The Wassenaar Arrangement and Controls on Cryptographic Products

(Wassenaar Controls, Cyber-Crime and Information Terrorism)

by Dr. Brian Gladman, Worcester, United Kingdom, August / September 1998

Introduction

This paper considers the current export controls for cryptographic products within the context of the objectives set for them by the Wassenaar Arrangement, the international agreement under which they are pursued. This analysis shows that these controls are not justified by this agreement and are in fact contrary to the principles on which it is based.

Background

The Wassenaar Arrangement is an international agreement between 33 participating nations with the following aims (copied verbatim from the Initial Elements):

1. The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States will seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.
2. It will complement and reinforce, without duplication, the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognised measures designed to promote transparency and greater responsibility, by focusing on the threats to international and regional peace and security which may arise from transfers of armaments and sensitive dual-use goods and technologies where the risks are judged greatest.
3. This arrangement is also intended to enhance co-operation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behaviour of a state is, or becomes, a cause for serious concern to the Participating States.

It is also stated that the arrangement will not be directed against any state or group of states and will not impede bona fide civil transactions. Nor will it interfere with the rights of states to acquire legitimate means with which to defend themselves pursuant to Article 51 of the Charter of the United Nations.

Key Features of the Wassenaar Arrangement Objectives

Firstly, from item 1 and 3 above it is clear that the major aim of the Wassenaar Arrangement (WA) is to prevent the build up of military capabilities that threaten regional and international security and stability. However item 4 indicates that it will not be used to prevent nations from acquiring the means to defend themselves and this places an immediate emphasis on controls that will prevent the development of offensive military capabilities which threaten regional or international stability and security.

When considering military products it will often be difficult to distinguish what is offensive and what is defensive. Some types of weapon – for example, medium and long-range missile systems – are clearly offensive in character; others – for example tanks – can be used in either role and still others – for example, fixed anti-aircraft batteries – have a purely defensive role. In practice the major difference between offence and defence is determined more by intent and the nature of actions taken than it is by the weapons used.

Nevertheless in considering regional weapons accumulations, the implementation of the Wassenaar Arrangement must take account of the different character of military products because those that can only be used for defence will often make a major contribution to regional stability. Purely defensive weapons make belligerent military action by neighbouring nations less likely to occur and less likely to succeed if they are initiated. It is important, therefore, that the nations involved in Wassenaar promote truly defensive capabilities whilst working to prevent accumulations of offensive weapons and seeking to control and monitor those that can be used for either offensive or defensive purposes.

Item 4 also stipulates that the Wassenaar Arrangement cannot legitimately be used to obstruct genuine civil transactions. This is very important because it means that products that are clearly designed and sold for civil – that is, non-military – use should not be restricted by controls justified

under the terms of the Wassenaar Arrangement. This part of the arrangement is significant because many dual use goods can be used to construct either commercial or military capabilities and it is practically impossible for the vendor to know to which purpose they will be put. This is especially true for basic components, for example, nuts and bolts or electronic components sold as general-purpose commodity products. Many dual use goods are of this character and, in contrast with complete military products or systems, their suppliers cannot reasonably be expected to know the purpose to which a purchaser will put them. This means that commodity products and those that are widely available cannot sensibly be controlled.

In order to avoid damaging genuine civil transactions Wassenaar export controls seek to identify particular characteristics of 'dual use' goods that make it possible or likely that they will be used in the construction of offensive military capabilities. For example, very high strength metal alloys are controlled and so are electronic components that work at both very low and very high temperatures. Of course such components are also used in civil applications, for example, civil aircraft construction, but these are relatively specialised requirements and controls can be imposed without a serious impact on such civil commerce.

Within the area being considered in this paper – cryptographic products – this means that commodity cryptographic products are outside the scope of Wassenaar controls since their control could not be achieved without undermining the extensive commercial market that is now involved. However, although there is a general exemption for commodity cryptographic software, the position of cryptographic hardware is less clear.

In any event the United States and a number of other countries still impose export controls on cryptographic products even where there is not even the remotest prospect that they will contribute to the development of offensive military capabilities. In practice these controls, which some nations seek to justify using the Wassenaar Arrangement, have a truly disastrous impact on genuine civil and commercial activities and hence contravene a key provision of the Wassenaar Arrangement. It appears, therefore, that this arrangement is being used by some nations to sustain controls on cryptography that are in no way justified by its aims.

Export Controls on Cryptography

There are a number of reasons why export controls on cryptography cannot be justified under the Wassenaar Arrangement.

Firstly, and most importantly, even if cryptography is assessed as important in military terms, it is a purely defensive technology with no offensive uses. Cryptographic products are entirely passive products whose only purpose is to defend and protect information assets from an aggressor who, for their own reasons, is seeking to gain access to them. Given its passive and entirely defensive nature, it is thus hard to see any case for the control of cryptographic products under the Wassenaar Arrangement – they simply are not capable of being used offensively in any direct way (some indirect uses will be discussed later).

Secondly, export controls on cryptographic products are now having a significant detrimental impact on genuine civil transactions and applications. The protection of national information assets, the development of secure electronic commerce and the protection of the privacy of citizens all now depend on civil cryptographic products that are subject to existing export controls. Export controls on cryptographic products have a severe impact on such civil transactions and this is in direct contravention of item 4 of section 1 (Purposes) of the Initial Elements where it is clearly stated that the Wassenaar Arrangement "will not impede bona fide civil transactions". In fact, this clause, when combined with the impact that cryptographic export controls are having on the civil market, might allow such controls to be legally challenged where the Wassenaar Arrangement is being used to justify them.

In practice, most nations participating in the Wassenaar Arrangement recognise this difficulty and now avoid the imposition of any controls that impact on the civil market for cryptographic products. It is only the United States and a few other nations that continue to interpret the Wassenaar Arrangement in a way that impacts on civil use.

Offensive Military Capabilities and Cryptography

Although cryptography is an entirely defensive technology, even offensive weapons have some defensive characteristics that give rise to cryptographic uses. To provide concrete examples, offensive medium and long-range missile systems require guidance and control telemetry and it is normal to protect these circuits using cryptographic products. Without such protection these missiles would be

vulnerable to actions that interfere with missile guidance and control commands and hence render them ineffective. Even a completely defensive technology can thus have indirect uses in the operation of offensive weapons.

Fortunately, however, the products designed for such applications have almost nothing in common with their commercial counterparts since they have to be designed to meet stringent military performance requirements. In consequence they invariably employ custom designs in products whose characteristics and costs make commercial and civil use inconceivable. Since these products can be easily distinguished from their commercial counterparts there will be no difficulty in setting out criteria that will allow them to be controlled without imposing any restrictions on products designed for civil use.

Governments use cryptography to protect information that is sometimes highly valuable to other neighbouring nations, for example, in determining whether they are planning or considering offensive military action. If a belligerent nation is threatening regional stability it will have to take a number of actions that will often be reflected in its information exchanges, both within its borders and with overseas countries and organisations that are sympathetic to its cause. In this respect governments use cryptography to protect such information exchanges in order to hide their intentions. Again therefore, even though cryptography is a purely defensive technology, it can be exploited by a belligerent nation to the possible disadvantage of its peaceful neighbours. Some may argue that this provides a reason for maintaining cryptographic export controls but in reality, for reasons that will now be explained, it does not.

Over the last 50 years the uses of cryptography have been almost entirely within government where it has been used to protect military, diplomatic and intelligence information. During this time many nations have built up extensive electronic intelligence gathering agencies that operate in support of national security by intercepting the electronic communications of other nations and organisations that they perceive to be of interest. Almost all of this activity is shrouded in extreme secrecy but just occasionally it becomes clear that electronic intelligence collection is pursued not just against enemies but also against friends. In addition some believe that some of these agencies are also involved in commercial and industrial espionage in support of their national industrial and commercial base.

Within government circles the fact that intelligence gathering is pursued against both friends and enemies is well known and this means that when national security is at stake, nations are not prepared to trust other nations when protecting their critical national information assets. Even in NATO, for example, each country goes to great lengths to separate its national secrets from those that it is prepared to share with its allies. And this is equally true of all nations.

Because of this, nations will not use cryptographic products supplied by other nations for protecting their critical information because they simply don't trust them. It is often rumoured that such products embody 'backdoors' that allow the exporting nation to read any traffic that they are used to protect. Although such actions have never been publicly substantiated, this hardly matters because, when national security is at stake nations are simply not going to take chances and will assume that it is true even if it is not. Hence, when they are protecting vital military, diplomatic or intelligence information, nations will invariably employ cryptographic products that are designed and implemented under close national supervision and control. The possibility that a belligerent nation would use civil cryptographic products provided by its peaceful neighbours is absolutely inconceivable and can be completely discounted.

Thus if there is any use of commercial cryptographic products to hide threats to regional and international stability and security, this will involve terrorist or criminal organisations and not belligerent nations. Two questions then arise: (1) does such use fall under the terms of the Wassenaar Arrangement; and (2) if so, are controls justified.

Clearly most criminal activity does not have any impact on regional or national stability and security and is not, therefore, within the scope of the Wassenaar Arrangement. However some major criminal activities and terrorist actions can pose threats to security and stability that could justify action under the terms of the Wassenaar Arrangement.

The question then becomes one of whether export controls can be effective in preventing the use of cryptography by major criminal and terrorist organisations. In practice it seems very unlikely that they can have any significant impact on the ability of such organisations to obtain or use cryptographic products. Products offering cryptographic information protection, especially software products, are widely available and very easy to obtain; within the space of 30 minutes on the Internet

any competent criminal or terrorist can easily obtain cryptographic software that is more than adequate for the sorts of use they are likely to pursue.

Many things are valuable to criminals and terrorists but this alone does not provide a reason for imposing controls. In considering whether a particular category of product should be controlled it is important to ensure that the benefits of denying this product to criminals and terrorists demonstrably outweigh the costs of forgoing its use by law-abiding companies and citizens – criminals find cars useful but society doesn't control the supply of cars because of this. Similarly it makes no sense to deny society the benefits of cryptography in an attempt to prevent criminal or terrorist use that is certain to fail.

Given these circumstances it is impossible to justify export controls on cryptography as in any way supportive of the objectives of the Wassenaar Arrangement. Even senior officials in the United States administration are prepared to accept that that such controls are inefficient for their intended purpose and manifestly unfair – William Reinsch, Head of the US Bureau of Export Administration, admitted just this in response to a question from the author at the recent EPIC cryptography conference in Washington DC. It is also worth noting that a US National Research Council report on cryptography policy[1], commissioned by the United States government and published in 1996, concluded, "on balance the advantages of more widespread use of cryptography outweigh the disadvantages."

In practice current cryptography export controls are an unfortunate 'hangover' from the earlier 'cold war' controls on which the Wassenaar Arrangement has been based.

The Civil Uses of Cryptography

As the economies of the nations of the world become increasingly information based there is a growing recognition of the importance of commercial cryptographic products in protecting both information and information processing assets.

Many companies now operate internationally in highly competitive markets and their advantage over their competitors increasingly depends on the effectiveness with which they co-ordinate and plan their actions and avoid knowledge of their intentions being seen by their competitors.

There is also a rapidly developing interest in electronic commerce, where there is universal acceptance of the role that cryptographic products will play in its development and in the protection of consumers. Cryptographic products are essential for making the Internet safe and hence have a central role in the prevention of criminal behaviour in cyberspace. In this respect, therefore, the free and unconstrained availability of cryptographic products is essential if society is to be able to defend itself against criminals.

Export controls are already doing significant damage to this civil market. The reality of export controls is not that they prevent criminals from obtaining cryptographic protection but rather that they prevent the vast majority of law-abiding companies and citizens from obtaining the protection they now need.

The detrimental impact on cryptographic product suppliers is enormous. There is already a big market for commercial cryptographic products but export controls prevent the companies involved from effectively exploiting this market. The cost is measured in millions, if not billions, of dollars and the economic harm being done is now immeasurable. This directly contravenes item 4 of the Wassenaar Arrangement where it is very clearly stated that it will not impede bona fide civil transactions. Moreover the radically different interpretations of Wassenaar controls on cryptography by different countries leaves some suppliers unable to compete in this market whilst others can supply civil products with no difficulties whatsoever. Of course some nations will argue that those who are not controlling civil cryptographic products are not meeting their obligations under the Wassenaar Arrangement but this is clearly incorrect since item 4 of its statement of purpose very clearly states that it "will not impede bona fide civil transactions".

Increasingly the economies of the developed (and developing nations) are dependent on networked computing resources. Irrespective of whether it is communications, electrical power generation, road, rail or air transport, stock exchanges, banks, finance houses, agriculture, hospitals or a host of other infrastructures, all now depend on regular and continuous information exchanges between networked computer systems for their continuing safe operation. In the absence of effective crypto-

[1] Cryptography's Role in Securing the Information Society, report of the Committee to Study Cryptography Policy, US National Research Council

graphic protection the computer systems that keep these infrastructures operating are wide open to attacks by terrorist and criminal organisations using only modest resources. Cryptographic export controls are preventing the protection of these civil infrastructures and rendering them easy and tempting targets for international terrorists and criminals. Far from impeding crime and terrorism, therefore, controls on cryptography are having precisely the opposite impact – they are helping to ensure the evolution of networked information infrastructures that are easy targets for criminal or terrorist actions that could easily put much of the infrastructure on which society depends at risk.

A thriving market for cryptographic products, free of all export controls, is now vital if the economies of western nations and the well-being of their citizens are not to be put at risk in this way. Far from threatening regional stability and international security, such a free and competitive cryptographic product market will quickly provide the products which are needed to protect the information based economies of the developed nations and safeguard their citizens in the face of 'information terrorism' and the activities of 'cyber-criminals'.

A careful study of the Wassenaar Arrangement shows that it is does not provide a basis for export controls that harm or impede civil activities but this is exactly what existing controls on cryptography do. Fortunately many nations now recognise this and are no longer using the Wassenaar Arrangement to justify controls that are so clearly out of tune with its provisions. However the inconsistency between nations creates many difficulties and leaves suppliers in those nations that operate stringent controls at an enormous disadvantage compared with those that that are located elsewhere. This inconsistency completely undermines any conceivable value that such controls might have.

It seems likely that a few nations might propose that controls should be strengthened to overcome this difficulty. Such proposals are extremely dangerous and need to be strenuously resisted. Consistency is vital if controls are to be effective but any changes must be consistent with the stated aims of the Wassenaar Arrangement and the only way this can be achieved for cryptographic products is by removing all such controls.

The Future of Cryptographic Export Controls

Given the earlier analysis there is no sound basis within the Wassenaar Arrangement for the continuation of any export controls on civil cryptographic products. For reasons already covered these are not going to be used in offensive military or weapons programmes or by aggressor nations to protect their critical communications or information assets.

Because cryptography is an entirely passive technology whose characteristics are of a completely defensive nature there is a clear rationale for the total removal of all controls on cryptographic products, including even those of a military nature. As a purely defensive technology, the widespread deployment of cryptography will contribute greatly to the maintenance and promotion of regional and international security and stability and hence to the objectives that the Wassenaar purports to support.

Contrary to the provisions of the Wassenaar Arrangement, export controls on cryptographic products now have a detrimental impact on 'bona fide civil transactions' and this alone means that they can no longer be justified by this agreement.

Worse still, the imposition of export controls on cryptographic products is preventing their use to protect the privacy of citizens and to protect the vital national infrastructures that now depend on networked computing resources for their safe operation. Export controls on cryptography hurt law-abiding companies and citizens without having any significant impact on the ability of criminals, terrorists or belligerent nations to obtain the cryptographic products that they need. Moreover such controls are now undermining the protection available with the civil information infrastructures on which society is increasingly dependent.

Far from hampering criminal and terrorist activities, controls on civil cryptographic products are promoting the evolution of a global information infrastructure that provides many easy targets for cyber-crime and information terrorism.

All controls on cryptography now need to be removed as a matter of urgency.

Acknowledgement

I am grateful for the contribution made by Professor David Jones, President of Electronic Frontier Canada, in commenting on an earlier paper and encouraging me to undertake a major revision of its content.