the delivery verification statements within six months after the implementation of the Act. The private sector was of immense help in the initial period of the STA 2010 implementation as the vast majority wanted to comply with the law.

Heavy Penalties under the Law

Although it is not the Secretariat's or civil servant's job to question the law, as front liners they cannot avoid facing questions and justify the thinking behind each and every provision in the law. STA 2010 is

the only strategic trade control law in the world that includes the death penalty as a potential sanction. A chargeable offense under the Act can also be registered for knowingly or unknowingly exporting strategic items without a permit. In addition, it imposes high fines (as high as RM 30 million) for offenses under the Act. These are no doubt effective deterrents but whether these are suitable for application in a trade related instrument is questionable. At least in one case, a marketing manager of a multinational company operating a distribution center in Malaysia wanted to tender his resignation as he was disturbed by the thought that he would be held liable under the law even if a mistake is committed by someone else as he bears overall responsibility in the company when a product is exported. In his view the penalties are too heavy for him to take personal responsibility.

Conclusions

Malaysia's decision to adopt strategic trade controls was an important one. It allowed the country to receive instant recognition as one of the countries that has joined the global non-proliferation fight. An additional advantage that strategic trade controls had vested on the country is the view that it is a safe place to conduct trade and locate investments in sensitive products and technology. The journey to implement strategic trade controls in Malaysia was no doubt difficult and challenging but the eventual result is satisfying. Malaysia has shown the world that given the right push and conditions, strategic trade controls can be implemented and enforced very quickly. If Southeast Asian nations have doubts about endorsing strategic trade controls, they need not look further than Singapore or Malaysia to be convinced. While the road to implementation will not be smooth, there are assistance programs available to help cross some of the hurdles when they arise. While a challenge, adoption and implementation of strategic trade controls is worth the journey.

Other References

Kelley Sayler, 'Malaysia, Export Controls, and the Nuclear Black Market," CSIS, March 24, 2011 <http://csis.org>.

Export Controls, Special Sessions, "EU Non-Proliferation and Disarmament Conference 2014 Special Session 7," September 4, 2014, <www.iss.org>.

The Strategic Trade Management Regime in the Philippines

KARLA MAE G. PABELIÑA[1]

Abstract

This paper will lay out the history of the Philippines' decision to adopt and implement strategic trade management, analyze the various initiatives taken towards the enactment of strategic trade legislation, and examine the key provisions of the Strategic Trade Management Act (STMA). It will also discuss the capacity-building and industry outreach programs conducted by the Philippines in partnership with various partner-states and international agencies.

Keywords

Export control, strategic trade control, Philippines, Strategic Trade Management Act

Introduction

On November 13, 2015, Philippine President Benigno S. Aquino III signed and enacted into law Republic Act No. 10697 or the Strategic Trade Management Act (STMA). The STMA enforces measures that will prevent the proliferation of weapons of mass destruction (WMD) from or within the Philippines. The STMA was passed in time for the 2016 Comprehensive Review of the implementation status of United Nations Security Council Resolution (UNSCR) 1540.

The journey towards the establishment of a strategic trade management regime in the Philippines has been long and arduous. It is marked by difficulties in reaching consensus on the development of an appropriate legal structure or institutional mechanisms to effectively implement a strategic trade management regime. The regime features the totality of legal, institutional and technical policies and procedures for controlling import, export, and transit of strategic and dual-use items. These include "the capacity to interdict and prevent illicit shipments (enforcement), installing of standardized licensing procedures and practices (national licensing system), and good industry coordination."[2]

[1] Karla Mae G. Pabeliña is a Foreign Affairs Research Specialist with the Center for International Relations and Strategic Studies of the Foreign Service Institute (FSI). She is a graduate of BA Political Science from the University of the Philippines, Diliman. She is currently persuing her Master in International Studies. She has background in security, development and international relations.

[2] Briefing paper of the Office of the Special Envoy on Transnational Crime (OSETC) on the Weapons of Mass Destruction-Commodity Identification Training (WMD-CIT) Program.

This paper will lay out the history of the Philippines' decision to adopt and implement strategic trade management, analyze the various initiatives taken towards the enactment of strategic trade legislation, and examine the key provisions of the STMA. It will also discuss capacity-building and industry outreach programs conducted by the Philippines in partnership with various partner-states and international agencies.

The Philippines and the Nonproliferation Regime

The Philippines' commitment to establishing a strategic trade management regime stems from its support and commitment to the principles of international law for the promotion of global peace and security.[3] The Philippines subscribes to and is party to all major nonproliferation and disarmament conventions including the Treaty on Non-Proliferation of Nuclear Weapons (NPT), Chemical Weapons Convention (CWC), Biological and Toxic Weapons Convention (BTWC), Convention on the Physical Protection of Nuclear Materials (CPPNM), Convention for the Suppression of the Financing of Terrorism (TFC), Hague Code of Conduct on Ballistic Missiles (HCOC), Program of Action on Small Arms and Light Weapons (PoA-SALM), Convention on Certain Conventional Weapons, and the Arms Trade Treaty (ATT).[4]

Recognizing that proliferation of WMD as well as their means of delivery to non-state actors constitute a threat to international peace and security, the Philippines together with France, Romania, the Russian Federation, Spain, the United Kingdom of Great Britain and Northern Ireland, and the United States of America co-sponsored UNSCR 1540, which was unanimously adopted by UN Member States in 2004. Resolution 1540 is a direct and binding commitment for all states to "refrain from providing any form of support to non-state actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use" WMD and their means of delivery; to "adopt and enforce appropriate effective laws which prohibit any non-state actor to manufacture, acquire, possess, develop, transport, transfer, or use" WMD and their means of delivery; and to "establish controls to prevent the proliferation" of WMD and their means of delivery.[5]

In the statement of Philippine Permanent Mission to the UN Ambassador Rafael Baja following the voting on the resolution, he argued that the Philippines' co-sponsorship is "recognition of the clear and present danger of WMD that could be used for terrorist activities falling into the hands of non-state actors."[6] He emphasized that "there is a serious gap in existing regimes in the terms of addressing this threat to the international peace and security" and adherence to resolution 1540 "reflects the Philippine Government's serious policy of countering terrorism."[7]

The Philippines' Vulnerability Factors

The commitment of the Philippines to resolution 1540 is in line with its stance against terrorism particularly in the Southern Philippines. Violent armed groups in the country have killed or injured more than 1,700 people in bombings and other attacks from 2000 to 2007.[8] One of the worst terrorist attacks in the

---

[3] Philippine Statement Delivered by H.E. Ambassador Lourdes O. Yparraguire at the General Debate 2015 Review Conference of Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, April 28, 2015, New York.

[4] The Philippines is also a party to the Joint Convention on the Safety of Spent Fuel Management and the Safety of Radioactive Waste Management (JC), Convention on Nuclear Safety (CNS), and International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT). It is a participant of the Proliferation Security Initiative (2005) and an active member of the Global Initiative to Combat Nuclear Terrorism (GICNT) and the G8 Global Partnership against the Spread of Materials and Weapons of Mass Destruction.

[5] Security Council Resolution 1540, S/Res/1540, April 28, 2004, <http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540(2004)>

[6] Remarks of Philippine Permanent Mission to United Nations, 4956th Meeting of the United Nations Security Council, April 28, 2004.

[7] Ibid.

[8] "Philippines: Extremist Groups Target Civilians," *Human Rights Watch*, July 30, 2007, < https://www.hrw.org/news/2007/07/30/

Philippines happened in February 2004 when a bomb planted by the Abu Sayyaf Group sunk SuperFerry 14, killing approximately 130 passengers.[9] The Philippines was also tagged as a "terrorist safe haven" and home to a number of militant groups including the Abu Sayyaf Group, Jemaah Islamiyah, the Communist Party of the Philippines/ New People's Army, the Moro National Liberation Front (MNLF), and the Moro Islamic Liberation Front (MILF).[10] The Philippines' concern over the proliferation of WMD to non-state actors is further amplified by two 'vulnerability factors' affecting the country – geographic and economic vulnerability.[11]

Geographic Vulnerability

The 2011 US State Department Country Report on Terrorism brought to fore the risk of the country's porous southern borders being used by non-state actors to transport WMD. There is a high risk of WMD trafficking, proliferation, and the spread of WMD-applicable expertise "given the high volume of global trade that ships through the region as well as the existence of proliferation networks looking to exploit vulnerabilities in states' export controls."[12]

The risk of the Philippines being used as transfer, diversion, importation, exportation, re-exportation, transit, and transshipment port is not remote. On May 26, 2012, Parviz Khani, an Iranian citizen, was arrested by the Philippine National Bureau of Investigation (NBI) agents at the Ninoy Aquino International Airport (NAIA) on request of the US Department of Justice after he was indicted in the District of Columbia for being part of a conspiracy to smuggle to Iran about 20 tons of specialized steel with "nuclear applications."[13] Khani had been attempting since 2008 to procure strategic items that may increase Iran's ability to enrich uranium and/or construct a heavy water moderated research reactor prohibited by UN Security Council resolutions.[14]

In November 2012, Daniel Frosch, an Austrian citizen, owner of a small spare parts export company reportedly involved in delivering Iran dual-use items such as accelerators, condensers and capacitors, was extradited from the Philippines to Austria.[15] Frosch is allegedly also connected with Industrial Equipment Service Group (IESG) Trading & General, a Philippine company providing electronic components and machine tools suspected to have dual use capacity.[16]

Economic Vulnerabilities

Globalization has impacted the Philippines in significant ways. Interactions and transactions are happening

philippines-extremist-groups-target-civilians>.

[9] Marichu Villanueva, "Superferry Sinking a Terrorist Attack," *Philippine Star*, October 12, 2004.

[10] United States Department of State, "Country Reports on Terrorism 2005," Office of the Coordinator for Counterterrorism, April 2006.

[11] Ronald A. Rodriguez, "Countering the Threat of the Proliferation of Weapons of Mass Destruction: Philippines Perspective and Responses," *Issues and Insights* 6:4, Pacific Forum CSIS, January 2006.

[12] US Department of State, "Terrorist Safe Havens (Update to 7120 Report) 5.1.a – 5.1.b. Strategies, Tactics, and Tools for Disrupting or Eliminating Safe Havens," Country Reports on Terrorism 2011, Chapter V, < http://www.state.gov/j/ct/rls/crt/2011/195549.htm>.

[13] "U.S. Charges Men in Plot to Violate Iran Embargo," *The New York Times*, July 13, 2012 <http://www.nytimes.com/2012/07/14/world/middleeast/two-men-charged-with-violating-iran-embargo.html?_r=0>.

[14] United States Department of State, "Increasing Sanctions Against Iran," Office of the Spokesperson, July 12, 2012, <http://www.state.gov/r/pa/prs/ps/2012/07/194924.htm>.

[15] Nick Gillard, "Catch Me if You Can: The Illicit Trade Network of Daniel Frosch," Proliferation Case Study Series, Project Alpha, King's College, London, 2015, <https://projectalpha.eu/proliferation/item/380-new-alpha-case-study-the-illicit-trade-network-of-daniel-frosch>.

[16] Ibid.

at unprecedented speed, growing magnitude, thickening density and increasing complexity. Globalization has provided new economic opportunities and security challenges for the Philippines. Economic integration is transforming the region into "a single market and production base, a highly competitive economic region, a region of equitable economic development, and a region fully integrated into the global economy."[17] The ASEAN Economic Community (AEC) is the seventh largest in world, and third in Asia, with a gross domestic product of $2.6 trillion in 2014.[18] Following the formal establishment of AEC in 2015, ASEAN is forging towards deepening its economic integration, ascending the global value chains into more sustainable production activities, higher technology intensive manufacturing industries and knowledge intensive industries.[19]

The risk that with freer trade of goods, the region may be used as a hub for the illicit trade, transfers or diversion of sensitive items and commodities that have WMD significance, raises security concerns. Governments of Southeast Asian countries are examining the feasibility of linking strategic trade management and trade facilitation endeavors, including the ASEAN single window initiative to expedite the free flow of goods while at the same time strengthening supply chain security.

Domestic Translation of International Commitments

Even if the Philippines recognizes its proliferation risks and is strongly committed to various international covenants, it has been constrained to fully comply with all the attendant requirements of its international obligations. The Philippines has been challenged to make substantial progress in effectively adopting domestic laws on countering the proliferation of WMD.[20] One such obligation involves the effective implementation of a strategic trade management regime.

In the sponsorship speech of Senator Antonio Trillanes before the Philippine Senate, he argued that while the other countries in Asia-Pacific were able to adopt appropriate pieces of legislation, the Philippines has been left behind in its commitment to the UNSCR 1540. The Philippines have control, regulation, and licensing activities that deal with prohibited and regulated items, but these activities are implemented by various government agencies. There is no comprehensive system that covers the entire list of controlled items under multilateral export control regimes.[21]

Towards Strategic Trade Management Legislation

House Bill No. 6268 and Senate Bill No. 3268

The first proposed bill on Strategic Trade Management was filed at the Fourteenth Congress in 2009. The draft legislative proposal was derived from the output of an inter-agency technical working group on Export Control headed by the Office of the Special Envoy on Transnational Crime (OSETC), with the Department of Trade and Industry (DTI), and the Bureau of Customs (BOC). House Bill No. 6268 and Senate Bill No. 3268 were concurrently examined by the Committee on Public and Safety at the House of Representatives, and the Joint Committees on National Defense and Security, Finance, and Public Order and Dangerous

[17] Association of Southeast Asian Nations (ASEAN), ASEAN Economic Community Blueprint, (Jakarta: ASEAN Secretariat, 2008).

[18] A Blueprint for Growth, ASEAN Economic Community 2015: Progress and Key Achievements (Jakarta: ASEAN Secretariat, November 2015).

[19] Ibid.

[20] The Philippines, as state party to the Chemical Weapons Convention, is also in the process of finalizing the Chemical Weapons Prohibition Act, which is still pending review at the Congress.

[21] Sponsorship Speech of Senator Antonio F. Trillanes IV, Sixteenth Congress Second Regular Session, May 12, 2015

Drugs, at the Senate.[22,23] Unfortunately the proposed legislation did not pass beyond the Technical Working Group (TWG) deliberations conducted by the Committees.

The main issues of contention include the rationale for the legislation, conceptual terms, and composition of the authorizing agency. There were differences on whether to include conventional or unconventional weapons, limit the legislation's scope to Chemical, Biological, Radiological and Nuclear (CBRN) materials, or focus only on strategic and dual-use items. There were disagreements regarding whether to adopt internationally-recognized definitions of concepts such as dual-use, strategic items, and weapons of mass destruction. There were unresolved questions on which should be the authorizing agency in Strategic Trade Management.[24] In establishing an organizational structure, the TWG tried to synchronize all government efforts and ensure that no functions were duplicated or existing authorities undermined. The proposed bills were shelved, and are currently pending in the Committees.[25]

House Bill No. 4030 and Senate Bill No. 115

As the previous attempt was unsuccessful, efforts started anew in enacting a law on Strategic Trade Management during the First Regular Session of the Fifteenth Congress in 2010. House Bill No. 4030 and Senate Bill No. 115 were filed and subsequently referred to the Committee on Public Order and Safety at the House of Representatives, and Joint Committees of Public Order and Dangerous Drugs, National Defense and Security, and Finance, at the Senate.[26,27]

A TWG was again convened in both houses to examine the technical and substantive issues or constitutional infirmities of the proposed bills. The TWG conducted public hearings and invited representatives from concerned agencies (OSETC, Philippine National Police (PNP), Department of National Defense (DND), Department of Environment and Natural Resources (DENR), Department of Health (DOH), Department of Foreign Affairs (DFA), Department of Trade and Industry (DTI), Department of the Interior and Local Government (DILG), Department of Budget and Management (DBM), among others) to provide technical guidance on the nature of the measures proposed.

Discussions during the TWG meetings on House Bill No. 4030 centered on: (1) organizational development aspect of the implementing office, as well as some protocols that define and strengthen the capacity of the licensing office and law enforcement, its implementation, monitoring and progressive responses to new developments and challenges in its implementation once enacted[28]; (2) the institutional arrangements of the proposed Strategic and Dual-Use Goods and Items Control Council (SDGICC) and the Strategic Goods and

---

[22] House Bill No. 6268: "An act preventing the proliferation of weapons of mass destruction by regulating the transfer of strategic goods and items providing penalties for their violations thereof and other purposes," was filed by Representative Rodolfo W. Antonino.

[23] Senate Bill No. 3238: "An Act to Prevent the Proliferation of Weapons of Mass Destruction by Regulating the Transfer of Strategic Items/ Goods which are Being Used to Carry out Acts of Terrorism, and for other Purposes," was filed by Senator Manny B. Villar.

[24] Senate of the Philippines, Transcript of Technical Working Group Meeting, Committee on Public Order and Illegal Drugs, January 21, 2010, Fourteenth Congress Third Regular Session.

[25] The Fourteenth Congress was until June 2010. The bills were unfortunately overtaken by events particularly the National Elections of May 2010.

[26] House Bill No. 4030: "An Act Preventing the Proliferation of Weapons of Mass Destruction by Regulating the Provision of Technical Assistance, Brokering, Financing, and Transporting Services in Relation to the Management of Trade in Strategic Goods," was filed by Representative Rodolfo W. Antonino.

[27] Senate Bill No. 115: "An Act to Prevent the Proliferation of Chemical, Biological, Radiological and Nuclear Weapons, as well as Conventional Weapons by Regulating the Transfer of Strategic Goods and Dual-use Goods, and for Other Purposes," was filed by Senator Gregorio P. Honasan.

[28] Position Paper of the OSETC transmitted to the Committee on Public Order and Safety, House of Representatives, March 1, 2011.

Services Management Council (SGSMC)[29]; (3) the proposed accrual of the administrative fines to a special fund administered by the Council[30]; (4) the basis of the funding requirement indicated in the proposed bill[31]; (5) the inclusion of specific agencies in the SGSMC such as the Government Arsenal under the DND[32], the Office of Transport Security, the Philippine Coast Guard, the Philippine Ports Authority under the Department of Transportation and Communication (DOTC)[33], Bureau of Export Trade Promotion (BETP) under the DTI[34], Center for Device Regulation, Radiation, Health and Research of the Food and Drug Administration (FDA) of the DOH,[35] Union of Local Authorities of the Philippines of the DILG,[36] and (6) the need for wide-ranging consultations by concerned agencies and other stakeholders in the development of a National Control List so that the proposed strategic trade management legislation does not impede trade activities and the conduct of legitimate research in the fields of biotechnology, agriculture and medicine.[37] The outcome of the TWGs on House Bill No. 4030 was a substitute bill drafted by the House Committee on Public Order and Safety which was ready for filling at the plenary.

Meanwhile, TWGs were also concurrently conducted on Senate Bill No. 115. The Senate TWGs convened and attempted to thresh out differing opinions on the functions and composition of an interagency council, extraterritoriality application, and the inclusion or non-inclusion of conventional weapons in the coverage of the bill. Another important issue examined was whether the creation of the council would make reference to establishing an "organizational structure," or whether an Office of an Executive Director would be charged with manning the day-to-day operations of strategic trade management. Under this office are the different units involved in licensing, monitoring, investigation, audit, internal compliance, and international relations. As the council is the governing and policy-making body, the TWG notes that translating the functions into formulation, implementation, coordination and monitoring would require such organizational structure.[38]

Nonetheless, the Office of the Executive Secretary, upon review of the pending bills filed in Congress, decided to draft an Administration version of the bill. Executive TWGs consisting of major departments/ agencies were created to address the issues and concerns that were otherwise not incorporated in the bills filed in Congress. The Presidential Legislative Liaison Office (PLLO) then made representations in Congress to stop consideration of pending measures until an administration draft was finalized.[39] Thus, the substitute bill for House Bill No. 4030 and the Senate Bill No. 115 did not progress beyond the Committee deliberations.[40]

House Bill No. 3206 and Senate Bill No. 1688

During the First Regular Session of the Sixteenth Congress in 2013, the House of Representatives and

---

[29] Comments of the DBM on House Bill No. 4030, transmitted to the Committee on Public Order and Safety, House of Representatives, June 10, 2011.

[30] Ibid.

[31] Ibid.

[32] Position Paper of the DND transmitted to the Committee on Public Order and Safety, House of Representatives, April 5, 2011.

[33] Comments of the PNP transmitted to the Committee on Public Order and Safety, House of Representatives, April 7, 2011.

[34] Position Paper of the DTI transmitted to the Committee on Public Order and Safety, House of Representatives, May 2, 2011.

[35] Position Paper of the DOH transmitted to the Committee on Public Order and Safety, House of Representatives, March 7, 2011.

[36] Position Paper of the DILG transmitted to the Committee on Public Order and Safety, House of Representations, June 8, 2011.

[37] Comments of the DFA transmitted to the Committee on Public Order and Safety, House of Representatives, March 2, 2011.

[38] Senate of the Philippines, Transcript of Technical Working Group Meeting, Committee on Public Order and Illegal Drugs, Joint with Committees on National Defense and Security and Finance, Fifteenth Congress Second Regular Session, April 17, 2012.

[39] Report of the Presidential Legislative Liaison Office on the Philippine Strategic Trade Management Act (STMA), February 24, 2016.

[40] Incidentally, the Philippine Senate convened as an impeachment court and tried Former Chief Justice Renato Corona. The hearing started on January 16, 2012 until May 29, 2012. Such impeachment proceedings may have affected the momentum of the Senate TWG deliberations.

Senate deliberated on House Bill No. 3206 and Senate Bill No. 1866, respectively.[41,42] House Bill No. 3206 and Senate Bill No. 1866 were subsequently referred to the Committee on Public Order and Safety at the House of Representatives, and the Joint Committees of Public Order and Dangerous Drugs, National Defense and Security, and Finance, at the Senate.

Concurrent with the deliberations of the Committees in the House of Representatives and Senate were the series of inter-agency consultations led by PLLO to come up with a consensus draft legislation on strategic trade management. This new draft legislation featured the consolidated comments and positions of various concerned agencies. Some of the major sticking points in the formulation of the consensus draft were the following:

- Justice Secretary Leila de Lima was opposed to the creation of a regulatory body for strategic goods for the reason that it would pose budgetary issues and require extensive capacity building for its officials. Secretary de Lima proposed that an inter-agency committee composed of the stakeholders be convened and that the Department of Trade and Industry be the agency to regulate trade.[43]

- The DBM proposed that the bill should clearly specify the role of the National Security Council (NSC), an existing government institution mandated to provide technical support and policy advice on all aspects of national security. The NSC, under the Administrative Code of 1987, is mandated to coordinate the formulation of policies relating to, or with implications on, national security. DBM also recommended that the functional relationship of STMA with the other government departments, including the National Intelligence Coordinating Agency (NICA), be clearly defined to avoid duplication of activities.[44]

After several inter-agency meetings, the consensus draft was finalized on January 28, 2015. Immediately, the PLLO submitted the new draft legislation to both the Committee on Public Order and Safety and the Senate Committee on National Defense as a substitute bill pending measures in both Committees.

Upon the recommendation of the Committee on Public Order and Safety, House Bill No. 3206 was substituted with House Bill No. 5822 or "An Act Preventing the Proliferation of Weapons of Mass Destruction by Regulating the Provision of Technical Assistance, Brokering, Financing, and transporting Services in Relation to the Management of Trade in Strategic Goods".[45] Meanwhile, Senate Bill No. 1866 was substituted with Senate Bill No. 2762 or "An Act Preventing the Proliferation of Weapons of Mass Destruction by Managing the Trade in Strategic Goods, the Provision of Related Services, and for Other Purposes." Committee Report No. 140 dated May 12, 2015 recommended the substitution of Senate Bill No. 1866 to Senate Bill No. 2762 for approval. This was followed by a period of debate, sponsorship speeches, and interpellations.

Senator Vicente Sotto III provided editorial amendments to Senate Bill No. 2762 or the draft Strategic Trade Management Act, particularly on Section V on the definition of Strategic Goods, Nationally Controlled Goods, and Section X on the Responsibilities of Persons. The bill with amendments was subsequently

---

[41] House Bill No. 3206: "An Act Regulating the Proliferation of Strategic and Dual-use Goods and Services, Providing Penalties for their Violation and for Other Purposes," or "Strategic Trade Management Act of 2013" was filled by Representative Francisco Ashley Acedillo.

[42] Senate Bill No. 1866: "An Act Regulating the Proliferation of Strategic and Dual-use Goods and Services, Providing Penalties for their Violation and for Other Purposes," or "Strategic Trade Management Act of 2013" was filled by Senator Antonio V. Trillanes.

[43] "DOJ Opposes Creation of Regulatory Office for Strategic Goods Trade" *Rappler*, October 6, 2013, <http://www.rappler.com/business/40683-doj-strategic-goods-trade-regulatory-office>.

[44] Report of the Presidential Legislative Liaison Office on the Philippine Strategic Trade Management Act (STMA).

[45] Minutes of the Meeting of the Committee on Public Order and Safety held on March 18, 2015, Sixteenth Congress, Second Regular Session.

approved for a Third Reading and unanimously adopted by the Senate. It was then transmitted to the House of Representatives for their consideration.

Since the two approved versions of the draft strategic trade management legislations were not identical, a bicameral conference committee was intended to be convened to harmonize the approved versions. However, upon intervention of the PLLO, the House of Representatives was convinced to adopt the Senate approved version as amendments.

On 13 November 2015, the consolidated bill was signed by President Benigno S. Aquino III which became Republic Act No. 10697 or "An Act Preventing the Proliferation of Weapons of Mass Destruction by Managing the Trade in Strategic Goods, the Provision of Related Services, and for other Purposes." R.A. No. 10697 is also known as the "Strategic Trade Management Act (STMA)."

The initiative to enact the STMA came from the Executive branch of the government. Since 2005, the OSETC convened a series of inter-agency consultations to lay the groundwork for the proposed strategic trade management legislation. Upon the initiative of the OSETC, draft legislations were filed in both the House of Representatives and the Senate in the 14th, 15th and 16th Congresses. Unfortunately, the proposed bills were not representative of the concerns raised by various stakeholders (DOJ, DBM, DFA, DTI, DOH, DOST, and DOTC, among others). Upon the instruction of the President, through the Executive Secretary, the PLLO was tasked to officially orchestrate the formulation and shepherding of the STMA. The PLLO raised the urgency of enacting the STMA through the inclusion of the measure in the legislative agenda priorities of the Cabinet Cluster on Security, Justice and Peace (SJP). The consensus STMA draft, which became the approved version of the bill, was a result of the initiative of the PLLO with other executive offices such as ATC-PMC, DTI, DOJ, DFA, DA, DILG, AFP, PNP, DBM and CSC. The PLLO also made significant interventions to break the impasse of the various agencies involved in the regulation of strategic and dual-use items.[46]

Key Provisions of the Strategic Trade Management Act

The STMA enforces measures to counter the proliferation of weapons of mass destruction (WMD) in the Philippines by regulating the movement or flow of dual-items, strategic goods and related services "consistent with its foreign policy, and national security interests, in support of efforts to counter terrorism, control crime and safeguard public safety."[47]

Implementing Structures and Mechanism

The central authority in all matters relating to strategic trade follows the rubric of the National Security Council (NSC), thus ensuring strong authority coming directly from the Office of the President through the Executive Secretary. The organizational setup of the NSC-Strategic Trade Management Committee (NSC-STMCom) is necessary for effective decision-making particularly in the exercise of its powers and functions.[48]

The NSC-STMCom is composed of the Executive Secretary as Chairperson, and the Head of Offices (as ex-officio members) of all the important government agencies necessary for the effective implementation of strategic trade management. These are the Secretary of Trade and Industry as Vice-Chairperson, the Secretary of Foreign Affairs, the Secretary of Justice, the Secretary of National Defense, the Secretary of the Interior and Local Government, the Secretary of Finance, the Secretary of Transportation and Communications, the

[46] Interview with the Presidential Legislative Liaison Office, February 24, 2016.

[47] "Section 2. Declaration of Policy," Republic Act No. 10697.

[48] "Section 7. Powers and Functions of the NSC-STMCom"

Secretary of Environment and Natural Resources, the Secretary of Science and Technology, the Secretary of Agriculture, and the Secretary of Health. The Anti-Terrorism Council (ATC) - Program Management Center (PMC) serves as the Secretariat.[49]

In the exercise of its functions, the following support agencies and bureaus also complement the NSC-STMCom:

- Bureau of Customs (DOF-BOC);
- Bureau of Animal Industry (DA-BAI);
- Food and Drug Administration (DOH-FDA);
- Bureau of Quarantine (DOH-BOQ);
- Philippine Nuclear Research Institute (DOST-PNRI);
- Information and Communication Technology Office (DOST-ICTO);
- Armed Forces of the Philippines (AFP);
- Philippines National Police (PNP);
- Philippine Coast Guard (PCG)
- Office of Transport Security (DOTC-OTS);
- National Bureau of Investigation (DOJ-NBI);
- Presidential Legislative Liaison Office (OP-PLLO);
- Office of the Special Envoy on Transnational Crime (OSETC); and
- Such other offices, agencies or units as necessary.

The Strategic Trade Management Office (STMO), the executive and technical agency for the establishment of strategic trade management, is lodged under the Department of Trade and Industry. The STMO will be the clearinghouse of all the licenses and authorizations for the trade of dual-use and strategic goods and related services. The STMO will develop and maintain the register and carry out registration activities; establish and maintain a comprehensive database information system on strategic goods and on persons engaged in the trade of strategic goods and the provision of related services. Also, in case of violations, the STMO has the power to issue warning letters, orders of corrective action and conduct investigations.[50]

National Strategic Goods List

Instead of using the term "National Control List", the Philippines opted to use the term "National Strategic Goods List (NSGL)" to refer to the descriptive lists of strategic goods subject to authorization. The NSGL will conform to international commitments and nonproliferation obligations pursuant to bilateral and multilateral treaties, international conventions and international nonproliferation regimes.[51] Industry outreach and consultations among the various stakeholders is being conducted to determine the goods, items, and technologies that will be subject to licensing.

End-Use Controls

The STMA imposes end-use controls on strategic goods that are not in the NSGL and related services. It also identifies the different circumstances where individual licenses or end-user certificates are required.[52]

Responsibilities of Persons in Strategic Trade Transactions

The STMA puts the responsibility of obtaining an authorization from the STMO on any person who

[49] "Section 6. Central Authority"

[50] "Section 9. Powers and Functions of the STMO"

[51] "Section 4. National Strategic Goods Lists"

[52] "Section 11. End-use Controls"

intends to engage in the export, import, transit, and transshipment of strategic goods. The STMA implicitly encourages the development and implementation by exporters of their own Internal Compliance Program (ICP) in the conduct of their strategic goods and services transactions. The STMA also requires that all records of the transaction and/or books of accounts, business and computer system, and all commercial and technical data be kept within a period of ten years from date of transaction.[53]

The STMA has extra-territorial application. It is applicable to any natural or juridical person operating within the Philippines as well as all Filipino persons providing import, transit, or transshipment of strategic goods wherever they may be located. It also identifies possible avenues for international legal cooperation in case an alien/ foreign national, or a Filipino residing in another country committed the violation.[54]

Exemptions from the Authorization Requirement

The STMA indicates the circumstances when the authorization requirement may be waived: the importing of strategic goods which will be used by the Philippine military or police forces; temporary exporting strategic goods to be used by Philippine military or police forces outside of Philippine jurisdiction, mainly in connection with military, peacekeeping or government humanitarian mission, and law enforcement activities.[55]

Liabilities, Violations, Penalties and Sanctions

The STMA imposes penalties and sanctions to officers of partnerships, corporations, and other juridical entities, government officials and employees as well as foreign nationals for the commission of criminal and administration violations. Should the persons or entity willfully and intentionally violate the provisions of the Act, they may be imprisoned for a period from six (6) years and one (1) day to twelve (12) years imprisonment, and fined from one million pesos (P1,000,000.00) to five million pesos (P5,000,000.00). Violations include failure to register, acts without an authorization; or acts in breach of the conditions and terms of an authorization or governmental end-use assurances; making false or misleading representations; conspiracy; forging or altering any documents issued by the STMO; among others[56]

The STMO may seek the assistance of the following agencies if there is prima facie evidence of criminal violations: (1) BOC on matters involving violations of import and export provisions of this Act as well as the Tariff and Customs Code; (2) PCG on matters involving violations that pertain to physical or outright smuggling on border security; or (3) PNP/NBI on acts involving violations outside the jurisdiction of the BOC and PCG.

The STMA grants the Regional Trial Court jurisdiction over criminal prosecutions for violation of any of its provisions, as well as over applications for the issuance and grant of applicable provisional remedies under the Rules of Court.[57]

International Legal Cooperation

The STMA also establishes the terms and conditions on international legal cooperation. The DOJ may request for assistance from a foreign state to: (1) take evidence or obtain voluntary statements from persons; (2) make arrangements for persons to give evidence or to assist in criminal matters; (3) effect service of

[53] "Section 10. Responsibilities of Persons"

[54] "Section 3. Scope and Coverage"

[55] "Section 15. Exemption from Authorization Requirement"

[56] "Section 19. Unlawful Acts"

[57] "Section 28. Jurisdiction"

judicial documents; (4) execute searches and seizures; (5) examine objects and sites; (6) provide or obtain original or certified true copies of relevant documents, records and items of evidence; (7) identify or trace property derived from the commission of an offense and instrumentalities of crime; (8) restrain dealings in property or freeze property derived from the commission of an offense that may be recovered, forfeited or confiscated; (9) recover, forfeit or confiscate property derived from the commission of an offense; and (10) locate and identify witnesses and suspects. Conversely, a foreign state may also request assistance in the investigation or prosecution for any violation of any of the regulated activities of the STMA.[58]

Implementing Rules and Regulations

Finally, the STMA indicated that an Implementing Rules and Regulations Committee shall be convened within six months from the effectivity of the STMA. The IRR Committee is composed of the member-agencies of the NSC-STMCom. Deliberations are conducted to examine (1) what would be included on the NSGL, taking into consideration the different control lists regimes, as well as particular goods and services that are prohibited in the Philippines; (2) the standard for the end-user certificates; (3) specific guidelines on the issuance, modification, suspension of authorizations and end-use assurances; (4) specific protocols to ensure seamless coordination of the various member-agencies of the NSC-STMCom.

Enacting strategic trade legislation is just the first step towards the establishment of an effective strategic trade regime. The Philippines needs to carry out the provision of the law. Currently, the country is in the process of defining the implementing rules and regulations on the application for authorization, issuance of certificates, appeals for licensing decisions, and many other guidelines to enhance coordination of the various concerned agencies in strategic trade management. Whether it can put forth harmonized rules that would give substance to the law, at a timely manner, is something to look into as the dedication and active participation of all concerned agencies are extremely necessary in this primordial stage of the STMA implementation.

Capacity Building and Outreach Programs

To complement the legislative initiatives to enact a Strategic Trade Management Act in the Philippines, capacity building activities and outreach programs have been conducted with the assistance of the US Department of State Export Control and related Border Security (EXBS) Program, US Department of Energy, National Nuclear Security Administration under its International Nonproliferation Export Control Program, Center for Information for Security and Trade Control, European Commission-Center for Excellence, Federal Office of Economies and Export Control, Pacific Forum CSIS, Malaysian Ministry of International Trade and Industry, Singapore Customs, and the International Atomic Energy Agency. The assistance provided were in the form of reporting, adapting the legal and regulatory framework, considering the adoption of control lists, coordinating efforts, developing new working methods, training relevant stakeholders, developing mechanisms to involve the industry and the private sector, and determining the deployment and use of detection and analysis equipment, physical protection measures, and enhancement of enforcement capabilities.

There have been preliminary consultations made during the deliberations of strategic trade legislations. The Philippine Exporters Confederation, Inc.(PHILEXPORT), in its position paper submitted to the Committee on Public Order and Safety, indicated the perceived "need to put in place an effective national export, import, transit and re-export control law to ensure that the traded chemical, biological, and nuclear commodities are not used to weapons that can cause large-scale destruction". Nonetheless, they noted that the measure "must be designed and implemented in a manner that minimizes the resulting increase in trade costs."[59]

[58] "Section 29. International Legal Cooperation"

[59] Position paper of the Philippine Exporters Confederation, Inc. submitted to the Committee on Public Order and Safety, House

An Enterprise Outreach National Capacity Building (EO NCB) program was also created in partnership with the US DOE, INECP. The EO NCB aims to engage all enterprises involved in the transfer of strategic goods and its related services. The program sought to raise awareness, promote self-compliance, and institute internal controls within enterprises. The EO NCB was launched during a two-day workshop on Enterprise National Capacity Building held in February 2015. The workshop also introduced the key elements of the Strategic Trade Management, and how various Philippine Semiconductor and Electronics Manufacturing Industries can contribute to its effective implementation.

To ensure the effective implementation of a Strategic Trade Management regime, Philippine government agencies need to step up its enterprise outreach activities. Further industry outreach activities need to be undertaken to assuage industries' concerns on the perceived difficulty of complying with the requirements of the STMA.

Conclusion

For a time, the Philippines had some difficulty enacting a law that would form the basis for the establishment of an effective trade management regime in the country. Such difficulty can be attributed to the challenge of synergizing domestic politics and foreign policy obligations. The Philippine government engaged in what Putnam regarded as "two level games", wherein they had to simultaneously cope with the pressures and constraints of their domestic political system and with the international environment.[60] Given the domestic political arrangement in the Philippines, it was difficult to pass a legislation without public consultation and support. Thus, even if the STMA was regarded as a priority bill, it took three congresses (14th, 15th, and 16th) to finally pass it into a law. Nevertheless, the Philippines has been steadfast in its commitment to the UNSCR 1540. It knows that the nonproliferation regimes is only as effective as the state's commitment to comply with their attendant obligations. Furthermore, non-participation of states increasingly viewed as prominent links to the WMD proliferation chain either as emerging dual-use innovators or manufacturers, critical transshipment ports and financial centers, or even breeding ground for terrorist sympathizers contribute to the erosion of any initiative aimed at stopping the proliferation of WMD.[61]

Recognizing too that it lacks significant technical expertise and resources to implement UNSCR 1540, and STM in particular, the Philippines has been very receptive of any capacity-building assistance and support provided by partner states. The challenge for the Philippines, nonetheless, is to have a clear assessment and comprehensive plan of what its existing capabilities are, what measures it is planning to undertake to effectively implement the STMA, and what further support are necessary to make these happen. As the country moves towards the effective implementation of its Strategic Trade Management regime, political will is needed to ensure momentum and garner support for the Act.

---

of Representatives, 18 March 2011.

[60] Robert Putnam, "Diplomacy and Domestic Politics: The Logic of Two-level Games," *International Organizations 42,* (Summer 1988).

[61] Brian Finlay, Johan Bergenas, and Esha Mufti, "Beyond Boundaries in Southeast Asia: Dual-Benefit Capacity Building to Bridge the Security/ Development Divide," The Stimson Center and the Stanley Foundation, January 2013, <http://www.stanleyfoundation.org/publications/report/SEArpt1012.pdf>.

Indonesia's Approach to Strategic Trade Controls: The Perspective of a Developing and Archipelagic Country

ANDY RACHMIANTO[1]

Abstract

As a developing country, Indonesia is focusing on economic and trade development. Therefore, export and import of goods, including strategic ones, are important. Despite Indonesia not being a member of any of the export control regimes, it is aware of the potential risks caused by the possible misuse of dual-use technologies and materials, in particular for proliferation. Therefore, Indonesia has adopted an array of laws and regulations that govern its export and import control system. Furthermore, Indonesia considers that existing nonproliferation instruments, particularly the Nuclear Nonproliferation Treaty (NPT), the Chemical Weapons Convention (CWC), and the Biological and Toxic Weapons Convention (BTWC), are critical elements to counter the proliferation of Weapons of Mass Destruction (WMD).

Keywords

Nonproliferation, export control, strategic trade control, Indonesia

Introduction

Indonesia has been accused of showing little enthusiasm for nonproliferation, including for strategic trade controls.[2] According to this view, Indonesia is unconvinced of the value of multilateral export control regimes and considers that these regimes are impeding access of non-nuclear weapons states (NNWS) to technologies associated with peaceful uses of nuclear energy. This would explain why Indonesia is not a member of any of these regimes and has not adopted a control list for most dual-used items. Similarly, the report of a Pacific Forum CSIS workshop on strategic trade controls held in September 2014 notes that despite being a party to the Nuclear Nonproliferation Treaty (NPT), the Biological and Toxic Weapons Convention (BTWC), the Chemical Weapon Conventions (CWC), as well as other international nonproliferation instruments, Indonesia does not have a strategic trade control system.[3]

[1] Director for International Security and Disarmament, Ministry of Foreign Affairs, Republic of Indonesia. He obtained a Master of Philosopy (M.Phil) degree from the School of International Studies, Jawaharlal Nehru University, New Delhi, India.

[2] Stephanie Lieggi, "The Nonproliferation Tiger: Indonesia's Impact on Nonproliferation in Asia and Beyond," NTI, March 2012, <www.nti.org>.

[3] Carl Baker, David Santoro and John K. Warden, "Closing the Nonproliferation Gap: Toward the Universalization of Strategic Trade Controls in the Asia-Pacific," Pacific Forum CSIS, (Taipei: Pacific Forum CSIS, 2014), pp. 5-6.

For the past few years, Indonesia has been the target of outreach activities conducted by members of export control regimes. Many question Jakarta's stance towards strategic trade controls by assuming that Indonesia is not fully aware of the increasing importance of strategic technologies and items, such as explosive materials, chemical substances, nuclear materials, drugs, and military equipment. Others, however, believe that it is unreasonable to conclude that Jakarta ignores the possible misuse of such technologies and materials, and their impact on security and proliferation challenges in the region. In reality, Jakarta is paying attention to the risk of proliferation, exemplified by numerous workshops, meetings, and seminars that representatives of the Indonesian Government's relevant agencies, such as the Ministry of Foreign Affairs, Ministry of Trade and Directorate General of Custom and Excise, have attended.

Indonesia has a long-standing commitment to the fulfillment of the three pillars of the NPT, as demonstrated through several leading roles including, among others: (i) Coordination of the Non-Aligned Movement/ NAM Working Group on Disarmament and Nonproliferation since 1994; (ii) Co-Presidency of Article XIV Conference of the Comprehensive Nuclear-Test-Ban Treaty (CTBT) from 2013 until 2015; (iii) Presidency of the Conference of State Parties and Signatories of Nuclear-Weapon-Free Zones (NWFZ) in 2015; and (iv) member of UN Secretary-General Group/Panel of Experts on Fissile Material Cut-Off Treaty (FMCT). Indonesia's approach to strategic trade controls needs to be discussed against the backdrop of this commitment.

This is the purpose of this paper, which begins with an examination of Indonesia's historical approach to nonproliferation generally and strategic trade controls specifically. The paper then describes Indonesia's current trade control system, including key legislation and implementing authorities. Finally, the paper identifies the limitations and challenges of Indonesia's system, such as its unique geographical features, budget and capacity constraints, and difficulties with interagency coordination. It concludes with a discussion of policy recommendations to strengthen Indonesia's controls.

Indonesia's Approach to Strategic Trade/Export Controls

Indonesia considers that existing nonproliferation treaties and conventions, notably the NPT, the CWC, and the BTWC are critical elements to counter the proliferation of Weapons of Mass Destruction (WMD). In the context of the CWC specifically, international cooperation on promoting the use of chemical science and transfer of technology is possible. Indonesia remains unconvinced with multilateral export controls regimes such as the Australia Group (AG) because they limit such cooperation.

In connection to the BTWC, Indonesia is concerned that strategic trade/export control regimes will make the BTWC less relevant and weaken multilateral efforts to strengthen the Convention. Furthermore, Indonesia is of the view that if informal mechanisms outside the Convention's framework continue to be emphasized, this will weaken the status of the Convention itself. The failure of multilateral negotiations to establish a protocol for the BTWC that would provide verification and control capabilities for the export and import of dangerous biological agents and the focus on trade controls instead sets a bad precedent. Without robust verification mechanisms, BTWC State Parties will be unable to verify whether biological agents are diverted to military or other non-peaceful purposes. In that case, inadequate verification will eventually hamper effective trade control of such agents.

In 2002, in his State of the Union Address, U.S. President George W. Bush first introduced a multilayered strategy to prevent proliferation. At that time, President Bush stated that the United States intended to "work closely with [allies] to deny terrorists and their state sponsors the materials, technology, and expertise to make and deliver WMD."[4] This intention was followed up with concerted efforts by the US "diplomatic machinery" to introduce initiatives such as strategic trade controls or other forms of international cooperation

[4] Sibylle Bauer and Ian Anthony, "Controls on Security-Related International Transfers," in *SIPRI Yearbook 2007: Armaments, Disarmament and International Security* (Bromma: CM Gruppen, 2007), pp. 25.

of like-minded partners outside the multilateral framework. In addition to furthering informal mechanisms, these efforts were supported by a series of initiatives to raise global awareness regarding the impact of WMD proliferation through various discussions at the United Nations. In the UN Security Council, these efforts led to the adoption of UN Security Council resolution 1540 in 2004 and some sanction resolutions intended to restrict the transfers of items specified on control lists to the Democratic People's Republic of Korea/DPRK and Iran.

One of the first attempts to convince Indonesia to participate in the export control regimes was during the visit of the US Secretary of State Condoleezza Rice to Indonesia in March 2006. In the midst of the bilateral consultations, Rice highlighted the importance of Indonesia as one of the littoral states to strategic maritime routes to participate in the Proliferation Security Initiative (PSI) to Indonesian Foreign Minister Hassan Wirajuda. At the meeting, Minister Wirajuda conveyed his concerns about the PSI, which applies "interdiction principles" and would have negative implications towards Indonesia's jurisdiction and sovereignty, particularly in some critical maritime areas, such as the Straits of Malacca. While Indonesia has no objection to the noble objective of the Initiative, it maintains that there are at least three rationales for Jakarta's rejection of the PSI. First, the "Interdiction Principles" of the PSI reverses the 1982 UN Law of the Sea Convention (UNCLOS).[5] Second, the process of formulating the PSI is selective, unilateral in nature and not multilaterally negotiated. Third, as the PSI contradicts the UNCLOS, it weakens the integrity of international law.[6]

In line with the US intention to strengthen international cooperation in countering proliferation of WMD, several informal export control regimes including the Australia Group (AG), the Missile Technology Control Regime (MTCR), the Nuclear Supplier Group (NSG), and the Wassenaar Arrangement on Export Control for Conventional Arms and Dual-Use Goods and Technology (WA) were reintroduced to several countries, including Indonesia. So as to expedite expansion of participation in these regimes, member countries have been actively conducting outreach activities to non-participating states in an effort to increase adherence to the control of those items targeted by the regimes. In Southeast Asia, Indonesia has been considered as one of the potential partners to be engaged due to its economic size and its strategic geographical position as a potential transit point for sensitive/strategic items and technologies. As a result, since 2006, relevant government authorities in Jakarta such as Ministry of Foreign Affairs, Ministry of Trade, Ministry of Industry, Ministry of Finance (Directorate General of Custom and Excise), Nuclear Energy Regulatory Agency (Bapeten), and National Nuclear Energy Agency (Batan) have been frequent recipients of delegations encouraging participation in the regimes. Nevertheless, despite its recognition of the growing challenges posed by WMD proliferation, Jakarta is yet to be convinced to participate as a member or participant of any regimes related to strategic trade.

There are three reasons that underlie Jakarta's position on strategic trade policy. First, it believes that the regimes could potentially hamper import and export of dual-use goods and technology. In accordance with the common position of NAM Countries, Indonesia believes that those regimes do not fully accommodate the interest of developing countries, particularly in the area of peaceful uses of sensitive materials and technologies. Indonesia is concerned over the absence of specific reference to the transfer of technology and international assistance in the provisions of those regimes, which is critical for developing countries. Second, the regimes were formulated in a selective, non-inclusive and limited manner outside the existing UN framework. Indonesia has always stressed the importance of multilateralism as a core principle in negotiations of disarmament and non-proliferation. Thus, despite its concern about WMD proliferation, Indonesia has asserted that the achievement of non-proliferation objectives must be pursued in a comprehensive, balanced, and inclusive manner under the applicable international law. Third, the regimes

[5] Rick Rozoff, "Control of the World's Oceans. Prelude to War?," Global Research, January 2009, <www.globalresearch.ca>.

[6] Andy Rachmianto, "Issues Behind Indonesia Joining the PSI," *The Jakarta Post*, June 11, 2006.

are equipped with guidelines, control lists, or trigger lists that could potentially impede the trade of dual-use goods. In the context of Indonesia, this may conflict with the obligations of the government to protect the interests of small-medium enterprises potentially affected by trade controls.

Nevertheless, Indonesia remains committed to international efforts addressing WMD proliferation, including strategic trade control. This commitment is visible in the form of activities such as:

(i) actively attending various international forums addressing the proliferation threat of WMD;

(ii) actively cooperating with the international community to combat the misuse of dual-use goods through information exchanges, joint-operations, and trans-boundary movement control;

(iii) becoming a State Party of and actively supporting the Nuclear Non-Proliferation Treaty, the Chemical Weapons Convention, the Biological and Toxic Weapons Convention, and the UN Programme of Action to Prevent, Combat and Eradicate the Illicit Trafficking of Small Arms and Light Weapons (SALW);

In Southeast Asia, efforts to promote nuclear disarmament and non-proliferation have intensified in recent years. During its chairmanship of the Association of Southeast Asian Nations (ASEAN) in 2011, Indonesia facilitated the conclusion of the negotiations on the revised Southeast Asian Nuclear-Weapon-Free Zone Treaty (SEANWFZ) Protocol between ASEAN member states and Nuclear-Weapon States (NWS).[7] Indonesia continues to encourage consultations between ASEAN Member States and NWS with a view to enable NWS to sign and ratify the Protocol of the SEANWFZ.

As one of the Annex II countries, Indonesia has also ratified the Comprehensive Nuclear Test-Ban Treaty (CTBT), which prohibits nuclear tests.[8] Indonesia has called on all states to start their own ratification process, particularly those whose ratification is required for the Treaty to enter into force. In the region, Indonesia also recognizes the importance of developing strong cooperation to improve and strengthen the non-proliferation regime through, for instance, the Asia Pacific Safeguards Network (APSN).[9]

Regarding efforts to strengthen its national legislation against WMD, since 2013, Indonesia has started the process of drafting a comprehensive law on nuclear security.[10] Indonesia sees the importance of strengthening its national legislation, which in turn can reinforce and complement the existing law, such as Law No. 10 on Nuclear Energy (1997).[11] The new draft law is expected to cover, *inter alia*, total prohibition on the use, possession and transfer of nuclear weapons, strengthening of transfer controls of nuclear and radioactive materials, and enhancing the national nuclear security architecture. In addition, Indonesia acceded to the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) in March 2014.[12] The accession to ICSANT strengthens existing legislation regarding nuclear security, improves the legal

[7] ASEAN Secretariat, "Chair's Statement of the 19th Asean Summit Bali 2011," ASEAN Secretariat, November, 19, 2011.

[8] CTBTO, "CTBT Brought Closer to Entry into Force by Indonesia's Ratification," News Release, February, 6, 2012, <www.ctbto.org>.

[9] Khairul and Ferly Hermana, "Indonesia's Pioneering Effort to Self-Assess Nuclear Security Culture," *1540 Compass*, September, 2012, <www.cits.uga.edu>.

[10] Government of Indonesia, "Statement of Indonesian Government at Main Committee III 2015 Review Conference of the States Parties to the Treaty on the Non-Proliferation of Nuclear Weapons," Permanent Mission of the Republic of Indonesia to the United Nations, May, 2015.

[11] Government of Indonesia, "National Report on Compliance to Convention on Nuclear Safety for the 6th Review Meeting 2014, "Nuclear Energy Regulatory Agency of Indonesia (BAPETEN), March, 2014.

[12] Government of Indonesia, "Statement of the Government of Indonesia at the 54th Meeting of the 70th Session of the General Assembly on Agenda Item No.87 of the Un General Assembly on Report of the International Atomic Energy Agency," Permanent Mission of the Republic Indonesia to the United Nations, November, 2015.

framework and reinforces national measures on nuclear security. Indonesia has also ratified the Convention on the Physical Protection of Nuclear Material (CPPNM) and its amendment.[13]

In short, although Indonesia is not a member of export control regimes, it has shown its commitment to preventing WMD development or transfer. Indonesia believes that the ultimate goal of the export control regimes is in line with its foreign policy, which, among other goals, seeks to limit the risk of having materials or technologies fall into the hands of individuals/groups who may illegally utilize them for purposes that threaten international peace and security.

Indonesia's Current System of Strategic Trade Controls

Indonesia has adopted an array of laws and regulations governing the export and import of strategic goods. Current regulations concerning strategic trade controls that have been formulated by the Indonesian Government are listed as follows:

1. Law Number 10 of 1995 and amended through Law Number 17 of 2006 regarding the Customs affairs;
2. Law Number 16 of 2012 on Defense Industry;
3. Law Number 7 of 2014 on Trade;
4. Law Number 10 of 1997 on Nuclear Energy;
5. Law Number 9 of 2008 regarding the Use of Chemical Materials and Prohibition on the Use of Chemical Materials as Chemical Weapons;
6. Law Number 15 of 2003 on Terrorism;
7. Several regulations on Small Arms and Light Weapons (SALW): Emergency Law Number 12 of 1951 on Fire Arms and Explosives and Decree of the Head of Indonesian National Police Number SKEP/82/II of 2004 which contains an established national system of export and import licensing and authorization of SALW;
8. Government Regulation Number 29 of 2008 regarding License of the Use of Pengion Radiation and Nuclear Material Resources;
9. Government Regulation Number 54 of 2012 on the Safety and Security of Nuclear Installations;
10. Government Regulation Number 2 of 2014 on Licensing of Nuclear Installations;
11. Presidential Decree Number 125 of 1999 regarding Explosives Materials;
12. Presidential Decree Number 58 of 1991 on ratification of Convention of Biological Weapon Decree of Minister of Trade Number 01 of 2007 regarding General Provisions on Export; also describing the categories of goods which differentiated as regulated goods, controlled goods and prohibited goods;
13. Decree of Minister of Finance Number 145/PMK.04 of 2007 regarding Customs Provisions on Export.

These regulations are related to strategic goods and materials, including nuclear, chemical, and explosive materials and are currently used as the main regulatory references. They cover three essential aspects, namely control, licensing, and enforcement. Acknowledging that there is room for improvement, Indonesia has also considered developing a more comprehensive regulation on tightening the control of transit and transshipment of goods, especially dual-use goods. In this regard, Indonesia is in the final stage of revising the government regulation on the safe transport of radioactive materials, determining the security requirements applying to the transport and shipment of nuclear materials and radioactive sources.[14] This revision is to be conducted in parallel with the drawing up of the new law on nuclear security.

Likewise, Indonesia continues to strengthen national coordination on the implementation of the Additional Protocol to the IAEA Safeguards Agreement with relevant stakeholders. Indonesia signed the comprehensive

[13] Ibid.

[14] Government of Indonesia, "National Progress Report of Indonesia at the Nuclear Security Summit 2014" Ministry of Foreign Affairs of Indonesia, March, 24, 2014

safeguards agreement with the International Atomic Energy Agency (IAEA) in 1980 and it ratified an Additional Protocol in September 1999.[15] Since August 2003, Indonesia has been implementing Integrated Safeguards, which function as the optimum combination of all safeguards measured available to the IAEA under comprehensive safeguards agreement and additional protocols to achieve maximum effectiveness and efficiency in meeting the IAEA safeguards obligation with available resources.[16] In terms of its application on the ground, Indonesia cooperates with the IAEA to strengthen the existing network of Radiation Portal Monitors (RPMs) in four key seaports, namely Belawan, Bitung, Semarang, and Makassar.[17] In the near future, Indonesia wishes to expand its monitoring program to selected border stations.

Laws and regulations regarding strategic trade controls have been developed in accordance with three general principles, identified as follows:[18]

a. Export of goods that may harm the Health, Safety, Security, Environment and Moral of Nation (K3LM) or, are contrary to international treaties are controlled;

b. The exportation and importation of those goods can only be done by companies that have been approved by the government as Registered Exporters (ET), Importer Manufacturer (IP) and Registered Importer (IT);

c. The export and import of hazardous goods is subject to verification or technical examination by an inspector appointed by the Minister of Trade in order to ensure the type of goods and the correctness of the documents.

Against this backdrop, the Ministry of Trade determined the that following strategic and dangerous goods are subject to government regulation and are controlled through licensing:[19]

a. Color multifunction machines, color photocopying machines and color printers. Regulated in the Minister of Trade Regulation Number 15/M-DAG/PER/3 of 2007 on the import provisions of color multifunction, color copiers and color printer engines;

b. Explosive materials. Regulated in the Presidential Decree Number 125 of 1999 on Explosive materials, Minister of Trade and Industry Regulation Number 230/MPP/Kep/7 of 1997 on regulated import products, Minister of defense Regulation Number 22 of 2006 on rules, regulation, control and development of commercial explosives business entities;

c. Dangerous Goods. Regulated in the Minister of Trade Regulation Number 44/M-DAG/PER/9 of 2009 on the importation, distribution and controlling of dangerous goods;

d. Precursors. Regulated in the Minister of Trade and Industry Decree Number 647/MPP/KEP/10 of 2004 on Import Provision of Precursor, Minister of Health Regulation Number 168 of 2005 on pharmaceutical precursors; Minister of Trade Regulation Number 47/M-DAG/PER/7 of 20012 on Export Provision of precursor;

---

[15] Ibid.

[16] Solichah, Mutiara. "Implementation of Integrated Safeguards in Indonesia: Nuclear Energy Regulatory Agency," Safeguard Symposium IAEA, 2010, <www.iaea.org>.

[17] Government of Indonesia, "National Detection Plan on the Illicit Trafficking of Nuclear and Other Radioactive Materials," Nuclear Energy Regulatory Agency of Indonesia (BAPETEN), 2015, <www.bapeten.go.id>.

[18] Government of Indonesia, "Strategic Trade Control in Indonesia," Ministry of Trade of Indonesia, Directorate Export of Industry and Mining Products, 2014.

[19] Ibid.

e. Nitrocellulose. Regulated in the Minister of Trade and Industry Decree Number 418/MPP/KEP/6 of 2003 on import regulation of nitro cellulose;

f. Ozone depleting substances. Regulated in the Minister of Trade Regulation Number 38/M-DAG/PER/10 of 2010 on revision of Minister of trade Regulation Number 24/M-DAG/PER/6 of 2006 on import provisions of ozone depleting substances;

g. PCMX 4 Chloro-3,5-Dimethylphenols. Regulated in the Minister of Trade and Industry Decree No.417/MPP/KEP/6 of 2003 on PCMX (4 Chloro-3, 5-Dimethylphenol);

h. Radioactive materials. Regulated in the Government regulations Number 29 of 2008 on the utilization license of the use of ionizing radiation sources and nuclear materials.

The licensing process for export-import activities, including for strategic goods and materials, has been incorporated into the Indonesian National Single Window (INSW). The INSW itself functions as an integrated online system for customs document handling and goods clearance. It enables the single submission of data and information, single and synchronous processing of data and information, and single decision-making for customs release and clearance. The INSW, which currently involves 18 relevant government authorities, was established on the basis of four main attributes, (i) one single national portal with one web-address to carry out all transactions related to trading and logistic activities; (ii) a national portal that functions as a "messaging-hub," connecting all related government authorities and traders; (iii) a mechanism for authorization of licensing, although permit and recommendation of export and import activities authorization remains within each government authority; and (iv) output of licensing, permit and recommendation from government authorities shall be uploaded or transmitted electronically to database of national portal, which then allow Directorate General of Custom and Excise to give approval in a timely manner for the needs of custom clearance and release.[20]

Several government institutions are responsible for strategic trade control management. For example, the Directorate General of Customs and Excise of the Ministry of Finance (Kemkeu) plays an essential role in the control of export and import activities at the commercial ports. In general, Custom officers have the authority to conduct several activities such as:[21]

a. Pre-service control. Control is conducted through a risk management system. This approach uses an intelligent operation method. In this regard, the target to be controlled is chosen by analyzing the supplier, means of transportation, country of origin and information gathering;

b. Control during service process. Control is conducted through selective random examination of samples or on Intelligence Notes resulting from analysis of custom documents;
c. Post-service control. Control of exported or imported goods that are not covered by the pre-service and during service controls, upon preliminary indication of violations of regulations. This control includes post audit of the importer and exporter.

According to Law Number 17 of 2006 on Customs and Decree of Minister of Finance Number 161/PMK.04/2007 on Export and Import Control of Restricted Goods, the Indonesian Government has the

[20] Government of Indonesia, "Indonesia National Single Window." Single Window Working Group Capacity Building Workshop," APEC - 2009/SCCP/SWWG/WKSP4/016, Singapore, April 2009.

[21] Government of Indonesia, "Indonesian National Report on the Implementation of Security Council Resolution 1540 (2004) - Annex to the Note Verbale Dated 28 October 2004 from the Permanent Mission of Indonesia to the United Nations Addressed to the Chairman of the 1540 Committee," October 2004.

authority to apply import-export prohibition and restriction known as *larangan terbatas* or *Lartas* on export and import of certain materials or goods which are listed on the INSW website based on suggestions and inputs submitted by technical ministries/agencies to the Ministry of Finance.[22] Such materials or goods include dual-use items such as explosive materials, radioactive materials, and pharmaceuticals/non-pharmaceuticals precursors.[23] In terms of detection, by referring to the list, customs officers are obliged to take necessary actions such as examination, termination, and foreclosure to control export and import activities of such materials and goods.[24] If there is an indication of criminal offences, customs investigation officers may conduct investigation procedures and prepare case files as well as related documents required to conduct legal proceedings. In addition, the two regulations also stipulate a provision on exemption of 'restricted ban' which is applied in the case of importers or exporters managing to obtain letters of recommendation from relevant technical ministries/agencies.

While the Directorate General of Customs and Excise of the Ministry of Finance (Kemenkeu) is responsible for the enforcement of laws and regulations, the Ministry of Trade (Kemendag) and the Ministry of Industry (Kemenperind) are the primary institutions that issue the licenses for almost all dual-use items. As for export and import of military equipment, Law Number 16 of 2012 on the Defense Industry appoints the Ministry of Defense as a license issuer. In this regard, the application to obtain a license should include the end-user certificate, letters of information on the country of destination, letters of documentation (picture), and export declaration. Once a license has been issued, customs officers will conduct physical inspections of the controlled military goods to be exported. For conventional weapons or small arms and lights weapons (SALW), in addition to license from the Ministry of Defense, recommendation from the Armed Forces Strategic Intelligence Agency (BAIS) and the National Police Chief are also required.[25]

As an integral part of enforcement, the formulation of strategic trade policy involves a number of relevant government institutions that interact with each other and provide input to relevant agencies on CBRN issues, including strategic goods and materials under a forum called the 'Chemical Biological Radioactive and Nuclear (CBRN) Working Group.' The Ministry of Foreign Affairs (Kemlu) is the focal point, and it is currently attended by representatives from the Coordinating Ministry for Political, Legal, and Security Affairs (Kemenkopolhukam), Ministry of Defence (Kemhan), National Disaster Management Agency (BNPB), Ministry of Health (Kemenkes), Ministry of Environment and Forestry (Kemen-LHK), Indonesian National Police (Polri), National Food and Drug Control Agency (BPOM), Nuclear Energy Regulatory Agency (Bapeten), Indonesian National Armed Force (TNI), State Intelligence Agency (BIN), State Ministry of Research, Technology, and Higher Education (Kemenristekdikti), and the Indonesian Institute of Science (LIPI).

Limitations of Indonesia's Strategic Trade Controls

As the world's largest archipelagic country with more than 17,000 islands scattered from Aceh Province in the west and Papua Province in the east, Indonesia has 5,800,000 square kilometers of maritime zone under its jurisdiction and one of the longest coastlines in the world. Indonesia's maritime zone comprises 300,000 square kilometers of territorial sea, 2,800,000 square kilometers of archipelagic waters, and 2,700,000 square kilometers of the exclusive economic zones (EEZ).[26] Geographically, Indonesia is also a littoral

[22] Government of Indonesia, "*Tentang Lartas, Kategori dan Perijinannya"*, [About Lartas, Categorization, and Its Licensing], Directorate General of Customs and Excise Ministry of Finance, March 29, 2014, <www.bctemas.beacukai.go.id>.

[23] Government of Indonesia, "Indonesia National Trade Repository: *Lartas* Information," Indonesia National Single Window (INSW), September, 2015, <www.insw.go.id>.

[24] Government of Indonesia, "*Tentang Lartas, Kategori dan Perijinannya"*, [About Lartas, Categorization, and Its Licensing], Directorate General of Customs and Excise Ministry of Finance, March 29, 2014, <www.bctemas.beacukai.go.id>.

[25] Government of Indonesia, "Strategic Trade Control in Indonesia," Ministry of Trade, Directorate Export of Industry and Mining Products, 2014.

[26] Sodik, Dikdik Mohamad. "The Indonesian Legal Framework on Baselines, Archipelagic Passage, and Innocent Passage,"

state of the Straits of Malacca, which is considered the longest and busiest straits used for international navigation, as well as for strategic sea lanes of communication. On that note, Indonesia's maritime zone is utilized by different kind of vessels, including commercial and oil tankers, military, and ships carrying dangerous materials. To accommodate international and domestic navigation, according to the Indonesian Ministry of Transport, no less than 500 modern and semi-modern seaports are now operating in Indonesia.[27] While these characteristics could be considered as an economic and strategic advantage, they also pose security risks for the Indonesian government, particularly regarding the potential threat to maritime security. Implementing a national strategic trade control program is challenging for Jakarta because thousands of its islands serve as exit and entry points. Indeed, they can be used for the illegal transit and transshipment of strategic dual-use goods.

Successful implementation of strategic trade controls relies on the availability of a sufficient number of enforcement officers and supporting facilities such as patrol vessels. In Indonesia, the General Customs and Excise Directorate of the Ministry of Finance plays an essential role in the control of export and import activities at the commercial ports. Unfortunately, Indonesia has only around 11,600 custom officers responsible for enforcement.[28] With regard to supporting facilities, Customs and Excise Directorate possesses only 173 patrol vessels, comprised of fast patrol boats which are very slender vessels, and speedboats to covers waters around the thousands of islands. The deployment and operations of all these vessels are coordinated under main customs operational ports located in Tanjung Balai Karimun, Pantoloan, Tanjung Priok, Batam, and Kepulauan Riau.[29] In terms of annual budget, for this fiscal year, the Customs and Excise Directorate had approximately US$ 274 million or equivalent to only 0.17 percent of the national budget (APBN).[30] These facts and figures suggest that Indonesia faces tough challenges in implementing comprehensive strategic trade controls and that it cannot be expected to do so without significantly improving its capacities.

Another problem is inter-agency coordination. The organizations managing exports and imports in Indonesia are not integrated. At the national level, there isn't one organization with the authority to deal with and coordinate strategic trade control. Different organizations and agencies have different mandates and authorities, compromising the effective and efficient control of exports and imports.

Conclusions and Recommendations

Several arguments are relevant to reinforce Indonesia's position with regard to strategic trade control. First, although Indonesia is not a member of any of the international export control regimes, it is aware of the possible misuse of dual-use technologies and materials and has adopted an array of laws and regulations that govern its export and import control system. Second, these regimes remain unable to accommodate the interests of developing countries, including Indonesia's, particularly in relation to the use of these goods and technologies for peaceful purposes. Third, procedurally, Indonesia is concerned that regimes negotiated outside the UN or other multilateral frameworks will contradict its interests as they were developed by producer countries or developed countries without proper involvement of developing countries. Fourth, Indonesia believes that the existing regimes, such as the NPT, CWC and BTWC are sufficient to fight WMD

Ocean Development and International Law 43:4, (October 2012), p. 330.

[27] Government of Indonesia, "*Sistem Informasi Geografis Prasarana Transportasi* [Geographical Information System on Transport Facilities]," Ministry of Transport Database, September 2015, <www.gis.dephub.go.id>.

[28] Nurhayat, Wiji, "*Wilayah Lebih Luas, Jumlah Pegawai Bea Cukai Ri Kalah Jauh Dari Malaysia* [with Wider Region, the Number of Ri's Custom Officers Is Less Than Malaysia's]," *Detikfinance Economy and Business*, October 2014, <www.finance.detik.com>.

[29] Government of Indonesia, "*Tambahan Kapal Patroli Bantu Bea Cukai Perkuat Pengawasan Laut* [Additional Patrol Vessel Strengthen Customs Capability of Maritime Surveillance," Directorate of Customs and Excise of Indonesia, October 2015, <www.beacukai.go.id>.

[30] Sasongko, Agung, "*DPR Setujui Anggaran Kemenkeu 2016 Sebesar Rp. 30,9 Triliun* [DPR Approves Rp. 30.9 Trillion Budget for Ministry of Finance]," *Antaranews*, October 7, 2015, <www.antaranews.com>.

proliferation. Significantly, these instruments have been able to accommodate the interests of developing countries, notably by guaranteeing their inalienable rights to the peaceful uses of materials and technology. Fifth, while several export control regimes offer financial incentives or other political advantages, Indonesia remains unconvinced that participation to such regimes is to its interests. To Jakarta, the rights and obligations of each member with regard to the "transfer of technology" and "international assistance" should be clearly guaranteed. Lastly, Indonesia itself is confronted with challenges in implementing strategic trade controls, especially given its geographical situation as an archipelagic state that creates so many unaccounted entry and exit points. This requires thorough scrutiny using the latest technology, such as Radioactive Portal Monitors (RPM) or Gamma Ray Container Scanners. The problem is that the Indonesian Government has limited resources.

Looking to the future, however, there are a number of actions that Jakarta should take, as follows:

a. The industry/public need to be well informed regarding the export control system and the government needs to review the readiness of the industry, especially small and medium enterprises (SME/SMI);

b. Existing regulations must be strengthened;

c. The allocation of budget for control mechanisms on export and import must be increased;

d. A common understanding on export control regimes between relevant ministries/agencies needs to be built;

e. Intelligent information sharing needs to be strengthened;

f. The implementation of control based import-export transactions (Custom Evaluation), which has been implemented by the Directorate General of Customs, needs to be improved;

g. The possibility to create an umbrella law to regulate export-import of dual use item needs to be discussed.

The implementation of the aforementioned actions would depend on the priorities laid out by the new government of President Joko Widodo. While non-proliferation is an important concern in Indonesia, it is outranked by many other priorities. Progress, in sum, will continue but remain slow.