PRESENTATION TO THE OSCE
FORUM FOR SECURITY COOPERATION (FSC)
Vienna – 31 May 2017

"The Wassenaar Arrangement's Work on Technology Proliferation Control"

Ambassador Philip Griffiths
Head of Secretariat
Wassenaar Arrangement on Export Controls for
Conventional Arms and Dual-Use Goods and Technologies

Introduction

Excellencies. Distinguished delegates. Let me begin by thanking the current Forum for Security Cooperation (FSC) Chair for inviting me to speak to you today about the work of the Wassenaar Arrangement (WA) in relation to the security challenges emanating from technological advances. I welcome this opportunity to contribute to the regular exchange of information between our organisations.

This information-sharing is one of the mandates given to the WA Secretariat by our Participating States. I and my predecessor have addressed the FSC on several recent occasions, the Director of the Conflict Prevention Centre has also given briefings to WA Participating States, and working-level contacts between the respective Secretariats have grown. There is scope to build further on these interactions based on the complementarities between our organisations, taking into account their different mandates and memberships.

After the first speaker's very interesting presentation of the complex challenges raised by this topic, I will focus on the operational level in terms of the work being done in one multilateral organisation from an export controls point of view.

WA Purpose

The primary purpose of the Wassenaar Arrangement, with currently 41 Participating States, is to promote transparency and responsibility in transfers of conventional arms and dual-use goods and technologies, with the aim of preventing destabilizing accumulations, as well as the acquisition of these items by terrorists.

Export controls and responsible transfer policies are a key part of the tool-kit available to governments in seeking to pre-empt proliferation risks associated with sensitive technologies that are relevant to military or terrorist capabilities.

Working multilaterally is also vital in order to ensure cohesive policy frameworks, coordinated approaches and a consistent application of controls, not only among key producers and exporters of sensitive items, but globally.

WA Work

Cooperation in the WA takes three main forms: agreeing on the Control Lists of items that require a national export licence and working to keep the Lists up-to-date with technological developments and changes in the international security situation, taking into account market trends; exchanging information and views on transfer risks in different parts of the world, as well as specific reporting of national decisions to approve or deny controlled exports outside the WA; and developing non-binding best practices, elements and procedures to guide national export control implementation.

While the risks traditionally associated with conventional arms transfers have not gone away, in the twenty years since the WA was established other challenges and threats have grown in importance, resulting from rapid technological advances, the increasing globalisation of business, extensive movement of people and ever-widening use of electronic communications and the Internet.

These days, transfers of defence and sensitive dual-use technologies may take many different forms, both tangible and intangible. Company mergers and acquisitions, joint ventures, offsets, co-production and/or joint research and development programmes are some of the methods used. New technology producers, integrators and end-users are emerging. Proliferators are finding innovative ways to circumvent existing export control systems and exploit weak links.

Additionally, whereas new technology with military applications used to be developed by the defence industry, the civilian sector is increasingly in the driving seat. It is more challenging for governments to identify and control exports of dual-use technology that have broad civil as well as military uses.

All of these developments complicate the task for governments in seeking to exercise effective export controls, as well as in maintaining an appropriate balance between national security and trade promotion interests. The complex web of actors and processes increasingly involved in defence-related trade highlights the need for robust and adaptive national export control frameworks and partnerships to ensure that exported technology or software is not delivered or diverted to an unintended recipient or use.

Technology

"Technology" is defined in both the WA Munitions List and the WA Dual-Use List as specific information necessary for the “development", "production, or "use" of a product. Munitions List goods and technologies are defined by their military characteristics. Dual-use goods and technologies controlled in the WA are those which are "major or key elements for the indigenous development, production, use or enhancement of military capabilities". They are evaluated against the criteria of foreign availability; controllability; the ability to make a clear and objective specification of the item; and non-duplication with other export control regimes.

When technology is listed in the WA, its transfer requires a national export licence, regardless of the means of transfer.

Not controlled in the WA is technology in the public domain, basic scientific research, or software which is generally available to the public by being sold from retail stock without restriction, or which is designed for installation by the user without substantial supplier support.

WA Control Lists

For most of its Participating States, as well as for other countries that apply them, the WA Control Lists account for the vast majority of export licence applications. The WA Dual-Use List contains more than 1,000 items in 9 categories, ranging from special materials and related equipment to electronics, computers, telecommunications, information security, sensors and lasers, navigation and avionics, marine, aerospace and propulsion. Of these, 170 items are classified as "sensitive" and 80 as "very sensitive", requiring extra vigilance.

In recent years, WA Participating States have invested significant technical resources in defining and updating export control parameters for emerging sensitive technologies that could be used for illegitimate purposes, including for terrorist acts. Its Participating States have increasingly seen the WA as the appropriate forum in which to address export controls in response to such technological advances.

Key to this work is capturing the specific technical functionalities or equipment of security concern, while not impacting commercial applications or legitimate trade and technology flows. This is particularly challenging when, as is often the case, there are close proximities between the technologies, equipment or components used for military/security purposes, and those that are used in industrial/commercial applications.

Also challenging, in order not to arrive at excessive or inapplicable controls, is the need to consider not only the inherent capabilities of relevant items but also their potential uses, including how to mitigate against the risks arising from their combination with commonly available items, such as in a hybrid warfare strategy.

The WA, operating by consensus, like the OSCE, also needs constantly to find a balance between different national perspectives of which specific or potential technological capabilities constitute a proliferation concern.

Let me give a few relevant examples of technologies recently addressed in the WA.

Recent WA Control List Changes

Since 2011-2014, as is widely known, the WA has agreed on new export controls related to mobile communications interception, intrusion software and Internet surveillance tools.

In respect of intrusion software, the WA control is on the export of certain operator-controlled surveillance (and law enforcement/intelligence gathering) tools which generate, deliver and operate intrusion software to exploit targeted computers and network-capable devices, typically to extract data covertly or to establish a persistent surveillance presence. The intrusion software itself is not controlled.

In relation to Internet surveillance tools, the control is on the export of systems, equipment and specially designed components for the surveillance of Internet Protocol networks. These systems comb vast amounts of Internet and other network traffic to produce personal and social information, including mapping the network activity and extracting the communications of targeted individuals or groups.

Here the security implications were initially seen as having more to do with human rights than with destabilizing accumulations of conventional arms. After further debate, however, it was agreed that these technologies can enhance military capabilities and, under certain conditions, may be detrimental to international and regional security and stability.

Work is continuing in the WA to build on these new controls without hindering the further development of industry expertise and international cooperation in cyber defence and vulnerability response.

Other recent attention has focussed on unmanned aerial vehicles (UAVs), taking into account substantial technological progress in this area, as well as on spacecraft equipment.

Here the challenge was equipment and technologies of concern which are increasingly available on the global market. In the case of UAVs, there was a need to better differentiate UAVs of concern from civil-use UAVs or model aircraft. Accordingly, technical parameters were introduced in 2014 concerning flight endurance factors and the ability to withstand severe environmental conditions. The new control also captures specific engines and flight control systems.

In respect of additive manufacturing (or 3-D printing), after detailed examination of the characteristics of high-performance 3-D printers available on the market, as well as a careful consideration of the feasibility of software-related controls, the WA currently continues to study the possibility of developing controls for the most sensitive applications.

In relation to robots and artificial intelligence, navigation capabilities, including the fusion of sensors information, are developing very rapidly to increase autonomy of weapons systems and robotisation of the battlefield. The WA is closely monitoring the evolution of sensors and their integration in weapons systems and the related software. In recent years, controls have been introduced or amended reflecting changing technical parameters of optronic cameras, radars and lasers.

It is not just a question of adding to the Control Lists, but also of amending or deleting

existing controls to take account of obsolescence or to strengthen common interpretation. For example, the WA has recently reviewed the concepts and uses attached to the word "technology" in the Control Lists. And in the last ten years, entries related to Security of Information have been regularly amended to take into account the fast evolution of products and technologies containing or using cryptography. Further de-controls have recently been agreed for equipment utilising such functions for consumer protection purposes.

Looking ahead, its Participating States can be expected to continue to use the WA to address new technologies of security concern, including further refining understandings in relation to cybertools, electronic forensics equipment, 3-D printing, thermal batteries, terrestrial equipment and components for satellites, as well as keeping sensitive item specifications up-to-date and relevant.

Turning to other areas of its work, as noted earlier, the WA is also a forum for the systematic exchange of information and views, as well as for setting standards for effective export control policy and practice.

WA Information Exchange

What is called a general information exchange is designed to focus at least three times a year on transfer risks in specific regions, suspicious acquisition/brokering activities, projects and programmes of concern, as well as terrorism-related issues. In practice, an individual Participating State may draw the attention of its partners to any matters that it considers relevant.

Specific information shared includes regular reporting of Participating States' arms transfers and transfers and denials of certain dual-use goods and technologies to countries outside the WA, with the aim of promoting transparency and consistency. Reporting of transfer denials brings to the attention of partners efforts to obtain access to a controlled item or technology that one Participating State considers to be contrary to the WA's purposes. Such reporting is therefore an important and timely warning mechanism that also helps to avoid inadvertent undercuts.

In addition, WA Participating State licensing and enforcement officers come together once a year and network intersessionally to share national export control implementation experiences, including case studies and practical lessons learned.

WA Standard Setting

In terms of its standard-setting work, almost all the WA's 25 or so best practice guidelines, elements and procedures developed over the years have a bearing on technology security, including those relating to export licensing, end-use and end-user assurances, catch-all, re-export, transit and trans-shipment, brokering, intangible transfers of technology (ITT) controls, internal compliance programmes (ICPs) for dual-use goods and technologies, as well as effective enforcement.

As well as remaining open to proposals for new guidelines, the WA agreed last year, as part of its self-assessment cycle, on a mechanism for the regular review and

updating of all its existing guidance documents. Topics addressed in some of these, such as ITT, as well as SALW, continue to receive close attention in the WA, given the increasing complexities and challenges of implementing effective export controls in these areas. End-use/r assurances and ICPs are also, inter alia, areas of ongoing discussion.

WA Outreach

Effective outreach is also important to achieving the export control objectives. The WA has an active outreach programme to non-member countries, including annual collective policy and technical briefings, bilateral dialogue and invited visits, with the objective of encouraging voluntary adherence to its Control Lists and standards.

An increasing number of other countries are among the WA's regular outreach partners, while several applications for membership are currently under consideration. Some countries have opted to apply the WA Control Lists without seeking to become a member. They may have done so directly, or by means of voluntarily following the consolidated European Union (EU) Control Lists.

The WA is also taking steps to strengthen dialogue with other export control regimes on technical issues to avoid Control Lists overlaps or ambiguities. Technical discussions are already taking place with the Nuclear Suppliers Group (NSG) and are starting with the Missile Technology Control Regime (MTCR) on specific Control List issues.

Summary

In summary, the WA strives to address security risks, including challenges associated with technological advances, by:

- Maintaining and strengthening information-sharing among its Participating States in a timely manner, including in relation to emerging technologies of concern.

- In this context, ensuring an appropriate interface between policy-related concerns and technical work. *(The respective WA subsidiary bodies inter-relate closely, supported by a permanent Secretariat, and report to the annual Plenary, which also has an intersessional decision-making mechanism. A recent initiative, resulting from last year's self-assessment, is to trial an informal discussion bringing together Participating State policy and technical experts on selected emerging technologies.)*

- Identifying and responding quickly enough to new technological developments or applications with security implications – in order to minimise the gap both before new controls can be agreed multilaterally, and before they are implemented in national practice. *(The WA has a fast-track procedure for Participating States to raise new Control List issues outside the standard list review procedure. While national implementation measures may lead to some unevenness in timing and interpretation of controls, developing common understandings and exploring the scope for coordinating national export control policies and practices are underlying principles of the WA's work.)*

- Setting the threshold technical specifications of controls to differentiate effectively items or technologies of security concern from those widely available on the civil market. *(National proposals for WA Control List changes are subject to an intensive consensus-building review among Participating State technical experts who consult industry. This process may take time but aims to find a reasonable and workable compromise in the controls. As all WA decisions are taken at the Plenary level, it is also assured that no solution will be adopted that has not been examined in all its aspects and agreed by all WA Participating States.)*

- Maintaining an appropriate balance between security concerns, which can be diffuse, and national commercial interests. *(Implementation of export controls is a national responsibility, but the WA provides a peer review mechanism, as well as promoting a level playing field for international trade in relevant items.)*

- Setting standards for effective export control procedures and practice. *(The WA has adopted best practice guidelines covering a wide range of implementation issues, including ITT and ICPs.)*

- Strengthening dialogue and engagement among all relevant actors at the national level (including licensing and enforcement agencies, industry, academia and researchers).

- Promoting the widest possible application of equivalent standards. *(The WA remains open to new members meeting the eligibility criteria and pursues an active outreach programme to non-WA countries.)*

Concluding Remarks

In conclusion, continuing to respond rapidly and coherently to the evolving international threat landscape - including complex security threats related to technological advances in both the defence and civilian sectors, as well as increasingly sophisticated proliferation and diversion risks, including through ITT - is an ongoing priority for the WA.

The WA partnership, based on a shared commitment to vigilance and restraint, aims to be a stabilising factor in the international trade and security environment.

I believe that, notwithstanding the challenges, WA Participating States can be expected to continue seeking to provide leadership by example for the broader international community in the quest for strengthened sensitive technology security through effective export controls.

Thank you again for this opportunity to speak to you today. The OSCE and the WA share common goals and commitments to contribute to regional and international security and stability by building confidence and promoting transparency and responsibility in transfers of conventional arms and dual-use goods and technologies.

The WA Secretariat stands ready to provide further information about the WA's work in this regard. We look forward to continuing interactions with the FSC to help our respective organisations leverage effectively off each other's work.

* * * * * * * *