WORLD NUCLEAR ASSOCIATION

Adapting export controls on nuclear technology and information transfer to the challenges of cyberspace

Supply Chain Working Group

Title: Adapting export controls on nuclear technology and information transfer to the challenges of cyberspace
Produced by: World Nuclear Association
Published: August 2019
Report No. 2019/003

Adapting export controls on nuclear technology and information transfer to the challenges of cyberspace

> *"Digital systems promise higher reliability, more functionality, better plant performance, additional diagnostic capabilities and many other advantages. But, of course, new digital systems also bring new challenges, including those related to nuclear safety and security."*
>
> Yukiya Amano, Former Director-General International Atomic Energy Agency[1]

This paper, originally produced as input to an industry outreach meeting held with government representatives from the Nuclear Suppliers Group (NSG), examines the challenges of controlling strategic nuclear technology and information in cyberspace and offers proposals aimed at improving the effectiveness and consistency of export controls internationally. 'Cyberspace' describes the domain of distributed and self-regulating computing, digital data storage and digitally encrypted telecommunication. The massive advances in information and communication technology (ICT) over recent decades have been called variously the Digital, Information, or Fourth (or Fifth) Technological Revolution.[2] Digital signals can represent, compress and store data without loss of quality on a colossal scale. We are already working with fifth generation portable computers and fifth generation cellular mobile communication networks. Digitalization is facilitating machine-learning, robotics and predictive analytics. It is revolutionizing manufacturing, plant operation and equipment servicing, not to mention energy distribution and household tasks.

The civil nuclear industry now relies on ICT systems for a host of functions just as other industries do. The 3-D models of nuclear facilities offer a wealth of detail on the make-up of structures, systems and components (SSCs) and their performance. Building information modelling allows the owner of a facility to assemble all the characteristics and information about it in one secure digital format.[3] Additive manufacturing techniques permit users of relatively simple extrusion or jetting devices to use 3-D digital models to create shapes by building up fine layers of self-bonding material (such as metal powders, plastics, or ceramics). The techniques can be applied to small components or even to build large structures. Each of these techniques relies upon Cloud computing to store the vast amount of data involved. To be sure, as the quotation from Yukiya Amano indicates, such ICT systems have potential vulnerabilities but it is important to recognize their security benefits as well. Encryption is an embedded feature of digital data storage and transmission and the information content is better protected than it ever was before.

Export controls on nuclear technologies grew up at a time when information was transmitted physically on paper and blueprints and through cables and

[1] IAEA Director-General's Statement at INDEX Conference on Nuclear Digital Experience held in Paris, France, on 26 June 2018 at <https://www.iaea.org/newscenter/statements/director-generals-statement-at-index-conference-on-nuclear-digital-experience>.

[2] The World Economic Forum has four industrial revolutions: i) industry and steam; ii) steel, oil and electricity; iii) digital; and iv) robotics, artificial intelligence, nanotechnology and biotechnology/genetic engineering; Carlota Perez, London School of Economics, distinguishes five technological revolutions as engines of growth: i) factories, mechanisation and water power; ii) steam power and railways; iii) steel and electricity; iv) oil, automobiles and mass production; and v) information and telecommunications.

[3] Models can be in 2-D (as in a traditional plan) to 6-D: that is, 3 dimensional, plus time or program information, plus cost information, plus facilities management information.

wires. Controlling access to the physical media that stored and transmitted information was in many ways a simpler task than it is today. It was therefore possible to license the transfer of information across borders on the basis that the information was delivered directly to authorized persons at the other end. Cyberspace has, however, changed the media of communication and export controls need to be adapted to remain fit-for-purpose.

In the 1970s large companies and government organizations ran their own mainframe computers but today they rely upon Cloud computing providers like Alibaba, Amazon, CROC, Google, IBM, i-Teco, Microsoft, Oracle, Salesforce and SAP. Cloud computing employs virtualization to allow customers to use proprietary application software, to run operating systems, to store data and develop their own bespoke software solutions and tools on the vendors' hardware and infrastructure[4] through a private or public wide area network (such as the Internet). The Cloud provides users with computing services more cost effectively than would be the case if they had to invest in their own hardware and software. Cloud computing vendors go to great lengths to protect their customers' data from intrusion and theft. However, the advantages the Cloud offers to transnational corporations in allowing access to corporate business systems from almost any location around the world also presents a real problem to the export control authorities. The key role played by Cloud computing providers in the chain of information transfer also raises issues with export control authorities.

Technology vendors in the civil nuclear energy business are internationally active and managing cross-border transactions is a core element of their activity. International partnerships with other global companies supplying engineering, procurement and construction (EPC) services, with original equipment manufacturers (OEMs) and professional and financial service providers are common features in nuclear power plant construction, operation and maintenance projects. Today's nuclear industry undertakes its business across multiple jurisdictions and information exchange across borders is an essential aspect of this activity.

Nuclear power plant operators share technical and performance information across borders through the World Association of Nuclear Operators (WANO), reactor user groups as well as within their corporate group. Much of the information shared in this way relates to maintaining the safety of nuclear power plants. In addition, reactor owners' groups also share information for improving the efficiency of operations, computer source codes and innovatory engineering.

It is sometimes alleged that the nuclear industry is behind the times because much of the reactor fleet is old. Nothing could be further from the truth. Nuclear power plant operators are involved in continual improvement both in terms of operating efficiency and safety. Generation II reactors, which form the bulk of the world's fleet, have been upgraded to operate with higher levels of safety and performance. In fact these two aspects of operation are linked because enhancing safety has a cost and this can sometimes only be absorbed if the nuclear power plant can reduce other operating costs through efficiency improvements given its need to sell electricity at the market price. (In regions where electricity prices have fallen as a result of cheap gas or renewable energy sources selling power for nothing, some nuclear power plant operators

[4] Cloud computing vendors own or manage the data centres, servers, backbone routers, fibre optic cables and uninterruptable power supplies that provide much of the physical infrastructure of cyberspace.

have chosen to halt operation altogether rather than invest in safety upgrades demanded by regulators.) The World Nuclear Association expects that further improvements in both safety and performance can be achieved at operating plants if the less well performing are permitted to catch-up with the best through cooperative fleet management on an international level. And this involves sharing technical data and know-how.

It is clear, therefore, that cyberspace presents export control authorities with particular challenges. Wide area networks can encompass several jurisdictions and digitally-coded technical information may potentially be accessed from almost any point around the world. Although The Cloud is a metaphor, it reflects the reality that sensitive technical information in cyberspace no longer exists at a single location and is diffuse. It is, of course, true that the infrastructure of the Internet or of private networks remains physical, although dispersed widely, and that the people involved in data transmission reside at particular locations, but they could be employed in several places or even work whilst on the move. Perhaps most importantly, however, organizations are legally established in a particular jurisdiction. The control of sensitive technical information in cyberspace needs to be considered in a different way; one that takes account of contemporary business operation.

Lastly, while cyberspace is vulnerable to unauthorized intrusion or surveillance by hackers for malicious purposes it is also a realm where counter-measures are developed and employed. Cybersecurity experts share their knowledge and techniques across borders, may design software that works in a similar way to a computer virus (executable software), and use penetration testing to uncover vulnerabilities in a customer's computer security system. Like transnational corporations, cybersecurity experts operate internationally and recognition of this fact has shaped discussions on information security within, for instance, the Wassenaar Arrangement that oversees export controls on conventional arms and dual-use goods and technologies.

1 Regulating cyberspace

Despite its relative novelty, cyberspace is subject to law and regulation at national and international levels.[5] The Council of Europe Convention on Cybercrime (2004), known as the Budapest Convention, and the International Code of Conduct for Information Security (2015) are the two main legal instruments so far devised, although each is backed by a distinct group of countries. The instruments seek to facilitate inter-governmental cooperation in safeguarding digital information and combatting the misuse of data and networks. Negotiations on an agreement on trade-related aspects of electronic commerce at the World Trade Organization (WTO) are expected during 2019.

The Budapest Convention has been accepted by 62 countries while the International Code of Conduct was put together by the six members of the Shanghai Cooperation Organization. All governments with nuclear power plants on their territory have signed one of the two instruments with the exception of Brazil, India, Iran, Mexico, Pakistan, South Korea and the Chinese province of Taiwan. In addition several major uranium producers are also parties to the instruments, including Australia, Kazakhstan and Uzbekistan, but excluding Namibia and Niger. There is also an overlap with countries participating in the Nuclear Suppliers Group (NSG) as illustrated in Figure 1. Once again almost all countries with nuclear power plants or uranium mines participate in the NSG, the main exceptions being Kyrgyzstan, India, Iran, Pakistan, Namibia, Niger, Tanzania, Tajikistan and Uzbekistan.

The two information security instruments are intended to facilitate international cooperation in combatting illegal activity in cyberspace while respecting human rights and the legitimate use of ICT.

Figure 1. Participation in the Nuclear Suppliers Group and multinational digital information security instruments

[5] Patryk Pawlak, *A Wild Wild Web? Law, norms, crime and politics in cyberspace*, Brief Issue paper, 23. July 2017: European Union Institute for Security Studies.

[6] NSG, *Guidelines for Nuclear Transfers*, IAEA INFCIRC/254/Rev.13/Part 1, 8 November 2016.

[7] IAEA, 2011, *Computer Security at Nuclear Facilities*, Nuclear Security Series No. 17, Vienna: International Atomic Energy Agency.

[8] Fratini Vergano European Lawyers, *Trade Perspectives*, 8 February 2019.

Articles 2 (2) and 2 (4) of the International Code of Conduct state:

> "Each State voluntarily subscribing to this Code of Conduct pledges … not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security; [and] …to cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds."

A further article (2 (9)) states:

> "All States must cooperate fully with other interested parties in encouraging a deeper understanding by all elements in society, including the private sector and civil-society institutions, of their responsibility to ensure information security, by means including the creation of a culture of information security and the provision of support for efforts to protect critical information infrastructure."

Article 23 of the Budapest Convention states:

> "The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

There exists, therefore, a strong commitment to international cooperation in relation to criminal activity in cyberspace and this includes 80 percent of countries with nuclear power plants.

The more recent information security instruments complement the well-established international regime for nuclear security. Under the Treaty on the Non-Proliferation of Nuclear Weapons (1970), the signatories have the right to participate in the fullest possible exchange of equipment, materials and scientific and technological information for the peaceful uses of atomic energy (Article IV), while prohibiting the transfer of nuclear weapons or other nuclear explosive devices either directly or indirectly (Articles I and II). The NSG issues guidance to governments on how to ensure that such transfers of equipment, materials, software and technology for peaceful use are not diverted to an unsafeguarded facility or activity and are physically protected.[6] The Convention on the Physical Protection of Nuclear Materials and Facilities as amended (2005) imposes obligations on its signatories to apply effective physical protection of certain nuclear materials but does not address the securing of strategic nuclear technology as such. Nevertheless, the guidance agreed by member states of the International Atomic Energy Agency (IAEA) and by the participating governments of the NSG provides a common world-wide framework to secure nuclear facilities and safeguard the technology, materials and equipment. This includes guidance on computer security.[7]

An agreement to regulate e-commerce is under negotiation by 76 member states of the WTO to make it safer and easier to do business online by guaranteeing recognition of electronic contracts and signatures, banning customs duties on electronic transactions and combating spam.[8] At present, tariffs are not levied on e-commerce transactions under a voluntary moratorium, although consumers can be charged a sales tax or value-added tax when purchasing software or an e-book. Should this policy on tariffs be made permanent it would mean that software and associated services (including 'software as a service' contracts entered into by Cloud computing providers) would be exempt from tariffs and, presumably, from any requirement to notify customs authorities of cross-border transactions involving software.

2 Current approaches to licensing intangibles for export

Technical information can be transmitted by various means, for instance, remote access to data platforms, by e-mail or through electronic and/or video/audio links. The multilateral regimes controlling the export of technology talk about technical data, technical assistance and software, but these are all, in fact, simply ways that information can be communicated. NSG Guidelines Parts 1 and 2 (2016 as corrected 2018) state:

> "Technical data" may take forms such as blueprints, plans, diagrams, models, formulae, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.
>
> "Technology" means specific information required for the "development", "production", or "use" of any item contained in the [Trigger] List. This information may take the form of "technical data" or "technical assistance".
>
> A "Programme" is a sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer.
>
> "Software" is a collection of one or more "programs" or "microprograms" fixed in any tangible medium of expression.

The export control regimes thus seek to control listed technology by controlling cross-border transfers of technical data, technical assistance and software. In the NSG Guidelines it is stated that the transfer of "technology" directly associated with any item in the Trigger 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".

Furthermore, the Guidelines state, the transfer of "software" directly associated with, especially designed or prepared for, the "development", "production" or "use" of any item in the Trigger List *will be subject to as great a degree of scrutiny and controls as will the item itself*, to the extent permitted by national legislation. For the purposes of implementation of the Guidelines for "software" transfers, suppliers should apply the same principles as for "technology" transfers.

Export control authorities first started to be concerned that Cloud computing services could result in export control violations in the late 2000s.[9] The European Union (EU) export control regulation states that an export includes:

> "transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community; it includes making available in an electronic form such software and technology to legal and natural persons and partnerships outside the Community."[10]

The EU Regulation of 2009 maintained the exact wording of the definition of technology found in the NSG Guidelines but introduced a

[9] John Villasenor, 2011, *Addressing export control in the age of Cloud computing*, Washington DC: Center for Technology Innovation at Brookings: p. 5.

[10] Council Regulation (EC) No: 428/2009, Setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items: Article 2 (2).

[11] Council Regulation (EC) No: 428/2009, Setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items: General technology Note: p. 20.

[12] Mark Bromley and Giovanna Maletta, 2018, *The challenge of software and technology transfers to non-proliferation efforts: Implementing and complying with export controls*, Stockholm International Peace Research Institute: pp. 22-23.

[13] European Council, Council Joint Action concerning the control of technical assistance related to certain military end-uses, *Official Journal of the European Communities*, L159, 30 June 2000: Article 1: p. 216.

[14] European Commission, Proposal for a Regulation of the European parliament and the Council: Setting up a Community regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items, COM (2016) 616, 28 September 2016: pp. 7 and 19.

[15] US Federal Register, Revisions to Definitions in the Export Administration Regulations, 15 CFR Parts 734, 740, 750 and 772, 81 (107), 3 June 2016, pp. 35593-35594. See also US Department of Commerce, Bureau of Information and Security, Export Administration Regulations, 27 December 2017; 15 CFR Part 734.20. Security boundaries should be controlled to permit only pre-authorized and verified access via gateways to a network, to the datasets, to the devices, applications and means of communication used to gain access, and to the recorded personal identity information of users. Boundary controllers should monitor the access and user behaviour within their perimeter.

[16] US Department of Energy, 2016, Guidance to the Revised Part 810 Regulations: Assistance to foreign atomic energy activities: p.12.

different form of words with respect to non-nuclear dual-use items. It stated: The export of "technology" which is required for the "development", "production" or "use" of [controlled] goods; and controls on technology do not apply to the minimum necessary information for patent applications.[11] This has been taken to imply that controls on technology should apply only if the information is detailed enough to allow the receiver to reproduce the dual-use item.[12] In another regulation relating to the control of dual-items for export, the EU defines technical assistance as "instruction, training, transmission of working knowledge or skills or consulting services".[13]

In 2016, the European Commission proposed to simplify the above definition by removing the words "to a destination outside the European Community; it includes making available in an electronic form such software and technology". The proposal was intended to facilitate "low-risk technology transfers, as they only become subject to control when the dual-use technology is made available to a person in a third country, which is in particular expected to facilitate the use of Cloud services".[14] It also advocated a general export authorization for intra-company transmission of software and technology taking place within the EU. The proposals were part of a package of modifications that await acceptance by the European Council and the European Parliament. If the proposals are accepted it would mean that the trigger for an export licence would be the status of the recipients of the data transferred (and not the country of destination) and those persons would have to be named on the export licence.

In other words, the export licensing criteria become 'who?' is the recipient and 'what?' information is being transferred, rather than 'where?' is the destination.

Currently, since the European Commission's recast of the regulation remains unapproved, the EU Regulation continues to require the licensing of both the recipient and the destination for an almost unlimited scope of information simply because it relates to a physical item on the Trigger List. Member States of the EU have the responsibility to implement the Regulation and the national export control authorities hold varying interpretations as to what the Regulation means in the context of their national laws.

The Ministry of Foreign Affairs of The Netherlands has, for instance, advised that export controlled information uploaded to a private Cloud (and only to a private Cloud) becomes an export when access is granted to someone who is outside of the country. All persons or entities having access to such controlled technology must be named on the export licence application, including system administrators and owners of a server or private Cloud service if they are able to read the data. Any data transfer involving controlled technology must be secured adequately using an appropriate encryption standard. It does not matter where a server is located as long as the Cloud computing provider does not have access to the controlled data, maintains security in compliance with the industry standard, and the data is encrypted end-to-end. In many cases the export of controlled technology falls under an EU general export authorisation.

The United States (US) Export Administration Regulations (EAR) were modified in 2016 to clarify that export controls on the technology related to dual-use items applied only to "transmitting or otherwise transferring" technical data and software to "foreign persons". The modification de-controlled transmission to another country provided that the technology, technical data or software was encrypted end-to-end to a specified standard. The encryption by the originator and the decryption by the receiver had to be undertaken within the two organizations' "security boundary" and that no third party has the ability to access and decrypt the encrypted data.[15] Thus a company based in the US can use Cloud computing and other means of electronic transmission (email, instant messaging, etc.) to transfer and store technology and software otherwise controlled by the EAR without facing export control requirements. Additionally US nationals located outside of the country are able to use secured remote access technology to access data on a US server without it being considered an export.

The encryption technology specified by the rules must meet or exceed Federal Information Processing Standard Publication 140-2 (FIPS PUB 140-2: 2002) and be supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current US National Institute for Standards and Technology publications, or other equally or more effective cryptographic means. The standard defines four levels of security that must be satisfied by the encryption process, with third party verification to ensure encryption products conform to the standard. The US standard is equivalent to the international standard ISO/IEC 19790: 2012 Security Requirements for Cryptographic Modules.

The EAR, which are administered by the Department of Commerce, do

not apply, however, to regulations administered by the US Department of Energy (DoE) and the Nuclear Regulatory Commission (NRC) in relation to the export of nuclear reactors and special nuclear materials (such as plutonium and enriched uranium). The DoE administered regulations are found in Title 10 of the Code of Federal Regulations Part 810 and these cover the export of non-sensitive nuclear technology, technical data and assistance. Part 810 was updated in 2015 to expand such exports under general licence to some 50 authorized destinations where the USA has agreements for civil nuclear cooperation and to the IAEA. Technology may be transferred to foreign nationals who are citizens of the authorized destination countries under a general licence but not to unauthorized countries. Under a general authorization the exporter must notify the DoE of any transfer but is not required to apply for prior permission. A specific authorization is also required for any provision of "sensitive nuclear technology" (enrichment, reprocessing of fuel, and heavy water production).

A specific authorization to transfer technology to a non-authorized destination may be granted so long as the country concerned has a safeguards agreement with the IAEA, including the 'additional protocol', and is adhering to NSG Guidelines and international nuclear safety conventions. There should also be a confidentiality agreement between the exporter and the end-user.[16]

The US regulations on nuclear technology transfer are silent on the use of Cloud computing and electronic media and in this regard they are out of line with the Department of Commerce regulations on other dual-use items. There is a clear difference in that the criteria for authorization in the Commerce Department's EAR are whether the end-user is a foreign person (who?) rather than the country of destination (where?), while the DoE regulation is based on permitted destinations plus nationality/citizenship (where and who?). Furthermore, the EAR allow for the transfer of technical data via servers and other physical infrastructure located in non-embargoed countries provided it is kept secure through encryption. Under the DoE regulations on nuclear technology, as they currently stand, there is no explicit approval to use Cloud computing and of using encrypted transmission but the onus is on the individual making the transfer to ensure that only the authorized recipient receives the information.

Lastly, it may be added that unlike the shipment of goods intangible transfers are less amenable to checks exercised by the customs authorities. An exporter of nuclear components who has neglected to obtain an export licence is likely to be identified as such at the border or other transhipment point. The same is not true in cyberspace.

[16] US Department of Energy, 2016, Guidance to the Revised Part 810 Regulations: Assistance to foreign atomic energy activities: p.12.

3 Proposals for consideration

The World Nuclear Association accepts that controls on strategic technologies are undoubtedly necessary since an attempt to acquire a weapon of mass destruction is going to require equipment, materials and knowledge of the technology; and this will in turn require technical data, technical assistance and computing power. This is the rationale for controlling each element as strictly as the other since all of them are important resources to a would-be proliferator. It would be irresponsible to argue that technical data, for example, should be de-controlled on the grounds that obtaining a blueprint of a nuclear weapon, as the Libyan government did in 2001, is insufficient to develop a nuclear weapon. The Stockholm International Peace Research Institute has pointed out that technical assistance is a key capability for weaponizing technologies and can be just as important as technical data and software.

On the other hand, some items on the Trigger List are more helpful to proliferation than others. A risk-informed approach allows for a ranking of dual-use technologies in terms of their usefulness in acquiring weapons of mass destruction, with, say, uranium enrichment carrying a greater proliferation risk than power reactor technology. In these cases an export licensing criterion of 'what?' appears more appropriate.

A further consideration balances the risk that a technology may pose against its value to society from peaceful applications. On a risk-reward basis, nuclear reactor technology poses a relatively low proliferation risk and a high peaceful-use value in terms of plentiful energy with low greenhouse gas emissions.

Imposing trade controls as a means to counter proliferation inflicts a larger economic cost onto society when a widely diffused and used technology with a relatively low proliferation-risk is subjected to export licensing. It suggests that alternative measures to counter the proliferation risk might be more cost-effective for society; for example, end-user controls to prevent diversion or misuse rather than controls on technology vendors, provided the latter maintained high standards of information security internally. Once again, the export licensing criterion is 'who?' is to be licensed.

The World Nuclear Association has argued that a global industry requires an effective export control regime where licences are issued on risk-based criteria. Figure 2 illustrates the model suggested. Under such an approach the export of components and complete power reactors should be made possible under general authorization, without prior individual licence, to another country that is a participating state in the NSG subject to notification being provided to the authorities of the exporting and importing countries concerned. Within free trade areas, such as the EU's single market, shipments should be notifiable but otherwise unrestricted.[19]

Nuclear fuel assemblies made of low-enriched uranium should not be subject to a requirement for licence approval prior to shipment between NSG participating states, as these states have accepted IAEA monitoring and most have also acceded to the Convention on the Physical Protection of Nuclear Materials and Facilities. There should be general authorization for low-enriched fuel exports with a simple reporting requirement to the export control authorities of the countries involved in the shipments.

Highly-enriched uranium, plutonium and some other nuclear materials,

[17] See Nuclear Threat Initiative <https://www.nti.org/learn/countries/libya/nuclear/> retrieved 31/01/2019.

[18] Mark Bromley and Giovanna Maletta, 2018, *The challenge of software and technology transfers to non-proliferation efforts: Implementing and complying with export controls*, Stockholm International Peace Research Institute: pp. 1 and 7-8.

[19] World Nuclear Association, 2018, *An effective export control regime for a global industry*, London: World Nuclear Association: p. 18.

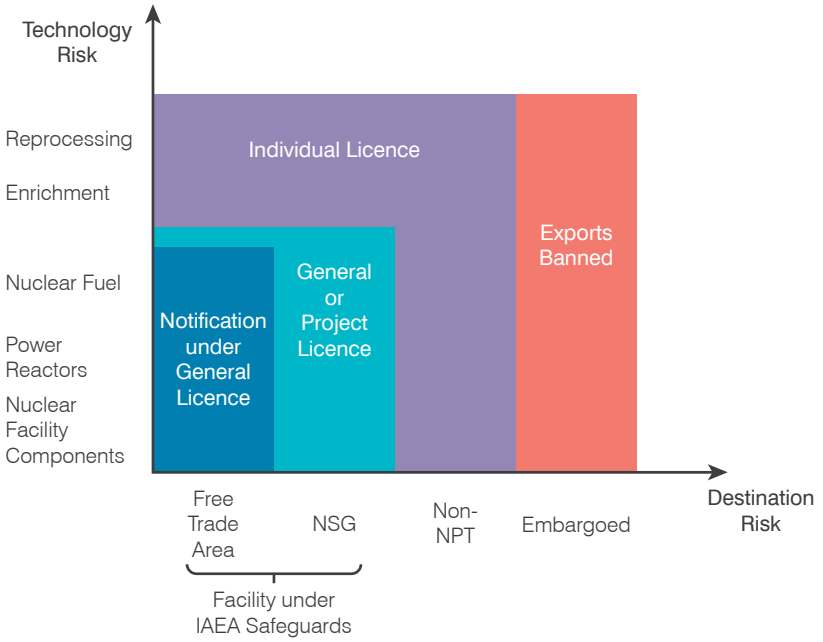

Figure 2. Model for a risk-based export control regime

and enrichment and reprocessing equipment, are associated with a higher proliferation risk. There is greater justification for licensing each transaction through an individual application to export these items.

With regards to intangible transfers of nuclear technology, the World Nuclear Association would like to see some further development, and possible codification, of good practice that would be more consistent and speed-up licensing. The following principles could be considered, for example:

Information stored in the Cloud is not considered an export unless and until it is accessed by a third party person or entity from another country, provided that:

a) Information in transit and information at rest is protected by a defined level of encryption;

b) The exporter has a knowledge and information security system that grades information and intellectual property according to its sensitivity, including whether the release of that information, data or design would allow another party to replicate the technology;

c) The exporter operates a user access management system to ensure that only authorised persons, such as employees and approved suppliers, can access and modify the information, even while travelling;

d) The exporter operates an information rights management system to protect sensitive information from unauthorized access through encryption, for example, so that the content of a file cannot be read or copied even if the file is stolen.

Information related to the safe operation of nuclear power reactors should be exempted from export control provided that the operator of the nuclear facility, who is licensed by the appropriate regulatory bodies for maintaining nuclear safety and

security, and the technology vendor have robust internal compliance systems with fully adequate documentation that may be audited by the export control authorities.

Good practice should be recognized by export control authorities, and companies that have adopted such practices could be granted general authorization to undertake export activities. For example, an export control authority could take into consideration the fact that an exporter had secured its "technology" (the technical data, software and knowledge for technical assistance) on the basis of sound information security criteria (for example, to the ISO/IEC 27001 and 27002: 2013 standard for Information Security Management and the Code of Practice for information security control). Providers of Cloud computing services contracted by the nuclear power plant owner or nuclear technology vendor would also have to demonstrate the requisite level of information security.

Were these principles to be established, the challenges facing intangible transfers in cyberspace are much reduced. Internal compliance programs are an absolute necessity for companies engaged in the export of controlled technology. The exercise of an appropriate level of information security is critical not simply to ensure that the company is not infringing export controls but also as a precaution against unauthorized intrusion into its computer systems. Prohibiting the private downloading of protected company information and use of the company's systems to surf the Internet by staff are just as important as making sure employees do not leave site with copies of sensitive designs stuffed into their briefcases, handbags or backpacks. In fact, a security-conscious workforce that uses Cloud computing services will be more secure because all transmissions can be tracked and a record kept. It is also easier to demonstrate compliance with licensing conditions within a comprehensively cyber-secure workplace.

The existing principle that the transfer of "technology" directly associated with any item in the Trigger List *will be subject to as great a degree of scrutiny and control as will the item itself*, would still apply. But under the export licence companies could decide on what information should be subject to which level of security controls, preferably on the basis of additional NSG guidance. The advantage for companies and organizations holding nuclear technology would be that their general licence regarding reactor components would also cover the associated intangibles and only a small portion of that information would have to be controlled to the highest level of security. It would permit employees, partner organizations and sub-contractors to access a wide range of information stored in the Cloud on the basis of normal commercial security arrangements.

It should also be mentioned that such general authorization of exporters to conduct their business would provide them with greater freedom to engage with their potential customers and suppliers, so that, for example, they could respond to calls for tender without a requirement to obtain an individual licence beforehand.

The large overlap between NSG participating states and states which have ratified international conventions on physical protection and information security means that individual export licences would only be necessary for a small number of countries remaining outside these conventions and the current multilateral control regime for nuclear technology. There would be an incentive for these states to sign the requisite agreements and the reactor vendors would be likely to encourage these governments to do so if export opportunities arose.

4 Conclusions

In summary, this paper proposes a shift of approach in the exercise of trade controls over strategic nuclear technology. It would be more effective to focus on the 'who?' and the 'what?' and to reduce the 'where?' criterion to a much smaller number of countries. With the advances in ICT and the existence of Cloud computing, information has become diffuse and potentially accessible from almost any location, so 'where?' is an outmoded trigger. However, information is now encrypted in generally secure formats. There are, to be sure, vulnerabilities, but at the same time there are massive benefits to be gained by companies and society. Instead of trying to license the information we should be aiming to regulate and monitor the users who can access it ('who?'). It demands that high standards of information security are applied by companies, with regulatory verification, and that malpractices are detected and prosecuted through the policing and justice system. Companies will also have to undertake an appropriate degree of due diligence to ensure that their customers and partners are bona fide.

Such a shift of approach fits well with the proposals advanced here for more general reform of the multilateral export control regime as it applies to the nuclear energy sector. Export control authorities could adapt the Authorized Economic Operator system used in the import of goods by the customs authorities to fit their requirements in controlling exports. It would permit governments to specify criteria for information security at nuclear power plant operators, and by nuclear technology vendors and their suppliers. Nuclear operators are already licensed in respect of their activities to ensure safety and security and in the safeguarding of nuclear materials. Adapting the licensing of nuclear trade by permitting a greater degree of general licensing does not imply that the industry will be less regulated. Arguably the shift in approach will mean more effective regulation as the control regime evolves to take account of the move of business activities into cyberspace.

Last year, at the first outreach event organized by the NSG with the nuclear industry, the World Nuclear Association and WANO raised the topic of general export control reform and the issues associated with controlling information in the Cloud. The ideas presented here have developed from those earlier proposals, where we suggested that the dialogue be deepened and widened. We recognize that reforms to the multilateral export control regime covering nuclear technology cannot be attempted without the involvement of other regimes and agencies. Specifically we put forward the suggestion that a wider dialogue might be organized by the International Framework for Nuclear Energy Cooperation (IFNEC) and bring together representatives of the IAEA, the Wassenaar Arrangement, the World Customs Organization and other relevant international agencies. We are grateful for the dialogue opportunity offered at this meeting and hope that this paper provides a good starting point for the discussions.

World Nuclear Association
Tower House
10 Southampton Street
London WC2E 7HA
United Kingdom

+44 (0)20 7451 1520
www.world-nuclear.org
info@world-nuclear.org

Adapting export controls on nuclear technology and information transfer to the challenges of cyberspace tackles the question of how best to control information in the age of Cloud computing and digitalization. The paper proposes to shift the focus in export control from 'where' to 'who' and 'what' technical information is licensed for electronic transfer. High standards of information security must be applied by companies, with regulatory verification, and companies must exercise an appropriate degree of due diligence to ensure that their customers and partners are bona fide.

The World Nuclear Association is the international organization supporting the people, technology and enterprises that comprise the global nuclear industry.

Adapting export controls on nuclear technology and information transfer to the challenges of cyberspace