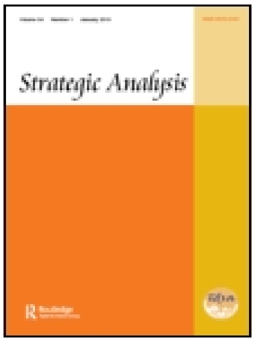

Routledge
Taylor & Francis Group

Strategic Analysis

ISSN: 0970-0161 (Print) 1754-0054 (Online) Journal homepage: http://www.tandfonline.com/loi/rsan20

Sensitive Nuclear Information: Challenges and Options for Control

Wyn Q. Bowen & Christopher Hobbs

To cite this article: Wyn Q. Bowen & Christopher Hobbs (2014) Sensitive Nuclear Information: Challenges and Options for Control, Strategic Analysis, 38:2, 217-229, DOI: 10.1080/09700161.2014.884441

To link to this article: http://dx.doi.org/10.1080/09700161.2014.884441

Published online: 19 Mar 2014.

Submit your article to this journal

Article views: 237

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=rsan20

Download by: [Masarykova Univerzita v Brne] **Date:** 13 March 2016, At: 15:57

Strategic Analysis, 2014
Vol. 38, No. 2, 217–229, http://dx.doi.org/10.1080/09700161.2014.884441

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

Sensitive Nuclear Information: Challenges and Options for Control

Wyn Q. Bowen and Christopher Hobbs

Abstract: This article starts by discussing sensitive nuclear information and how malicious non-state actors could exploit this to facilitate acts of nuclear terror. Our analysis shows that there is a significant information security challenge in this area due to the diversity of sensitive information, the different communities within which it resides and the range of mechanisms by which it could be transferred. We then turn our attention to assessing different steps that could be taken to protect sensitive nuclear information. Here there are limits to the effectiveness of international instruments and national laws and consequently bottom-up initiatives designed to promote responsible self-governance should be developed and supported.

Introduction

To date, international 'nuclear security'[1] measures and policy instruments have largely focused on securing fissile and other radioactive materials, onsite and in transport, both through improving physical protection systems and recovering material outside of regulatory control. In contrast, protecting non-physical or intangible aspects—such as sensitive nuclear information and its transfer—have been relatively neglected in terms of policy measures and instruments. However, notable and focused exceptions include the Science Centres in Russia and Ukraine which have sought to redirect former weapons personnel to work on civil projects with the aim of reducing their incentives to sell or share sensitive weapons information and knowledge. This relative lack of attention is a significant gap in the nuclear security framework as sensitive information, if accessed by unauthorised individuals, can serve to significantly reduce the barriers to nuclear terrorism.[2] Relevant information exists in a wide variety of domains and could be used by non-state actors to defeat security systems protecting fissile and radiological materials; in the design, manufacture and/or delivery of an improvised nuclear device (IND) or a radiological weapon; and to plan and launch attacks against nuclear or radiological facilities.

The policy gap was recognised politically at the second Nuclear Security Summit (NSS) in Seoul in March 2012 when information security was identified as one of the 11 areas of priority and importance within the summit communiqué.[3] In addition, many of the participating governments signed a 'Multinational Statement on Nuclear Information Security'. The statement was the outcome of a work package on securing sensitive nuclear information led by the UK government following the inaugural NSS in Washington, DC, in April 2010. Among other things, the statement politically committed

Dr. Wyn Q. Bowen is Professor of International Security and Director of Research in the Defence Studies Department, King's College London.
Dr. Christopher Hobbs is Lecturer in Science and Security in the Department of War Studies, King's College London.

© 2014 Institute for Defence Studies and Analyses

the signatories to 'developing and strengthening' their 'national measures, arrangements and capacity for the effective management and security of such information'.[4]

This article discusses the different types of sensitive information relevant to nuclear terrorism, examining where it resides and how it might be transferred to non-state actors. Consideration is given to explicit and tacit knowledge in nuclear weapons programmes, the civil nuclear industry and within academic and research communities. The second part of the article then considers initiatives that have been, and could potentially be, developed to enhance nuclear information security.

The bulk of the research for this article was conducted in 2011 for a project in support of the UK government's work on protecting sensitive nuclear information ahead of the 2012 NSS.[5] It should be noted that nothing in this article should be construed as representing the views of the British government.

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

Sensitive nuclear information

It is important to begin framing the issue of sensitive nuclear information by differentiating between two types of knowledge: explicit and tacit.

Explicit and tacit knowledge

Explicit knowledge encompasses 'information or instructions that can be formulated in words or symbols and, therefore, can be stored, copied, and transferred by impersonal means, such as in written documents or computer files'.[6] Jennex and Zyngier note that explicit knowledge 'can be directly expressed by knowledge representations and is commonly known as structured knowledge'.[7] An example here would involve documentation related to the security plans and security regime at a civil or military nuclear facility[8] which will be subject to change over time. To retain value for security practitioners, or individuals with malign intent, access to the most up-to-date version of such documentation is obviously going to be very important.

Tacit knowledge is developed through the process of doing—working knowledge—and so it is more difficult than explicit knowledge to transfer to others. As MacKenzie and Spinardi argue, it is 'knowledge that has not been (and perhaps cannot be) formulated explicitly and, therefore, cannot effectively be stored or transferred entirely by impersonal means'.[9] Collins describes tacit knowledge as 'knowledge or abilities that can be passed between scientists by personal contact but cannot be, or have not been set out or passed on in formulae, diagrams, or verbal descriptions and instructions for action'.[10] Of course, the development, possession and transfer of tacit knowledge are not just confined to the scientific community and are relevant to all professions and activities. A frequently used analogy relates to riding a bike:

> Most of us, for example, know perfectly well how to ride a bicycle yet would find it impossible to put into words how we do so. There are (to our knowledge) no textbooks of bicycle riding, and when children are taught to ride, they are not given long lists of written or verbal instructions. Instead, someone demonstrates what to do and encourages them in the inevitably slow and error-ridden process of learning for themselves.[11]

A distinction has been made between two different types of tacit knowledge: 'personal tacit knowledge' and 'communal tacit knowledge'. In the context of bio-security, for example, Tucker has noted that a bioterrorist would need to acquire both types where personal tacit knowledge 'refers to hands-on laboratory skills developed by working

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

with biological agents and specialized equipment', while communal tacit knowledge 'derives from close working relationships with specialists from various disciplines'.[12]

The distinction between explicit and tacit is important when it comes to framing the challenge of protecting nuclear security information. Explicit knowledge might come in the form of nuclear weapon blueprints or a line diagram illustrating the layout of a civil nuclear facility. However, if tacit knowledge was also available to supplement the explicit knowledge in both of these scenarios, then the security problem increases significantly. For example, the significance of blueprints will greatly increase if a terrorist group can recruit a technician, or technicians, with experience of working on particular elements of warhead manufacture. Similarly, a security guard's detailed understanding of the day-to-day operation of a civil nuclear facility would give major added value to a diagram illustrating its layout.

Furthermore, while it may be possible for terrorists to design, build and deliver an IND based on explicit knowledge alone, it is clear that harnessing tacit knowledge would provide a short cut and allow for significant savings in terms of time, effort and resources. For example, if a terrorist group only has access to a small amount of fissile material, it cannot afford to make mistakes or to be wasteful (through failed experiments, for example) and so the acquisition of existing tacit knowledge—for example related to machining nuclear materials—is likely to be hugely important. As such, protecting both forms of knowledge is clearly central to the concept of nuclear information security.

State-level nuclear weapons programmes

Within states with either current or past nuclear weapons programmes exists knowledge that relates directly to the design, manufacture and delivery of such weapons, and data connected with the locations and physical properties of special nuclear and related materials. Schaper offers some fine-grained examples of critical knowledge related to weapons. For example, explicit knowledge of 'the chemical composition of pit material' is crucial as 'small amounts of alloys can alter the physical properties of the pit metal' and 'facilitate its machining, affect its phase stability or its corrosiveness'. Another example offered relates to the 'details of the arrangement of the conventional explosives' for a weapon.[13]

A RAND report on the former Soviet Union deconstructs where this sensitive nuclear weapons knowledge is likely to exist, presenting a typology of individuals 'that are in the [NBC weapons] complexes and the knowledge they possess that would be useful to states or terrorist groups seeking to acquire nuclear, biological, or chemical weapons or the know-how to develop their own weapons':

RAND Typology[14]	Description
Type I	'Senior facility managers or chief scientists who are most likely to have an end-to-end knowledge of the materials and processes needed to develop NBC weapons capabilities'.
Type II	'Scientists and engineers with detailed knowledge and experience in specific aspects of the weapons development process. Their narrow, but important, knowledge could involve the weaponisation process, component design, plutonium or uranium metallurgy, the production of weapons-grade materials, or testing methods'.

(*Continued*)

(*Continued*)

RAND Typology[14]	Description
Type III	A 'larger group of potentially significant personnel' including skilled technicians 'who possess the actual know-how for achieving the desired results and products'. For example, 'they might have practical knowledge of the technologies and techniques for manufacturing nuclear pits…'
Type IV	'Administrative and security personnel who are likely to possess sensitive information about the facilities or institutes in which they work and the Types I, II, and III personnel found at those facilities or institutes'. Such people could help to identify where nuclear materials, and with whom sensitive knowledge, resides at a facility, the opportunities that might exist for recruiting individuals with specialist knowledge, and how to gain access.
Type V	'Former employees and retired personnel who are a proliferation risk if they possess knowledge on programs of interest to proliferants'. For example, such individuals could provide a link to current employees potentially willing to provide explicit and tacit knowledge 'through a trusted former colleague'.

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

Types I, II and III 'are likely to be concentrated in the research and production facilities' for nuclear weapons, the 'facilities that produce' nuclear materials and also, but not as significantly, 'at facilities responsible for weapons or material storage or demilitarization, such as nuclear warhead disassembly facilities'. It is noted that 'a nuclear weapons program requires expertise that is widely distributed among a larger, more specialized workforce' than for biological and chemical weapons.[15]

Perhaps the key facet of Types IV and V is the 'enabling information of interest' they possess of relevance to proliferators, whether these are state or non-state actors, and which could 'substantially improve those parties' chances of successfully finding and acquiring the weapons-critical expertise or information they are seeking'.[16]

Importantly, the RAND report notes that non-state actors will probably be 'satisfied with crude capabilities' relative to the requirements of state-level actors. In short, 'a terrorist group needs basic materials and skills to make a simple fission device that will achieve the group's goals'. Obviously, this can be realised without the much more challenging and sophisticated capabilities needed to develop a 'credible nuclear deterrent'. More specifically, 'if a terrorist group is able to acquire a stolen weapon, it will need only access to technicians or bomb designers who know enough to detonate the device'. Moreover, if the group is seeking to build an IND then it 'will need fissile materials, machining equipment, a simple weapon design, and a few technicians with the skills to work the nuclear material, fit the explosives, and assemble the device'. Consequently, 'a terrorist group will be most interested in nuclear materials, Type III technicians, and possibly weapons designers'.[17]

Civil nuclear industry

Beyond weapons-critical knowledge there is evidently a great deal of explicit and tacit knowledge residing in the civil nuclear sector. This knowledge could be exploited for terrorist purposes, whether this relates to the acquisition of nuclear material or to the security of a nuclear facility or transport that may be the target of a sabotage attack.

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

As the International Atomic Energy Agency (IAEA) notes, 'Nuclear organizations deal with large amounts of information and, a large proportion of that, may be of a sensitive nature: from details of physical protection plans to systems controlling reactor operations there are many examples available'.[18] While this section focuses on civil nuclear security, the material covered is equally applicable, of course, to the security of military nuclear sites.

In its 2005 publication 'Finding a Balance', the UK's Office of Civil Nuclear Security (OCNS) provided important insight into categories of information that need to be protected in these respects.[19] There is insufficient space here to cover all 14 categories but it is informative to highlight one area to demonstrate the types of sensitive knowledge that need to be protected. In terms of the 'Security of Nuclear Material and Facilities' category, for instance, various elements of information should be considered sensitive because they would be of utility to terrorist groups planning to attack a site by revealing locations of materials, details of protective measures that are in place and any 'assessed vulnerabilities' that may exist. Specific examples here might include security plans with 'detailed descriptions of the security regime in place at a site and precise detail of where within the site nuclear material is stored and details of other areas vital to the site', and 'security procedures for the issue, receipt and control of stock; names of authorised key holders; arrangements for monitoring and guarding', among other things.[20]

In addition to providing information that could facilitate a sabotage attack or the theft of nuclear material, the civil nuclear sector 'can provide crucial experience in matters such as the chemistry, metallurgy, handling, and machining of fissile materials and also in neutronics', all of which may be relevant to the design and construction of an IND.[21] As Schaper notes, 'Specialists who are able to work with the neutronics theory in order to design reactor cores are equally able to develop codes that describe the criticality, neutron distribution, and energy release in compressed spheres'.[22] Here explicit and tacit knowledge accumulated in a civil context could be transferred after a period of inculcation into a nuclear weapons programme.

Research and academic communities

Technical knowledge and skills relevant to the development of an IND or a radiological weapon also exists within certain parts of the academic and research communities, including scientists and engineers working in non-nuclear areas, such as metallurgy, detonics and explosives or computer modelling and simulation. For example, in the case of an IND, knowledge of electrical and electronic engineering is relevant 'for the design and construction of detonation circuitry' for the more sophisticated 'implosion' method, as is the field of detonics because of the requirement to achieve explosions and 'blast waves of particular shapes'.[23]

Although such individuals working at universities or research institutes may have never worked on a weapons programme, they are experienced in carrying out original research and applying their knowledge to unfamiliar areas. As described by Dallas, an individual qualifying with a Masters or Doctoral degree 'not only knows how to operate and analyse a system, she knows how to reconstruct it, modify it and experiment on it'.[24] The ability to innovate means that research scientists or engineers following a period of experimentation have the potential to be able to apply their knowledge to the construction of nuclear or radiological weapons. Zimmerman and Lewis estimate that a physics team (without any prior nuclear weapons knowledge) consisting of a senior physicist and two post-doctoral physicists could ‘render the design (of an IND) in three to six months’.[25] Here it is important to note that communities containing research-trained scientists and engineers with ‘dual-use’ knowledge of utility to non-state actors interested in performing acts of nuclear terrorism exist in states without advanced civil nuclear programmes or nuclear weapons.

Transferring sensitive information to terrorists

The Nuclear Suppliers Group and related export control provisions have long defined intangible technology transfer (ITT) to include the fax, the internet, email and conversations between individuals whether these occur in person or via the phone/ internet.[26] Timothy Clinton argues that there are two dimensions to ITT: the transfer of explicit knowledge such as ‘technical data in non-physical form’, for example ‘blueprints, schematics and diagrams’ using the internet, fax and so on; and the ‘transfer of knowledge as technical assistance’, whether this comes in the form of ‘instruction, skills training or consulting’, i.e. tacit knowledge.[27] In terms of the former, the internet allows an individual or company in one country to ‘transfer strategic technology’ ‘many thousands of kilometres away’ in an instant.[28] For the latter, successful transfer might only take place after a prolonged period of face-to-face interaction. Although developed in the counter-proliferation context, these distinctions are equally valid in describing how transfer of sensitive nuclear knowledge might take place from the aforementioned communities to non-state actors.

Transfer mechanisms can be further deconstructed into witting and unwitting. In witting transfer an individual working within an organisation containing sensitive nuclear knowledge would pass such information to a malicious external actor. Such individuals may be motivated by financial, ideological or other reasons and could be implanted by terrorist groups, coerced or blackmailed into divulging sensitive information. The threat posed by the ‘insider’ is particularly dangerous because they are ‘able to take advantage of their access rights and knowledge of a facility, as well as their authority over staff, to bypass dedicated security measures’.[29] They are also more likely than a purely external adversary to be able to hide their tracks and so carry out a prolonged as opposed to an abrupt theft of sensitive information. In the physical realm there have been numerous examples where technicians, scientists, guards and managers, acting individually or in collusion, have utilised their privileged access, authority and knowledge to circumvent security systems and smuggle nuclear materials out from both civil and military facilities.[30]

Although incidences involving cyber insiders within the nuclear enterprise have not been widely reported, there are examples from other industries. In 2005 Yonggang Min, a research chemist in DuPont, used his privileged access to the company’s electronic data library to download 22,000 sensitive proprietary documents in advance of taking up a position at a rival firm.[31] Potential cyber insiders are not just confined to scientific and technical staff, according to a study by Shaw et al. Within a workforce, IT professionals are a particularly vulnerable sub-group, due to the following common personal and cultural attributes: introversion; ethical ‘flexibility’; minimal organisational loyalty; sense of entitlement; and lack of empathy.[32] It should also be noted that insiders do not necessarily need to transfer sensitive knowledge in order to carry out acts of nuclear terrorism. Instead they could choose to personally exploit such information to launch a sabotage attack. In 1982 Rodney Wilkinson, a temporary

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

nuclear safety worker, smuggled limpet mines into the Koeberg nuclear power plant in South Africa while it was under construction, using his inside access and knowledge to place them on the reactor heads and several other targets.[33] Their subsequent detonation on December 18 is estimated to have caused more than $50 million worth of damage, delaying the commissioning of the plant by 18 months.

By contrast, in unwitting transfer situations individuals may be unaware that the information they hold is sensitive and inadvertently transfer this to a wider audience. An illustrative example involves the US Government Printing Office (GPO) posting on its website in 2009 a draft document 'containing sensitive details about hundreds of civilian nuclear sites across the country'. The document was put together for the IAEA and 'contained descriptions of sensitive civilian sites, including the locations of facilities that store enriched uranium and other materials used in nuclear weapons'. The document was removed from the website after being posted for one day when the GPO received inquiries from the media.[34] The unwitting transfer of sensitive knowledge would seem particularly relevant for research scientists and engineers, with studies suggesting that there exists a widespread lack of awareness in individuals within these communities as to how their specialist knowledge could be misused.[35] Here unwitting transfer could take place in the classroom, a laboratory or a meeting/demonstration room. A relevant example might be a 'former government scientist working as a consultant to a foreign entity'.[36] Alternatively it might involve the wider dissemination of sensitive information through the publication of research findings. Concerns over this particular transfer mechanism were raised recently in the biosciences following the submission of research papers on the transmissibility of H5N1 ('bird flu') in mammals.[37]

Protecting sensitive nuclear information: creating a web of prevention

It is clear that because of the diversity of sensitive information types, the different communities within which they reside and the variety of methods by which transfer to terrorist groups could take place, that there can be no single approach to nuclear information security. However, there is a range of steps that could be taken at the international, national and organisational levels to further protect sensitive nuclear information. Although the impact of specific measures will vary across the different nuclear knowledge communities, if implemented together they can form at least a partial web of prevention and help to further raise the barriers to nuclear terrorism. These measures, together with recent efforts in this area, are discussed below.

International legal instruments: emphasising information security and increasing membership

The nuclear security regime consists of a patchwork of binding instruments, ad hoc initiatives and international organisations. Legally binding international instruments in this area tend to be limited in scope or membership, lacking in effective verification provisions and focused primarily on the physical protection of nuclear material. For example, the Convention on the Physical Protection of Nuclear Material (CPPNM), currently limited to civil material in international transport, specifies different categories of nuclear material and corresponding protection levels but does not do the same for sensitive information.[38] However, the Amendment to the CPPNM, agreed in 2005, both extends the scope of the convention to civil material in domestic storage

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

and transport, and calls on states to 'establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities'.[39] However, the amendment is not yet in force and requires two-thirds of the state parties to ratify it. As of September 2013, just over half had done so.[40]

In contrast, the International Convention on the Suppression of Acts of Nuclear Terrorism (ICSANT) is wider ranging in scope, covering nuclear and radiological materials and facilities used for both military and civil purposes. It also contains reference to the transfer of sensitive nuclear security knowledge, calling on states to include 'measures to prohibit in their territories illegal activities of persons, groups and organisations … to knowingly provide technical assistance or information' to terrorist groups.[41] However, it does not go so far as to specify principles or specific steps for the protection of sensitive nuclear information. Membership of ICSANT is also limited, with only 88 state parties as of September 2013.

Considering the lack of international legal coverage for nuclear information security, it might appear prudent for the international community to focus efforts on the negotiation of a new international convention focused on protecting nuclear security sensitive information. However, there is currently little appetite on the part of many states for 'new instruments that impose additional obligations related to the use of nuclear energy'.[42] Consequently, at least in the short to medium term, it would seem prudent to focus on emphasising information security provisions within existing nuclear security relevant treaties, ratifying the amendment to the CPPNM and increasing membership of ICSANT. That said, a nuclear security 'event' would likely change this situation rather dramatically. Hence, it may also make sense to formulate in parallel the basis of such a convention so that something can be put in place quickly if the current political-security context changes.

Promoting adherence to information security guidance

Moving beyond formal regulation, the IAEA has produced a number of nuclear security guidance documents, such as recommendations for the physical protection of nuclear material (INFCIRC/225), which has become widely recognised as the international standard for the protection of nuclear material and facilities against non-state actors. Having undergone a major revision in 2011, INFCIRC/225 now emphasises the fundamental information security principle of 'confidentiality' and the need for states to take a 'graded approach' in specifying 'what information needs to be protected and how it should be protected'.[43] It also places greater emphasis on incorporating 'insiders' into threat assessment, although it stops short of recommending the use of specific measures such as vetting and human reliability programmes. That said, INFCIRC/225 remains primarily focused on protection against physical attacks, containing over 60 recommendations addressing guards and response forces and just a handful of references to sensitive nuclear information. Consequently, the IAEA should consider placing a greater emphasis on nuclear information security in the next revision.

Information security also features prominently in the IAEA Fundamentals Document, the 'Objective and Essential Elements of a State's Nuclear Security Regime', published in 2013, identifying the 'establishment of regulations and requirements for protecting the confidentiality of sensitive information and for protecting sensitive information assets' as one of the fundamental 'legislative and regulatory

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

framework, and associated administrative measures, to govern the nuclear security regime'.[44] More specific guidance on implementation is provided in the IAEA technical documents, 'Computer Security at Nuclear Facilities', 'Preventive and Protective Measures against Insider Threats' and 'Nuclear Security Culture'.[45]

Although not legally binding, states should commit to incorporating international guidance on nuclear information security into their national laws and practices. Here the IAEA can play a supporting role through the range of nuclear security evaluation and advisory services that it offers.[46] In turn, the international community must support the IAEA in these activities by providing funds earmarked for the performance of advisory services, with a particular focus on information security.

Increased sharing of certain nuclear security relevant information

Although the focus of this article has been largely on information protection, sharing certain nuclear security relevant information can also serve to enhance security measures and practices. However, sharing nuclear related information must be balanced against the risk of assisting groups interested in carrying out acts of nuclear terror. For example, providing lists of the key technologies and types of knowledge that could be used in the development of an IND might assist in enhancing the awareness of those in academia and industry about what needs to be protected, but it also carries with it the risk that such lists will get into the hands of terrorists and provide roadmaps ripe for exploitation. In the civil nuclear sector the UK Office of Civil Nuclear Security (OCNS) has noted that, 'It may seem paradoxical to identify publicly the types of information that could be used by terrorists. But the balance of advantage is in increasing awareness. In any case, there is nothing sensitive about, for example, stating that information about the quantities and whereabouts of plutonium is sensitive. It is the actual information that is sensitive'.[47]

An important aspect of this security is the protection of information about civil nuclear material and operations and, of course, information about security measures. However, such knowledge and information is also a necessary, often essential, part of running the business. Some information may need to be available to a large number of people. Not all of these are part of the industry, for example planners, police and so on. Members of the public may also have a legitimate interest in information about nuclear facilities and operations. The problem is how to reconcile these apparently conflicting requirements. How can information be made available to those who need it while keeping it from those who could take advantage of it for their own malign ends? Few would advocate total openness of all nuclear related information. But if some knowledge is to be restricted, how do you decide what that is, to whom it should be restricted, and how do you ensure that they are able to keep it secure?[48]

Striking the optimum balance between sharing knowledge to enhance security measures and practices and ensuring that such information does not get into the hands of terrorists is evidently one of the key challenges in the context of nuclear information security. At present it would appear that this balance is weighted very much towards the restriction of information. This stems from a pre-existing culture of secrecy in the nuclear sector because of the strategic nature of nuclear technology. However, arguments in favour of sharing more information can be made by drawing on the experiences of other industries such as the financial sector where banks share information on incidences of fraud. Moving, at least partially, towards the sharing end of the spectrum could therefore enhance nuclear security. Here the World Institute for

Nuclear Security (WINS) has demonstrated how within the nuclear industry it is possible to share information across a wide range of nuclear security areas, via the holding of international workshops and the publication of Best Practice Guides (BPGs), including: ‘Human Reliability as a Factor in Nuclear Security’, ‘Security of IT and IC Systems at Nuclear Facilities’, ‘Managing Internal Threats’ and ‘Nuclear Security Culture’.[49]

Increased focus on ‘bottom-up’ approaches

In addition to incorporating information security provisions into states’ national laws and corresponding regulations for the nuclear industry, it is important to consider how to promote responsible self-governance in nuclear security from the ‘bottom up’. This is particularly pertinent in research and academia, communities that have been established to ‘proliferate’ new knowledge and where there exists little awareness of the threat posed by nuclear terrorism. These are also communities where increased formal regulation would likely be difficult to implement due, for instance, to concerns as to how this might impact on academic freedoms. In this environment more effective approaches could include the development of non-binding codes of conduct and the launch of new nuclear security education and training programmes. If successful, these initiatives would have the benefit of reducing the risk of unwitting transfer of sensitive nuclear information, both by raising awareness among scientists and engineers that the information they hold could assist non-state actors in carrying out acts of nuclear terror, and providing guidance on how it could be safely disseminated.

In exploring such approaches it is useful to draw lessons from the biosciences. Due to the intrinsically ‘dual-use’ nature of biotechnology, where knowledge and skills used for the purposes of drug development and production can readily be used in the manufacture of pathogens, the biosecurity community has long focused its efforts on securing the human factor within life-sciences research and teaching. Recent initiatives include a biosecurity Code of Conduct (CoC), developed by the Royal Netherlands Academy of Arts and Sciences in 2007.[50] This code, which is aimed at both individuals and organisations (including scientists, research funders and journal editors), outlines the threat posed by the ‘dual-use’ nature of the biosciences, provides guidance on publication policy and the broader communication of research findings and suggests appropriate levels of accountability and oversight. It is designed to raise awareness and encourage individuals to take personal responsibility for ensuring that both their own and others’ sensitive knowledge is not used for malicious purposes.

A similar approach is currently being pursued for nuclear security within the UK, with the development of a Nuclear Information Security CoC by a small expert group convened by the Institute of Physics. This initiative is aimed at raising awareness, providing guidance and promoting responsible self-governance when it comes to sensitive nuclear knowledge. To be effective, such a code must take into account the concerns of the scientific and engineering communities, including possible restriction on academic freedoms and impact on existing workloads. Consequently, scientists and engineers together with nuclear security specialists have taken an active role in the code’s formulation.

Such a code will only be effective if it is effectively socialised within the broader scientific and engineering communities and consequently it must be promulgated

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

through appropriate education, training and other outreach activities. The wider importance of nuclear security human resource development (HRD) was strongly emphasised at the 2012 Nuclear Security Summit (NSS) as 'fundamental to promoting and sustaining a strong nuclear security culture'.[51] The importance of enhancing security culture both within nuclear facilities and within the wider scientific and academic community is just as relevant to protecting of sensitive nuclear information as it is to securing nuclear materials. Only through encouraging individuals working directly with such information to take active ownership and assume responsibility for its security can it be truly protected. A recent study by the WINS demonstrated that there is currently a substantial supply versus demand gap for nuclear security HRD, with over 100,000 professionals with accountability worldwide but only a handful of existing academic programmes.[52] The international community has sought to fill this gap with the launch of education and training networks, commonly collectively referred to as 'Nuclear Security Centres of Excellence'.[53] These initiatives, such as the International Nuclear Security Education Network (INSEN), offer a mechanism through which to promulgate information security as an essential part of nuclear security.

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

Conclusion

This article has examined nuclear information security by outlining the types and sources of such information, where it resides and how it could potentially be transferred to non-state actors with malign intent. It is clear that there exists a significant information security challenge in this area spanning various sectors and types of personnel in industry, the defence sector and academia. While formal and informal international instruments do address this challenge, there is scope to enhance how they do this. But recognising that there are limits to such approaches is important if the aim is to improve nuclear information security provision around the globe. The key here will be developing and supporting initiatives that address the challenge from the bottom up and the promotion of responsible self-governance in relevant sectors.

Notes

[1] The International Atomic Energy Agency (IAEA) defines nuclear security as 'the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities'. Concepts and Terms, IAEA, at http://www-ns.iaea.org/standards/concepts-terms.asp?s=11&l=90

[2] Charles D. Ferguson and William C. Potter, *The Four Faces of Nuclear Terrorism*, Center for Nonproliferation Studies, Monterey Institute of International Studies, Monterey, CA, 2004, p. 3, at http://www.nti.org/c_press/analysis_4faces.pdf

[3] 'Seoul Communiqué: 2012 Seoul Nuclear Security Summit', Seoul Nuclear Security Summit, March 2012, at http://www.cfr.org/proliferation/seoul-communiqu-2012-nuclear-security-summit/p27735.

[4] 'Nuclear Security Summit, Seoul, 2012: Multinational Statement on Nuclear Information Security', Office of the Press Secretary, The White House, March 27, 2012, at http://www.whitehouse.gov/the-press-office/2012/03/27/nuclear-security-summit-seoul-march-2012-multinational-statement-nuclear

[5] The project involved desk-based research and interviews with some 10 government and business specialists working in the field of nuclear security and also in aviation and cyber security.

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016

6. Donald MacKenzie and Graham Spinardi, ‘Tacit Knowledge, Weapons Design, and the Un-invention of Nuclear Weapons’, *The American Journal of Sociology*, 101(1), July 1995, p. 45.
7. Murray E. Jennex and Suzanne Zyngier, ‘Security as a Contributor to Knowledge Management Success’, *Information System Frontiers*, 9(5), November 2007, p. 494.
8. Office for Civil Nuclear Security, ‘Finding a Balance: Guidance on the Sensitivity of Nuclear and Related Information and its Disclosure’, April 2005, Issue 2, p. 10, at http://www.hse.gov.uk/nuclear/ocns/balance.pdf.
9. Donald MacKenzie and Graham Spinardi, no. 6, p. 45.
10. H. M. Collins, ‘Tacit Knowledge, Trust and the Q of Sapphire’, *Social Studies of Science*, 31(1), February 2001, pp. 72–73.
11. Donald MacKenzie and Graham Spinardi, no. 6, p. 45.
12. Jonathan Tucker, ‘The Bio-weapons Threat is Broader and Closer than Commonly Thought’, *Bulletin of the Atomic Scientists*, March 2008.
13. Annette Schaper, ‘Looking for a Demarcation—between Nuclear Transparency and Nuclear Secrecy’, Peace Research Institute Frankfurt (PRIF) Reports No. 68, 2004, p. 18.
14. John V. Parachini, David E. Mosher, John Baker, Keith Crane, Michael Chase and Michael Daugherty, *Diversion of Nuclear, Biological, and Chemical Weapons Expertise from the Former Soviet Union: Understanding an Evolving Problem*, RAND, National Security Research Division, Santa Monica, CA, 2005, pp. 18–19, at http://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/RAND_DB457.pdf
15. Ibid., pp. 20–21.
16. Ibid., pp. 20–21, 24.
17. Ibid., pp. 28–29.
18. IAEA, Security of Information and Computer Systems, at http://www-ns.iaea.org/security/infosec.asp?s=4&l=30
19. Office for Civil Nuclear Security, April 2005, p. 10.
20. Ibid., p. 11.
21. Donald MacKenzie and Graham Spinardi, no. 6, pp. 83–84.
22. Annette Schaper, ‘The Transferability of Sensitive Nuclear Weapon Knowledge from Civil Science to Military Work’, Paper prepared for the 5th International Summer Symposium on Science and World Affairs, Cambridge, MA, July 1993.
23. Donald MacKenzie and Graham Spinardi, no. 6, pp. 83–84.
24. Liz Dallas, ‘The Role of Tacit Knowledge in Nuclear Proliferation’, Paper presented at the International Studies Association Annual Convention, San Francisco, April 3–6, 2013, p. 22.
25. Peter D. Zimmerman and Jeffrey G. Lewis, ‘The Bomb in the Backyard’, *Foreign Policy*, 157, November–December 2006, p. 36.
26. See, for example, ‘Controls on Tangible and Intangible Technology’, ExportControl.Org, at http://www.exportcontrol.org (search on ‘tangible’).
27. Timothy Clinton, ‘Intangible Technology Transfer and Catch-All Controls’, ExportControl.Org, June 18, 2003, at http://www.exportcontrol.org/library/conferences/1379/D2-04-Clinton-ITT.pdf
28. Bent Lindhardt Andersen and Dorthe Høst Sarup, ‘Towards Simple, Transparent and Harmonised Export Controls’, in Dorothea Auer (ed.), *Wassenaar Arrangement: Export Control and its Role in Strengthening International Security*, Diplomatische Akademie, Vienna, January 2005, pp. 20–21, at http://www.wassenaar.org/links/Favorita_Paper.pdf
29. ‘Managing Internal Threats’, World Institute for Nuclear Security (WINS) - International Best Practice Guide, March 2010, at https://www.wins.org/.
30. Lyudmila Zaitseva and Kevin Hand, ‘Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users’, *American Behavioral Scientist*, 46(6), 2003, pp. 822–826.
31. ‘Guilty Plea in Trade Secret Case’, US Department of Justice, February 15, 2007, at http://www.justice.gov/criminal/cybercrime/press-releases/2007/minPlea.pdf
32. E. Shaw, K. G. Ruby and J. M. Post ‘The Insider Threat to Information Systems: The Psychology of the Dangerous Insider’, *Security Awareness Bulletin*, No. 2-98, Political Psychology Associates, Ltd., June 1998.
33. David Beresford, ‘Truth is a Strange Fruit: A Personal Journey through the Apartheid War’, Jacana Media (Pty) Ltd, July 1, 2010, pp. 105–107.

34. Joby Warrick, ‘Sensitive Details about US Civilian Nuclear Sites Accidentally Posted Online’, *Washington Post*, June 3, 2009, at http://www.washingtonpost.com/wp-dyn/content/article/2009/06/03/AR2009060300028.html
35. J. Kidd and C. Hobbs, ‘Report on the Adequacy of the United Kingdom’s Export Controls to Prevent the Proliferation of Weapons of Mass Destruction’, Memorandum to the Quadripartite Select Committee, July 2007, at http://www.publications.parliament.uk/pa/cm200607/cmselect/cmquad/117/117we40.htm
36. See ‘Intangible Technology Transfers: Managing the Risk’, ExportControl.Org, at http://www.exportcontrol.org (search on ‘tangible’).
37. Michael Tu, ‘Between Publishing and Perishing? H5N1 Research Unleashes Unprecedented Dual-Use Research Controversy’, NTI, May 3, 2012, at http://www.nti.org/analysis/articles/between-publishing-and-perishing-h5n1-research-unleashes-unprecedented-dual-use-research-controversy/
38. See ‘Convention on the Physical Protection of Nuclear Material (CPPM) and Amendment thereto’, IAEA, at http://www-ns.iaea.org/security/cppnm.asp
39. ‘Nuclear Security—Measures to Protect against Nuclear Terrorism: Amendment to the Convention on the Physical Protection of Nuclear Material’, GOV/INF/2005/10-GC(49)/INF/6, September 6, 2005, at www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf.
40. ‘Convention on Physical Protection of Nuclear Material (CPPNM) and Amendment thereto’, IAEA, at http://www-ns.iaea.org/conventions/physical-protection.asp?l=42
41. International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT), p. 5, at www.un.org/en/sc/ctc/docs/conventions/Conv13.pdf
42. Wyn Q. Bowen, Matthew Cottee and Chris Hobbs, ‘Multilateral Cooperation and the Prevention of Nuclear Terrorism: Pragmatism over Idealism’, *International Affairs*, 88(2), 2012, p. 357.
43. ‘Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities’ (INFCIRC/225/Revision 5), IAEA Nuclear Security Series, No. 13, 2011, p. 16.
44. ‘Objective and Essential Elements of a State’s Nuclear Security Regime’, IAEA Nuclear Series, No. 20, 2013, p. 5.
45. ‘Computer Security at Nuclear Facilities’, IAEA Nuclear Security Series, No. 17, 2011; ‘Preventive and Protective Measures against Insider Threats’, IAEA Nuclear Security Series, No. 8, 2008; ‘Nuclear Security Culture’, IAEA Nuclear Security Series, No. 7, 2008.
46. ‘Nuclear Security Advisory Services’, IAEA, at http://www-ns.iaea.org/security/advisory.asp?s=4&l=26
47. Office for Civil Nuclear Security, April 2005, p. 3.
48. Ibid., p. 5.
49. Best Practice Guides accessed via the membership area of the World Institute for Nuclear Security (WINS) website (www.wins.org) on October 8, 2013.
50. ‘A Code of Conduct for Biosecurity: Report by the Biosecurity Working Group, Royal Netherlands Academy of Arts and Sciences’, 2007, at http://www.fas.org/biosecurity/resource/documents/IAP%20-%20Biosecurity%20code%20of%20conduct.pdf
51. Seoul Nuclear Security Summit Communiqué.
52. ‘Global Need Analysis for Nuclear Security Training’, World Institute for Nuclear Security (WINS), April 2013, at https://www.wins.org/files/wins_white_paper_global_needs_analysis_web.pdf
53. Alan Heyes, ‘An Assessment of the Nuclear Security Centres of Excellence’, Stanley Foundation Policy Analysis Brief, May 2012.

Downloaded by [Masarykova Univerzita v Brne] at 15:57 13 March 2016