

Center for International Trade and Security

The Monitor

Nonproliferation, Demilitarization and Arms Control

Vol. 6, No. 3

Summer 2000



The University of Georgia

IN THIS ISSUE:

CONTROLLING INTANGIBLE TECHNOLOGIES

Weapons of Mass Destruction and Intangible Technologies: the Limits of Law <i>by Terence Palfrey</i>	3
Controlling the Transfer of Technology by Intangible Means in UK <i>by Bridget Butt</i>	10
U.S. Controls on Technology Transfer by Intangible Means <i>by Timothy Williams</i>	12
Controls on Intangible Technology Transfer: German National Legislation <i>by Andreas Kleine</i>	16
Globalization and Control of Intangible Technology Transfers: a Major Challenge to Export Controls in the 21st Century <i>CITS Working Paper presented at the Conference in Moscow, May 2000</i>	20
Equipment Assessment Project for MPC&A Cooperation with Russia <i>by Daniel Miller; Kara DeCastro, Ron Melton, Yves Dardenne, Charles Ringler, Kathleen McCann</i>	26

MPC&A

Considerations in Implementation of Integrated Safeguards <i>by Rodney Martin, Ronald Melton, and Ned Wogman</i>	31
The Role of Russia's Gosatomnadzor in MPC&A Implementation <i>by Yuri Volodin, Boris Krupchatnikov, Alexander Sanin</i>	33
Sustaining MPC&A Systems in the Newly Independent and Baltic States <i>by G.A. Sheppard, J.R. Mason, P.W. Robinson, M. Soo Hoo</i>	36

DOCUMENTS

Decree of the RF President No. 822	40
Comments on the Presidential Decree <i>by Mikhail Ryzhov and Marina Belyaeva, MINATOM</i>	40
Agreement between the U.S. and Russian Government Concerning the Management and Disposition of Plutonium (Excerpts)	41
Comment on U.S.-Russian Cooperation for Plutonium Disposition <i>by Laura S. H. Holgate</i>	42
Agreement on the Establishment of a Joint Warning Center	45
Joint Statement by the U.S. and Russian Presidents on Principles of Strategic Stability	45

BOOKNOTES

L.Feoktistov, <i>Useless Weapons</i> (in Russian)	46
V.M.Kuznetsov, <i>Russian Nuclear Energy Past, Present, Future: View of an Independent Expert</i>	47

NEWS FROM THE CENTER

Sam Nunn Policy Forum	48
Moscow Conference	50
Conference in Obninsk	51
Workshop in Minsk	52
Minatom Training Program	53
Workshops in Ukraine	53
Center Team Travels to India	54
CITS-CSIS Cooperation	54
A Trip to Cuba	54

CONTROLLING INTANGIBLE TECHNOLOGIES

Controlling the proliferation of weapons of mass destruction is the foremost international security challenge of the next century. With the exponential global diffusion of information and technology, it has become increasingly easy for pariah states and terrorist groups to obtain whatever they need to develop weapons and delivery systems with awesome destructive capabilities. Further, consistent with the traditional principles of supply and demand, the cost of acquiring the needed technology, equipment and materials to build and deliver such weapons has declined substantially as the availability of the tools to make them has increased. Export controls will continue to play a key role in any regime to control and manage the risk of proliferation of WMD.

We have entered a stage where the most serious acts of proliferation may involve transfers of know-how rather than hardware. Therefore, it is crucial that authorities have the ability to control technology, especially intangible technology that can be passed via the fax machine, internet, or academic conference, while maintaining obligations to transparency and the free flow of information.

The papers below were presented at CITS sponsored conference "Globalization and Control of Intangible Technology Transfers: a Major Challenge to Export Controls in the 21 Century" held in Moscow, Russia in May 2000. The Center intends to continue its research project on intangibles and hold additional fora. We would welcome any comments and inputs from our readers.

WEAPONS OF MASS DESTRUCTION AND INTANGIBLE TECHNOLOGIES: THE LIMITS OF LAW

by *Terence Palfrey*

Introduction

This paper is concerned with issues related to intangible technologies as they impact strategic weapons technology and export controls. In the aftermath of the Scott Report recommendation that "A comprehensive review, in my opinion, required, and long overdue, of the power of the government to impose controls on exports from the United Kingdom,"¹ subsequent Green (Cm 3349)² and White (Cm 3989)³ consultation papers identify one area of concern as how to control the transfer of sensitive technology by electronic means. In particular, attention has focused on military and dual use technology, which can be controlled (arguably) in a tangible form, but not if transmitted by intangible means, i.e. fax, internet, e-mail, or orally. Consideration has been given to the relationship between export controls for military and dual use goods and a parallel control regime for associated intangible technology. The proposal of the UK government introduces a general power to control the transfer of technology by intangible means, limited "for the time being" to weapons of mass destruction (WMD) related information.

Although the Scott Report was critical of HM Customs and Excise (Customs), it remains the law enforcement agency responsible for export control cases. During the 1980s and early 1990s Customs representatives prosecuted a series of cases through the criminal justice system amidst a maelstrom of controversy. At the time of Scott, Customs used "State-

ment of Enforcement Needs Regarding Department of Trade and Industry (DTI) Export and Transshipment Licensing" as a policy guide. This document makes particular reference to the transport of sensitive goods to sensitive destinations and the makes enforcement of export sanctions a top priority in no uncertain terms. The statement of enforcement makes it clear that there is no room for discretion concerning fraudulent intent involving proscribed or sensitive destinations; a criminal prosecution is required.⁴ Other measures include selective intelligence (presumably including post-shipment verification), anti smuggling checks (inland and borders), audit checks and seizure of prohibited goods.⁵ They also have available a range of administrative penalties.

Despite the document's clarity, perusal of Customs' annual reports since the Scott Report was published in 1996 reveals that it has not been a very active prosecutor of strategic export control cases. However, Customs officials do seize considerable amounts of material. Seizure triggers a compulsory civil forfeiture process which can sometime be protracted and involve third parties.⁶ Because of the imbalance in the number of seizures versus prosecutions, it is difficult to ascertain the seriousness of the problem concerning transfers of technology. It may be that, in a majority of cases, no criminal prosecution is required, the offenses being minor breaches of law and punishable by small fines. But if prosecution is infrequent because of difficulties in compiling evidence, the attempt to control intangible technology will present even greater obstacles. Still, despite the difficulties, maintaining an effective export control system demands criminal prosecutions in appropriate cases. Only the belief that the law will be enforced and penalties applied will deter potential violators. Those charged with pursuing violators

must be confident that they have a decent chance of winning a prosecution and this means that the laws they are being asked to enforce must be well drafted and up to date.

The present proposals aimed specifically at intangible technology transfers and strategic weapons cannot be considered in isolation from wider issues concerning law enforcement, computers and the Internet. Many of the issues concerning the transmission of sensitive or illegal information and abuse of communications systems overlap with a wider range of cyber-threats linked to money laundering, pornography, organised crime and terrorism. The flow of data into law enforcement/security services and between the agencies involved is obviously important. So is the ability to access communications and operate surveillance and effective investigations. Recent government initiatives have emphasised these issues. New surveillance facilities have been established. Whilst earlier proposals to introduce key escrow as a response to a perceived law enforcement problem with encryption have largely been abandoned, the Home Office has introduced the Regulation of Investigatory Powers Bill. The Bill contains controversial powers that allow law enforcement agencies to obtain decryption keys and intercept and or monitor e-mails and internet traffic. These developments will be discussed later in this paper.

Legal problems are generated by these issues, of course, because of the need to balance the concerns of e-commerce and civil liberties with the legitimate needs of national security and law enforcement. Two types of legal questions arise. First, effectiveness requires a set of workable laws dealing with problems of technology and jurisdiction, proper powers of surveillance and investigation and the ability to conduct prosecutions to a positive and expeditious conclusion. The second type of question is one concerned with rights issues: fairness, transparency and consistency, broadly what might be termed justice and rights issues.

Often the perceptions of those engaged in law enforcement and those concerning themselves with broader issues concerning sanctions and licensing differ substantially; policy makers often have unrealistic assumptions about what law and law enforcement in particular can deliver. These misunderstandings are compounded at the international level with differences in legal systems; yet the problems at hand are global in dimension because of the nature of the technology in question and some sort of multinational agreement is required. The study of legal theory and comparative law may yield a set of commonly accepted values, terminology and standards which all export regimes can accept as the basis for effective law enforcement. The legal process may still be compromised by diversity of approaches and traditions, but at least then the practical and theoretical limits of the law will be made explicit.

This paper first outlines in more detail the UK's legal framework, initiatives and proposals for change. Second, consideration is given to understanding entrenched problems fac-

ing investigators and prosecutors, problems aggravated by intangible technology transfers. Finally, consideration is given to the role (and limits) of legal theory as a basis for developing common standards for law enforcement agencies.

Government Measures And Proposals Concerning Intangible Technology Transfers

Government measures and proposals are a mixture of context specific (to arms control) and wider surveillance and investigatory tactics regarding computers and the internet. Cm 3349⁷ identifies control over the transfer of technology by intangible means⁸ as a key issue in strategic export controls:

A UK person or company, might, without being directly involved in an attempt to produce a weapon of mass destruction, nevertheless, provide a service or information which could assist such a programme. The existing end-use control is intended to prevent the export of equipment which might be used in such programmes but the Government considers that it would be desirable to introduce measures to prevent other ways in which such programmes might be given assistance, such as the transfer of technological information by intangible means or provision of technical services. In view of this, it is proposed to make it an offence to do something that would promote or facilitate the development or production of weapons of mass destruction either if the government has informed someone that what he is doing poses such a risk or if someone knows by other means or has grounds for suspecting that a particular course of action might assist such a programme.

Cm 3989 is at times ambiguous as to exactly what it is proposed to control. The consultation paper states its overall aim: "to enable the Government to impose controls on intangible transfers of technology".⁹ It is then explained that whatever the means by which the transfer is effected, secondary legislation would state that all technology subject to control in documentary form should be controlled when exported intangibly.¹⁰ The scope of proposed controls are explained under a heading, "transfer of technology by intangible means."¹¹ In Cm 3989,¹² the government, referring back to earlier representations,¹³ acknowledges that some doubts were expressed about the practicalities of enforcement of any legislative changes. However, the intent is to proceed and introduce a new power controlling the transfer of technology by intangible means, for example, via fax or e-mail.¹⁴ This power would also extend to the publication of controlled technology on electronic networks such as the World Wide Web; such publication would also become an offence.¹⁵ It is further explained that, whilst the power would enable the government, if need arose, to introduce the same controls on other types of technology, it would, for the time being, limit new offences to technology having to do with weapons of mass destruction.

Submissions to both consultation papers were considered by the Trade and Industry Committee on 10 November 1998.¹⁶

It was accepted that proposed new controls over the export of intangibles raised genuinely complicated issues requiring resolution.¹⁷ The Committee acknowledged the practical difficulties in regulating the transfer of technology and clarified the provisions by limiting the extension of licensing requirements and regulation of electronic transfer of documents to technology related to weapons of mass destruction.¹⁸ The outcome is that the UK has proposals for a general power which would be granted to the state to control the transmission of all technology, in various mediums, including the WWW, restricted "for the time being" to weapons of mass destruction and long range missiles. However, the legal formulation of such a power remains a considerable problem.

In addition to the possibility of new amendments to the existing law, there are a raft of other measures proposed which also have bearing on the issue of intangible transfers of technology. For example, Customs is pressing for the clarification of and expansion of powers concerning investigation and surveillance.

The United Kingdom maintains export controls on cryptography pursuant to its participation in the Wassenaar Arrangement and adherence to the EU Dual-Use Control List.¹⁹ Linked to proposals outlined above, the Department of Trade and Industry (DTI) has considered the problem of encryption as part of a wider debate on the regulation of electronic commerce. The DTI has produced a White Paper followed by a Consultation Paper²⁰ and a Secure Electronic Commerce Statement²¹ outlining its concerns regarding encryption. If the encoding is intended to send data securely over the Internet, then the keys required to decode the message should be deposited with a government sponsored body. Security services claimed that they must be able to access net traffic and that the encryption provision is simply another form of authorized wire tapping. Some proposals included key escrow provisions providing for the licensing of trusted third parties who would then hold the copies of private encryption keys.

Under pressure from business there was a shift in policy.²² The key escrow provisions have now been considerably restricted and the most contentious aspects removed. Warrant and surveillance provisions now appear in the Home Office Regulation of Investigatory Powers Bill. As the name suggests, this Bill is designed to update the law on surveillance and investigatory powers. Some of the measures in the Bill will allow law enforcement and security agencies to obtain 'keys,' special codes and to unlock scrambled messages. The Bill contains provisions allowing law enforcement agencies to obtain decryption keys. Under the Bill, authorities have the right to demand that companies decode data or face a possible two year jail sentence if they fail to do so. Companies will be able to claim that they are innocent or incapable of decrypting the information, but the onus of proof shifts to them in these instances. The Bill also requires Internet Service Providers (ISP's) to install systems that let the authorities monitor their subscribers.

In 1999, a government organisation known as the National Infrastructure Security Co-Ordination Center (NISCC) was established.²³ One of its functions is to protect critical computer systems and electronic infrastructure from 'cyber-attack.' A new e-mail surveillance centre, the Government Technical Assistance Centre (GTAC) is currently being built with 'hardwire links to ISPs' and the power to monitor e-mail and internet messages.

Legal Problems With Investigating And Prosecuting Export Control Cases

Before commenting further on the legal implications of these changes, let us consider the problems encountered by Customs in their law enforcement activities. The main concern in this paper is with the use of the criminal law and justice system.

Licensing issues are the domain of the DTI. If the matter is sensitive, then copies of applications are also forwarded to the Communications and Electronic Security Group (CESG). However, other Government Departments may also be consulted, in particular the Foreign and Commonwealth Office and Ministry of Defence. Once the DTI has granted a licence, any question of law that arises falls to Customs alone to investigate and enforce.²⁴ Obviously there may be close cooperation between the two agencies, especially if it is alleged that the application was not accurate and the licence possibly fraudulent. Customs law enforcement operates under a tripartite system in which investigators, prosecutors and administrators work together, particularly on some issues, for example, deciding how to dispose of a case. Although cooperation is routine, all parties must maintain 'Chinese walls' between functions, maintaining proper independence between investigators and prosecutors.²⁵ As a result of Scott Report recommendations in export control cases, the Attorney General alone has supervisory authority over Customs.²⁶ The Attorney General also heads the Crown Prosecution Service, the independent Service which conducts prosecutions within the ranks of the police. Customs follows the same evidential code as that developed for the Crown Prosecution Service, but remains one of several agencies in the UK with an independent prosecution function.

The legal liability framework starts with the Import, Export and Customs Powers (Defence Act) 1939 (IEC) which allows for the operation of a number of export controls. Export of Goods Control Orders are made from time to time and govern controls of the export of restricted goods and licensing requirements. Strategic Goods (military and high technology industrial equipment) are subject to the Export of Goods Control Order, Council Regulation (EC) No 3381/94, which sets up a Community Regime for the control of export of dual-use goods and enforcement of the dual-use and Related Goods (Export Control) Regulations. There is also an EU Code of Conduct for arms exports which outlines standards for licensing military exports. Strategic export con-

trols is a composite term, directed first at the prevention of the proliferation of weapons of mass destruction and their delivery systems and second, towards the accumulation of conventional weapons which might be used for internal repression, international aggression or destabilisation. Customs' main criminal offences are found in the Customs and Excise Management Act 1979 (CEMA) sections 68, 167 and 170 and cover prohibitions, smuggling and breaches of licensing requirements. These are discussed later in this paper.

Apart from the existing licensing and Customs regime, other controls do exist. The transmission of classified information in electronic form is already covered under the provisions of the Official Secrets Act (OSA). The legislation is not dependent on a particular means of communication--both oral and electronic transfers would be covered. The problem with the OSA is that it is intended for use with official secrets and classified material and it is probably undesirable to use such legislation as a blanket deterrent.

a. Law enforcement in export control cases. Most of the following comments are drawn from examples collated from the Scott Report.²⁷ The Report considered a number of past licensing prosecutions involving various items including lathes for alleged shell/missile production, alleged parts for construction of a Supergun, alleged silenced sub-machine guns, alleged transmitter linked systems, and alleged electrical capacitors believed to be designed for use in nuclear warheads. Many of the cases collapsed at various stages in the criminal justice process and the Scott Report and various media accounts elaborate on some of the difficulties plaguing the prosecution. What follows is a short summary of some of the issues. They are developed into some general observations about prosecution issues, many not exclusive to export control cases.

The defendant(s) (individuals and or company) may run a profitable company. Once an investigation and or prosecution goes public, their business may be damaged terminally.²⁸ A particularly difficult decision facing prosecutors is whether the evidence warrants beginning an investigation of a company given the risk of attracting media attention and damaging trading.²⁹ The investigation may be expensive and time consuming and, if items are seized, there may be complex third party civil actions resulting from contract violations. The evidence will have to be stored and collated in a way acceptable to court procedures. The agency may have only a limited capacity to take on such cases; relative resources and costs must be factored in.

The case may well involve sensitive material. Not all of this may be disclosed³⁰ and investigators may not themselves be privy to all the available information. The investigator may not be willing or able to disclose all sources of information and methods used to obtain it. Applications for disclosure by the defence may be time consuming and expensive and ultimately hurt the prosecution. The criteria determining

what may and may not be disclosed may be questioned by the defence and any refusal to disclose may arouse suspicion. There may be insinuated links to the executive, suggesting a cover up. In some cases, ministerial "public interest immunity certificates" may be in operation, protecting internal dealings of the Crown, advice to Ministers or national security aspects³¹ and making some evidence unavailable to the court. The need to safeguard sensitive information provides the defence with "ammunition" and exposes the prosecution to the allegation that it is being less than open with the facts.

Such cases can run into other problems. It is not unusual for the defence to embroil the case in links to the security services, foreign and defence policy issues and conspiracy theories. There is also ample opportunity to exploit tensions within the licensing system³² and between licensors and the law enforcement system. There may be transshipment and end use problems.³³

A burnt earth defence may be deployed. Questions of consistency may arise-- perhaps on previous occasions the authorities approved similar exports or did so for other companies. It may be suggested that informal indications were given by authorities that the export in question did not require a licence. In addition there may be confusion of a technical nature: what was and was not covered? What are the distinctions between certain listed and non-listed items? How should "special design packages," which draw together a set of standard designed equipment into an aggregation, be treated in licencing? There can be different constructions on interpretation.³⁴ Although the onus is on the defendant to establish whether or not a licence is needed, this reversal can be used as an argument suggesting confusion or indecision amongst regulators and inconsistent interpretations on dual-use goods. If standards are seen as inexplicit, it becomes difficult to state with much conviction what criminal conduct is alleged to have occurred and what the prosecution must prove.

Technical issues in these cases often require expert witnesses, thus delaying the process and increasing the expense. Extensive delays become grounds for abuse of process applications. By the time the case is completed, the regulatory regime may have altered its lists in response to technological developments, removing the item in question and making the case look obsolete.³⁶

Courts may see such cases as technical and not deserving substantial punishment, especially when it is inappropriate, for security reasons, to articulate the ramifications of the breach in court. They also may be reluctant to punish corporations because of the difficulty in assigning culpability. Former employees may be blamed and the corporate offence is interpreted as a negligent lapse rather than a deliberate evasion.

These cases garner much publicity which can be a deterrent to their prosecution. Customs found themselves in a dilemma in the Scott Inquiry when attractive alternatives to pros-

ecution were available to them; sensitive cases were not taken to court where they would have inevitably attracted publicity.³⁷

Finally prosecutions can prove very expensive. The State has paid out significant sums in compensation in connection with failed prosecutions, including sums for the destruction of business activity.³⁸

b. The added problem of intangible technology in a criminal investigation/prosecution. The scale of additional problems caused by the transfer of sensitive or illegal information transmitted on the Internet or via other modern technological links is difficult to determine from published material or past experience, but there is no doubt that it will be considerable. The following general observations give an idea of the nature of some of these difficulties.

First, there is the problem of locating evidence: does it reside in a file server, network, back-ups, electronic bulletin boards, or in the electronic mail system? The sheer amount of information may be enormous and the job of downloading time consuming, expensive and potentially corruptive of evidence. In a PC, the information may be in various locations, presumably anticipated by the warrant, but data could also be contained in monitors, laser printers and scanners. Network PCs may be linked to file servers, electronic mail, electronic bulletin boards, and voice mail supported by backup systems. Networks and bulletin boards present their own unique problems. Bulletin boards may have a mixture of legal and illegal material and authorities investigating illegalities must be attuned to privacy considerations of others making use of the service.

Second, there are problems of access and specificity, especially if warrants or wire taps are required. How do you isolate the desired material and target the suspected offenders? Can the different components in the "system" be isolated and categorised? Is it possible to seize certain items and leave a commercial system still operative? Can the role of the computer or ISP or other medium in the offence be determined? If the case crosses borders, then cooperation with other authorities will be required; it may be necessary to locate the destination of the illicit material first, before much evidence has been gathered concerning the native offender, and this poses problems of diplomacy. One way to avoid these problems could involve approaching those who store the material and asking for their cooperation, but then there is the question of who can give consent. An employee, owner, partner? Who owns the information? What are the requirements of the Data Protection Act - especially in networks and industrial systems?

Another tier of problems arises if hardware must be seized. Computer systems are connected sets of individual components; seizing the whole system, even if practicable, may damage the commercial activity of a business. It may be necessary to categorize seizures on the basis of whether the computer or components are themselves the centre of the crime

or simply instruments used to facilitate the crime. A decision must be made about whether to search on site or seize. Obviously, if a large amount of evidence needs to be examined then seizure must be anticipated and the warrant drafted accordingly.

Once seized, the hardware may need disassembling, photographing, and transporting. Static electricity and the presence of magnetic interference can corrupt information. Hardware must be moved and preserved in a climate controlled environment. Data which is removed must be stored in a way that is accessible and useful in a criminal prosecution. Again, there are privacy considerations to be taken into account, especially for privileged and confidential information such as lawyers' communications. Any seizure may trigger High Court action from lawyers, preventing the continuation of the investigation..

A third tier of problems arises when the search for information begins. Experts may need to be brought in and, if the case involves ISPs, there is the danger of damaging or destroying equipment and information incidental to the investigation.

Seizure of the information is quite different from seizure of the computer and far more complex. Unlike hardware, information can be encrypted and hidden. The information may itself be the product of crime, of instrumental use in the commission of crime, or designed to perpetrate criminal activity. A further range of problems may arise if unexpected data is retrieved. The data retrieved must correspond to specifications of the warrant or the warrant is corrupt. Investigation sometimes requires "fishing expeditions" which are costly and time consuming if, for example, the data is encrypted. A further problem confronting investigators is known as commingling--the data may be in a particular directory or stored at random. The search itself may trigger destruction inadvertently or the system may have a built-in capability of this kind.

Additional problems may include the need for a chain of evidence, record keeping, preservation, return of equipment and clarity of presentation.. When the case is presented to prosecutors and the courts, it is crucial that it can be exhibited and its evidential status established.³⁹ If evidential information is encrypted, it is likely that complex and lengthy explanations will be needed concerning interpretation.

Legal Issues and The Limits of Law

The initiatives aimed at intangible technology transfers are best understood by superimposing them on already existing problems with the law enforcement system. It is possible to isolate a range of underlying legal problems and procedures which can be anticipated.

a. Drafting and amending laws. There is a need to sort out legal terminology. Cm 3989 illustrates the problems. For example, why is the term "intangible transfer of technology" adopted? Is technology the same thing as scientific or tech-

nical knowledge? It is probably not intangible technology that is transferred, but information with a scientific, technological, economic or sensitive content. Are controls designed to restrict exports or transmission of information across borders or both?⁴⁰ The term “intangible transfer of technology” seems misleading. With reference to the IEC 1939 and CEMA 1979, there is a need for clarity regarding what, exactly, the law is controlling the transmission of. In particular, is the focus to be on the transmission or export of technology, documentation, or information itself? It seems that various combinations of these are envisaged, making the proposals muddy and potentially obscure.⁴¹

As the original rationale of the IEC was to prevent trading with the enemy, the legislation may be better repealed. The prohibitions of the IEC are framed in terms of carriage of goods.⁴² The legislation was passed two days before the outbreak of the Second World War to prevent trade with the enemy. Power is given in the primary legislation for controls to be specified by secondary legislation. The IEC needs to be altered to include in its scope the export of information by transmission overseas. The meaning of “goods” and “export” will have to be clarified to include intangible property transmissions and information.

If a breach occurs, then Customs can use an offence under section 68(2) CEMA or section 170 CEMA. Section 170(1)(a)(iii) of CEMA refers to “goods with respect to the importation or exportation of which any prohibition or restriction for time being in force under or by virtue of any enactment”. Section 170(1)(b) states “...is in any way knowingly concerned in carrying, removing, depositing, harbouring, keeping or concealing or in any manner dealing with such goods...with intent to defraud...commits an offence.”⁴³ Again, this legislation will need amending.

The underlying problem, besides the policing difficulties, is with the term “goods” in both the IEC and CEMA. Whilst it may be possible, as the legislation stands, to think of “goods” or even “documents” (qua goods) being exported or imported, it does not catch “information” in its net. In the UK it is not criminal theft to take information/intangible property, for example, intellectual property. So if someone intercepts or takes confidential information they cannot be accused of stealing. This is a policy problem rather than a legal problem. It might be possible to draft a new law (or use the following wording to clarify the meaning of “goods” and “documents”) based on the wording of the US Espionage Act 1996. The US legislation contains an interesting approach. A trade secret is defined as all forms and types of financial, business, scientific, technological, economic or engineering information including patterns, plans, compilations, program devices, formulas, designs, phototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and regardless of how stored, compiled, or memorialised physically, electronically, graphically, photographically or in writing.⁴⁴

b. Resourcing the agency. There is also the problem of funding. It is supposed that Customs should enforce any new legislation. Given the apparent importance of the issues, it might be assumed that any legal changes would be fully funded. The White paper allows that there will be a small increase in the number of licensing applications, imposing additional resource requirement on government departments (FCO, DTI and MOD), but the size of the projected increase means that the impact would be limited. The DTI estimates that the total resources required for export controls reorganisation are £25.000 p.a., salary for one new staff member in license processing. Extra enforcement activity by Customs is expected to cost £500.000 per year. However, these figures seem to ignore the the potential costs involved in policing the flow of sensitive technology by surveillance, investigation and prosecution. Adequate staffing and funding are crucial⁴⁵ if enforcement is to be implemented effectively.

c. Surveillance, investigations and human rights. There is clearly a need for law enforcement officials and security personnel to access data flow.⁴⁶ The relation between intelligence gathering and criminal investigation and prosecution is changing in the UK as a result of advances in technology. Some commentators make much of what they see as the emergence of a “surveillance society,” a system which engages in surveillance and intelligence gathering for general security purposes without necessarily intending any sort of criminal prosecution. In such a society, discussions of privacy rights have no place in the public arena at all.⁴⁷

Considerable concern has been expressed concerning the DTI encryption proposals and The Regulation of Investigatory Powers Bill. There is already a tradition of intercept warrants in the UK-The Interception of Communications Act, Security Service Act 1989, Intelligence Services Act 1994 and Police Act 1997 Part 111 and questions have been raised as to whether the Regulation of Investigatory Powers Bill is necessary at all. Human rights groups question whether the problem is extensive enough to warrant such a legislative response,⁴⁸ citing the lack of evidence that encryption is commonly used by professional criminals. They argue that regulation alone will prevent dissemination of most technology and in the rare cases that it fails, law enforcement agencies can simply crack codes as they have in the past.⁴⁹ They also point out that effective encryption prevents crime (for example fraud). Generally speaking, the concern is that far reaching controls are being introduced without a thorough investigation of the extent of the problem.⁵⁰

It is expected that some of the provisions in the Bill will be challenged under the Human Rights Act 1998, pitting national security considerations against privacy concerns. The outcome of any such challenge is difficult to predict. The Convention contains a mixture of absolute, strong and prima facie rights. The rights to privacy and freedom of communications and trade are qualified by references to state interference as might be necessary to protect the interest of

national security, public safety or economic well being of the country. There are also other layers of protection. The Data Protection Act 1998 restricts the free trade of data and is based on a EU Directive on Data Protection. The Data Protection Registrar has the power to obtain warrants and prosecute cases. However, its primary emphasis is on raising public awareness of the need for security in the use of information technology. The Government has also introduced a Freedom of Information Bill which, it claims, 'would radically transform the relationship between Government and Citizen.' However, it has been much criticised for the number of exclusions favoring the activities of law enforcement agencies. There is a great deal of public concern over sacrificing privacy rights without sufficient cause. With reference to the U.S. proposals concerning a Federal Intrusion Detection Network (FIDNET), the Electronic Protection Information Centre (EPIC) argues that backers of the U.S. security plan are "trying to apply twentieth century notions of national defence to twenty-first century problems of communications security."⁵¹

Developing Legal Standards

This paper has highlighted a specific set of proposals dealing with intangible technology transfers and set them in a national legal context. However, what starts to emerge is idea that any national legal responses are restricted by the global nature of the problem addressed. Effective multilateral controls require some sort of international consensus on the means of control.

In addition to some of the issues surrounding Wassenaar already mentioned, there has been a lack of international consensus on encryption and also on the legal terms used to describe the transmission of technology. The MTCR control regime promotes adherence to common export policy guidelines applied to an integral common list of controlled items. Guidelines have been issued for controlling sensitive missile relevant technology transfers.⁵² The MTCR can only be implemented through the domestic laws of member states, resulting in disparate interpretations of MTCR based laws in various states and creating some discord amongst members.⁵³ The Australia Group also promotes control of relevant dual use items and technology for chemical and biological weapons; the Nuclear Suppliers Group seeks to control the flow of technical information regarding the development, production and use of controlled goods.⁵⁴ A law-based export control system would seem to be a vital first step, but such a system requires not only political consensus but agreement about key legal terms. Lack of consensus on legal meanings is often responsible for the lack of clarity in international agreements and has a nullifying effect on enforcement.⁵⁵

Translating any single theory of law into a global rationale is problematical.⁵⁶ There is debate about the significance of the phenomenon of globalization and appropriate national responses. The term refers to the creation and con-

solidation a unified world economy. The academic literature tends to divide into two schools: strong globalization theorists who postulate the collapse of the nation state and sceptics who point to the need for a historical perspective and believe that the rhetoric is overblown. A strong globalizer might argue that the technology in computing, for example, is advancing so rapidly that the law cannot keep up. Use of the internet breaks down national borders, they claim, and ultimately erodes the sovereignty of the state. Sceptics respond, "the Internet is nothing new--Victorians had one!"⁵⁷ Those espousing a historical view point out that advances in technology have always challenged existing legal frameworks and that globalizers are simply exhibiting the age-old tendency of men to think of their own time as one of revolutionary change.⁵⁸ The historicists acknowledge that the increasing interdependence of nations inevitably changes the significance of national boundaries, but hesitate to predict centralisation or homogenisation. Reaction to increased interdependence may increase nationalism. Technological advances like the Internet may be changing the significance of national and societal boundaries but it does not follow that it makes them unimportant. In business, a common saying is "think global act local." This slogan has its applications to the issues of nonproliferation and export controls in that multilateral pressures are certainly at work, but national frontiers still figure prominently.

The issue contains within its framework a plethora of legal organisations and networks cutting across geographical divisions and raising difficult questions concerning the sovereign state, governments, people, nations, societies, communities and classes, multi-nationals, formal and informal trade, arms trade, and criminal networks. As a result of these unprecedented developments, different levels and types of law must come into play. For example, international public law as traditionally conceived cannot fully cope with global issues such as the environment, nonproliferation and international crime. Along with international capitalism we are seeing the emergence of transnational private regulation based on international arbitration systems. Human rights are derived from international conventions. Some commentators have suggested that the emergence of many different legal orders represents a disengagement of law and state and that the future will see the development of global legal standards.

Any attempt to find a consensus on legal terminology and standards requires comparison of systems.. The problem is that comparative law is largely a construct of Western capitalist systems, emphasising legal doctrine and tending to be descriptive and explanatory rather than evaluative and prescriptive. The best work in this field engages questions central to this paper: "the lessons to be learnt from foreign solutions to 'shared problems'."

Of all the issues discussed here, probably the most fundamental is compatibility of language--a recurring problem for international agreements and nations considering the

adoption of best practice in law enforcement. Anyone involved in extradition cases knows how difficult it is to explain to another jurisdiction how two sets of laws may contain common elements and generate similar criminal offences. This in turn begs the question of the emergence of a meta language of legal theory that transcends individual legal cultures. A meta language, for example, can be used to compare different systems⁵⁹ in which common features can be identified, locate shared values and establish common legal standards. Whilst there are problems with definitions such as a "legal person," "judge," "trial," or "corruption," there is some degree of consensus obtainable by the use of comparators--standard measures or indicators that provide the basis for comparison and evaluation. The setting of best practice standards is a technique used in the nonproliferation literature where there are sophisticated global compliance and export control standards.⁶⁰ A rudimentary rating system also exists, constructed by human rights groups for encryption policy. There are conventions on human rights. It perhaps it goes without saying that there should be minimal levels of corruption within an export control regime--but must "corruption" be commonly defined or will a local definition suffice? Transparency International (TI) has developed a Corruption Perception Index which is based on a broadly defined notion of corruption. They use a general analytical framework aimed at constructing a "national integrity system."⁶¹ There are also transnational rating systems for credit liability which are based on comparative techniques establishing common standards and benchmarks. It is important to note that many of these "standardisations" are not derived from any particular state legal system.

The UK examples illustrate that legal due process values such as fairness, independence, openness, legality, timeliness, finality, proportionality, respect for personal privacy and human rights, and observance of sufficiency of evidence criteria can be used to assess the performance of an agency. Due process values are usually the product of common law systems but can also be found in different types of legal orders.⁶² They are easy to state and not always easy to observe.⁶³ But, once stated, they are a good benchmark for assessing any system. They add a normative content to what would otherwise be a rather sterile assessment exercise: seeing if an agency conforms to performance measures and standards based on results--only half the picture-- or out of principle. They also allow a wider evaluative base than that generated from the regulatory literature which is based merely on compliance costs and cost-benefit analyses. Due process norms reflect both normative (fairness) and instrumental (expertise) values which, taken together, would enhance the effectiveness of emergent export regimes and act as a useful check on the conduct of more established ones. ■

Note: For considerations of space, footnotes from the presentation have been omitted from The Monitor. Please,

contact us to obtain a full copy.

Terence Palfrey is a Professor at the Law School, Leeds Metropolitan University, UK.

CONTROLLING THE TRANSFER OF TECHNOLOGY BY INTANGIBLE MEANS IN UK

by Bridget Butt

The UK's principle export control powers date from 1939 and, as one might imagine, are out of date in a number of important respects. Current legislation gives government the power to control only physical exports, but plans are emerging for new legislation that would allow it, for the first time, to introduce controls on the transfer of technology by intangible means.

The UK review of national legislation on intangible transfers coincides with the European Community's review of its Dual-Use Goods Regulation. The EC will soon be introducing controls on the transfer of dual-use technology by electronic means. This article first examines the compatibility of the UK's national legislation and the EC Regulation and then addresses some of the continuing difficulties presented by intangible technology transfers legislation.

In July 1998, the UK published a White Paper on Strategic Export Controls which set out its proposals for new export control legislation¹. The White Paper included, first, a comprehensive list of offences involving illicit production of weapons of mass destruction (WMD). The UK already has legislation in place to punish those involved in illegal weapons-related activity, but at present these laws focus more on chemical weapons than on nuclear and biological weaponry. The White Paper brings legislation dealing with nuclear and biological weapons into line with that aimed at chemical weapons and strengthens laws against WMD manufacture and transfer more generally. Under this revised legislation, it will be an offence, punishable by life imprisonment, to develop, produce, use or possess WMD or to engage in military preparations purporting use of such weapons. It will also be an offence for a UK citizen or visitor to assist someone else in any of these activities.

More controversially, the Paper included a second provision establishing licensing requirements for the transfer of technology by intangible means. Current legislation provides the government only with powers to control tangible exports. The White Paper proposes legislation that grants the state power to control *all* transfers of technology, whatever the means. This new governmental power would allow for the introduction of the following secondary legislation specify-

ing the actual controls:

- All documents and software containing controlled technology are to be subject to export licensing requirements. This includes technology sent by fax, email, post or on computer disk.
- Technology transferred in non-documentary form, either orally, through personal demonstration, or the provision of technical services, is subject to control only if there is any reason to suspect that this information could assist in the development or production of WMD or ballistic or cruise missiles capable of ranges exceeding 300 km.

The controls the White Paper places on non-documentary transfers are more limited than those placed on written communications because licencing such transfers would be extremely difficult, if not impossible, requiring extensive use of limited enforcement resources and endangering rights of free speech.

Finally, the Paper would also make publication, in any form, of technological information relevant to the development of weapons of mass destruction illegal. This provision would prevent sensitive information from being placed on the World Wide Web where it could easily be accessed by proliferators.

Relationship Between National and European Controls

In 1998 the European Commission published a proposal for a revised Dual-Use Regulation which included an extension of the Regulation to intangible transfers of technology. After two years of discussion, the European Community is close to agreeing on a new Regulation which will introduce controls on the transfer of dual-use technology by electronic means, including email, fax and telephone. If passed as expected, this legislation will become effective in the next few months. It will, therefore, be in place earlier than the UK's own national legislation. The Regulation bears many similarities to the White Paper proposal with one major exception: the EC Regulation applies not only to transfers by fax or email, but also to those made by telephone. In response to this discrepancy, the British Department of Trade and Industry (DTI) has proposed inclusion of a parallel provision in its own legislation. If this provision is added, the responses of the UK and the EC to the threat of intangible transfer of technology will be aligned as they are already for transfers of tangible materials.

Public Reaction

The White Paper is a document crafted with extensive public input. Industry representatives, academics, non-governmental organisations and members of the public were solicited for their views on the subject. Not surprisingly, most were in favor of strengthening laws prohibiting involvement in production or use of WMD-related materials. However, the introduction of controls on the transfer of technology by

intangible means was an issue of great concern to both industry leaders and academics. Issues raised included:

- The position of multinational companies and those engaged in collaborations with other companies abroad.
- The effect of inevitable delays brought about by new licensing requirements on commerce. Obtaining a license for the electronic transmission of, for example, software, would be incredibly cumbersome and would interfere with the ability to do business.
- The problem of enforceability.
- The categorization of information and software available on the Internet. Would the new legislation apply to information presently considered to be in the public domain?
- The application of the law to publication of materials already available in other countries.
- The freedom of academics to communicate by electronic mail with counterparts abroad, for example, as part of an international research project.
- The position of universities recruiting foreign students in subjects potentially of proliferation concern.
- The problem of academic freedom and independence from government control.

Possible Solutions

The British government is confident that the concerns raised by members of the public in the consultation process can be addressed. Industry's concerns about international business partnerships and delays caused by licensing requirements could be resolved through the widespread use of open individual export licences (OIELS). These permits allow companies to export a specified range of goods to specific destinations and must be renewed every two years. Companies dealing in sensitive materials or information or doing business in sensitive locations, of course, would not be eligible for OIELS; they would be required to conform to the new comprehensive licensing requirements for transfer of materials and information.

It has been proposed that the concerns expressed by the academic community could be allayed a) by excluding information in the public domain from these controls and b) exempting academic institutions and university professors from the requirements. These options are now under consideration by the DTI which plans to present the revised White Paper to Parliament this winter. ■

*Note:*¹ For considerations of space, footnotes from the presentation have been omitted from The Monitor. Please, contact us to obtain a full copy.

Bridget Butt is a staff member of the Export Control Organisation of the UK Department of Trade and Industry.

U.S. CONTROLS ON TECHNOLOGY TRANSFER BY INTANGIBLE MEANS

by *Timothy Williams*

Introduction

Intangible technology transfer (ITT) is becoming an important proliferation concern in the export control community worldwide, and certainly within the multilateral nonproliferation regimes. However, there are varying interpretations of what is meant by the term "intangible technology transfer," which adds to a situation where there currently may be more questions than answers. While the threat of proliferation via ITT is real, very serious, and growing, each country may view the issue differently and take different paths to control either what is transferred, and/or the methods by which the transfer occurs. Controlling ITT is an area that needs an on-going exchange of ideas on how to define the scope of the problem, and how like-minded parties can work cooperatively on developing solutions to fit both national and international needs.

The United States considers ITT as divisible into two distinct areas, the transfer of technology by intangible means and the transfer of intangible technology. While these two areas may be closely related, they differ significantly. One way to envision the difference is to consider the transfer of intangible technology as "what" is transferred, and the transfer of technology by intangible means as "how" the transfer occurs. An example of intangible technology transfer would be "problem resolution" at a scientific conference where discussion and ideas were freely exchanged. One colleague contacts an acquaintance and requests assistance in working a solution to a particular problem concerning controlled aerospace technology. The problem may be discussed and worked over lunch or perhaps taken home and then resolved at a later date via phone. Such an exchange of data, while not written down or documented, constitutes an exchange of technology. This is an example of intangible technology (the solution to a specific problem) transferred by intangible means (telephone).

The first area, transferring controlled technology by intangible means, is an area in which the United States does have export controls in place to address most technology transfers. Some of the concerns in the United States regarding the second area, the transfer of intangible technology, are inherent in a variety of possible scenarios: scientific conferences and/or academic technical exchanges, foreigners' visits to domestic company facilities, domestic experts' visits to foreign facilities, and/or foreign nationals working for domestic companies.

The U.S. defines "technology" as specific information which is required for the "development," "production," or "use" of a product. "Technology" may take the form of "technical data" or "technical assistance," including manuals and

instructions which are written or recorded on other media or devices to include (but not limited to) disk, tape and read-only memory devices. Hence the United States feels that it is incumbent on our export regulations to cover the transfer of controlled technology (including "know how" and "know why"), be it in written or in more intangible electronic forms, except for technical data that is in the "public domain" (i.e. libraries, company brochures, and scientific papers released to the public).

Examples of Transfer of Technology by Intangible Means

One example of an in-country technology transfer would be a telephone conversation between two individuals who were working on a project in the United States. If one of the individuals is a foreign national and that person is verbally given information which is controlled under U.S. export laws, then a transfer has occurred which would be covered by the "deemed export" provisions of U.S. export regulations.

An example of an international transfer could be classified as problem resolution. It can be as simple as an engineer responding to a question sent in an e-mail from a foreign national who attended a technical conference. The foreign national explains what he is doing and that he has run into a problem. He is working on the filament winding of a large diameter pipe and can not achieve more than 50 percent of the predicted strength for the pipe. After some back and forth discussion, the U.S. national determines the problem is in the winding pattern and provides a solution suggesting a new winding pattern and a different resin, based on his past experience and knowledge of the system. In determining if there has been an export violation, the deciding factor would be if controlled technology was transferred which would have required an export license to the foreign engineer's country. In this case the technology which was transferred would be considered controlled, and an export license should have been requested before any detailed discussions of the solution to the problem occurred.

Another example of an international electronic transfer of technology would be a situation where a U.S. individual receives a license for the installation of a piece of equipment. While the equipment is being installed, the customer requests information about the equipment and how to operate it. Technical information is normally provided to a customer under the routine exchange of form, fit and function specifications, so that the foreign customers can properly operate the exported equipment. However, in this case the customer requests additional information on the operation of the equipment, which is beyond the scope of the export license. To better aid the foreign customer, the U.S. equipment installer requests additional information be faxed or e-mailed to the customer on how to enhance their operation of the equipment and provides examples of production techniques which are not released with the purchase of a machine.

If the additional requested information is beyond routine form, fit, function technical data, it would require a technology export license.

Transfer of Technology by Intangible Means

In today's electronic world, transferring controlled technology through intangible means, such as the Internet, fax, telephone, or e-mail is a growing area of concern. Twenty years or even ten years ago no one realized the scope or impact the computer and the Internet would have on global communication. The ability to almost instantaneously transfer data, files or other information to any location in the world has resulted in tremendous communication benefits, as well as some serious problems. In many ways, more damage can be done using intangible technology transfer methods than by conventional means of written communication since a computer's main disk can hold billions of bits of information and fit into a briefcase, while the same amount of written material would fill several large boxes.

Intangible technology transfer is familiar to most technical experts and is a form of transfer people actually use on a routine basis, sending data or technology electronically via fax, telephone or email through the Internet. ITT would also include the transmission of data that has been recorded on electronic media such as CDs or computer disks. The United States does not differentiate between transfers of technology via hardcopy or by electronic means such as the Internet.

The Immigration and Naturalization Act gives the United States the legal authority to exclude foreign nationals who seek to enter the United States to engage in any activity that would violate or evade U.S. law controlling the export of goods, technology, or other sensitive information. The Arms Export Control Act governs the import and export of defense articles and services, including technical data transfers. The International Traffic in Arms Regulations establishes policies and procedures and contains the United States Munitions List, which identifies the defense articles, defense services, and related technical data controlled for export and temporary import. The Export Administration Act and the International Emergency Economic Powers Act govern the export of dual-use commodities, technology, and software on the Commerce Control List (CCL) contained in the Export Administration Regulations (EAR). Other export controls are contained in sanctions laws, presidential executive orders, the Foreign Assistance Act, and the Atomic Energy Act. In implementing these laws and regulations, the United States conducts a thorough review of the specific case to distinguish between legitimate transfers to benign end-uses and/or end-users and transfers that could contribute to WMD and missile proliferation.

Through the Export Administration Regulations (EAR), the United States controls the export of technology sent over the Internet and the same controls and rules governing any other technology export apply to Internet exchanges. Simi-

larly, an e-mail of controlled technology to a foreign destination or a foreign person is treated as an export just like technology exported via conventional methods. In essence, the United States controls the data or technology regardless of how it is stored or transferred.

Authorizing Entry to the United States to Access Advanced Technology

A foreign national might be able to obtain access to U.S. intangible technology in many ways, the range of scenarios including study at U.S. academic institutions, teaching, conducting research, participating in exchange programs, attending meetings or conferences, being temporarily trained, or employed.

The first opportunity to control whether a foreign national might be able to obtain access to such technology comes when that person applies for a visa to enter the United States. A foreign national's eligibility for a visa is determined by the U.S. consular services after a review of the applicant's background information and intended activities in the United States.

All visa applications are screened for known criminal activity and against an "alert list" of problematic persons. U.S. consular officers are instructed to consult Washington if the foreign applicant is suspected of any illegal technology transfer activities. Consular officers have been provided with a list of scientific and technical fields of technology transfer (including missile proliferation) concern called the Technology Alert List (TAL) for screening purposes. Consular officers give particular scrutiny to visa applicants proposing to engage in activities on the TAL if those applicants are nationals of countries listed in the "projects, regions, and countries of concern" lists that are part of the EAR. Visa applications can be denied if U.S. officials know, or have reasonable grounds to believe, that the foreign person seeks to enter the U.S. to engage solely, principally, or incidentally in any activity to violate or evade any U.S. law prohibiting the export of goods, technology, or sensitive information.

Despite rigorous U.S. screening procedures, the visa application process is not infallible and will not catch every potential proliferator. For example, foreign persons might be able to misrepresent information in their visa application to avoid having their applications referred for more detailed checks, and it is possible that so little is known about a foreign person that a check in Washington would not reveal his intentions to engage in illegal activity. It also is difficult to guard against foreign persons trying to evade the visa screening process by entering the United States on the basis of working in a benign institution and/or academic discipline (e.g., a small liberal arts college studying English literature), and then subsequently changing to a university and/or field of study of potential concern (e.g., a large polytechnical university studying astronautics).

Transfer controls after entry into the United States

The United States also has in place procedures for trying to restrict a foreign national's access to controlled intangible technology once that person enters the United States. Controlling access to sensitive technology through a licensing system is the best way to control the acquisition of knowledge. The ability to control the technology is lost when it is released to the foreign person who then leaves the country.

Technology includes technical data (e.g., diagrams, manuals, blueprints, etc.) and technical assistance (e.g., instruction, skills training, working knowledge, consulting services, etc.). Pursuant to U.S. laws and regulations implementing export controls, the transfers of controlled technology (which include release in the United States of technical data, or know-how, during plant visits, training courses, and certain other circumstances) are controlled by licenses. These technical data licenses are reviewed for the applicable foreign policy, nonproliferation, and national security concerns, and may be denied or approved with the same type of conditions or restrictions as an actual U.S. export to the foreign national's home country. The foreign national's access to sensitive technology is generally referred to as a "deemed export."

Once a foreign national has entered the United States, the ability to monitor or restrict that person's access to intangible technology diminishes. However, while the ability to control is reduced, it is not precluded altogether. Consistent with U.S. law, the export licensing process tries to ensure that students, businessmen, and others do not gain illegal access to intangible technology. The success of this effort depends heavily on close cooperation and coordination between governmental agencies, academic institutions, and industry. Given the free and open nature of our society, experience has shown that many academic institutions and commercial entities are often unaware of U.S. laws and regulations governing intangible technology transfers. Hence, currently one of our primary objectives is to better educate U.S. industry regarding their responsibilities by routine outreach seminars in Washington and around the country.

Controls on Electronic Transfers

Under U.S. export regulations, a transfer of software or technology constitutes an export when the actual shipment or transmission of an item is made outside of the United States, or is released to a foreign national in the United States. The United States also controls all electronic transmissions of non-public data that will be received abroad. It has been determined that any upload to public electronic bulletin boards, Internet file transfer protocol, or World Wide Web sites can be considered as having made the information available for access by a foreign national, and hence would be considered an export. As exports, these types of transfers would be subject to the same rules, review and prior approval process as more traditional exports and would require export licenses. Government agencies do seek to educate businesses,

individuals and universities through various programs and seminars to ensure that they know these types of transfers are controlled and require an export license.

Encryption software controls via Internet in EAR

The United States recognizes the scope of the risk posed by the Internet and other kinds of electronic transfers and is actively engaged in working to reduce the risk of illicit transfers of technology. The U.S. controls found in the EAR identify the export of encryption software to include:

(1) downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and world Wide Web sites) outside the U.S. (except Canada); or,

(2) making such software available for transfer outside the United States (except Canada), over wire, cable, radio, electromagnetic, photo optical photoelectric or other comparable communications facilities accessible to persons outside the United States (except Canada), including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites.

The person making the software available on the Internet must take adequate precautions to prevent an unauthorized transfer of encryption software. We have found this requirement to be effective in reducing the risk of illicit transfers of encryption.

Training Efforts

An active and ongoing training program is a key element in helping industry to understand and correctly implement export regulations. The Departments of Commerce and State hold annual national seminars open to all individuals interested in export licensing, as well as regional seminars throughout the year. These seminars cover a broad range of export topics including "deemed" exports, and other related changes to the regulations. In addition, U.S. government personnel routinely visit industry and host industry programs dedicated to explaining the regulations. Several types of seminars are designed to train company personnel on how to understand and use the export regulations, and to help train companies on how to implement an export management system. Special two-day licensing seminars are also held, with emphasis on specialized export licensing topics of interest to a particular company or a specific group of companies.

Scientific and Academic Constraints

Under U.S. laws and regulations, providing export-controlled data to a foreign national who is not a permanent resident alien (i.e., who does not have a "green card"), who is not an alien accorded political refugee status, or who is not an alien with asylum status, is "deemed" to be equivalent to physically exporting that data to his/her country of nationality. Therefore, a university would have to obtain an export license before transferring to a foreign student technology controlled

on the U.S. Munitions List or the Commerce Control List. It should be noted that, except in limited circumstances involving encryption controls, the United States does not regulate software, technical data, or technology that is in the public domain or is otherwise considered publicly available (e.g., printed books and materials).

The United States also has in place laws and regulations that make it illegal to provide a foreign person with export-controlled technology without an export license. This applies to academic institutions, as well as to foreign students. A college or university is required to inform the U.S. Immigration and Naturalization Service when foreign students change universities or fields of study from those for which their visas were granted. However, no prior government approval is required to change fields, and the reporting by academic institutions is inconsistent at best.

In addition, U.S. "catch-all" controls would require a university to obtain a license for the transfer to a foreign student from a listed country of missile proliferation concern of any goods, software, or technology (except information in the public domain or basic research) if the university knows it will be used in missile activities or is intended for an MTCR-class missile project in that country.

Technical Assistance and Industry Constraints

Controls on "non-documentary" transfers of technology, such as oral exchanges with employed or visiting foreign nationals, are more difficult to enforce. These types of technology transfers also fall under the "deemed export" regulation, which deals with foreign nationals working in U.S. companies, or participating in plant visits where any technology transferred to a foreign national in the U.S. would require a technology license in order to be exported to the foreign national's home country.

Intangible technology transfers have occurred via individuals traveling outside U.S. borders to speak at seminars, design and integrate systems, provide services and do consulting. One example: a country purchases vibration test equipment or a chemical vapor deposition furnace or other complex piece of equipment. The machine comes with the basic hardware set up, software to operate the equipment, and a handbook or manual on how to use the machine. However, if the company purchasing the machine needs additional help in overcoming a specific problem, then it might require information considered to be controlled technology. Since some technology is more a form of "art" than "science," not easily conveyed through manuals, the technology required to solve a problem or provide a solution to a company's question may not be written down, but only available through the company's experienced staff. Such intangible technology needs to be controlled at the same level as written text. In the United States there are several ongoing information programs run by the Departments of Commerce and State which seek to educate industry under U.S. law.

An export license is required before controlled technology or technical data is to be discussed with foreign persons during visits to factories, participation in technical training or research, business discussions, or during employment. All such export license requests are reviewed by an interagency group on a case-by-case basis. Finally, as in the case of academia, a company must have an export license to transfer to a national of a listed country of missile proliferation concern any goods, software, or technology (except information in the public domain or basic research) that the company knows will be used in missile activities or is intended for an MTCR-class missile project in that country.

While the problems of intangible technology transfers appear to be growing in this electronic and inter-connected world, export legislation joined with education appear to be the means for controlling intangible exports. "Catch all" controls and modern export regulations enable countries to control all exports destined for a "weapons of mass destruction" (WMD) or missile related end-user and provide a strong legal and regulatory basis that allow a country to deal with the challenges of an electronic global society.

Conclusions

While the problems of intangible technology transfers appear to be growing as the world becomes more electronically connected, updated export legislation and modernized regulations joined with education appear to be the most effective means for controlling ITT exports globally. The United States hopes all countries will soon recognize the risk inherent in the unregulated transfer of technology. The guiding purpose of all the control regimes is not to shut down the export of goods and services but to control the necessary exports and strengthen global nonproliferation efforts. Without control of the key element—technology—there is a major gap in our ability to prevent the spread of WMD and their missile delivery systems. Some general conclusions include:

- U.S. export control laws and "catch-all" controls are designed to allow the United States to restrict data and technology transfers of national security, foreign policy, and/or proliferation concern regardless of the method employed to transfer the data.

- The U.S. seeks to enhance control of technology transfer by making industry and educational institutions more aware of the security and proliferation threats inherent in intangible technology transfers, and by making them more aware of their responsibilities under U.S. law with regard to such transfers.

- Continued dialogue with like-minded countries may help provide more and better answers to some general ITT challenges facing all countries in the electronic information age.

- The U.S. will continue to work with other countries to share information on possible export violations and to seek from other countries any information they may have on possible export violations.

In implementing intangible technology transfer controls, the United States must continue to factor in U.S. constitutional protections. We should also keep in mind the need for continued improvement in our regulations and means of enforcement. Together, these steps will ensure that our export policies can deal with today's technology and the changes that will surely come with tomorrow's technology. ■

Timothy Williams is an expert at the U.S. Department of Commerce

CONTROLS ON INTANGIBLE TECHNOLOGY TRANSFER: GERMAN NATIONAL LEGISLATION

by *Andreas Kleine*

Introduction

The Federal Republic of Germany is one of the leading exporting nations of high technology goods in the world. These products and technologies are used in a range of industries, for example, the automotive, aeronautic and aerospace, nuclear, chemical, telecommunication and machine tool industries.

One of our fundamental interests is to make international trade as free as possible, because we believe that free trade contributes to peaceful world development. On the other hand, the export of critical goods and technology, which can be used for the development and production of weapons of mass destruction and their delivery systems, must be controlled. Therefore, Germany became a member of the different export control and non-proliferation regimes like the Zangger-Committee, the Nuclear Suppliers Group (NSG), the Missile Technology Control Regime (MTCR), the Australian Group and the Wassenaar Arrangement.

Of these regimes, Zangger-Committee and the NSG are political associations convened to control the proliferation of nuclear weapons as well as the goods and software used for general civil and military nuclear purposes and their associated equipment and technology.

Nuclear Export Controls

Nuclear export controls owe their origin to the Non Proliferation Treaty (NPT) Article III.2, and were initially restricted to equipment and materials only. Therefore, the 1974 Guidelines of the Zangger Committee (an NPT Exporters Committee which defined a list of plants, equipment, material usable for military or civil nuclear purposes) made no

mention of nuclear technology controls.

Nuclear export control and non-proliferation regimes have changed a lot during the last 26 years. In 1978 the NSG (Nuclear Suppliers Group) was founded. Its Guidelines focused mainly on equipment and materials and were very similar to the Guidelines of the Zangger Committee. These were published as INFCIRC/254, Part 1 (also known as Trigger List Guidelines). In 1992, members of the NSG agreed to the NSG Dual Use Arrangement which included comprehensive controls on the *technology associated with the development, production or use of the commodities on the control list*. The Dual Use Guidelines and Annex were published as INFCIRC/ 254, Part 2.

In 1993, NSG members noted that the treatment of technology in NSG Part 1 and Part 2 was different. In 1995, they agreed to harmonize technology controls between Part 1 and Part 2 of INFCIRC 254. The notes regarding technology control in both Part 1 and Part 2 of INFCIRC 254 state that "technology" directly associated with any item on the list will be subject to as great a degree of scrutiny and control as will the item itself, to the extent permitted by national legislation. Controls on "technology" transfer do not apply to information "in the public domain" or to "basic scientific research."

The reason for applying the same controls to technology as to any item on the control list itself is clear. Without the transfer of technology, neither industrial development (design of production plants, development of products or materials etc.) nor the development of weapons of mass destruction and their delivery systems is possible. Therefore, knowledge and technology are key elements, not only for the development of science, education and industry, but also for the development and production of military goods.

An example of what the term "technology" encompasses

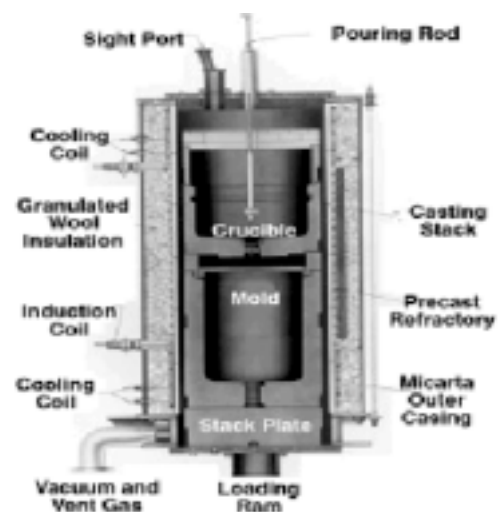


Figure 1: Schematic of a typical induction furnace as an example to explain the term *technology*

is shown in fig. 1.¹

Vacuum or controlled environment induction furnaces are used to heat or melt metal. Fig. 1 shows some of the key features of such induction melting furnaces. There are only a few manufacturers worldwide that produce such equipment.

Production or use of equipment for melting uranium or other nuclear relevant material, requires thorough knowledge, not only about development and technical design, but also about melting procedures and the metallurgy of the material being processed.

Before going into detail, some terms used in the Guidelines on technology controls must be defined:

1. "Technology" means specific information required for the "development", "production", or "use" of any item contained in the list. This information may take the form of "technical data" or "technical assistance."

2. "Basic scientific research" refers to experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena and observable facts, not primarily directed towards a specific practical aim or objective.

3. "In the public domain" refers to technology that has been made available without restrictions upon its further dissemination.

4. "Technical data" may take the form of blueprints, plan diagrams, models, formulae, engineering designs and specification, manuals and instructions written or recorded on other media or devices such as disk, tape or read-only memories.

Each significant term used in the Guidelines is defined, with one exception. The term "transfer" itself has not been defined.

Transfer of Technology

Technology transfer in the context of this paper means the movement of controlled information from one country to another. The controlled information can be either in tangible or intangible form. The differences between the transfer of information by tangible or intangible means are shown in Table 2 through some examples.

In this paper, "Intangible Technology Transfer" means "transfer of information by intangible means" such as fax, oral communication and technical assistance.

Within the last decade, the use of electronic media for data and information transfer in business, science and communication has increased dramatically. Organisations with hundreds of offices spread over a wide geographical area routinely expect to be able to examine the current status of production and profits at the push of a button. New terms like fax, mobile phone, Internet, e-mail, World Wide Web, etc. have become incorporated into most national languages.

The use of these new and sophisticated information technologies is not only of interest for information exchange in the areas of business, communication and science. This new

technology for information transfer has also become of great interest to governmental bodies especially as it pertains to national security and export control.

Through these new electronic communication techniques, technology directly associated with any item on the export control list can be easily moved from one country to another with high speeds, usually out of the reach of customs control.

Furthermore, in a globalized world economy, companies act as global players and universities and research organisations are in competition worldwide. Exchange of technical information, technical assistance, and technical experts (scientists, students, engineers and technicians) across national borders has become necessary in order to keep abreast of technological developments elsewhere and stay at the frontline in research activities. Thus, transmission of information as quickly as possible, using phones, emails and faxes, has become a priority for academic and industrial enterprises..

Therefore, export control regimes are confronted not only with the problem of transfer of controlled technology by electronic mail but also by personal contact. These transfers may involve:

- technical assistance by engineers or technicians (e.g. to install or repair machines in nuclear plants),
- scientific exchanges between persons of one country with persons of another,
- foreign students who are studying in critical fields of science and technology .

All these transfers of (controlled) information can be done either by tangible (e.g., papers about research results) or intangible (e.g., scientific presentations) means. In the following pages, I present a survey about government legislation in Germany regarding the control of technology transfer either by tangible and intangible means.

German Legislation on the Control of Technology Transfer

The German Foreign Trade Law (AWG) is based on free foreign trade but the state also reserves the right to impose restrictions. Thus every export transaction is allowed unless not expressly prohibited or subject to approval. These principles underlie the free trade orientated policy of the Federal Republic of Germany.

According to Section 7 of the AWG, foreign legal transactions and dealings can be restricted

1. to guarantee the security of the Federal Republic of Germany,
2. to prevent disturbance of peaceful coexistence among nations, or
3. to prevent a major disruption in the foreign relations of the Federal Republic of Germany.

In a practical sense, the contents and licensing requirements pursuant to Section 7 of the AWG are essentially re-

Table 1: Examples for the terms Development, Production, Technical Assistance and Use that are used in the Guidelines

DEVELOPMENT	PRODUCTION	TECHNICAL ASSISTANCE	USE
Design	Construction	Instruction	Operation
Design Research	Production Engineering	Skills	Installation
Design Analysis	Manufacture	Training	Maintenance
Design Concepts	Integration	Consulting Services	Repair
Assembly and testing of prototypes	Inspection	Working knowledge	Overhaul
Design data	Quality Assurance		
Process of Transforming design data into a product	Testing schemes		
Configuration and integration design; layouts			
Pilot production			

quirements within the framework of international agreements like the Wassenaar Arrangement, the Missile Technology Control Regime, the Nuclear Suppliers Group and the Australian Group. In addition, national controls have been introduced to reduce the risk of proliferation of critical technologies.

The restrictions on the export of goods and technology are defined in the German Foreign Trade Regulation (AWV). Sections 4 b, 5 and 45 are especially important. The Export list (AL) is an Annex to the AWV and lists goods (movable objects and software) and technology subject to the provisions of section 5 AWV.

As mentioned above, export licences are required not only for goods but also for technology related to goods contained in the export list (AL). However, the export list controls production documents, physical models, production data etc. only if these documents and models will be exported in physical or tangible form (as movable objects).

The German government recognized a decade ago that the transfer of *controlled* technology (not only the technology listed in the NSG Guidelines) and the transfer of *not controlled* critical technology by tangible and intangible means posed a potentially serious proliferation risk. Therefore, the national export control legislation was extended by introducing new sections into the AWV.

In 1991, Section 5 c was introduced. It is an example of nationally-based “catch all” regulations for non-listed goods and technology. It is worth noting that in this provision the term technology is limited to documents (construction blueprints, models, formulas etc.) only. According to this regulation, production documents for goods not listed in the Ex-

port list require an export licence if they are

- intended for the use in construction or operation of a plant used exclusively or partially for manufacturing, modernizing or maintaining goods, ammunition or armaments as defined in part I, section A of the AL,

- if the consignee or purchaser of the technology is established in a country mentioned in country list K, and

- if the exporter knows that the exported technology is intended for armaments in country list K.

Another “catch all” regulation is Section 5 d of the AWV, which came into effect in 1992. It refers not only to technology (in the same manner as in Section 5 c), but also to a special group of goods and documents which are intended for nuclear purposes only. According to this regulation, an export licence is also required for goods and production documents (technology) not listed in the Export list if

- they are intended for use in constructing or operating a plant serving nuclear purposes or for installation in such a plant,

- the consignee or purchaser of the technology is established in a country mentioned on country list K, and

- the exporter knows that the exported technology is intended for nuclear applications in one of the countries listed in country list K.

In addition, the exporter has to conform to “catch all” clauses under EU law. Article 4 EC-Regulation (the so-called EC Dual Use Regulation) controls technology such as production documents, physical models, production data, etc. only if these documents will be exported in physical or tangible form. It contains an authorization requirement for exports from the European Community concerning items not listed in Annex I of the EC-Regulation. This is required when the exporter has been informed by competent authorities that the items in question (including technology) are or maybe intended for use in connection with the production or proliferation of weapons of mass destruction (chemical, biological or nuclear weapons and missiles capable of delivering such weapons). Accordingly, the exporter must notify the authorities if he is aware that the dual-use items (not listed in Annex I) which he proposes to export are intended for any of the uses referred to Article 4 EC Regulation.

It must be noted that section 5 AWV and Article 4 EC-regulation define the control of technology in its tangible form only. Therefore section 4 b was introduced into the AWV which covers the control of technology in its intangible form.

Control on Intangible Technology Transfer

Introduction of section 4 b AWV represents the most important development in the export control legislation regard-

ing the intangible transfer of information or technology. It states that transfer of technology by intangible means, like fax or e-mail, is equivalent to the transfer by tangible or physical means. The tangible or intangible transfer of documents about technology or software requires a licence from the authorities. The intangible forms mentioned in this section also include the oral transfer of information (e.g. by telephone). The control applies to all countries on the basis of the erga omnes principle.

Section 4 b and Section 5 AWV, therefore, make it possible to control the tangible or intangible transfer of listed and (critical) non-listed technology.

Transfer Of Know-How And Technical Services

As mentioned earlier, the non-documentary (intangible) transfer of information by individuals must be taken into account when we discuss export control. Such transfers include

- conversation between persons (either personal or by telephone)
- movement of persons from one country into another (industrialists, consultants and academics)

To control the transfer of know-how and technical services, section 45 was introduced into the AWV. Licences are required (section 45 AWV) for the transfer of know-how not publicly available. This includes

- technologies, technical data, and technical methods expressly itemised in the export list, or
- knowledge pertaining to the development, production or use of nuclear, biological or chemical weapons of mass destruction or their delivery systems.

The form and location of the transfer are not important in the licencing provisions. "Transfer" in the form of passive agreement (e.g. allowing a party to access to a computer in which relevant data are stored) is also covered by these provisions. Transfer of knowledge derived from publications and lectures does not require a licence unless it is transferred

to specific relevant recipients. However, the transfer of such knowledge within the framework of scientific cooperation does require an export licence.

A special information leaflet was published to inform scientific and research institutions about this new section of the legislation.. Except in a fairly small number of cases, we do not expect any conflicts with the principle of freedom of science, research and teaching at universities and research institutes.

Section 45 b was introduced in 1991 to control the export of **technical services**. This regulation refers to services related to

- military goods,
- nuclear, biological and chemical weapons or missiles capable of delivering these weapons, and
- conclusion of contracts and any service connected with the construction and operation of nuclear plants.

Licences are required if the services are performed by residents (regardless of their nationality) or non-resident Germans and in all non-OECD countries. Section 45 b was later extended by introducing regulations on technical services in relation with missiles, regardless of the country in which the service is rendered.

Technical services encompassed by this regulation are any activities in connection with the development, production, assembly testing, maintenance and application of military goods, nuclear, biological and chemical weapons, missiles, and plants for nuclear purposes. "Activities" in this context refers not only to tangible activities but also to the verbal transfer of (controlled) know-how. It is of no relevance whether the services relate to defence goods directly or indirectly since dual use items are potentially subject to military applications.

Controllability

Customs authorities are important actors for enforcement of export control regulations on tangibles because they can physically stop goods from leaving the country. However, information that is transferred by intangible means is not easily controlled. Therefore, we think that specialized legislation aimed at control of intangibles is necessary.

Certain questions have to be taken into account:

- What is the aim of export control in general? For example, is the export of listed software via the Internet less sensitive than by CD-ROM? As mentioned above, such transfers are difficult to control. Is that sufficient reason not to regulate such transfers?

- Should practicability be the only criterion for having controls? For example, certain tangible technologies like small electronic devices can be used for nuclear bombs, but cannot be detected by customs control. Should these also be deleted from the export lists because they are not controllable?

Technology	Methods of Transfer	
	Physical or Tangible Form	Non-physical or Intangible Form
Technical information for development and production	Blueprints	Electronic mail
Technical Assistance	Information stored on a computer disc	Fax
Use technology	Technical instructions	Demonstration
		Telephone
		Speech; Teaching

- What kind of political signal we are giving to the world if we fail to pass legislation on intangible technology transfer?

- What is the difference between delivery of controlled information to a critical customer or a country by tangible and intangible means?

Clearly, it is necessary to subject all forms of technology transfers to legislation, whatever the practical and political difficulties. Failure to do so makes existing export control regulations vulnerable. For instance, exporters should not have the ability to undercut national export controls simply by selecting alternative and uncontrolled means of the transfer.

Conclusion

Countries of concern involved in the development of nuclear weapon systems not only need goods to implement their projects, but also the necessary technology, know-how and technical assistance to advance these projects. Export controls on the tangible transfer of technology have currently become obsolete due to technical developments in the field of electronic communication systems, i.e. computer networks, Internet, email, etc. These developments mean that the intangible transfer of technology and the transfer of information and know-how must be subject to export controls.

Therefore Germany has implemented legislation to control the intangible transfer of technology. It covers the transfer of controlled information and know-how, technical services and assistance through electronic means and through personal contact or telephone communications.

In order to maximize the effectiveness of export control legislation and prevent the development of weapons of mass destruction in sensitive countries, Germany has extended its legislation to intangible transfers of technology. ■

Notes:

¹ U.S. Department of Energy, Office of Arms Control and Nonproliferation

Andreas Kleine is an official in the International Export Control Regime Division of the Federal Ministry of Economics and Technology in Germany.

GLOBALIZATION AND CONTROL OF INTANGIBLE TECHNOLOGY TRANSFERS: A MAJOR CHALLENGE TO EXPORT CONTROLS IN THE 21ST CENTURY

CITS Working Paper presented at the Conference in Moscow, May 2000

The profound changes of the last ten years, particularly the widespread integration of people, markets, and ideas through globalization, have precipitated several major challenges to international export control efforts. The electronic revolution has provided industry with a whole new set of tools for research and development, product design, and production control. The storage and transmission of electronic technical data by electronic means is rapidly replacing more traditional methods.

The rapid pace of global integration has made it easier to exchange goods and information through "intangible" networks that are not easily controlled. Companies that finance, design, and produce technologies increasingly do so through global financial, informational, and production networks that cannot be easily regulated.

The wide availability of inexpensive computers and communication devices has increased the potential flow of intangible transfers, the control of which poses the most serious challenge in the legal and regulatory area of export controls.

A recent case highlights the importance of the problem and the difficulties associated with it. According to an article in *Defense News*, a Loral employee sent results of the company's review of the investigation into the 1996 Long March Rocket failure to Chinese authorities by fax without permission. The company received a fine and claimed that the employee did not know that fax transmission was considered an export.

The inadequacy of existing regulations for controlling intangible technology transfers is becoming increasingly apparent, presenting export control and nonproliferation experts with a challenge that will likely persist well into the 21st century.

What is Intangible Technology Transfer?

Although there was a great deal of emphasis on controlling WMD *material* after the Cold War, the acquisition efforts of proliferators were concentrated on obtaining *technology and knowledge*. Even substantial amounts of plutonium are useless without the knowledge of how to use it. The terms with which the issues of intangible technology transfers are framed as follows:

Technology includes specific information required for the development, production, or use of product, including:

Technical data refers to blueprints, plans, diagrams, models, formulae, tables, engineering design and specifications, written or recorded manuals and instructions, or any other media or devices, such as disks, tapes, and read-only memo-

ries.

Technical assistance includes instruction, skills, training, working knowledge, and consulting services. Technical assistance may involve the transfer of technical data.

Intangible technology transfer (ITT) is a transfer by intangible means. This includes:

- scientific meetings, discussions, exchanges, presentations, visual inspections, consulting, demonstrations, technical assistance, lectures and seminars, teaching, training, education of foreign nationals, etc.
- communication by electronic means, such as e-mail, fax, telephone, Internet, publications, etc.

There is no clear definition of intangible technology transfer, and neither is there a consensus as to how it differs from the transfer of intangible technology, but there is an ongoing debate on this issue. However, it is most commonly understood that “intangible technology transfer” refers to *how* the transfer occurs, the means of transfer, while the “transfer of intangible technology” refers to *what* is transferred (technical solutions to problems, expertise of scientists, etc.).

It matters little how it is defined; the point is that technology as a means or end of transmission must be controlled. For the purpose of this article, both definitions will be referred to as intangible technology transfer (ITT).

With the ease afforded by communication technologies, countries seeking sensitive information for WMD programs can now use the Internet and other channels to obtain sensitive design information. ITT can take place in two ways:

1. In the home country, through personal communication with foreign nationals directly or indirectly (via fax, e-mail, or telephone) and through educational forums (courses, presentations of scientific research, consulting sessions, demonstrations and exhibitions, etc.) or
2. abroad, e.g., while on a visit or work assignment.

A broad interpretation of “technology” makes it possible to include intangible technology transfers in the group of controlled items. The Nuclear Suppliers Group (NSG), the Wassenaar Arrangements (WA), and the Missile Technology Control Regime (MTCR) all require control over technology used for the development, production, or use of any item controlled, tangible or intangible. Some countries (like the U.S.) mention technology in the legislation, and ITT is implicitly encompassed by the term. Other countries (like the UK) do not include ITT on the list of controlled items.

At its 1998 Plenary Meeting at Edinburgh, the NSG conducted a survey of its members. Of the twenty-three responding members, only five had legislation specifically applicable to intangible nuclear technology transfers; several more were involved in proposals for the introduction of such legislation. Eleven of the responding governments had controls in place on the human types of intangible technology transfers (i.e., the activities of students, scientists, and technicians, with visa controls the favored sort). Of the eleven, five had a jurisdiction defined by a variant of territoriality in conjunction

with nationality, four were concerned with transfers from nationals to foreigners, and three were to be applied on a case-by-case basis. Nine of twenty-three respondents described regular educational and awareness-raising programs, seven noted irregular or on-demand public information dissemination, and seven reported no such activity at present. There was general agreement that for the firms, individuals and educational and research establishments capable of exporting nuclear technology, an approach that co-opted their own interest in nonproliferation was a sensible precaution. Only two of the respondents reported legal action taken in response to alleged breaches of controls on ITT.

There is a need for clarity and consensus regarding the appropriate laws, enforcement measures, and technical tools that should apply to the transmission of intangibles, particularly the export of technology-embedded information or documentation. Various combinations have been proposed but all have potential difficulties.

Why are They a Problem to Control? Challenges Posed by Intangible Transfers

There are three major aspects of the ITT problem: sociopolitical, legal, and technical. Intangible technology transfers are among the most difficult transfers to control. The problem begins with questions of what to control, how to control it, and how to find the balance between openness and security. Members of the academic, industrial and scientific community have been vocal in their concern that restrictions on communications and trade will abridge freedom.

The first and most perplexing set of questions deals with ethical and legal considerations and constitutional rights. It is very difficult to strike a proper balance between academic freedom, freedom of speech, rights of privacy, and security concerns in controlling intangible technologies. Does a democratic country have the right to restrict the communications of its citizens, listen to telephone conversations, and penetrate e-mail correspondence?

The second major challenge is logistical, having to do with finding practicable ways of controlling intangible technology transfers. It is nearly impossible to detect intangible technology transfers. Control depends largely upon the voluntary cooperation of technology producers and users. The licensing of intangible transfers is burdensome both for applicants and the licensing authority.

The following questions challenge both policy formulation and implementation of intangibles control:

How old must the technology or information be for its transfer not to pose a threat to security? Technologies and information often emerge and become obsolete rapidly. On the other hand, recent findings in the U.S. DOE archives (after the recent security breach at Los Alamos) indicated that out of 948,000 pages of declassified information, 14,890 pages included sensitive and restricted information. Finding a “magic number” is problematic.

The same dilemma arises regarding people who possess sensitive information. For how long should they be under surveillance? When does their knowledge become obsolete? In Russia, people holding sensitive jobs are monitored and subject to restrictions on foreign travel for five years after they leave their position. Is this a reasonable precaution? Too stringent? Too lenient?

Technology in the “public domain” or categorized as “basic scientific research” is excluded from the definition of technology subject to control within regimes. How is public domain defined? Is the Internet considered public domain? Some information, considered classified in one country, is published in open sources in another. And how should it be decided what types of fundamental research are subject to control? What does “basic” mean? Fundamental training in nuclear physics has the potential for dual-usage. Aspects of basic physics, say, understanding turbulence in aerodynamics, are essential knowledge for building a missile. In many areas, basic research and sensitive weapons research overlap. Experts sometimes publish articles as basic research when these articles are in fact more advanced (sometimes authors are genuinely unsure about how to categorize their work; other times articles are intentionally mislabeled to avoid licensing paperwork). Although it seems upon reading the legislation that public domain and fundamental research are defined fairly clearly in U.S. law, and although specific definitions appear in Export Administration Regulations, loopholes remain. Legislators are confronted with the question of what reasonable restrictions would be for education in sciences with potential for use in the production of WMD.

In the U.S., fifty-two percent of masters and doctoral students in technical and engineering science are foreigners, mainly from China and India. Should these students be prohibited from taking classes? In Russia, foreign students are a major source of funding for poor universities. If foreign students are barred from studying legally at Russian technical universities, the danger is that Russian professors, strapped for cash and presented with eager and well-funded pupils, will take them on as private students resulting in undetectable and uncontrollable brain-drain.

The major problem, however, is not with students or teachers, but with employees or partners of companies in the U.S. or abroad that deal in sensitive knowledge outside of the public domain or classified as applied research. The ubiquitous presence of dual-use technologies in the private sector, dependent on exports for its profits and opposed to government interference, is a source of great concern for export control experts. In Russia the percentage of dual-use technologies owned by the private sector is 51 percent. In the U.S. and other Western states, the percentage is much higher.

The problem is international in scale, impossible to address simply through national legislation and controls. In this age of interdependence and globalization, we speak about international security, international business, and international

trade. It has become evident that legislation and controls need to be standardized in all countries. The problem with national differences in export control laws is felt most profoundly by companies with international contracts or engaged in joint projects. In a high-tech industry, it is very unlikely that a product is produced, from start to finish, within a single country. Increased international cooperation means that, by the time a product is completely assembled, its components may have come from more than a dozen factories in as many nations. U.S. industry complains that strict export control regulations make it impossible to compete in the world market, and that as a result it loses billions of dollars a year. There are similar complaints from industry all over the world.

Another problem is maintaining security in the commercial sector. Controls are largely viewed as barriers to free trade, causing endless paperwork and costing time and money. Companies often are punished for violations they do not understand and it is expected that breaches in security extend far beyond the number detected and punished. Industry already is fairly successful in finding ways around security requirements in exporting tangible items; cheating is much easier in the case of intangible transfers. Differences in export control regulations among nations become a strategic point in competing with other companies: locating facilities in countries with less stringent export controls on both tangibles and intangibles can only be an advantage.

It is an oft made point in both industry and government sectors that export controls should be reformed to meet the requirements of a new global reality. International trade, especially multinational ventures, suffer from the rigid requirements of international export regulations. On the other hand, threats to international security and proliferation are as great now as they were during the Cold War. Finding a balance between the interests of business and security is no easy task.

How Intangible Technologies Are Controlled in Different Countries

Different countries take different approaches to the control of ITT (see table). Several countries control transfers of IT on the national level. Most control data or technology regardless of how it is stored or transferred. Although no system is perfect, there has been some success. In the U.S., several agencies are involved in control of ITT: the Departments of State, Energy, and Commerce, along with enforcement agencies and immigration services. The U.S. regulates exports of any sensitive technology, tangible and intangible, through several laws; technology transferred through the Internet or fax is subject to the same controls and licensing requirements as any other export, as are telephone conversations when sensitive information might be transferred. “Export” is understood to mean any transfer of technology and data to outside the U.S. or to foreign nationals within the U.S.

According to ITAR 125.2 (c) article, “a license is required for oral, visual, or documentary disclosure of technical data

Table 1: Government Positions on Intangible Technologies Transfers (ITT) ³

Country	Is ITT under Control?	Issue of Concern	Discussion Held in the Framework	Governmental Position
Argentina			MTCR	Control over ITT should be perfected
Australia	No		WA	The issue is discussed. However, success depends on convincing skeptics about the possibility of adequate control and enforcement
Austria			NSG	Internet exchange should not be controlled. Waiting for progress in the EU. Technical support to the IAEA should be limited
Belgium			NSG	Concern on "jurisdiction borders"
Bulgaria	Yes		WA	
Canada	No	Internet, e-mail, information on conferences and in the process of education and training in the institutes	NSG, MTCR	Skeptical that control could be undertaken without violation of constitutional rights. Legislative issues are closely tied with technical ones. Study issues of regulation and enforcement
Czech Republic	Under catch-all		NSG, MTCR, WA	Currently is under catch-all, but is interested in more effective restrictions
Finland	Yes	Export of services, including e-mail and internet	NSG, WA	Strong interagency coordination is necessary
Germany	Yes	People, oral discussions, lectures, computers with confidential information and internet, permission to use files, notes or reports. May occur in Germany or elsewhere.	MTCR, NSG, EC, WA	Licensing requirements are for all forms of transfers. Prefers better control over ITT within the framework of MTCR. Control and enforcement is difficult. A number of agencies work on taxation and export control to cross-check violations. Germany proposed that a statement on mutual understanding on ITT control be added to the WA Military Items List
Hungary	Yes	E-mail, phone	MTCR	Technology should be controlled independent of means of transfer
Ireland	No			Under revision. In the context of EU, considers control over scientific transfers unconstitutional
Italy	No. According to EU rules, catch-all is used when possible	Internet, personal contacts (scientific exchanges, graduate studies)	MTCR, NSG, WA	Legislation is necessary to control ITT independent of the mean of transfer. Suggest ITT control in the framework of the EU. Consider cooperation between states and regimes as very important. It is easier to control ITT for development and production of WMD.
Japan	Yes		MTCR, NSG, WA	Technology is to be controlled independently of the means of transfer. Technology is defined as information required for design, production or use of goods in the form of technical data or technical assistance. Enforcement is required.
Luxembourg		Phone, fax, internet		The issue is in being discussed, but does not include such ITT as technical service
Netherlands	No		NSG, MTCR	There is no essential control on nuclear ITT, or enforcement. Adequate control over technical assistance in development and production. Suggests discussion within the EU framework.
New Zealand	No			Examine disposal issues
Norway			NSG, WA	Relations between government and the industry are very important.
Portugal	No		WA	
Russia	Yes	Computer disks, people, internet	MTCR, NSG	Harder to control. Necessary to work out general understanding. Few details.

Spain	Yes	Citizens visiting other countries, internet. ITT is under catch-all clause according to the EU rules	NSG	Hard to control and enforce
Sweden	Yes		MTCR, WA, NSG	Technology transfers should be controlled whether tangible or intangible. Critical issue is containment of missile technology. Freedom of speech is a problem. Difficult to catch violators.
Switzerland	Yes	Mostly control over visas and university education	MTCR, WA	Sensitive technology and not the means of transfer is controlled. Sometimes violations of ITT are persecuted. Issue of the threshold between the controlled and public information most important.
UK	No	Fax, e-mail	MTCR, NSG, WA	At the end of 1998 strategic export control was extended to include ITT. Issues of academic contacts and censorship have to be discussed. EU control has to be in progress. New legislation is expected in 2000-2001.
Ukraine			NSG	Hard to control because of lack of transparency
US	Yes	People, internet, discussions, fax, phone, technical data, technical assistance, training/education	Bilateral agreements, NSG	Legislation is based on the Law on Immigration and Naturalization, Atomic Energy Law, Nuclear Nonproliferation Law, and Export Administrative Regulation Act. Violations are punished equally both by tangible and intangible means. The problem is balancing freedom of speech and proliferation issues. In the context of nuclear technology control, technical assistance and technical data does include ITT. Also see Export Administrative Regulations Act. Section 743. Amendment No 1. Department of Commerce
<i>Note: EC – European Council, MTCR – Missile Technology Control Regime, NSG – Nuclear Suppliers Group, WA – Wassenaar Arrangement</i>				

by U.S. person to foreign persons.” The U.S. tries to control the entry of foreign individuals to the U.S. and restricts their access to sensitive areas through screening applications, background checks, and document checks. The methods of obtaining information include observation, interviews, audits, surveillance, and technical analysis. In the event of suspicion, visits to the company-sponsor are made to ensure that the foreign expert is indeed invited for legitimate purposes.

There is a special encryption law controlling software transfers and exports. In accordance with EAR, the distributors of encryption are required to adhere to special security measures. US companies must investigate inquiries and requests for encryption outside the U.S. and Canada.

Controlling electronic correspondence is very problematic because the same technologies are used in both the civilian and the military sectors and even experts may not be aware of the end-use of their expertise (deemed export). This is why outreach, education, and training are so important. U.S. outreach efforts include publication of special manuals and question-answer sessions held at the Bureau of Export Administration (BXA), in which exporters are trained in procedures and licensing requirements for ITT.

Many countries (particularly the U.S., Japan, Germany, Italy, and Russia) have their own ways of detecting violators of the information space, and it is in their interest to share this information. For example, the U.S. Department of Commerce has about 100 specially trained inspectors for computer crimes investigations; eight of these have advanced training in the recovery of computer evidence. These experts keep abreast of new developments in the field, monitor websites dealing with sensitive issues and track the transit of encryp-

tion within companies. They also are trained to serve as witnesses in court.

Reports presented at the 1999 Munich conference on export control in missile technology indicate that similar measures are being considered or implemented by Germany, Japan, China, and Hungary, among others.

After the recent security breach at Los Alamos and subsequent investigations, a DOE Action Plan has been prepared and implemented to tighten security in DOE facilities (laboratories). For instance, access to computers with sensitive information is now more tightly controlled; these computers no longer afford an opportunity to copy information to a floppy disk or send e-mail; access of foreigners to DOE facilities is highly restricted. Scientists with clearance to visit foreign states require special licenses and their presentations are reviewed for secret information; DOE has also implemented stricter requirements for reporting interactions with foreign individuals from sensitive countries, including email correspondence; laboratory directors are responsible for scrutinizing foreign visitors, in coordination with the DOE Counterintelligence Office. DOE is also requiring counterintelligence polygraphs for those who work in special access programs (SAP) and sensitive areas who have knowledge of nuclear weapons design or have hands-on access to nuclear weapons (about ten percent of the total cleared population within the Department of Energy). Such persons must undergo financial reviews and newly rigorous background investigations conducted by local field offices of the FBI. The DOE plans to create an audit trail to track unclassified computer use and protect classified computer networks; the action plan also calls for the creation of counterintelligence

Table 2: Effectiveness of Selected Forms of Technology Transfers⁴

Forms of Technology Transfers	Effectiveness	Areas of Cooperation			
		Devices	Semiconductors	Jet Engine	Plane Fuselages
Joint ventures Turn-key facilities Licenses with broad technical assistance and expert training	High	High High High	High High High	High High High	High High High
Exchange of technical results on the basis of existing contract Probation Technological equipment (with know-how)	High	High High Medium-high	High High High	High High Medium	High High Medium
Design documentation with technical data Technical consultations Licenses (with know-how)	Medium	Medium Medium Medium	Medium High Medium-high	Medium-high Medium-high Medium	Medium-high Medium-high Medium
Commercial offers (with technical documentation) Technological equipment (without know-how) Commercial visits (companies, plants, institutes, etc.)	Moderate	Small Small Small	Small Medium-high Medium-high	Medium Small Small	Medium Small Small
Licenses (without know-how) Items sale (without technical assistance and technical data) Commercial offers (without technical documents) Technical literature Trade and industry exhibitions	Small	Small Small Small Small Small	Small Small Small Small Small	Small Small Small Small Small	Small Small Small Small Small

training programs and a counterintelligence analysis program.

The EU currently controls only physical transfers but is working on plans to include control of oral transfers and electronic communications. The UK is planning to introduce legislation expanding government control of exports to ITT. Although Russia’s national export legislation applies to intangible as well as tangible technologies and transfers, it also has recently created special legislation aimed at controlling ITT.

What Should Be Done? Recommendations

New means of ITT require new and common solutions in export control legislation in order to allow the same level of

control already in place for transfers of technology in tangible forms. Transfers of technology by electronic means should be treated in the same way as transfers in tangible form.

Although currently there is no completely effective solution to the problem of controlling intangible technology transfers, there is widespread agreement that form of transfer does not alter the necessity of control and that all nations should coordinate their efforts toward this end.

Several elements emerge as crucial to ITT control:

1. Public outreach and industry information. Sometimes violations occur due to a lack of knowledge or understanding of the consequences of transfer. There should be appropriate education and training.

- Control of ITT should be reasonable, and the bureaucratic procedure should be made as user-friendly as possible to encourage companies to report transfers--simple, transparent, and expedient.

- There should be system of incentives, of “sticks and carrots”, for industry regarding ITT, just as there is for export of tangibles. Those who comply with the rules would receive some benefits (like reduced time for license application); those who do not comply or are under suspicion should be monitored and subject to trade restrictions.

2. Effective national legislation including licensing of ITT. ITT control should be included in the export legislation of all countries. Violations should be penalized.

3. International cooperation among governments, experts, intelligence communities, and NGOs. Information about violations, suspected violations, solutions to technical problems, innovations and successful experiences in controlling ITT should be shared.

- Enforcement procedures should be established.

- Streamlining of norms and procedures across countries to prevent competitive market advantage for violators and countries with lax controls.

4. Effective training for investigators

5. Improvement of techniques

- Adapting Internet control techniques used in other areas (e.g. pornography, commercial information) for use in ITT control to strengthen nonproliferation regimes.

- Creation of a computerized database of sensitive foreign individuals in the country and a tracking system to follow migrations of graduate students, foreign experts, etc.

- Creation of a computerized database of individuals leaving the country.

- Development of a system to audit compliance with regulations on intangible technologies transfers (electronic communications). This will make non-compliance costly and risky.

6. And above all, there should be a balance between the openness of a democratic society and the requirements of security. ■

MPC&A

EQUIPMENT ASSESSMENT PROJECT FOR MPC&A COOPERATION WITH RUSSIA

by Daniel Miller; Kara DeCastro, Ron Melton, Yves Dardenne, Charles Ringler, Kathleen McCann

Introduction

The Equipment Assessment Project is a key element of the Program-Wide Sustainability Initiative. The Program-Wide Sustainability (PWS) initiative has been created within the National Programs Division of the Office of International Material Protection and Emergency Cooperation. The primary objectives of PWS are to ensure that upgraded Material Protection, Control and Accounting (MPC&A) systems installed in Russia will operate as intended long into the future and to implement sustainability in a standardized and consistent manner.

Sustainability is the process of ensuring the protection of material for the long-term and promoting Russian ownership of the MPC&A process. Sustainability is a complex concept as it applies to the MPC&A Program especially when trying to foster Russian acceptance and ownership of the MPC&A process. It is not merely the life cycle support for MPC&A systems. Sustainability represents the compilation of the concepts of logistics engineering and maintenance management for a system, the cultural assimilation of MPC&A practices by the Russian nuclear community, and Russian Government support for MPC&A. Additionally, long-term sustainability involves development of a commercial infrastructure that supports MPC&A. This includes finding qualified in-country vendors of certified MPC&A equipment and the establishment of a vendor development program that furthers the role of Russian companies engaged in the business of manufacturing, sales, and maintenance of MPC&A equipment.

Succinctly, the definition of sustainability within the context of the MPC&A Program is the effective, economical, and long-term operation and support necessary by the Russian nuclear complex to ensure the proper protection, control, and accounting of nuclear material.

Background

Over the past several years, the MPC&A Program has implemented several initiatives designed to address the issues of operability, maintainability, and supportability. However, these initiatives or projects were conducted independent of each other and in an uncoordinated fashion. Therefore, beginning in Fiscal Year (FY) 2000, the Equipment Assessment Project will consolidate those previous efforts into one integrated project. This consolidation will promote syn-

ergy between the various equipment and vendor evaluation activities and help reduce Program overhead and costs.

Elements of the Equipment Assessment Project were initiated as early as FY97. These activities include (1) conducting assessments of physical protection systems, (2) data collection and data analysis of physical protection systems performance, (3) establishment of a physical protection equipment testing facility at the Interdepartmental Special Training Center (ISTC), (4) publication of a physical protection "consumer report," and (5) an assessment of Russian alarm communications and display systems. During this same period, efforts were started to investigate the Russian certification process, to publish a primer on certification, and to conduct a preliminary evaluation of MPC&A equipment vendors. Material control and accounting (MC&A) tasks initiated during FY98 and FY99 included MC&A systems analysis, integration of MC&A instrumentation and measurement methods at Minatom enterprises, and the long term supportability and sustainability upgrades for the Canberra U/Pu Inspector. Other activities initiated in FY99 were the Y2K analysis of installed MPC&A equipment and the exploration of a vendor development program.

Scope

The scope of the Equipment Assessment Project cuts across the entire MPC&A Program. The Project addresses equipment requirements and evaluates equipment and equipment vendors for upgrades at civilian sites, Minatom and Minatom defense-related sites, Navy sites, and transportation activities. Because Equipment Assessment will evaluate equipment across the entire MPC&A Program, the project team must make a concerted effort to coordinate its activities with all project site teams that are tasked with MPC&A equipment installation. Under Equipment Assessment, priority is given to assessment/evaluation of equipment in accordance with current program guidance; beginning with the most critical of MPC&A equipment necessary for immediate installation. From this point, assessments and evaluations will be performed on remaining elements of MPC&A equipment.

Project Goal

The goal of the Equipment Assessment Project is to ensure the effectiveness and long-term sustainability of MPC&A systems by establishing a capability to objectively evaluate equipment and vendors. By institutionalizing the process, Equipment Assessment assists project site upgrade teams in selecting the most appropriate, commercially available, and sustainable MPC&A equipment using standardized criteria. Appropriate selection of equipment contributes to the continued operation of MPC&A, which in turn reduces the risk of theft or diversion of weapons useable nuclear material in the Russian Federation. There are three components to the Equipment Assessment goal: (1) assess and evaluate MPC&A equipment and vendors for use at Russian sites, (2) promote

long-term sustainability of MPC&A equipment through vendor evaluation and development of an MPC&A business infrastructure, and (3) promote Russian ownership of the process.

Objectives and Strategies

Equipment Assessment Project objectives and strategies are developed to support the project's goal and to ensure integration of project activities with the efforts of other site project teams within the entire Russian MPC&A Program. These objectives include assessing and evaluating the operational effectiveness and long-term sustainability of MPC&A equipment, identifying the Russian certification process, evaluating equipment vendors, and promoting the development of Russian vendors for MPC&A equipment and services.

These objectives will be met by pursuing the following strategies. First, the Project will establish and institutionalize the process of evaluating MPC&A equipment and suppliers. Concurrently, a mechanism will be developed for reporting the results of evaluations to help drive equipment and vendor selection. Additionally, the Project will work with Russian authorities to identify the Russian certification process and assist U.S.-Russian site upgrade project teams in resolving certification problems with MPC&A equipment. Finally, the Project will develop a strategy to promote equipment services and vendor development to improve Russian equipment performance and vendor service.

Initial efforts for this fiscal year focused on completing work initiated in FY99. These efforts include (1) completing a "consumer report" type document based on initial assessments and evaluations of Russian MPC&A equipment, (2) continuation of Russian certification process improvement, (3) vendor evaluations, and (4) final acceptance of the ISTC as a testing facility for physical protection equipment.

New efforts for FY2000 involve:

- continued evaluations of U.S. installed equipment and remaining Russian equipment,
- evaluations of new equipment identified for potential future use,
- comprehensive evaluations/testing of equipment/ systems with identified performance problems,
- development of a comprehensive database of all equipment located at all MPC&A sites,
- development of a comprehensive MPC&A Consumer Report, and
- development of a vendor development program.

It is important to note that evaluations and reports will be an iterative process. Deliverables (i.e., future Consumer Report documents) generated as a result of this project are intended to be dynamic in nature. As the project expands to the evaluation stage, so will the amount and level of information on MPC&A equipment. Moreover, cultivation of Russian capability in performing assessments and evaluations will

change the ownership of this document.

Project Organization

The Equipment Assessment team is organized to address the primary functional areas of overall project management, physical protection, material control and accounting, certification, vendor evaluation, and vendor business development. The Project Team is comprised of the following personnel:

- DOE Headquarters Project Lead,
- Field Project Lead,
- U.S. Physical Protection Task Lead,
- U.S. MC&A Task Lead,
- U.S. Certification Task Lead, and
- U.S. Vendor Evaluation Task Lead.

Project activities are organized into four main task areas:

1. Physical Protection Equipment Assessment,
2. MC&A Equipment Assessment,
3. Equipment Certification, and
4. Vendor Evaluation and Vendor Development.

Project Task Areas

Physical Protection

Physical protection system installations have begun at many sites using equipment from many Russian and non-Russian vendors. However, there is limited knowledge of the quality, reliability, or sustainability of equipment that has been and is being installed. As physical protection system equipment is selected for future sites, it is necessary to develop a more thorough body of knowledge of the capabilities of Russian MPC&A equipment, as well as the capabilities of non-Russian equipment in austere Russian environments. Assessment and evaluation of the equipment will allow U.S.-Russian project personnel to fully understand the protection levels that the equipment will provide so the level of risk reduction can be determined for each site and long-term sustainability can be promoted.

Several subtasks make up the physical protection assessment and evaluation effort. These subtasks include (1) data collection and data analysis, (2) conducting operational surveys, (3) test facility enhancements, (4) controlled environment testing, and (5) promoting Russian ownership of the process. The combined results of these subtasks will produce information that project site upgrade teams can use to make informed choices regarding equipment selection for site upgrades. First, the data collection and data analysis activity that began in FY99 will be fully integrated into the Interdepartmental Special Training Center (ISTC) testing regime. Further, there will be minor enhancements to the ISTC's testing labs that will give the testing facility the capability to perform the full range of tests necessary to accurately determine equipment performance. Additional physical protection equipment will be purchased for performance testing. The MPC&A community will be surveyed as to their opera-

tional experience with physical protection equipment.

The majority of physical protection assessment and evaluation activities will be conducted at the ISTC. Over the past two years, the MPC&A Program has been working cooperatively with the ISTC to develop an independent comprehensive test facility. The purpose of the ISTC test facility is to gather performance data on MPC&A physical protection equipment through testing, data collection, and data analysis. The results of the testing, data analysis, and operational surveys will be compiled and published in a comprehensive consumer report for MPC&A equipment.

One of the principle outcomes from the performance data will be the publication of a MPC&A comprehensive consumer report that incorporates equipment assessment and evaluation results. This report, MPC&A Consumer Report will be a living document and will be updated annually as new MPC&A equipment is tested and evaluated by the U.S. and Russian Equipment Assessment Team. This report will take into account all of the equipment assessment tasks of physical protection and material control and accounting equipment, as well as manufacturers' business state-of-health and ability to support installed equipment. The report will also comment on certification and attestation of equipment.

MC&A Equipment Assessment

The primary objectives of this major task area are to develop a process to assess and/or evaluate MC&A equipment and to turnover the responsibility for the process to the Russians. There exist companies and institutes that produce different types of MC&A equipment. The challenge for the U.S. MPC&A Program is that the equipment quality, reliability, and sustainability are unknown. Additionally, in several instances, the equipment has not been certified for use at nuclear sites in Russia. These issues complicate the task of MPC&A site project personal trying to decide on what piece of equipment is best suited for MC&A functions at Russian nuclear sites. Installation and use of MC&A equipment will improve material control and accounting of nuclear material in Russian institutes and enterprises. However, this improvement in nuclear material control and accounting can only be accomplished if the equipment (1) is certified in accordance with Russian standards, (2) is able to meet MC&A performance requirements, (3) is reliable, (4) is operated and maintained properly, and (5) can be supported by vendors or manufacturers on site.

Originally, the purpose of the Material Control and Accounting Systems Analysis Project (MCASAP) was to assure long-term use of MC&A equipment and measurement methods in Minatom institutes and enterprises and by GOSATOMNADZOR (GAN) inspectors. The project supported use of indigenous MC&A equipment, when possible, by identifying potential equipment and suppliers in Russia and by examining performance parameters and quality control to determine the effectiveness of such equipment. This

Project has assisted in the development of Russian infrastructure for supplying and supporting MC&A equipment in Russia.

It must be noted that although MCASAP was a new effort beginning in FY99, it was created by combining two previously funded projects that were separate, but coordinated, in FY98 (the Measurement Techniques & Reference Materials Project & the MC&A Instrumentation Project). This union was deemed appropriate due to the close coordination between the use of MC&A instrumentation and the analytical techniques that are required for effective MC&A. Initially, these projects were not specifically created to test and evaluate the performance of MC&A instrumentation. Rather, the projects were established to help indoctrinate the Russian Federation as to the benefits of incorporating MC&A instrumentation, techniques, and methodologies into a site's comprehensive MPC&A program. These efforts focussed on establishing working groups and promoting training to garner support in the use of effective MC&A technologies within the Russian Federation nuclear complex. As a result, there were a number of tasks funded under this project work plan that are a continuation of commitments that were made under past projects, but are still relevant to the current MC&A equipment assessment effort.

In order to accomplish the primary objectives, the following subtasks have been implemented:

- gathering information as to the operational needs of MC&A,
- assessing and evaluating equipment,
- developing measurement methodologies and standardized operating procedures,
- disseminating equipment assessment and evaluation results, and
- promoting of Russian ownership MC&A equipment as assessment and evaluation process.

The last subtask is the most important. It formalizes and institutionalizes the MC&A equipment assessment and evaluation process and transitions responsibility for this activity to our Russian partners.

Equipment Certification

Since the inception of the MPC&A Program, there has been a number of barriers that the joint project teams have been forced to overcome while upgrading MPC&A systems at Russian nuclear facilities. One of the most complex program impediments has been the Russian equipment certification requirement. To help joint project teams navigate the murky waters of Russian certification, the Certification Project began as an activity in FY99 to conduct a comprehensive analysis of the Russian certification process and published a roadmap or "Primer." The Primer has been distributed widely throughout the Program and is now available electronically via the MPC&A web site.

In addition to publication of certification Primer, other

certification activities include development of a Common Criteria Translation, Common Criteria Protection Profiles for MC&A and physical protection systems, and certification process improvement.

Common Criteria Translation is the creation of an official Russian language version of ISO 15408, the Common Criteria for Information Security Evaluation. This activity is a necessary step for the Russians to adopt the Common Criteria as the standard Russian information security evaluation criteria. When this has been accomplished, Russia will be in a position to join the mutual recognition of common criteria evaluations, which is an important step in eliminating the need for ongoing Russian-specific evaluation of commercial software products as new versions are released by manufacturers.

Common Criteria Protection Profile for MC&A Systems builds on previous MPC&A Program support for the Russians to develop information security criteria for MC&A systems. (This was work that was required in order to get the current certificates for Windows NT, SQL Server, and Oracle.) This effort will result in a Common Criteria formulation of functional information security requirements and assurance requirements. This is a necessary step to enable the Russians to take full advantage of the Common Criteria within the MC&A elements of the Program.

Common Criteria Protection Profile for Physical Protection Systems will be developed addressing the functional information security requirements and assurance requirements for physical protection systems. This effort will build on regulatory documents prepared by the Minatom regulatory project.

Certification Process Improvement will involve streamlining or otherwise improving the Russian certification systems for information security or technology goods and services as they relate to use in nuclear facilities. The objective is to strengthen the functional testing aspect and reduce cost wherever possible.

Vendor Evaluation and Vendor Development

The success of the MPC&A Program and the long-term viability of MPC&A systems in Russia are contingent on a self-sustaining in-country capability to service, maintain, operate, and upgrade MPC&A-related equipment and instrumentation. The goal of the vendor development task is to identify, prioritize, and support potential vendor development initiatives that will sustain an in-country capability to service, maintain, operate, and upgrade MPC&A related equipment and instrumentation.

The historical Soviet approach to handling weapons-usable materials was different from the U.S. approach. MPC&A evolved in the U.S. from full government responsibility to the current situation that includes use of commercially available equipment and services. In Russia, this evolution has not really occurred for two reasons: (1) significantly different

economic systems; and (2) philosophical and structural differences in the approach to MPC&A in the two countries. The result is that there are few, if any, viable commercial entities in Russia capable of supporting Russian MPC&A equipment and service needs in the long run.

Development of a commercial infrastructure that supports MPC&A is one of several key elements to program-wide sustainability. The first step is to identify and evaluate Russian vendors that demonstrate a capability to provide equipment and or services. A team was formed to gather information from potential MPC&A suppliers located in the Moscow, St. Petersburg, and Ekaterinburg regions of Russia. The team researched potential MPC&A vendors and established a list of companies on which to conduct case studies. A questionnaire was developed which covers thirteen topics, ranging from management practices to financial resources. Data was collected first via the written questionnaire and then through personal interviews and a tour of the facilities. All information collected was analyzed and incorporated into the report "An In-Depth Market Analysis of Russian MPC&A Vendors." This report is a "living document" and will be updated as part of the comprehensive consumer report. The update will provide summary information on each company analyzed, the team's rating of each company, and programmatic recommendations. The rating of each company is a significant resource for site leads making procurement decisions.

From a review of the previous MCASAP and PPSAP reports, as well as the certification work, it is apparent that additional companies and regions need to be surveyed and included in the market analysis report. The team is proposing two additional trips to conduct case studies on potential MPC&A vendors. These trips will include vendors identified in the MCASAP and PPSAP consumer reports that have not yet been evaluated as part of this project. The team will modify the current questionnaire based on feedback from the last case study, transmit the revised questionnaire, translate answers received, and travel to the identified sites to collect information and tour facilities. The information collected, as well as team recommendations, will be incorporated into the market analysis report and submitted to DOE.

The ratings of the vendors contained in the market analysis report rely heavily on information obtained from the various vendors. It is desirable to obtain independent verification of the information collected during these case studies. During this subtask, feedback from sites on the actual performance of the vendors will be gathered and incorporated into the market analysis report. In addition, information will also be collected to keep the market analysis report current (i.e., confirming that a vendor is still operating in a specific location). The vendor team will develop a questionnaire and will use the in-country resources of the MVD team to collect this information.

In FY99, a white paper was developed that described the conceptual elements of the vendor development program. This

program has been incorporated into the vendor evaluation task and was renamed vendor development. In addition, initial agreements were made with five U.S. MPC&A equipment companies interested in participating in vendor development initiatives. These companies can support the initiative by providing training in basic business practices, promoting collaborations between vendors for the purposes of marketing a product, or participation in technology transfer activities.

As part of the vendor development task, a review will be conducted on equipment and services required by the MPC&A Program. Information gathered from other Sustainability Projects (including Site Operations, Warranties & Maintenance, Physical Protection Systems Analysis, MC&A Systems Analysis) will be used to identify trends in purchased equipment. The MPC&A Program's Technical Survey Team, an independent advisory group, has made the recommendation that the MPC&A Program should provide sites with equipment that is "adequate" for the intended use. While this is an important objective, there are other factors that influence the selection of equipment, such as initial investment and long-term life cycle support costs. Therefore, the vendor development team will perform a cost-benefit analysis on some of the more widely used equipment to assess these factors. This cost analysis will be provided to U.S. site project leads in order to incorporate sustainability costs into their procurement decisions. As the MPC&A Program has established a policy which states that equipment purchased for the Russian sites must be certified (except in unique cases), the vendor development team will also incorporate into the cost-benefit analysis which equipment is certified for use at the Russian sites. This cost-benefit analysis will be posted on the MPC&A web site.

Specific criteria will be developed for vendors to participate in the vendor development initiative. These criteria will be based on overall MPC&A Program needs, the viability of the business, and whether or not the vendor's equipment can be certified as well as equipment performance and equipment sustainability costs. Gaps between MPC&A equipment and service requirements (such as licensed installers and certified equipment) and quality providers will be analyzed and prioritized for potential initiatives. The MPC&A databases containing equipment performance information will be used as guidance. Coordination with Russian testing centers is also anticipated.

One of the components of the vendor development task will be to provide assistance to some of the Russian vendors to facilitate their participation in supporting the MPC&A Program. These vendors will be potentially viable businesses that can service the long-term E&S needs of the MPC&A Program and will benefit from assistance designed to strengthen their business practices. Potential business consultants and organizations (such as the Foundation for Russian-American Economic Cooperation – FRAEC) will be utilized to assist in promoting best business practices to Russian MPC&A

equipment and services vendors.

In addition to promoting best business practices, initiatives between Russian vendors will be developed that may include collaboration between a systems integrator and an equipment manufacturer. Russian and U.S. vendors will also be evaluated for the purposes of mentoring, marketing a product, or participation in technology transfer activities. These potential initiatives will be defined once the vendor development task strategy has been established and the list of potential companies has been determined.

Indigenization

As part of the effort to promote Russian ownership of the MPC&A Program, the Equipment Assessment Project Team will solicit and recruit Russian personnel as core team members to participate on all project tasks and supporting activities. The approach involves establishing a Russian Equipment Assessment project team that closely resembles the U.S. project team. Early involvement of Russian personnel in the development stage of the project will insure that the project is designed on a model that closely fits Russian operational methods, ensures Russian buy-in to the MPC&A culture, and adopts best business practices. It is the ultimate goal that the Russians become experts in these issues and are able to perform all of these activities with limited or no involvement from the U.S. personnel.

Conclusion

The Equipment Assessment Project is a critical component to Program-Wide Sustainability. The results of these task areas, when combined provide a synergistic body of knowledge that qualitatively and cost effectively promotes sustainability. The Project provides a tool to assist site upgrade teams to select the most appropriate, commercially available, and sustainable equipment using standardized evaluation criteria. Just as important is the effort to improve the commercial infrastructure to support MPC&A in Russia by promoting the development of indigenous vendors that provide equipment and services. Finally, the entire Equipment Assessment process must be institutionalized and transitioned to Russian ownership, if it is to remain an effective sustainability activity. ■

Note: The paper was presented by **Daniel Miller** at the 41 INMM meeting in New Orleans, Louisiana, July 17-21, 2000, and will be published in the conference proceedings.

Daniel R. Miller is Project Lead, Equipment Assessment Project with Aquila Technologies Group; **Kara De Castro** is Vendor Evaluation Task Lead, Equipment Assessment Project at Brookhaven National Laboratory; **Ron Melton**, Ph.D. is Certification Task Leader, Equipment Assessment Project at Pacific Northwest National Laboratory; **Yves Dardenne**, Ph.D. Material Control and Accounting Task Lead, Equipment As-

essment Project at Lawrence Livermore National Laboratory; **Charles Ringler** is Physical Protection Task Lead, Equipment Assessment Project at Sandia National Laboratories; **Kathleen McCann** Headquarters Program Lead, MPC&A Program-Wide Sustainability at the Department of Energy

CONSIDERATIONS IN IMPLEMENTATION OF INTEGRATED SAFEGUARDS

by Rodney Martin, Ronald Melton, and Ned Wogman

Introduction

International safeguards have traditionally relied on a monitoring and inspection system based on nuclear material accountancy at declared facilities. In recent years, efforts have been directed toward implementing an integrated safeguards system to detect diversion from declared activities as well as undeclared activities. As the International Atomic Energy Agency pursues implementation of additional safeguards measures with a focus on the entire State, the safeguards system must necessarily evolve toward the collection and analysis of ever-increasing amounts of data. However, the Agency cannot simply add these new measures on top of existing safeguards approaches, but must carefully evaluate the mechanisms for integrating the combination of traditional and enhanced safeguards tools into a functional safeguards system.

In moving to a safeguards system based on a State-wide analysis of data and information, it is important to have a thorough understanding of the data and information generated by the various safeguards tools. Other issues of importance include the acquisition and storage of the increased volume of data and information, techniques to promote data and records quality and traceability, and finally the architecture for evaluation of combinations of a wide variety of data types to achieve safeguards objectives. This paper examines a number of these evaluation factors and provides examples of process considerations needed to assure effective implementation.

Data Considerations

It is important that the origin or provenance of data and information be documented and traceable. In this context, data should include information as to origin, e.g., instrument number, literature reference, etc.; date and time of origin; other parameters that may affect performance, e.g., calibration, tests, settings, climatic conditions, etc.; and information on any processing or treatment of the data. This type of information, commonly referred to as "metadata," adds im-

portant descriptive information about the data generated by the safeguards tool and is generally a critical portion of the safeguards system. Without the associated metadata, it will usually not be possible to use the primary data to arrive at a credible safeguards conclusion. However, the collection, storage, and linkage of the metadata with the primary data add to the system complexity for the management of safeguards information. When the provenance of a specific collection or set of data has been established, it is important to protect the data in a manner that allows for detection of tampering .

Another factor to consider regarding the new tools used in the integrated safeguards system deals with the effectiveness of the measures employed. In this context, evaluations of background levels and variations, interference, detection probability and false alarm rates, and confidence limits for signature identification should be completed. The United Nations Monitoring, Verification, and Inspection Commission (UNMOVIC) is going through a similar process of looking at background and detection capabilities to determine the most effective set of tools/measures to use in monitoring for proliferation activities in Iraq.

In addition to evaluating these data characteristics, it is important to examine the magnitude of data acquired from possible signatures and components of an integrated safeguards system. The quantity of data not only influences the collection and storage options, but may impose unrealistic conditions for analysis of the data. For example, if detection were dependent on searches of open source literature and the number of documents was in excess of 500,000, an analyst could not complete a review of this large volume of information within a reasonable timeframe without software tools. Consequently, some analytical tool(s) must be employed to focus the analyst's attention on key components for detailed examination.

System Architecture

As the IAEA moves to implement strengthened safeguards measures, including the Additional Protocol, it will create new databases that will store and manipulate information from a wide variety of tools and methodologies. Many of these databases will involve acquisition, storage and analysis of data and information not previously employed in non-proliferation analyses. While the protocol and format has been developed for a number of these databases, there needs to be a structure for utilization of information from the various databases to perform safeguards analyses designed to detect proliferation activities. The general approach being developed by UNMOVIC, with a few modifications, can be utilized for application by the IAEA in other states. In this approach, the Freeze Frame model of the nuclear fuel cycle and weapons development process is used to define processes that a state with proliferation aspirations would follow in developing nuclear weapons. The Freeze Frame approach is similar to the Physical Model and there are some overlaps,

but the Freeze Frame model relies more on signature detection of a process whereas the Physical Model is more oriented toward proliferation pathway analysis. For each of the processes portrayed in the Freeze Frame, a set of signatures can be defined and corresponding methodologies evaluated for detection of the specific signatures indicative of that proliferation process. The sensitivity of various detection methodologies can be evaluated relative to expected signature strength and also relative to both normal background and site-specific interferences. In addition, it is possible to evaluate detection sensitivity for a variety of scenarios, e.g., normal versus accidental conditions and varying environmental conditions. These types of comparisons are being developed for the UNMOVIC Nuclear Action Team .

This is consistent with the creation of databases associated with strengthened safeguards concepts. However, there are a number of advantages to employing the Freeze Frame model for establishing the safeguards approach. Using Freeze Frame, an analysis structure can be developed that combines divergent databases into a powerful safeguards evaluation tool that can be applied on a country-specific basis. By assessing a state's capabilities, it is possible to focus on the most probable proliferation processes and to minimize or eliminate some unlikely pathways. For example, a low-technology country that only has LEU-fueled reactors may not need analyses of data associated with sophisticated isotopic enrichment capabilities. Even if a particular process were not eliminated, it may be feasible to prioritize resources so that less effort is expended on lower probability proliferation scenarios. Using this approach, analyses could be oriented toward more generic indicators for some processes and if evidence of an undeclared nuclear activity is detected, then the Agency would take action to detect a specific process signature. By performing analyses of a State's nuclear programs and technologies, it should be possible to optimize signature detection tools and methodologies so that the safeguards system is tailored for that particular State.

It is also possible to perform selective screening using this approach. In this way, various methodologies and techniques can be evaluated for detection of process signatures. One should use the best case example for evaluation; if this turns out not to be a feasible option, then less sensitive techniques would not be evaluated and this detection mechanism would not be selected for use. If multiple techniques are sufficiently sensitive, then the analyst can examine other factors in the selection process, such as resource requirements, ease of operation, and use of data for multiple applications. In this way IAEA resources would be optimized toward using the "best" tools to monitor for proliferation signatures. This approach would also permit prioritization of resource application, a graded approach where less effort would be assigned to less attractive targets and materials. It would allow an approach with the greatest "return" at the lowest cost.

Although the design of the proliferation detection sys-

tem is based on analysis of individual tools and methodologies, it should be recognized that indicators from a combination of sources may result in a more powerful tool for detection of proliferation. It should also be possible to use relational data patterns, comparison with models, duplicative and correlated indicators, pattern recognition and a variety of other analysis techniques to enhance the capabilities and reliability of the safeguards system. The use of combinations of data to detect anomalies adds to the complexity of the system and makes it much more difficult for an adversary to spoof the system than reliance on an individual detection technique.

System Reliability

Because of the international reliance on IAEA systems for detection of proliferation, the IAEA must factor quality assurance into all of the tools and methodologies used to achieve safeguards objectives. In this context, it is important that reliability be factored into safeguards system design and that techniques be developed to assure system performance. Attention has been focused on "data authentication," as defined by the IAEA to assure that information has been transferred from an authorized source, within a specified time window, and that it has not been altered, removed, or substituted. However, less attention has been applied to techniques to assure system performance. While the use of calibration standards provides some amount of assurance, as the IAEA moves to implement unattended and remote monitoring it becomes more important to implement additional techniques to increase confidence that the system is functioning correctly.

An approach describing a methodology based on measurements and tests of sequential patterns to validate operational performance for unattended or remote monitoring applications has previously been described. This same approach can also be used to increase confidence in the acquisition and storage of information associated with strengthened safeguards systems. Again, in this case, tests can be conducted to assure consistency between duplicative and correlated data, comparisons made between associated metadata and data derived from other sources. Multiple authentication measures should be implemented to provide the highest level of assurance possible in operational performance, and in the safeguards data and information.

Conclusion

Effective utilization of increased amounts and types of information is critical for the IAEA to achieve its nonproliferation objectives. To be successful, the IAEA must develop a system for the acquisition, management, and analysis of this diverse information. This paper suggests that examination of data characteristics and implementation of information authentication tools will be important in developing the acquisition and storage components. Finally, the Freeze

Frame approach could be used to structure the management and analysis of the strengthened safeguards databases. By focusing on detection of a process signature, the Agency can prioritize and optimize its resources and utilize different detection methods with differing resource requirements and detection probabilities in consideration of varying conditions within and between states. ■

Notes: Contact the Center for full footnotes. The paper was presented by Rodney Martin at the 41 INMM Conference in New Orleans, Louisiana, July 17-21, 2000.

Rodney Martin, Ronald Melton, and Ned Wogman work with Pacific Northwest National Laboratory.

THE ROLE OF RUSSIA'S GOSATOMNADZOR IN MPC&A IMPLEMENTATION

by Yuri Volodin, Boris Krupchatnikov, Alexander Sanin

The Russian nuclear materials control and accounting (MC&A) program has undergone many changes over the last five years. New technologies have been introduced, personnel have been trained, and new regulations have been developed. Gosatomnadzor of Russia (GAN), as the state oversight authority for the control and accounting of nuclear materials used for civil purposes, has the responsibility to assure that nuclear materials are controlled, accounted for, and used only for peaceful and defensive purposes. The Federal Law "On the Use of Atomic Energy" established the authority of government oversight agencies for the safe use of nuclear energy in a number of areas, including nuclear material protection, control, and accounting. Gosatomnadzor of Russia is one of these agencies. It is active in the following major areas:

- development, adoption, and implementation of the rules and regulations on issues related to MPC&A;
- safety-related licensing activities regarding the use of atomic energy;
- oversight of compliance with rules and regulations on the use of atomic energy and technical specifications of operating licenses, including conducting inspections related to performance of its duties, and overseeing the State System for Nuclear Material Accounting and Control;
- imposition of sanctions against organizations subject to GAN oversight; and
- monitoring and compliance with RF obligations under international agreements regarding safety assurance in the

use of atomic energy.

Legal and regulatory basis

The legal basis for the work of Gosatomnadzor includes several documents:

1. Presidential decree #1923, September 15, 1994, "Priority Measures to Modernize the Nuclear Material Control and Security System";
2. Government Decree #34, August 13, 1995, "1995 Priority Measures to Develop and Implement the Nuclear Materials Control and Accounting System";
3. Presidential order #350-rp, July 26, 1995, "Issues Regarding Governmental Oversight of Nuclear Safety and Radiation Protection", Federal Law "On the Use of the Atomic Energy", July 26, 1995;
4. Presidential decree #26, January 21, 1997 "Federal Executive Branch Agencies Authorized to Regulate the Safe Use of Nuclear Energy";
5. Governmental Decree #1205, October 14, 1996, "Conceptual Design of the State System for Nuclear Material Accounting and Control";
6. Governmental Decree #574, May 8, 1996, "Regulations on the Procedure for Exporting and Importing Nuclear Materials, Equipment, Special Non-Nuclear Materials and Related Technologies";
7. Governmental Decree #264, March 7, 1997, "Physical Protection Rules and Regulations for Nuclear Materials, Nuclear Facilities, and Nuclear Material Storage Points";
8. Governmental Decree #1511, December 1, 1997, "Regulations on Procedures for Developing Federal Rules and Regulations Regarding the Use of Atomic Energy";
9. Governmental Decree #746, July 10, 1998, "Organizational Rules for the State System for Nuclear Material Accounting and Control";
10. Federal Law "On the Administrative Responsibilities of Organizations for Violations of Legislation Regarding the Use of Atomic Energy," May 12, 2000; Draft of the "Basic Nuclear Material Control and Accounting Rules" (implementation expected in the first half of 2001);
11. Draft for "Requirements for Establishing Material Balance Areas at Nuclear Facilities and Nuclear Material Storage Points" (implementation expected in 2000);
12. "Agreement between the Gosatomnadzor of Russia and the RF Ministry of Internal Affairs on Collaboration in the Conduct of Governmental Oversight of the Physical Protection of Nuclear Material, Nuclear Facilities, Radiation Sources, Radioactive Substances, and Nuclear Material and Radioactive Substance Storage Points," 1999.

Recently a number of documents dealing with physical protection *per se* were adopted. These include "Methodology for Assessing Vulnerability of Nuclear Material and Nuclear Facility Physical Protection Systems" and "Instructions for Conducting the Inspection of Physical Protection

Equipment at Potential Hazardous Nuclear Sites."

The regulatory basis will be completed when the "Regulation on Government Nuclear Material Control and Accounting" is released.

Licensing and Oversight

Licensing is one of the essential elements of Gosatomnadzor's activity. License technical specifications are required for different activities with atomic energy. These licenses could also establish special requirements regarding support for activities conducted by the safety regulation agency in the performance of its duties, and includes material protection, control, and accounting. As a result of a violation of compliance with the regulations, sanctions could be imposed. Sanctions have been included in a number of regulatory documents and recommendations regarding the imposition of sanctions were provided by the Guidance Document RD-03-43-98. In 1998 21 licenses were revoked; 10 licenses were suspended; 252 stop work orders were issued; 2750 violation remediation notices were issued; 42 officials were fined a total of 1116 rubles (about \$223); 376 warnings were issued to officials; and 43 incidents were referred to law-enforcement agencies. Because of the lack of methodological guidance and insufficient work experience, there were not many sanctions in the area of MPC&A, although a number of work stoppages occurred.

Gosatomnadzor also performs governmental oversight of nuclear material protection, control, and accounting at 62 potentially hazardous nuclear sites. Of these sites, 38 fall within the jurisdiction of Minatom; 6 within the jurisdiction of the Russian Federation Shipbuilding Ministry (*Rossudostroyeniye*), and the remaining sites within the jurisdiction of other ministries. 59% of the sites fall into category 1; 25% - category 2; 7% - category 3; and 9% - into other categories.

In 1999 Gosatomnadzor conducted 387 inspections of PP systems (including special inspections at Leningrad, Kalinin, Balakovo, Beloyarsk, Kola, Smolensk, Kursk, Novovoronezh NPPs; "Mashzavod" (Elektrostal); the Siberian Chemical Complex; the Novosibirsk Chemical Concentrate Plant; the Radium Institute, and the Bochvar Research Institute for Inorganic Materials, etc.) The oversight is organized and conducted by the regional offices through their MPC&A departments, established in the Central, Northern European, Urals, Siberian, and Far East regions.

The Gosatomnadzor of Russia Directorate performs methodological organization for Nuclear Material Protection, Control, Accounting, Safeguards Assurance and Nonproliferation. In 1999, 655 violations of the requirements in physical protection rules and regulations were found. Although the number of violations increased over the years, it was because of the increase in the number of inspections. The average number of violations dropped in 1999 (in 1998 - 2 violations, in 1999 - 1.6 violations). A number of warnings to the

site directors were issued for failures to meet deadlines for compliance with the violations notices issued as a result of physical protection inspections.

Gosatomnadzor continues to conduct joint verifications of physical protection status with representatives of Interior internal security troops in accordance with guidance documents developed by Gosatomnadzor and approved by Interior internal security troops. In 1999, 102 special inspections were conducted to verify the status of nuclear material control and accounting at 49 enterprises and organizations subject to Gosatomnadzor (GAN) oversight (71% of the total number). 205 nuclear material control and accounting violations were discovered (164 violations of standard documentation and 41 violations of license technical specification). 23 of them were not corrected by the established deadline.

In 1998 two cases of significant discrepancy between nuclear MA data and measured characteristics were discovered. As a result, unscheduled inventories were conducted. In 1999 four cases of measurement discrepancy between actual and declared values were found but the result might relate to the number of inspections and to the fact that better equipment was used. Non-destructive assay instruments were used in 39 inspections, and 235 samples were measured. As a result, six instances of significant discrepancy between nuclear material accounting data and measured characteristics were discovered.

International Cooperation

Along with training, PP at six potentially hazardous nuclear sites were upgraded in 1999 within the framework of the Agreement between the GAN and DOE regarding cooperation in the Area of NM MPC&A (June 30, 1995). These included the Moscow Engineering Physics Institute (MEPhI), the Joint Institute for Nuclear Research at Dubna; the Karpov Physics and Chemistry Research Institute (PNPI), the Nuclear Physics Institute at Tomsk Polytechnic University, and the Krylov Institute. Major areas of upgrading included: hardening physical barriers (walls, ceilings, gates, doors) in nuclear material storage areas and in buildings where nuclear facilities are situated; installing automated access control and identification equipment at access points and in secure buildings and structures; installing guards signaling systems and television surveillance systems for access control points, buildings, structures, and the perimeter of secure areas; installing portal monitors to detect the unauthorized transit of nuclear material and metal; and developing computerized control panels for physical protection systems.

The first stage of modernization has been completed. The new stage includes:

- ensuring the operability, sustainability, and effective operation of the modernized PP systems;
- using operating experience to fine tune the PP systems;
- consolidating nuclear material for transferring it from

potentially hazardous nuclear sites with a low level of protection to other sites; and

- limiting the number of sites that handle direct use nuclear material.

The sites are signing contracts for out-of warranty servicing of PP systems and purchase of spare parts, etc.

The US DOE support remains crucial for Russian MPC&A activities. However, it is appropriate to think about effectiveness and sustainability of the projects. Serious gaps remain in the MPC&A regulatory basis, as well as the lack of established practices in applying regulations in this area, and underestimation the need to expand the project with analyzing effectiveness of regulation application. ■

Note:

¹ This review is made based on the presentations by Yuri Volodin at the INMM 41 annual meeting in New Orleans, Louisiana, July 17-21., 2000. Paper will be published in the conference proceedings.

Yuri Volodin is the head of the MPC&A Division at Gosatomnadzor, Russia. **Boris Krupchatnikov, Alexander Sanin** work for MPC&A division at Gosatomnadzor, Russia

SUSTAINING MPC&A SYSTEMS IN THE NEWLY INDEPENDENT BALTIC STATES

by G.A. Sheppard, J.R. Mason, P.W. Robinson, M. Soo Hoo,

The collapse of the Soviet Union left weakened governmental controls over nuclear materials within its successor states and increased concern about the potential for nuclear weapons proliferation. Among the greatest concerns were weapons-usable fissile materials (plutonium and highly-enriched uranium) that might be vulnerable for theft or diversion. These materials are potential targets for countries that wish to develop nuclear weapons capability or terrorist groups who seek to possess an improvised nuclear device.

A mission of the US Department of Energy (DOE) in the Soviet successor states is to reduce the threat of nuclear proliferation and nuclear terrorism by rapidly improving security and accountability of all weapons-usable nuclear material in Russia, the NIS, and the Baltic States. The DOE MPC&A program has supported the installation of MPC&A system upgrades at numerous sites in these states. In collaboration with NIS states the DOE upgraded site physical protection (PP) systems, material control and accounting (MC&A) systems, and measurement capabilities.

An upgraded PP system usually has several layers of intrusion detection and assessment, delay, and entry control. The innermost layer would be a vault or storage room in which nuclear materials is stored. Its floors, walls, ceilings, and door are hardened to resist penetration. Intrusion detection sensors and closed-circuit television (CCTV) cameras are located around and within the vault. The vault door is usually thick and equipped with several different locking mechanisms. The next layer encompasses the building housing the vault. Ground-accessible windows are barred, doors are hardened, locked, and equipped with entry control hardware, unused openings are blocked, and intrusion detection sensors and CCTV assessment cameras are installed. At some facilities, the outermost layer is a fenced perimeter that is equipped with intrusion detectors, lighting, closed-circuit television cameras, a clear zone, and a vehicle barrier. One or more personnel and vehicle portals are provided by controlling the entry and exit of personnel and vehicles through the perimeter. At such facilities, a central alarm station is the focus of guard activity. It features an entry control system, a computerized alarm panel, a camera switcher and monitors, an intercom system, and a radio-base station.

DOE upgraded facility capabilities for tracking nuclear material inventories by providing computers, software, and in some cases, bar code systems; training and assisting with development of procedures that govern many of the details of managing nuclear material inventory, including assessing and handling nuclear materials; taking, verifying and reconciling physical inventories; reporting to regulatory authori-

ties; and controlling ingress and egress of material and authorized personnel from protected areas.

To measure HEU, an Active Well Neutron Coincidence Counter was provided in a few cases. DOE supplied gamma spectroscopy instruments of both high and low energy resolution to measure the isotopic content of nuclear materials nondestructively. Calibration standards were also provided. Selected sites were provided with digital scales and calibrated mass standards to accurately weigh nuclear materials. DOE provided training and assistance in developing operating, maintenance, and performance-training procedures for all systems with which facilities were equipped. Following the completion of the upgrades at the sites selected in Ukraine, Kazakhstan, Belarus, Uzbekistan, Latvia, Lithuania, and Georgia, responsibility for sustaining them was transferred to the International Safeguards division (NN-44) at DOE's Office of Arms Control and Nonproliferation in 1999.

Sustaining MPC&A Upgrades

As MPC&A system upgrades are completed and the facilities assume the responsibility to employ them, the next issues of focus are: sustaining the upgraded MPC&A systems, establishing and nurturing national MPC&A infrastructures, and broadening the scope to include international safeguards activities, particularly those related to the activities of IAEA.

To maintain the increased capability to protect dual-use nuclear materials and to continue to meet the DOE nonproliferation goals, a strategy was developed to address the longer-term operation and maintenance of the MPC&A systems that have been put in place. This is important because at sites where there has been no subsequent effort, we have observed evidence that the newly installed MPC&A systems are not being used or maintained adequately. Our current program is designed to establish the procedures and the infrastructure to sustain the MPC&A upgrades implemented at the sites in the Soviet successor states. The program is not designed to upgrade sites further. Areas of work include personnel training in the operational and maintenance fields, equipment warranty/ maintenance contracts, and independent systems evaluations. A sufficient national infrastructure and international cooperation are other areas considered vital to long-term sustainability. While a significant portion of the first year's efforts focused on site activities, some level of effort at the national level is also needed to ensure the MPC&A systems and culture are sustained.

Because the MPC&A upgrades at the facilities are not uniform in scope and the extent of the countries' nuclear programs varies, activities that sustain them must be determined on a site-by-site, state-by-state basis. Site upgrades have been reviewed to determine the completeness of the MPC&A systems and the levels of activity needed to sustain them. We are using these evaluations to fine-tune a graded approach to sustaining the MPC&A system based on the type and amount

Table 1: MPC&A Sites in the NIS/Baltics

Country	Site	Location	Facility Type	Pu	HEU Inirradiated	HEU Irradiated	LEU Inirradiated
Kazakhstan 2,3	BN-350 breeder reactor	Aktau	Fast Breeder Reactor	x	X	X	
	Institute of Atomic Energy	Alatau	Research Reactor		X	X	
	Institute of Atomic Energy	Kurchatov	Research Reactor		X	X	
	Ulba Metallurgical Plant 5						
Ukraine 6,7	NSC/Institute of Physics and Technology 8	Kharkiv	Research Center		X		x
	Institute for Nuclear Research 9	Kyiv	Research Reactor		X	X	
	Institute for Nuclear Energy and Industry	Sevastopol	Research Reactor		X	X	
	South Ukraine Nuclear Power Plant	Yuzhnoukrainsk	VVER Power Reactor (3)				X
Belarus	Sosny Institute of Nuclear Power 10	Minsk	Research Center		X	X	
Uzbekistan	Institute of Nuclear Physics 11	Tashkent	Research Reactor		X	X	
Latvia	Institute of Nuclear Physics 12	Salispils	Research Reactor		X	X	
Lithuania	Ignalina Nuclear Power Plant 13	Ignalina	RBMK Power Reactor (2)				X
Georgia	Institute of Physics	Tbilisi	Research Center		Removed to the UK in 1998 14	Removed to the UK in 1998	Removed to the UK in 1998

of material under protection.

The following activities provide details on the measures taken to sustain MPC&A technologies, infrastructure, and culture in the non-Russian Soviet successor states. Not all measures are suitable for all countries. Our activities are focused both at the site level and at the state level, and some cut across international boundaries.

Site-Level Activities to Sustain MPC&A

The key elements necessary for sustaining safeguards and security upgrades at the site level are the following:

- documentation describing the system upgrades;
- procedures for maintaining and operating them;
- training on use of these procedures;
- operational evaluation to determine how well the plans are being executed;
- supplies of spare parts and critical components, and
- extended warranty service plans.

To the extent possible, all site-level sustainability activities are consistent with organizational biases and influences.

System Assurance. An annual system assurance visit will be performed at each site by a small team composed of DOE employees, National Laboratory staff members, and/or IAEA evaluators. These visits will give first-hand knowledge of the current sustainability issues specific to each site/country and allow efficient tailoring of generic MPC&A sustainability plans and documentation for consistency with IAEA criteria and facility attachments. Assessments made during system assurance visits will be used as a model upon which facility operators can base their own self-assessments and operational evaluations. System assurance visits take approximately one week per country for Latvia, Lithuania, Belarus, and Uzbekistan. Because they have multiple sites, Kazakhstan and Ukraine each require two weeks to perform system assurance visits. For each site, there are an additional 2 or 3 weeks of work needed in the U.S. to review and update the plan to sustain MPC&A systems.

Site Documentation. We have compiled and continually update site-specific documentation that includes descriptions of the systems, personnel and organizational roles and responsibilities, and the means by which applicable regulatory requirements are to be met.

Remediation. System assessments and operational evaluations may reveal vulnerabilities or problems that were overlooked as MPC&A upgrades were designed and installed, or that have developed due to the changing situations or equipment obsolescence. These problems will be remedied appropriately, keeping in mind that major safeguards and security upgrades should have already been completed.

Operations, Maintenance, and Performance Test Procedures. Written operating procedures are needed to ensure the accomplishment of such tasks as transferring nuclear material, operating the alarm monitoring station, and establishing access control privileges. The procedures will also in-

clude emergency instructions for the response of facility personnel or by contractors, but this is specified in these documents. To ensure proper operation of the equipment, it is also important to ensure that there are procedures for periodic performance testing of the systems.

Operation and Maintenance Training. Training procedures and operator qualification requirements are necessary to support system reliability and to ensure currency and continuity of operations and maintenance knowledge. The procedures must be consistent with equipment manufacturers' recommended practices.

Operational Evaluations. Operational evaluations consist of site self-assessments and independent evaluations. The evaluation frequency and applicable procedures must be documented. The system assurance assessment and site documentation described above will be used as the basis for performing operational evaluations.

Extended Warranty and Spare Parts. Most equipment installed during MPC&A upgrades was guaranteed for only one year. Purchased warranties extended for an additional two years will establish the mechanisms for longer-term system maintenance and upkeep. Stocks of spare parts and critical components will assure timely repair of failed components and reduce potential down-time. Because this can be a relatively costly process to initiate, facilities with limited financial resources will be targeted for support in this area.

State-level Activities to Sustain MPC&A

For each country possessing a substantial, on-going nuclear program, a national infrastructure is needed to ensure that site-level safeguards systems are sustained. While a significant level of effort to develop a state-level infrastructure is beyond the scope of this program, some level of effort is warranted and will help establish links to other countries and international organizations that would continue development of national infrastructure.

State System of Accountancy and Control. In Ukraine and Kazakhstan, the U.S. has worked with the state nuclear regulatory bodies to help them establish components of their state systems of accountancy and control. Training, copies of the US laws and regulations, computer systems, software, and nondestructive assay equipment have been provided. We will work with the State Nuclear Regulatory Administration of Ukraine to develop an automatic capability to generate reports to the nuclear national data that are submitted by Ukraine's nuclear facilities via their Automated Inventory/Material Accounting System.

National Training. In addition to physical improvements, an important component of a program of MPC&A upgrades is enhancement of the safeguards culture of the recipients. To facilitate this culture enhancement and to help insure that the work of protecting nuclear materials will continue after U.S. assistance ends, safeguards training courses have been identified and provided in many of the subject states. Most

of the following extant or planned MPC&A training courses and workshops have been offered to participants from one or several of the subject states:

- fundamentals of MPC&A;
- fundamentals of nondestructive assay;
- statistics, variance propagation, and measurement control;
- structure and measurement of a safeguards seals program;
- computer training;
- nuclear materials physical protection – transportation, vulnerability assessment;
- design basis threat analysis;
- MPC&A survey procedures;
- MC&A inspection;
- material accounting for nuclear safeguards;
- basic information security; and electronic security systems, MPC&A procedures development.

International Cooperation

It is significant that none of the non-Russian Soviet successor states possesses nuclear weapons and that all have signed the IAEA Nonproliferation Treaty (NPT). This accession requires that the countries sustain viable MPC&A systems. In most cases this viability depends heavily on the MPC&A system improvements made in collaboration with the U.S. Other areas in which our program overlaps or is influenced by the IAEA are the Newly Independent State (NIS) Coordinated Technical Support Program and the International Physical Protection Advisory Service (IPPAS).

In 1993, the IAEA initiated the NIS Coordinated Technical Support Program to coordinate the MPC&A assistance of donor countries, which include the U.S. Much of the assistance was focused on developing state systems of accounting and control. Assistance in implementing the IAEA safeguards procedures was also provided. Further, the MPC&A program has used INFCIRC/225/Rev.3 as a guide document in enhancing the existing physical protection features at NIS sites. This guidance provides these countries additional reasons and rationale to sustain the MPC&A improvements. As a part of the program, we will continue to coordinate with the IAEA to develop plans to sustain MPC&A systems consistent with IAEA safeguards practices and physical protection guidelines and to provide assistance when necessary.

It should be noted that an additional revision of the IAEA's guideline on physical protection of nuclear material (INFCIRC/225/Rev.3) was published after we had completed most of the MPC&A upgrades. In addition to the physical protection of nuclear materials, the new document (INFCIRC/225/Rev.4) addresses protecting nuclear facilities against sabotage and reconciling safety and security issues that sometimes conflict. Although we have no plans at this time to upgrade existing systems to comply with the new guidelines, we expect that the pressure to do so will build as they gain

wider acceptance. ■

Notes: Contact the Center for complete footnotes.

G.A. Sheppard, J.R. Mason, P.W. Robinson, and M. Soo Hoo work at the U.S. Department of Energy/NN-44. Paper was presented by Gregory Sheppard at the 41 annual INMM meeting in New Orleans Louisiana, July 17-21, 2000. Paper will be published in the conference proceedings.

DOCUMENTS

DECREE

of the RF President
No. 822
May 6, 2000
(unofficial translation)

On Amending the Decree of the Russian Federation President No. 312 of March 27, 1992 “On Controlling the Exports from the Russian Federation of Nuclear Materials, Equipment and Technologies.”

1. Introduce into the Decree of the RF President No. 312 of March 27, 1992 “On Controlling the Exports from the Russian Federation of Nuclear Materials, Equipment and Technologies” the following amendments:

a) after paragraph two, include new paragraphs three through eight of the following content:

“In exceptional cases, such exports from the Russian Federation into a country not possessing nuclear weapons and not having placed its nuclear activities under the IAEA safeguards may be carried out based on individual decisions of the Government of the Russian Federation, under the following conditions:

- the delivery does not contradict international obligations of the Russian Federation;
- the government of the recipient country provides an official obligation excluding any circumstances under which the supplied materials, equipment and technologies can be used to develop a nuclear explosive device;
- the delivery is carried out exclusively for the purpose of safe operation of the existing on the recipient country territory nuclear installations;
- IAEA safeguards are applied to such installations.

The Government of the Russian Federation can establish additional conditions for such exports to occur;”

b) paragraph three becomes paragraph nine.

2. The Government of the Russian Federation is to bring all its normative acts in accordance with this Decree. ■

Vladimir Putin
RF Acting President

COMMENTS ON THE PRESIDENTIAL DECREE

by *Mikhail Ryzhov*, Director, Department of International and Foreign Economic Relations, MINATOM; and *Marina Belyaeva*, Senior Expert, MINATOM

Prior to 1992, Russia remained among the few countries that did not fully support the demand of the group of nuclear suppliers known as “full-scope safeguards.” This was due to many reasons. The first was that there were a number of countries with which Russia cooperated and which were not parties to the treaty and had not put all their installations under the safeguards of the International Atomic Energy Agency.

Among these countries were Cuba, where the USSR began building a nuclear reactor, and India, with which the Soviet Union had an inter-governmental agreement and was negotiating a contract to build nuclear plants. When the USSR accepted the demands for full-scope safeguards it was important that its international contract obligations not be broken. So, when the 1992 presidential decree on full-scope safeguards was adopted, Russia proceeded with the understanding that all agreements signed prior to 1992 remained in force in their original form, i.e., they were not covered by the NSG rule. In other words, the rule did not apply retroactively.

Since 1992 however, Russia has scrupulously adhered to this principle and has not signed any new contracts. In 1996 Moscow was the venue of a summit meeting of the G-8 that re-emphasized the provision on the priority of safety over all the other priorities. Russia took a relaxed view of this because we thought that giving a new prominence to any one element always lead to unpredictable consequences. But the seven developed countries managed to put into the document of the summit the provision on the priority of safety considerations over all other considerations, including the requirements of export control.

By that time the group of nuclear suppliers had introduced an addition to its rules. Under this addition, if countries that have not put their nuclear facilities under IAEA safeguards need technical assistance, and such assistance is prompted by the requirements of safety, such assistance is allowed. It is true that it is only allowed under certain conditions, such as consultations, approvals, and explanations. But such a provision exists. So, the Russian approach was different from that of the group of nuclear suppliers for over seven years. And because this question kept cropping up, it was decided in 1999 to harmonize the requirements of the Russian national legislation with international obligations. There were always questions as to why the national legislation contained provisions and standards that differed from internationally agreed upon principles.

In 1999 a corresponding amendment was introduced. In the intervening period these provisions were being agreed to by various agencies, and by the presidential administration.

Finally, on May 6, 2000, this addition was signed by the then Acting President. Let me repeat that the only requirement consists of the recognition of exceptional cases that are determined only by safety considerations. The decree expressly states that this standard does not apply automatically, but only if the government issues a special decree. Additional conditions apply. First, the assistance should be directed only to the installations under IAEA control. Second, Russia may require additional approvals. Third, the recipient country should renew its assurances that this assistance and these materials will not be used for the production of nuclear explosive devices or nuclear weapons. Finally, equipment assistance must be related to safety upgrades. ■

(Source: Press-conference, May 30, 2000)

AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED STATES OF AMERICA AND THE GOVERNMENT OF THE RUSSIAN FEDERATION CONCERNING THE MANAGEMENT AND DISPOSITION OF PLUTONIUM DESIGNATED AS NO LONGER REQUIRED FOR DEFENSE PURPOSES AND RELATED COOPERATION
(Excerpts)

The Government of the United States of America and the Government of the Russian Federation, hereinafter referred to as the Parties,

Have agreed as follows:

Article II

1. Each Party shall, in accordance with the terms of this Agreement, dispose of no less than thirty-four (34) metric tons of disposition plutonium.

2. Each Party's declaration on quantities, forms, locations, and methods of disposition for disposition plutonium is set forth in the Annex on Quantities, Forms, Locations, and Methods of Disposition.

3. The Parties shall cooperate in the management and disposition of disposition plutonium, implementing their respective disposition programs in parallel to the extent practicable.

4. The reciprocal obligations set forth in paragraph 1 of this Article shall not prejudice consideration by the Parties of what additional quantities of plutonium may be designated by each Party in the future as no longer required for defense purposes.

5. The Parties shall cooperate with a view to ensuring that additional quantities of weapon-grade plutonium that may be withdrawn from nuclear weapon programs and designated in the future by the Parties as no longer required for defense

purposes are:

a) brought under and disposed of in accordance with the terms of this Agreement; or

b) subject to other measures as agreed by the Parties in writing that provide for comparable transparency and disposition.

6. Each Party shall have the right to mix blend stock with disposition plutonium provided that for nuclear reactor fuel containing disposition plutonium the mass of blend stock shall:

a) be kept to a minimum, taking into account the protection of classified information, safety and economic considerations, and obligations of this Agreement; and

b) in no case exceed twelve (12) percent of the mass of disposition plutonium with which it is mixed.

The resulting mixture of disposition plutonium and blend stock shall be weapon-grade plutonium.

7. Each Party's disposition plutonium shall count toward meeting the thirty-four (34) metric ton obligation set forth in paragraph 1 of this Article once the other Party confirms in accordance with agreed procedures that the spent plutonium fuel or immobilized forms meet the criteria specified in the Annex on Technical Specifications, which is an integral part of this Agreement. Blend stock shall not count toward meeting that thirty-four (34) metric ton obligation.

Article III

1. Disposition shall be by one or more of the following methods:

a) irradiation of disposition plutonium as fuel in nuclear reactors;

b) immobilization of disposition plutonium into immobilized forms; or

c) any other methods that may be agreed by the Parties in writing.

2. The following are the nuclear reactors that may be used for irradiation of disposition plutonium under this Agreement: light water reactors in the United States of America and in the Russian Federation; the BOR-60 at Dimitrovgrad and the BN-600 at Zarechnyy in the Russian Federation; and any other nuclear reactors agreed by the Parties in writing.

Article IV

1. Each Party shall take all reasonable steps, including completion of necessary technical and other preparatory activities and feasibility studies, to complete construction and modification and to begin operation of disposition facilities necessary to dispose of no less than two (2) metric tons per year of its disposition plutonium in accordance with Article III of this Agreement, if the assistance specified in the multilateral agreement referred to in paragraph 8 of Article IX of this Agreement for this disposition rate is being provided for achievement of milestones in the Russian Federation specified in the Annex on Schedules and Milestones, which is an

integral part of this Agreement.

2. Each Party shall seek to begin operation of facilities referenced in paragraph 1 of this Article not later than December 31, 2007.

3. Pending conclusion of the multilateral agreement referred to in paragraph 8 of Article IX of this Agreement for the disposition rate specified in paragraph 1 of this Article, the Parties shall proceed with research, development, demonstrations, design and licensing activities under this Agreement, on the condition that assistance for such activities is being provided pursuant to paragraph 1 of Article IX of this Agreement.

4. Each Party shall notify the other Party whenever it reaches a milestone set forth in the Annex on Schedules and Milestones or, if not reached at the specified time, the reasons for that delay. If a Party does not reach a milestone at the specified time, it shall make every effort to minimize the delay. In these circumstances, the Parties shall establish in writing a revised mutually-agreed schedule of work for achieving the milestone.

5. Once facilities specified in paragraph 1 of this Article are constructed or modified and begin operations, each Party shall proceed to dispose of disposition plutonium to achieve a disposition rate of no less than two (2) metric tons per year at the earliest possible date.

6. If, prior to December 31, 2007, a Party begins to dispose of disposition plutonium, such plutonium may count toward meeting the thirty-four (34) metric ton obligation set forth in paragraph 1 of Article II of this Agreement if:

- a) the criteria specified in the Annex on Technical Specifications are met; and
- b) monitoring and inspection measures agreed in writing by the Parties are applied to such disposition activities.

Article VII

1. Each Party shall have the right to conduct and the obligation to receive and facilitate monitoring and inspection activities in accordance with this Article and the Annex on Monitoring and Inspections, which is an integral part of this Agreement, in order to confirm that the terms and conditions of this Agreement with respect to disposition plutonium, blend stock, spent plutonium fuel and immobilized forms, and disposition facilities are being met.

2. Disposition plutonium and blend stock shall become subject to monitoring and inspection under this Agreement, in accordance with the Annex on Monitoring and Inspections and procedures developed pursuant to that Annex, either (a) after receipt but before processing at a conversion or conversion/blending facility, or (b) upon receipt at a fuel fabrication or an immobilization facility, whichever (a) or (b) occurs first for any given disposition plutonium or blend stock.

3. Each Party shall begin consultations with the International Atomic Energy Agency (IAEA) at an early date and undertake all other necessary steps to conclude appropriate

agreements with the IAEA to allow it to implement verification measures beginning not later in the disposition process than: (a) when disposition plutonium or disposition plutonium mixed with blend stock is placed into the post-processing storage location of a conversion or conversion/blending facility; or (b) when disposition plutonium is received at a fuel fabrication or an immobilization facility, whichever (a) or (b) occurs first for any given disposition plutonium.

4. If agreed in writing by the Parties, the exercise of each Party's right set forth in paragraph 1 of this Article may be suspended in whole or in part by the application of equivalent IAEA verification measures under the agreements referred to in paragraph 3 of this Article. The Parties shall, to the extent practicable, avoid duplication of effort of monitoring and inspection activities implemented under this Agreement and appropriate agreements with the IAEA. ■

COMMENT ON U.S./RUSSIAN COOPERATION FOR PLUTONIUM DISPOSITION

By Laura S. H. Holgate

The Office of Fissile Materials Disposition has come a long way in developing a path forward for disposing of surplus fissile materials, both in this country and in Russia. We are already disposing of surplus U.S. highly enriched uranium and are completing the groundwork for disposing of surplus U.S. plutonium. With the signature in September by the United States and Russia of a bilateral agreement on plutonium disposition, we are moving ahead promptly to complete the necessary designs, construct the facilities, and begin disposing of surplus U.S. and Russian plutonium.

This important nonproliferation mission has received significant support from the United States Congress and from other nations. Our objectives, strategies, and goals reflect the collective input of a diverse group of interested parties. Congress, Federal, state, and local governments, Tribal officials, non-government organizations, and the public have all contributed to shaping this program through more than 90 public meetings and thousands of comments received by mail, phone, fax, and our web site, as well as through frequent meetings, conferences, and other public events.

History

Since the end of the Cold War, significant quantities of plutonium and highly enriched uranium have become surplus to defense needs, both in the United States and Russia. Continued implementation of arms reduction agreements is expected to result in further weapons dismantlements and increases in stockpiles of these surplus, weapons-usable fis-

sile materials.

If acquired by terrorists or states of concern, these surplus materials could be made into crude nuclear weapons for use against the citizens of the United States, Russia, or other nations. The National Academy of Sciences has characterized this threat as a “clear and present danger” to national and international security.

This threat led President Clinton to announce a framework for United States efforts to prevent the proliferation of weapons of mass destruction. A key element of this framework committed the United States to undertake a comprehensive approach to seek to eliminate, where possible, the accumulation of stockpiles of plutonium and highly enriched uranium, and to ensure that where these materials already exist, they are subject to the highest standards of safety, security, and international accountability.

In support of this strategy, the Department of Energy and the Department of Defense reviewed estimates of the fissile materials required to support U.S. security needs. As a result, President Clinton ordered that 200 tons of fissile materials—enough for thousands of nuclear warheads—be permanently withdrawn from the U.S. nuclear stockpile and never again used to build nuclear warheads. Then, Russian President Yeltsin made the first official declaration of excess Russian fissile materials, stating that up to 50 metric tons of weapons plutonium and up to 500 metric tons of highly enriched uranium were excess to Russian defense needs.

Approach for Surplus U.S. Plutonium Disposition Program

Nearly all isotopes of plutonium can be used to make a nuclear weapon. As a result, the disposition of plutonium requires the application of more complicated technologies than does the disposition of highly enriched uranium, and there is less public agreement on a path forward. The Department’s strategy for disposition is to convert surplus U.S. plutonium to the “spent fuel standard”, where the material is converted to forms as inaccessible and unattractive for retrieval and weapons use as the residual plutonium in spent fuel from commercial reactors. Once the surplus plutonium meets the standard, it cannot be used in nuclear weapons without significant processing.

The Department of Energy is using a hybrid strategy to dispose of surplus U.S. plutonium. The hybrid strategy relies on two technology approaches: **irradiation**, in which the surplus plutonium is converted to a mixed oxide (MOX) fuel and irradiated in existing, domestic reactors; and **immobilization**, in which surplus plutonium is mixed with ceramic and then surrounded by vitrified high-level radioactive waste. Both approaches will effectively convert the surplus plutonium to the “spent fuel standard” recommended by the National Academy of Sciences. Pursuing both approaches in parallel is important because it provides insurance against possible difficulties with the implementation of either tech-

nology by itself and helps ensure an early start to plutonium disposition.

In support of the hybrid strategy, the Department will construct and operate three key plutonium disposition facilities at the Savannah River Site in South Carolina. The first, a pit disassembly and conversion facility, would disassemble classified nuclear weapons components (pits) and convert the resulting plutonium metal into an unclassified plutonium oxide powder, suitable for disposition as well as for international inspection. The second, a MOX fuel fabrication facility, would produce MOX fuel assemblies, for irradiation in existing, commercial reactors. The production of MOX fuel involves mixing plutonium oxide from the pit disassembly and conversion process and uranium oxide, and then forming the resultant product into fuel pellets. These pellets are then placed into MOX fuel assemblies, and subsequently shipped to domestic reactors for irradiation. The third key facility, an immobilization facility, would convert surplus plutonium that is not in “pit” form into a plutonium oxide powder and embed the powder in a ceramic matrix to form “pucks.” The “pucks” would then be stacked in steel cans. The cans are then arrayed inside a large steel canister, into which molten high-level radioactive waste is poured.

Approach for Surplus Russian Plutonium Disposition Program

While the United States considers surplus plutonium to be a proliferation risk, Russia views its excess plutonium as an important energy source. For this reason, Russia’s preferred approach for plutonium disposition relies exclusively on the irradiation of MOX fuel in nuclear reactors for power generation. Russia intends to dispose of all of its surplus plutonium in reactors following conversion of their plutonium metal to an oxide form and subsequent manufacture into mixed oxide fuel.

Both the United States and Russia are moving ahead with parallel programs to dispose of a combined 68 metric tons of surplus weapon-grade plutonium in accord with the terms of the bilateral agreement on plutonium disposition. Key provisions of the agreement include:

- *Material covered.* The agreement commits each side to dispose of at least 34 metric tons of weapon-grade plutonium. Should additional material be declared excess in the future, the agreement allows the two sides to dispose of it in accordance with the terms of this agreement.

- *Disposition techniques.* The agreement allows for disposition either by irradiating the plutonium as MOX fuel in nuclear reactors or by immobilizing the plutonium in glass or ceramic form surrounded by vitrified high-level radioactive waste to meet the criteria specified in the Agreement.

- *Disposition rates.* The two countries plan to begin operation of industrial-scale facilities no later than December 2007 in order to dispose of at least two metric tons per year of weapon-grade plutonium. A plan will be developed to

identify additional reactor capacity inside and/or outside Russia to permit at least a doubling of the disposition rates in both countries.

- *Financing.* Proceeding with plutonium disposition in Russia is dependent on assistance from the United States and other nations. The \$400 million pledged by President Clinton as part of his Expanded Threat Reduction Initiative would assist Russia in jump-starting the effort needed for plutonium disposition. Preliminary estimates indicate construction of plutonium conversion and MOX fabrication facilities and modification of Russian nuclear reactors will cost about 2 billion dollars. Russia will need to contribute some resources, and the United States government is working with members of the international community to identify financing for this program.

- *Inspection, monitoring, and nonproliferation conditions.* The agreement includes provisions for monitoring and inspection activities to confirm that the facilities are being dedicated to the disposition of excess weapon-grade plutonium, that the disposition rates are being met, and that the disposed plutonium meets certain agreed standards. Both parties intend to work toward allowing certain bilateral inspection and monitoring rights to be satisfied by IAEA-equivalent verification measures, to the extent practicable.

Completion of this bilateral agreement also sets the stage for additional agreements and discussions with Russia and others on several elements. First, we need to resolve nuclear liability issues so that cooperation and work under this agreement can be extended into the construction and operation phases of the disposition program in Russia. Second, we must negotiate multilateral arrangements for international financing of the Russian Program and develop plans to increase the disposition rate beyond 2 metric tons per year. Third, we now need to develop the details of an inspection and monitoring regime that will provide the United States, Russia, and the world community with assurance that plutonium disposition is being carried out according to the terms and conditions of the bilateral agreement. There is a tremendous amount of work ahead.

In anticipation of the bilateral agreement, the United States and Russia have conducted tests and demonstrations of proposed plutonium disposition technologies under a Scientific and Technical Cooperation Agreement since 1998. Both countries have developed a plutonium disposition roadmap, or logic flow, and an associated nominal schedule for the Russian plutonium disposition program. The early parts of this roadmap focus on technology development in the areas of plutonium conversion and nondestructive assay, irradiating MOX fuel in reactors, and immobilization. Key elements of this work include:

- Assisting Russia to design and build a demonstration facility for converting weapons-origin plutonium metal to an oxide form suitable for use in MOX fuel and for interna-

tional inspection.

- Developing a MOX fuel fabrication process that would be compatible with surplus weapons-grade plutonium, testing the resulting fuel, and qualifying it for use in VVER-1000 reactors and the BN-600 reactor.

- Assisting Russia to assess the feasibility of converting Russia's BN-600 reactor, a fast-neutron reactor, into a net burner of plutonium.

- Working with Russian institutes and private industry to develop gas turbine, modular helium reactor technology as an option to supplement Russia's existing reactor capacity to dispose of surplus plutonium.

- Examining the technical feasibility of burning a small quantity of MOX fuel made from surplus U.S. and Russian weapons plutonium in a Canadian test reactor. Irradiating MOX fuel in Canadian nuclear reactors is one of several options being examined to increase the rate of disposing of Russian surplus weapons plutonium.

- Assisting Russia in developing glass and ceramic technologies suitable for immobilizing plutonium-containing materials at Russian sites.

Collectively, this cooperative work with Russia supports President Clinton's Expanded Threat Reduction Initiative to reduce the global danger from weapons of mass destruction. Along with other countries, we continue to conduct a number of demonstrations of key plutonium disposition technologies in Russia because we believe the development of this knowledge will enable the Russians to accelerate efforts to dispose of their surplus plutonium in accordance with the provisions of the bilateral agreement on plutonium disposition.

Looking Ahead

With the necessary Records of Decision issued for our domestic program and the bilateral agreement on plutonium disposition in place, our office will begin full implementation of the efforts to dispose of surplus U.S. and Russian weapon-grade plutonium. The U.S. commitment to this program sends a clear message to Russia and the rest of the world that we consider the disposition of surplus fissile materials to be one of our highest national priorities. We aim to finish this important job of reducing the global danger from the proliferation of weapons of mass destruction. ■

Laura Holgate is Assistant Deputy Administrator, Office of Fissile Material Disposition, U.S. Department of Energy

US-RUSSIAN SUMMIT IN MOSCOW, MAY 2000

AGREEMENT ON THE ESTABLISHMENT OF A JOINT WARNING CENTER FOR THE EXCHANGE OF INFORMATION ON MISSILE LAUNCHES AND EARLY WARNING

President Clinton and President Putin today signed the Memorandum Of Agreement Between The Government Of The United States and Government Of The Russian Federation On The Establishment Of A Joint Center For The Exchange Of Data From Early Warning Systems And Notifications Of Missile Launches.

This agreement - which is the first time the United States and Russia have agreed to a permanent joint operation involving U.S. and Russian military personnel - is a significant milestone in ensuring strategic stability between the United States and Russia. It establishes a Joint Data Exchange Center (JDEC) in Moscow for the exchange of information derived from each side's missile launch warning systems on the launches of ballistic missiles and space launch vehicles.

The exchange of this data will strengthen strategic stability by further reducing the danger that ballistic missiles might be launched on the basis of false warning of attack. It will also promote increased mutual confidence in the capabilities of the ballistic missile early warning systems of both sides.

The JDEC will build upon the successful establishment and operation during the millennium rollover of the temporary joint center for Y2K Strategic Stability in Colorado Springs. The JDEC will be staffed 24 hours a day, seven days a week, with American and Russian personnel.

The JDEC is also intended to serve as the repository for the notifications to be provided as part of an agreed system for exchanging pre-launch notifications on the launches of ballistic missiles and space launch vehicles. This agreement is currently being negotiated separately. ■

JOINT STATEMENT BY THE PRESIDENTS OF THE UNITED STATES OF AMERICA AND THE RUSSIAN FEDERATION ON PRINCIPLES OF STRATEGIC STABILITY

- The Presidents of the United States of America and the Russian Federation agree on the need to maintain strategic nuclear stability. Agreements between them help accomplish this objective.

- They are dedicated to the cause of strengthening strategic stability and international security. They agree that capability for deterrence has been and remains a key aspect of stability and predictability in the international security environment.

- The Presidents, welcoming the ratification of START-II

Treaty and related documents by the Russian Federation, look forward to the completion of the ratification process in the United States.

- They announce that discussions will intensify on further reductions in the strategic forces of the United States and Russia within the framework of a future START-III Treaty, and on ABM issues, in accordance with the Moscow Statement of 1998 and Cologne Statement of 1999 by the Presidents.

- They agree on the essential contribution of the ABM Treaty to reductions in offensive forces, and reaffirm their commitment to that Treaty as a cornerstone of strategic stability.

- They agree that the international community faces a dangerous and growing threat of proliferation of weapons of mass destruction and their means of delivery, including missiles and missile technologies, and stress their desire to reverse that process, including through existing and possible new international legal mechanisms. They agree that this new threat represents a potentially significant change in the strategic situation and international security environment.

- They agree that this emerging threat to security should be addressed and resolved through mutual cooperation and mutual respect of each other's security interests.

- They recall the existing provision of the ABM Treaty to consider possible changes in the strategic situation that have a bearing on the provisions of the Treaty, and, as appropriate, to consider possible proposals for further increasing the viability of the Treaty.

- The Presidents reaffirm their commitment to continuing efforts to strengthen the ABM Treaty and to enhance its viability and effectiveness in the future, taking into account any changes in the international security environment.

- In reinforcing the effectiveness of the ABM Treaty under present and prospective conditions the United States of America and the Russian Federation attach great importance to enhancing the viability of the Treaty through measures to promote greater cooperation, openness, and trust between the sides.

- The United States of America and the Russian Federation note the importance of the consultative process and reaffirm their determination to continue consultations in the future to promote the objectives and implementation of the provisions of the ABM Treaty.

- The key provisions recorded in our agreements and statements, including at the highest level, create a basis for both countries' activities regarding strategic arms under present-day conditions.

- Such an approach creates confidence that the further strengthening of strategic stability and further reductions in nuclear forces will be based on a foundation that has been tested over decades and advances both countries' interests and security.

- The Presidents have directed the development of con-

crete measures that would allow both sides to take necessary steps to preserve strategic stability in the face of new threats, and called on their Ministers and experts to prepare a report for review by the Presidents.

- They agree that issues of strategic offensive arms cannot be considered in isolation from issues of strategic defensive arms and vice versa — an interrelationship that is reflected in the ABM Treaty and aims to ensure equally the security of the two countries.

- The United States of America and the Russian Federation intend to base their activities in the area of strategic offensive and defensive arms on the principles set forth in this document. ■

BOOKNOTES

L.Feoktistov, *Useless Weapons* (in Russian)
(Lev Feoktistov, *Oruzhiye kotoroye sebya ischerpalo*) SLMK,
pp. 247, Russia, 2000

This book, with an introduction by Mikhail Gorbachev, is an unusual one. Its author is one of the leading nuclear scientists who headed Soviet weapons projects for about 50 years at one of the key Soviet nuclear laboratories at Chelyabinsk-70. However, unlike many in the nuclear industry who favor the renewal of nuclear weapons testing and production of nuclear weapons, he calls for immediate and total nuclear disarmament. He considers the tendency towards the “nuclearization” of Russian foreign policy and the new arms race very dangerous. According to Feoktistov, there is no way to control nuclear proliferation as long as nuclear weapons remain a valuable instrument of the foreign policy of “elite” countries and are forbidden for others. Nuclear disarmament depends on political will. Even if a civilian facility does not produce nuclear materials, it can still be converted for weapons material production. Thus, only the total elimination of nuclear weapons will make the world safer.

To support his ideas the author cites Nilse Bore’s reply to one of the KGB consultants in 1945. When questioned about the protection from the atomic bomb, the great physicist replied: “The only method to prevent the use of a nuclear bomb could be establishing an international control over all the countries. It is necessary for the whole of mankind to understand that with the discovery of nuclear energy the final destiny of all nations is closely tied. Such international cooperation and international sharing of scientific inventions could lead to the abolition of war, hence to the abolition of the use of nuclear weapons.”

This book is about the history of Soviet nuclear weapons, the role of the Ministry of Atomic Energy, the role of Chelyabinsk-70, and the role of the scientist himself. But it is also about the future of the nuclear industry and of nuclear weapons. According to the author, he wrote the book in part because of the dramatic changes in Russian and world policy over the past ten years. The number of nuclear and near-nuclear weapons states has increased, while Russia is threatening to MIRV its new single-warhead ICBM and deliver a preventive nuclear strike in response to US plans to establish a NMD system. Several years after the end of the Cold War, when it seemed that nuclear weapons would not play any role in world policy, the world is once again entering an arms race. To answer the question about the future of nuclear weapons, Feoktistov reviews the reasons why leading Soviet nuclear scientists, such as Sakharov, Tamm, Landau, and himself left the field of nuclear research at the height of the Cold War.

According to the author, in the mid-'70s he and other leading scientists realized the nefariousness of further nuclear development. Future development was no longer necessary even for purposes of security – rather, it was driven by the obligations of the military and political elite.

The book is based on thorough research, includes documents, interviews, and archive material. In the epilogue the author suggests some new ways for the development of the nuclear industry. These include civilian nuclear energy programs, international projects of Plutonium conversion, and spent-fuel reprocessing. ■

V.M.Kuznetsov, *Russian Nuclear Energy Past, Present, Future: View of an Independent Expert*
(*Rossiyskaya atomnaya energetika. Vchera, segodnya, zavtra. Vzglyad nezavisimogo eksperta*), Moscow, Golospresna, 2000 (in Russian).

Vladimir Kuznetsov, is a member of the Independent Expert Association on the Safe Use of Atomic Energy, the Russian Ecological Congress. He has published widely on different issues of Russian atomic energy. He is a regular contributor to Minatom's newspaper "Atompress" and is well known as an expert in this area.

This book provides a comprehensive overview of Russian atomic energy. It covers various aspects of the issue in several sections:

- nuclear power plants, or NPPs (technical features, their role in development and maintenance of the Russian energy and fuel cycle, their safety and security, their history of operation in Russia, program for the development of Russian nuclear energy for 1995-2010)
- nuclear research facilities (classification, safety and security, disturbances, spent fuel and nuclear waste, energy production at the NPPs, and the main financial obstacles)
- nuclear submarines (history and accidents)
- new NPPs (including floating NPPs and other types of new reactors)
- withdrawal operation of nuclear facilities (national and international cooperation, and radioactive wastes)
- physical protection of nuclear facilities
- nuclear legislation
- transportation of nuclear and radioactive materials
- certification of equipment, items and technologies for nuclear installment, radioactive sources and storages
- state regulation of the use of nuclear energy.

Besides covering a broad number of issues, the author also includes an appendix with governmental documents and regulations related to nuclear energy.

Another important feature is a chapter on physical pro-

tection and governmental regulation of nuclear materials. This chapter outlines the history of physical protection at nuclear facilities, cases of nuclear smuggling, and the main problems with physical protection. Finally, the author covers subjects traditionally not referred to in most books on atomic energy – nuclear submarines, transportation, and NPP closures and dismantlement.

The book is a mine of facts, information, and statistics. Each of the author's conclusions is supported by facts and figures. This makes the book very useful for experts in the area, and could be considered a reference book. Its tables and diagrams are useful and balanced. For example, writing about accidents at NPPs, the author uses statistics from Gosatomnadzor as well as nongovernmental organizations.

This book identifies the most problematic areas in Russian atomic energy, analyzes the errors of the NPPs operation and nuclear waste storage, and could be used in solving state control problems, improving legislative bases, and educating the public about nuclear energy. ■

NEWS FROM THE CENTER

SAM NUNN POLICY FORUM

The fourth Bank of America Sam Nunn Policy Forum: “Globalization, Technology Trade and American Leadership: A New Strategy for the 21st Century” took place at the University of Georgia on March 27, 2000. This year’s forum brought together noted academic, government, and private sector experts on international affairs, public policy, and technology to discuss issues of immediate and future importance to the nation.

The 2000 Nunn Forum addressed the importance of high tech commerce to American leadership and security in the 21st century. Technology trade, the subject of the Forum, is essential to American prosperity and security. Yet, outdated governmental policies are unable to stay abreast of economic and technological changes and increasingly impede the achievement of U.S. interests. The current debate centers upon the need of U.S. industry to stay competitive (i.e., export) and the sometimes countervailing need to ensure that U.S. security is not undermined by such trade.

The 2000 Forum raised and sharpened this debate, promoting constructive business-government dialogue. Participants discussed ways to insert the issue of export controls into the presidential campaign and provide guidance to the next administration and worked to clarify the complex issues currently stalling policy legislation in Congress.

This essay is a summary review of the findings reached and the recommendations proposed at the 2000 Forum.

Findings

U.S. export controls have undermined the capacity of the United States to conduct joint military operations with its allies.

Current policy has driven a serious wedge between the United States and its allies in the North Atlantic Treaty Organization (NATO). U.S. allies could not execute some missions in Kosovo, for example, because export controls restricted access to spare parts. Relatively minor shifts in end-use or item modifications within the alliance results in months of delay if the items require a new or altered U.S. license. European defense contractors have already removed U.S. parts from their designs for some products because of export control restrictions, and an increase in these occurrences threatens the interoperability of NATO weapons and logistical systems and the ability to coordinate wartime and peace-keeping missions.

Globalization means that technology and manufacturing networks no longer conform to national patterns; it also means that the United States no longer dominates several key tech-

nology markets:

Although no one fully understands the ramifications of globalization on export controls and national security, an export control policy resting on Cold War assumptions about the nature of security and economics will fail to sustain U.S. national security in the 21st century. Increasing foreign availability of sensitive items, for example, suggests that the window of time export controls can buy will get smaller over time, so that adversaries will face smaller delays in matching or countering U.S. military technologies.

This example illustrates only a few of the many of issues fostered by greater globalization. Consolidation, integration, and privatization of defense industries reflect an increased interest in rationalization, sustainability, and profitability of the allied defense industrial base. In several key commercial sectors, such as aerospace manufacturing, encryption software, and high-performance computers, the United States has lost or is losing the kind of market dominance that made unilateral export control policies effective. Export controls that do not recognize these new transnational patterns of research, development, and production for military and dual-use items will undermine U.S. efforts to maintain its historical military advantage which has been largely based on technological prowess and economic prosperity. Export controls based only on a *national* view of economics and security no longer serve U.S. national security and economic welfare.

The United States relies too heavily on export control policies to address its concerns about foreign entities that threaten or potentially threaten U.S. security.

The inability to pass a new Export Administration Act in the 1990s and the reluctance of several allies to support U.S. export control initiatives reflect a general lack of consensus at home and abroad about the opportunities and constraints inherent in export control policy. To some U.S. allies, U.S. national security controls have become too entangled with export controls imposed for reasons of foreign policy. This seems especially true of controls aimed at countries with which the U.S. has ambiguous relations such as China, India, and Pakistan. The Clinton administration has not offered a new export administration bill this term and partisan, ideological, jurisdictional and parochial divisions in Congress have defeated legislative efforts at comprehensive export control reform. Consequently, the United States has developed an increasingly *ad hoc* legal framework for export controls that does not integrate export controls effectively into an overall national security framework. Without a consensus on how export controls best function as a tool for U.S. national security, the United States at times uses export controls for purposes that conflict with broader national security goals.

In the emerging global economic environment, U.S. export controls require radical changes to meet the post-Cold War challenges to U.S. national security.

The system of controls is broken. Changes in the inter-

national economic and security environment have outpaced efforts to adapt U.S. export controls. Economic globalization, the growth of the Internet, the integration of defense industries, and other forces demand a new kind of governance. Currently, the State Department has insufficient resources to make timely and consistent licensing decisions. The State and Defense departments also lack an effective real-time electronic interagency licensing system for munitions items. Policies that classify items with both significant commercial and military applications as munitions items, such as encryption software in the past and satellites in the present, exacerbate this problem by overloading the licensing system. The munitions licensing process was not designed to handle items with significant commercial applications. As the division between military and commercial items becomes more and more artificial, the inadequacies of the munitions licensing process is undermining U.S. leadership in defense, technology, and commerce.

More important, trying to combat the variety of emerging threats from rogue states, terrorists, and other adversaries with export controls that were designed to fight the Soviet Union in the Cold War does not make sense. Government and industry, for example, must share information effectively to identify end-users of concern and their operatives, which was not formerly a necessity for controls based on the country of destination. During the Cold War, the U.S. and its allies generally agreed on what items to control and controlled them for the same target countries. In the post-Cold War era, the U.S. and its allies do not share that consensus, especially on how to treat end-users in those countries that fall somewhere between friend and foe, such as China, India, Pakistan, and even Iran. In the international arena, the unanimity of the former Coordinating Committee on Export Controls (COCOM) has given way to several arrangements, such as the Australia Group, the Missile Technology Control Regime, the Nuclear Suppliers Group, and the Wassenaar Arrangement, where controls are left to the national discretion of each participant. Coupled with the globalization and privatization of defense and dual-use industrial and technological capabilities, effective export control policies not only require domestic interagency and multilateral coordination, but also inter-arrangement coordination and new partnerships between government and industry.

Recommendations

The munitions export control process needs reform now, and export controls as a whole need radical reform in the near future.

The State Department needs additional funds to improve the efficiency, consistency, and effectiveness of its licensing process now. State and Defense Department personnel need better training on defense cooperation policies in order to provide clearer guidance on implementing export control regulations. Institutional fixes, however, will prove insuffi-

cient. In the next administration, the United States needs to create a new export control policy that addresses the impact of globalization on national security, including the role of changes in manufacturing processes, technology transfer, and the blurring of the distinctions between munitions and dual-use items. The United States must pass a new Export Administration Act to codify these reforms.

The United States government should create a system of waivers allowing a freer flow of military and dual-use items with its closest allies, especially with those that share similarly tight export controls on military and dual-use items.

As a short term remedy, the State Department needs to create a new mechanism for defense exports to foreign entities in allied or friendly countries that have similar export control policies and practices. The United States should extend its current negotiations with Canada and the United Kingdom to other close allies as soon as possible.

In the long term, both the munitions and dual-use licensing process should help create freer transfers of military and commercial items among allies and other friendly countries to enhance U.S. security interests. Freer access should serve as an incentive to create a community of nations with the highest common standards of export controls.

The United States should exercise more control over the technology transfer process of exporters instead of its current focus on individual transactions.

For both munitions and dual-use licensing, the government should create a new partnership with industry. Increasing industry self-governance, where companies create compliance systems that government agencies regularly audit, can increase industry compliance. By offering meaningful licensing benefits and reduced penalties for companies that engage in best compliance practices, the United States can increase industry confidence in the system and promote effective and efficient export controls. The increasing globalization of industry means that this approach can build trust in the system and compliance among U.S. and foreign multinationals.

The next administration should undertake interrelated dialogues to build a new consensus on a national security-based export control policy in Congress and with its allies and friends.

The next administration cannot initiate radical reform of U.S. export controls without creating a firm base of support in Congress. Export control reform needs to appear on the agenda of both parties with support from the leading presidential candidates. In addition, interested members of Congress should form an informal, bipartisan group to discuss U.S. export control policies on a regular basis. In particular, the group should consider the opportunities and constraints inherent in export controls for national security purposes and the impact of globalization on such policies.

Without a simultaneous and parallel multilateral consensus, however, U.S. export control reforms will founder. With that in mind, United States should initiate both formal and

informal discussions within the NATO framework on easing restrictions on inter-allied technology transfers. At a minimum, the group should aim to expand the bilateral discussions the United States has begun with its closest allies, although it should not limit itself to that agenda. At the same time, the United States should set specific goals of improving coordination of licensing and enforcement in the export control arrangements. In both cases, creating a freer flow of critical technologies should work as an incentive.

For national security export controls, the United States must embrace globalization or be engulfed by it.

Export controls remain an essential tool for U.S. national security. Globalization, however, has resulted in greater international integration in the defense industry and far more foreign availability of sensitive items than anticipated under current U.S. munitions and, to a lesser extent, dual-use export control policies. The Defense Science Board Task Force on Globalization and Security, for example, concluded recently that arms export controls must shift emphasis from technology protection to capability preservation through promoting technology transfers to enhance allied defense capabilities. Creating the political consensus for reforming export controls, however, depends on demonstrating that the benefits for national security are as great as the economic benefits such policies would provide. ■

MOSCOW CONFERENCE

On May 19, 2000, the Center for International Trade and Security (CITS) of the University of Georgia co-sponsored a conference in Moscow on “*New Challenges To Export Controls In The 21st Century – Globalization And Intangible Technologies Transfers.*” Other co-sponsors were the Institute for World Economy and International Relations (IMEMO) of Russia’s Academy of Science and the Moscow-based Center for Export Controls (CEC).

More than 60 participants from different Russian governmental agencies (Ministry of Trade, Ministry of Education, Ministry of Science and Technology, Ministry of Defense, Ministry of Atomic Energy, Ministry of Justice, Federal Agency on Protection of Intellectual Property, Ministry of Foreign Affairs, Russian Aerospace Agency, etc.), NGOs (Scientists for Global Security, Carnegie Endowment for International Security, PIR-Center, AST-Center, etc.), and non-Russian agencies and organizations (German Ministry of Economics and Technology, U.S. Department of Commerce and Department of Energy, UK Department of Trade and Leeds University, Ukrainian Committee on Export Controls) attended the conference.

This conference was a follow-up to one hosted by CITS in September 1999. At that time, the issue of intangible tech-

nology transfers (ITT) was referred to as a long-term challenge to systems of export control. It was suggested that it might be useful to discuss the issue informally with invited governmental, nongovernmental, legal, and technical experts.

The Moscow conference included three panels – *Scope of the Problem; National Experience and Experience Within the International Export Control Regimes; and Roundtable Discussion: Dealing with this Problem on a Long-Term Basis.*

Presentations and discussions covered the consequences of globalization for export controls, as well as the definitions of terms in the area intangible technology transfers and related problems of enforcement. The Center for International Trade and Security introduced the working paper for comments and recommendations (printed earlier in this issue).

Conference participants acknowledged that the problem of ITT is not new but that it has assumed a new importance, recently becoming an intensely debated issue within all the export control regimes and certain states.

In the age of globalization and information, with the increasing development of electronic devices and the Internet, the role occupied by information, technology, and know-how increases in importance. Just after the Cold War, the major concern was the smuggling of nuclear materials. However, materials alone are not enough to make a bomb. Certain knowledge, know-how and technology are necessary. Many rogue states face difficulties with designing delivery systems. Intangible technology transfer is the easiest and the most efficient means of technology export, some speakers warned.

Although it is necessary in preventing proliferation to control the export of technology in any form, tangible or intangible, controlling intangible technology poses a much greater challenge. Decisions must be made regarding what to control, how to control it, and what the balance should be between openness and security. In order to arrive at answers, these questions must be considered by technical experts, industry leaders, politicians, academicians, and lawyers, sharing ideas informally and making recommendations to regimes. Participants at the conference had the opportunity to share the perspectives of their industries and institutions with others grappling with these questions.

Many expressed concern that most relevant terms lack clear and generally acceptable definitions. There is not only the problem of defining ITT, but also in defining such notions as “export,” “transfer,” “foreign trade activity,” and even “fundamental knowledge,” “public domain,” and “basic scientific research.”

It is very difficult to find a proper balance between academic freedom, freedom of speech, the right of privacy and security concerns in controlling intangible technologies. How can academic, economic, and scientific freedoms be safeguarded in the pursuit of nonproliferation goals? Employees stream across borders, performing the same job in different locations and receiving training in new areas. Should

their movement be restricted? How? What about students working in sensitive areas? Students are notoriously hard to track, even within the U.S. using the INS system of reporting. The line distinguishing basic and applied research is far from clear, making it difficult to restrict students' access to certain classes. Also, restricting access denies foreign students the opportunity to pursue a standard curriculum.

Conference participants identified lack of appropriate legislation, enforcement, and cooperation at the international level as major barriers to successful ITT control. Many discussed the absence of legal precedents of successful convictions for ITT-related infringements. The few known cases involved catching amateur Internet users who were unaware of export control legislation. Currently, the level of expertise of those charged with preventing illegal exports is inferior to that of criminals engaging in industrial espionage and cracking confidentiality codes on the Internet. Legislative efforts lag at least five years behind advances in technology. Experts often fail to recognize an ITT act, aggravating the existing difficulties.

Participants also discussed the issue of liability.. Who should be responsible for sensitive information and its illicit dissemination? ISPs? Website designers who make content decisions?

The emergence of dual-use technologies in the civilian sector is another challenge. The problem is most serious for those companies having international contracts or joint projects. How are the joint ventures supposed to work if components of the product are produced in a dozen countries, each with its own export control regulations, including restrictions on ITT? How are technology and expertise to be shared? In some Western countries it takes 30-40 days to get a license for a telephone conversation. These are the problems facing industries attempting to comply with regulations. Most companies, however, especially those involved in international ventures, do not even understand export control requirements in the ITT context.

It is hard to find a technical solution to controlling intangible technology transfers. Detecting and controlling intangible technology transfers depends in large part on the willingness of suppliers to voluntarily recognize and follow procedures. The licensing of intangible transfers is cumbersome business both for applicants and for the licensing authority. Another problem with enforcing ITT controls is that there are no reliable ways to prevent an illicit transfer to a questionable end-user.

Discussion of national experience in controlling ITT provided a mixed and sometimes confusing picture. There are three categories of states with regard export control-- those countries which prefer to delay the development and implementation of national legislation on ITT; those which are active within the international regimes and would like to see ITT control legislation on the national level (like the U.S. and Germany); and those which advocate control on the national

level, but are unwilling to integrate international regulations into national laws (Russia).

In **Russia**, legislation on export controls was adopted last year. Control of ITT is included in the legislation, but there are no mechanisms for enforcement. Russian conference participants acknowledged the necessity of controlling ITT for nonproliferation and export control.

To control ITT, **Ukraine** tries to regulate, among other things, contract negotiations. In Ukraine, contracts negotiations require a license, and in applying for one an exporter must explain the content of the negotiations and deal. However, the only effective mechanism of control is the enforcement of state secret laws. There are many ITTs that are not state secrets, yet are still sensitive transfers.. Ukraine is attempting to establish an agency to handle these negotiations. (For information on the UK, the U.S., and Germany see articles in the current issue.)

As of now, not a single country or international regime can claim that it has the legal basis, technical means, and effective procedures for controlling ITT.

Participants of the conference proposed to establish a working group on ITT control, consisting of key presenters at the Moscow conference. Its main task would be working out the recommendations for ITT control based on the experience of different countries and the new ideas coming out of the next meeting. The CITS working paper and any revisions to it will serve as the group's starting document. ■

CONFERENCE IN OBNINSK

Dr. M. Beck and M. Katsva participated in the Second Russian International Conference on Material Protection, Control and Accounting in Obninsk Russia on May 22-26. Conference was hosted by the The Institute of the Physics and Power Engineering (IPPE).

Over the last several years, Russian enterprises and government agencies have gained a great deal of expertise and taken on large scale projects aimed at upgrading nuclear security. Moreover, the federal government has set forth a legislative base for protecting nuclear materials at sites. Much of the work and the equipment for upgrading MPC&A systems at the site level has resulted from U.S. and other international assistance. While there is little doubt that U.S. assistance has prompted the emergence of an MPC&A "community" in Russia, there have been problems with assistance programs that have yet to be resolved. However, there have been problems related to assistance programs that remain unresolved, including: access to sites, equipment maintenance and certification and communication between DOE and site managers.

There are growing signs of progress in enhancing MPC&A

policies and practices in Russia: the number of participants in the first conference was about one hundred, while the second conference had nearly four hundred participants, which suggests that the nuclear MPC&A community is growing; legal/normative base for MPC&A at Russian sites is more developed; several nuclear facilities have consolidated nuclear materials in order to reduce vulnerabilities; Russian site managers have become increasingly adept at and interested in integrating new technologies for enhancing nuclear material protection and accounting; site managers and teams are beginning to develop a more integrated approach to MPC&A. Russian facilities have also borrowed and learned from U.S. accountancy practices and norms. Russian experts are developing sophisticated tools to analyze vulnerabilities in physical protection procedures. There is a growing interest in taking advantage of technological options for nuclear security (however, sustaining equipment and computerized systems remains problematic) and willingness to discuss the "insider threat" and related social issues (labor unrest, etc.) impacting nuclear security.

Presentations reflected the emergence of technical expertise on all aspects of PP and MC&A at nuclear sites throughout Russia.

However, many problems remain. They include: lack of standardized reporting procedures for audit; lack of a clear distinction between military and civilian nuclear facilities resulting in problems of regulatory jurisdiction; maintenance and sustainable use of MC&A and PP equipment is problematic; dependence on U.S. and foreign assistance to finance nuclear security upgrades; lack of security culture within Russia's nuclear complex means that some personnel often do not know why they are installing equipment at sites. (This need for a security culture prompted UGA to launch a training program with MINATOM's Institute for Higher Education with support from the Ploughshares Fund, Merck and DOE.) Social conditions at nuclear facilities remain bleak and heighten prospects of "insider" diversions of fissile materials. Communications with DOE remain problematic (no agreement on final objectives exists) and there appears to be remnants of Cold War thinking, which impedes cooperation and trust on these issues.

Dr. M. Beck delivered a paper "Developing a Framework for Evaluation of MPC&A Systems."

All conference presentations will be published in the coming months by the conference organizers. ■

WORKSHOP IN MINSK

On May 22, 2000, the Center for International Trade and Security co-sponsored a workshop "*Export Controls in the 21st century*" in Minsk, Belarus. The workshop was designed to promote greater NIS cooperation in controlling proliferation, to discuss trends in international nonproliferation export controls, and to examine what progress Belarus has made in implementing its export control policy.

The workshop was attended by more than 30 participants from the Ministry of Foreign Affairs, Security Council, Ministry of Defense, and other export control related institutions, as well as by industry representatives. The Deputy Minister of Foreign Affairs, Vladimir Sadokho, who read a greeting message from the Minister, opened the Conference.

The first panel was devoted to a discussion of Belarus's participation in the regimes. On May 19, 2000, Belarus joined the NSG as a full-fledged member. Belarus Foreign Ministry officials expressed gratitude to CITS for the workshop on NSG in 1998, which was instrumental in shaping Belarus's policy towards the NSG. It was pointed out that the next logical step for Belarus is to join the MTCR. Although joining MTCR is not on the immediate agenda, Belarus Foreign Ministry and other governmental officials would like to learn more about the regime and its challenges and prospects. Eventually, the Belarus government will be considering joining the MTCR, and it has to be well-prepared in terms of understanding the regime and the experiences of some of the other members, especially Russia and Ukraine, when it does. Foreign Ministry officials asked CITS to help collect relevant data.

The other two panels considered national systems of export controls, the need for U.S. assistance, and problems arising from the Russian-Belarus customs union. Issues of wider cooperation between the two governments were discussed as well. Belarus adopted export control laws even earlier than Russia did. However, they are not yet functional, remaining vaguely worded and without means of enforcement. To try to address these problems, Belarus recently adopted changes to its Criminal Code and licensing regulations.

The two issues of most seeming interest to the participants were internal compliance and interaction between non-governmental and governmental organizations. Industry representatives expressed an interest in training sessions, especially in internal compliance programs (ICP). There were questions to CITS representatives, as well as to the representatives from the Russian and Ukrainian Centers on Export Controls participating in the workshop, about basic requirements for ICP.

The non-governmental community of experts in the area of export control in Belarus needs to be expanded. The governmental agencies, like the Foreign Ministry and the Institute of National Security, have expressed an interest in establishing an NGO in Minsk which would deal with export con-

trol.

Participants raised questions about the impact of the emerging Russian-Belarus union on both countries' export control systems and their harmonization. Although Russia is a member of almost all the international regimes, Belarus just recently joined the NSG and is not a member of any other regime. Very little has been accomplished in putting Belarus' export control systems on the same footing as other regime members.

Belarus participants identified such problems as lack of equipment at customs and its failure to meet international norms and standards. Belarus has an open border with Poland (custom union) and is a member of the customs union with Russia. As a result, sensitive items could be transferred across the Belarus border without interference. In the past, Belarus had received equipment (custom equipment, radiometric and computer equipment), training, and legal and technical assistance from a number of Western countries. It has also been assisted in establishing pre-licensing and post-licensing control and licensing procedures. However, the assistance was recently cut off and remains suspended. Belarus experts specifically identified a need for assistance in internal compliance programs, pre-licensing and post-licensing control and licensing procedures, end-user and end-use identification, and transit control.

Because U.S. export control assistance to Belarus was abruptly suspended, the bulk of delivered hardware cannot be operated without a continuous supply of spare parts, maintenance service, and additional training. Cooperation with Russia is important but cannot substitute for technical assistance from U.S. sources. ■

MINATOM TRAINING PROGRAM

As part of its ongoing program at the Minatom Institute for Professional Training, a team from CITS traveled to Moscow in April and May to teach courses on material protection, control, and accounting (MPC&A), nonproliferation export controls, personnel, industrial management and business planning at nuclear facilities and defense conversion. The program is carried out jointly with the Minatom Institute and is funded by the U.S. Department of Energy. The main focus of the program is to ensure the sustainability of DOE's efforts in Russia and to promote the nonproliferation, safeguards, and security of nuclear materials there.

The program targets three groups of nuclear managers:

- mid- and top-level managers from Russian nuclear facilities where DOE has completed or is completing MPC&A upgrades;
- mid-level managers from the economics, personnel, and

planning departments of the same facilities; and

- participants of the Presidential Program for Young Managers, a Russian federally-funded project to educate and upgrade the skills of its pool of young industrial managers.

The April and May sessions are the second and third, respectively, installments of the program, which started in November 1999. It has been enthusiastically received and reviewed by the participants, the administration of Russian nuclear facilities, and the Minatom and DOE officials. The next training session is expected in October 2000. ■

WORKSHOPS IN UKRAINE

In May 2000, CITS co-sponsored two workshops in Kiev, organized by the newly created Kiev-based Research Center for Nonproliferation Studies. A workshop "*The Role of Non-Governmental Organizations and Media in Illicit Arms Exports Coverage*" was held on May 17. The total number of participants was 32. A group of leading Ukrainian journalists included Sergei Zgurets and Valentin Badrak, who cover arms trade issues for both Ukrainian media and Radio Liberty/Radio Free Europe. Representatives from Ukrainian, Russian, Belarussian, Kazakhs and U.S. non-governmental organizations took part in the workshop. Dr. Victor Zaborsky, CITS Senior Research Associate, made a presentation "The Role of U.S. NGOs in Improving Export Controls."

On May 19, a seminar "*Arms Trade and Problems of Export Controls*" for Ukrainian arms trading businesses took place. In addition to a large contingent from "Ukrspetsexport," a major state-run arms trading mediator, there were representatives from the military-industrial complex, including Malyshev Plant, Yuzhmash, and Artem Plant. The discussions centered on Ukrainian and U.S. experience with licensing and compliance with the multilateral export control regimes. Twenty-five people attended the seminar. The non-Ukrainian participants were the same as on the May 17 event. Dr. Zaborsky made a presentation "U.S. Export Control System – Should It be Fixed Or Replaced?"

The Research Center for Nonproliferation Studies, directed by Vladimir Chumak, has published proceedings (in Russian and Ukrainian) from the two workshops in a special issue of its quarterly publication *Nonproliferation and Arms Control*. ■

CENTER TEAM TRAVELS TO INDIA

During April-May 2000, Professor Gary Bertsch and Drs. Anupam Srivastava and Seema Gahlaut made a trip to India to pursue two primary objectives. One was to participate in a three-day international symposium, "Indo-US Partnership in Peace," (April 12-14) sponsored by the Manipal Academy of Higher Education (MAHE) in the southern Indian State of Karnataka. The symposium and the resultant *Manipal Declaration* noted the significant potential and need for deepening and widening Indo-U.S. relations in the coming decade, and the participating institutions/individuals agreed to pursue coordinated and policy-relevant activity toward that end.

The second objective was to raise awareness of the Center's India related work, as well as to consult with existing contacts for future work. As such, Center personnel traveled through five cities (Bombay, Manipal, Bangalore, Trivandrum, and New Delhi) where they met a wide range of senior policy officials and analysts. Meetings with the political leadership included the Vice President of India, Deputy Chairperson of the Upper House of the Parliament, ministers and top leaders of the ruling BJP party, leader of the Opposition Congress Party (Ms. Sonia Gandhi), former Prime Minister I.K. Gujral, and former Finance Minister, Dr. Manmohan Singh, among others. Meetings with the bureaucratic leadership included the Principal Scientific Advisor (PSA) to the government of India, Dr. Abdul Kalam, Executive Director of Technology Information Forecasting and Assessment Council, and Scientific Advisor to the Confederation of Indian Industry, Y.S. Rajan, chief of Indian Defense Research and Development Organization, Dr. V.K. Atre, and senior officials of the Ministries of External Affairs and Defense.

In addition, Professor Bertsch was interviewed for *AsiaNet* television, whose audience spans 55 million people across 23 countries. Drs. Srivastava and Gahlaut made presentations at the prestigious *National Defense College* and the *United Service Institution of India*. Dr. Srivastava also addressed a select gathering at the *India Development Foundation* which included the former foreign secretary, A.P. Venkateswaran.

The opinion leaders in India strongly encouraged the Center to undertake a wider range of research and policy-relevant work addressing common Indo-U.S. challenges and opportunities. Pursuant to that, the Center is working to launch an "India Initiative" that, with cooperation and support from the University of Georgia and the wider community, will embrace a range of activities intended to contribute to a closer bilateral relationship. ■

CITS-CSIS COOPERATION

Gary Bertsch and Richard Cupitt of CITS are co-chairing the Multilateral Export Control Regimes Working Group of a new project of the Center for Strategic and International Studies (CSIS) in Washington, DC. The CSIS project on "Technology and Security in a Networked World" is headed by a blue-ribbon commission co-chaired by Joe Nye, Bill Owen, Jim Schlesinger and Jim Woolsey. The working groups and Commission, of which Bertsch is also a member, will be meeting through the fall and winter to prepare a report outlining new directions for promoting both U.S. security and technological competitiveness in the 21st century. ■

A TRIP TO CUBA

Senior Research Associate Dr. Jonathan C. Benjamin-Alvarado visited Cuba on June 21-28. The purpose of this visit to Havana was to gain clearances from the appropriate government agencies and ministries to conduct a three year study of sustainable energy development in Cuba. During the trip Dr. Benjamin-Alvarado met with Dr. Fidel Castro Diaz-Balart of the Instituto Superior de Ciencia y Tecnologia Nuclear, Dr. Hugo Perez Rojas, Director of Grupo Fisica Teorica, Instituto Cibernetica, Matematica y Fisica, Dr. Ismael Clark Arxer, President of Cuban Academy of Sciences, Dr. Hugo Ponts Duarte, Ministerio de Economia y Planificacion, Centro de Estudios de Economia y Planificacion, Rosa Maria Vasallo, and Iroel Sanchez Espinosa of Instituto Cubano del Libro. Points of discussion included cooperation in research, international academic exchanges, and the establishment of nuclear safety working groups. ■

The Monitor

is published by the Center for International Trade and Security at the University of Georgia. The views and opinions expressed here do not necessarily state or reflect those of the University of Georgia or the editorial staff. *The Monitor* welcomes submissions to be considered for publication.

Center Director	• Gary Bertsch
Center Co-Director Emeritus	• Martin Hillenbrand
Associate Director for Research and Washington Liaison	• Richard Cupitt
Associate Director for NIS Projects and <i>Monitor</i> Executive Editor	• Igor Khripunov
Assistant Director for Research and Administration	• Michael Beck
<i>Monitor</i> Managing Editors	• Dmitriy Nikonov • Maria Katsva
Office Manager	• Melissa Oliva

The Center for International Trade and Security seeks to contribute to enlightened economic and security policies through its research, teaching, and service programs. Its activities are supported by the W. Alton Jones Foundation, the Carnegie Corporation of New York, the MacArthur Foundation, the Japan Foundation Center for Global Partnership, the Japan-United States Friendship Commission, the Chiang Ching-Kuo Foundation, the John Merck Fund, the National Council for Eurasian and East European Research, the Ploughshares Fund, the Rockefeller Foundation, the U.S. Institute of Peace, the University of Georgia, the U.S. Department of Energy, and others.

Translations of official documents in this publication, unless marked otherwise, are unofficial, and are published for the sole purpose of informing the readers of their content.

Center for International Trade and Security
The University of Georgia
204 Baldwin Hall, Athens, GA 30602-1615
telephone +(706) 542-2985; *fax* +(706) 542-2975
E-mail: cits@arches.uga.edu
WWW: <http://www.uga.edu/cits>

