Key Findings and Recommendations
Workshop on Strategic Trade Controls in the Asia-Pacific
December 5-6, 2017, Taipei, Taiwan

The Pacific Forum CSIS and Chengchi University's Institute for International Relations, with support from the Taiwan Coast Guard, Prospect Foundation, and the US State Department's Export Control and Related Border Security Program, held their seventh annual strategic trade control workshop on Dec. 5-6, 2017 in Taipei. Some 40 participants representing relevant government agencies and nongovernment organizations attended in their private capacities. Discussions focused on proliferation networks, proliferation financing, the relationship between strategic trade controls and trade sanctions, controlling research and technology transfers, promoting industry compliance, and implementing strategic trade controls in Southeast Asia. Each session included short presentations to introduce the topic followed by an extended discussion offering all participants the opportunity to share ideas and experiences related to the issue. The exchange between practitioners and policy analysts provided valuable insights, which are summarized below.

This workshop was the first time the group devoted full sessions to proliferation networks and financing. Proliferation networks may be usefully described by their "resilience," that is, their vulnerability to shocks, their elasticity or ability to bounce back from shocks, and their adaptive capacity. The most significant drivers of resilience are access to resources, technical knowledge, and expectation of enforcement. Lowering a network's resilience makes it more vulnerable to enforcement.

North Korea maintains a type of semi-state control over its proliferation networks and makes heavy use of the diplomatic pouch (bag) system to avoid scrutiny. Previously, the international community focused on the DPRK's acquisition of WMD-related materials, but more attention is currently placed on North Korea's efforts for missile and nuclear program financing, which include using the ledger system, offshoring of funds, large cash withdrawals from or deposits into overseas accounts, and heavy use of foreign currencies.

As DPRK overseas missions are often used to conduct illegal activities, recent sanctions resolutions have called for the closure of these missions. Six missions have been closed since the latest round of sanctions, but there are still 47 overseas. The trade-off with closing missions is that it also reduces diplomatic presence in Pyongyang and visibility into the regime.

Concepts from criminology that can be applied to proliferation networks include competitive adaptation, which occurs when one node of the network is shut down and proliferators find an alternative path. Also, proliferators engage in risk calculus. The expectation of getting caught matters more than penalties.

It is difficult for financial institutions to screen for the transfer of dual-use goods since they do not have access to export control classifications for goods, and documentation normally does not include the specific purpose of a transaction. "Non-documentary trade" (e.g., wire/electronic transfers) accounts for about 80 percent of global trade transactions, which often has no human intervention, and provides little in the way of transfer details that might match a proliferation red flag warning.

Information-sharing mechanisms on proliferation risk assessments between governments and financial institutions should be developed, although there are secrecy, classification, and privacy concerns on both sides. Regulatory restrictions also limit government access to financial information. Banks are not incentivized to ask for help from the government because reputation matters in the banking world.

Smaller financial institutions tend to be more risk tolerant than larger institutions and have fewer resources for implementing monitoring mechanisms. Compliance is expensive, so smaller banks may have vulnerabilities that illicit actors can exploit.

Asian countries are currently working on implementing Financial Action Task Force on Money Laundering (FATF) recommendations, which are primarily focused on money laundering and terrorism financing. Although proliferation financing is lower on the list of priorities, there are overlaps since perpetrators often employ similar techniques and involve the same networks.

There are limitations to the actions governments can take against the anti-money laundering networks. Systems, legal authorities, and resources differ – in some states, a government agency can investigate, but in others, they can only collect and share information. In all cases, interagency cooperation is a critical component of success.

Strategic trade controls (STC) and sanctions have different objectives and characteristics, but also points of convergence. Overlapping areas include fighting terrorism, nonproliferation objectives, compliance with rules and regulations, restrictive measures, supply chain management, and international obligations. Tools of STC can be used for sanctions implementation, especially by Customs authorities. STC and sanctions are implemented by the same governmental bodies in many countries. In many systems, especially in Asia, nonproliferation sanctions are written into the STC regulations.

Industry outreach has a critical role to play in both STC and sanctions implementation. Yet sanctions are more complicated because they go beyond controlling dual-use and arms exports. Thus, industry associations are useful in determining which companies might need outreach. There are some industry groups that can facilitate outreach efforts, too.

It takes a change of mindset to have a compliance culture within a particular company. Outreach often invokes control or threatens companies, rather than being a discussion about business or benefits. One challenge is how to make a compliance culture attractive.

Many UN sanctions are ineffective because member states do not have domestic mechanisms to incorporate them into their legal structure. There are two issues: commitment at the national level and the capacity to implement sanctions. Many countries in Southeast Asia do not even have an STC system or enforcement mechanisms in place, so implementation of sanctions is a daunting goal.

Intangible technology transfer is a mode of technology transfer that includes emails, cloud computing, software download, conferences/seminars, deemed exports (in the United States), and general conversations. The Wassenaar Arrangement has specific language on how to deal with technology transfers as well as best practices for implementing intangible transfer of technology controls (2006).

While straightforward in principle, controlling technology transfer is often complicated in practice. For instance, Taiwanese engineers are being recruited by mainland Chinese companies, which impinges upon Taiwan's Trade Secrets Act, Civilian Relations Law, the Straits Act, the Employment Service Act, and the Fair Trade Act. In response, the Taiwan government is currently considering an amendment to the Trade Secret Act that would cover all transfers of intangible technologies, data, services, and even conversations.

Challenges in controlling the transfer of technology include enforcement, determining foreign versus domestic components, the necessity of technical knowledge, and the evolution of technology. The most significant challenge, however, is the mindset that cross-border research is for the common good. Many

researchers believe that research is science and therefore should be shared with everyone. There is a need for confidence-building between authorities and academics.

Reducing the risk of transferring technology through academic research activities requires researchers to be aware of the potential for proliferation and authorities (regulators/licensing) to understand the risks associated with academic activities related to WMD. While awareness in the academic community is similar to industrial activities *if* end-uses and end-users are known, the potential end-uses and end-users are often unknown or not easily identifiable during research and are not a consideration for the researcher.

Japan's Ministry of Economy, Trade and Industry (METI) is focusing on intangible technology controls and outreach to academia. Currently, 40 universities are members of the third-party non-profit Center for Information on Security Trade Controls (CISTEC). Most members use services related to product classification of premature technologies.

Governments and multilateral export control organizations are bringing Internal Compliance Programs (ICPs) and the role of industry more to the forefront. Many states have tried to incentivize or oblige adoption of ICPs. For example, in the EU, to be an authorized economic operator, having an ICP is part of the certification process. Also for generalized licenses, the recipient has to have an ICP in place.

Companies face sector-specific but also cross-sector challenges in ICP. One cross-sector challenge is managing multinational supply chains, which often affects smaller subsidiaries brought into larger organizations. If a company wants to be compliant with export controls, it has to be compliant across the whole supply chain. While there are large companies with very experienced compliance officers, it is much more challenging for small subsidiaries to implement the same type of compliance measures.

Taiwan has been very active in promoting ICPs. The government offers various incentives to companies that institute ICP, such as long-term licensing, multi-destination licensing, a shorter screening process, and publicity in the media.

Strategic trade control systems in the ASEAN countries are developing at an uneven rate. Singapore and Malaysia have established robust systems. The systems in the Philippines and Thailand are currently under development. Myanmar has shown an awareness of the need for controlling exports and is currently working on modifying its primary trade legislation. Laos has expressed some interest in developing a comprehensive trade control system. Brunei is still in an awareness-raising stage. Cambodia is open to outreach and awareness programs, but it is unclear where it is heading. In Vietnam and Indonesia, there are still many obstacles to progress. It was noted that without Indonesia, STC in ASEAN would not have desired global effect.

There is still a need to generate political support for STC in Southeast Asia. Resistance to the idea of controlling trade remains strong as the focus is on trade facilitation within ASEAN. Developing positive incentives should be an important part of promoting STC adoption in the region. Having an export control system in place could be a condition for preferential market access to the EU or the United States. Linking export controls with trade should expedite the former's development.

Singapore and Malaysia can be used as good examples of successful adoption of an STC system in Southeast Asia. Both countries have been able to attract high technology industries, have become important centers in the global high technology supply chain, and have established high-volume transit and transshipment centers.

In an effort to provide participants the opportunity to better understand how STCs are implemented at a major node of the global transportation system, the organizers are planning to conduct the eighth

workshop in Kaohsiung, Taiwan. The primary focus of the workshop will be on transit and transshipment issues as well as the relationship between licensing and detection of proliferation activity. The visit to the port will also address port security, including challenges and best practices that can be shared with other countries in the region.

For more information, please contact Carl Baker [carl@pacforum.org] or Crystal Pryor [crystal@pacforum.org]. The report and findings reflect the view of the organizers; this is not a consensus document.