"This paper provides an overview of key principles from the field of radiological sources security, and discusses how they could be adapted to improve the security of the chemical industry, and especially of chemical substances in non-sensitive or less-sensitive commercial and industrial context, such as non-scheduled and Schedule 3 chemicals."

VERTIC BRIEF • 31 • JUNE 2019

B R I E F

# Securing a diverse global industry

## Key lessons from the field of radiological security to support OPCW chemical security efforts

Dr. Chris Englefield, Isognos Ltd. and Alberto Muti, VERTIC

VERTIC

"Radiological sources are widely and beneficially used in a wide range of industries around the world, but they have the potential to be diverted to malicious use."

## Introduction

This paper provides an overview of key principles from the field of radiological sources security, and discusses how they could be adapted to improve the security of the chemical industry, and especially of chemical substances in non-sensitive or less-sensitive commercial and industrial context, such as non-scheduled and Schedule 3 chemicals.

Much like the most dangerous chemical substances and precursors covered by the CWC Schedules, special nuclear materials worldwide (plutonium, uranium) are carefully controlled and accounted for, and almost exclusively used in specific, dedicated and highly secure facilities. However, the worldwide chemical industry is much broader in scope than the nuclear fuel cycle and encompasses a great range of substances; some of these, like chlorine, have a number of civilian uses and are very widespread, but can still be dangerous to human life if misused deliberately or accidently. Similarly, radiological sources are widely and beneficially used in a wide range of industries around the world, but they have the potential to be diverted to malicious use. The consequences of misuse include radiological harm, which can be fatal. In addition, there is potential for significant social, psychological, economic and political disruption.

In the post-9/11 world, 18 years of development and learning have been achieved in securing these materials in diverse and complex contexts, whilst maintaining operability and high levels of accessibility to the facilities holding the sources. Costs on industry have also been limited. International efforts to spread the relevant technologies are coordinated by the IAEA. The UK has spearheaded efforts in this sector, establishing its statutory regime for radiological security in January 2006. Other countries, such as Hungary and Spain, have also been leading the way in this sector and may provide examples for a broader study from this sector in the future.

Building on examples of IAEA coordination and UK practice, this paper will identify lessons learned from radiological security that could be used to inform the security of the chemical industry, with a focus on less-sensitive, but still dangerous, chemicals, such as Schedule 3 or on-scheduled chemicals of concern.

The conclusions include 13 recommendations and proposals on how the OPCW could build on lessons from the field of radiological security to assist securing toxic chemicals, especially ones in common industrial or commercial activities. A glossary of terms used in the sphere of radioactive sources is also provided.

## Commonalities of usage for radioactive sources and toxic chemicals and pre-cursors

Both radioactive sources and toxic chemicals and pre-cursor substances, have a long history of use in a wide diversity of sectors. Some of these are listed in Box 1. Most of these have not previously had a deep security tradition and so did not already have inhouse or even established routine access to a consultant security adviser. The range of numbers of employees extend from one or a few, to large corporations; some with HR departments, others without. All industries are obviously cost-sensitive and so require minimum impacts of security measures on productivity.

Industry usually operates at fixed facilities, though the scale of operations varies greatly, and some industries utilising radioactive sources use mobile facilities. This provides variable scope for installed physical protection systems and so requires some flexibility in approach in order to meet

**Box 1: Overview of exemplar usage contexts for radioactive sources**

- Hospitals – diagnosis and treatment
- Universities – research and teaching
- Range of industries:
  - Industrial radiography
    - in a dedicated facility
    - in a field situation
  - Oil and gas exploration
    - Onshore
    - Offshore
  - Process control
    - Minerals
    - Oil and gas
    - Chemicals
    - Food production
    - Road laying
  - Metallurgy
  - Archaeology and Art Conservation

the needs of adequate security while still ensuring that operability of the process is not unduly compromised.

Another commonality is "multiple publics" – any organisation will have a workforce and customers, some of whom will visit the premises and so have more or less access to radioactive sources or toxic chemicals. Access controls may need to be limited in some cases, and in a few situations free access to most of the facility will be essential. Note for example, the need for staff, patients and visitors to access a hospital 24 hours per day. In the case of some medical procedures, patients have to be left alone with the source while it is in use for their treatment; this would be avoided in other security contexts.

Security is required across the whole life-cycle of radioactive sources, and toxic chemicals. The level of protection needs to be similar during what may be multiple transportations; usage, storage and at end of life. Again, lessons have been learned here that are more generally applicable.

In developed countries, where safety regulation is mature, there may be perceived conflicts with statutory safety requirements. In fact, experience has shown that there can be pragmatic solutions so that source security can be balanced against radiological and general safety expectations of employers and regulators. Part of this can be regarding the resilience of these arrangements, as well as sustainability and this seems likely to be something that could be used to inform such questions on the context of increased security arrangements for toxic chemicals and precursors.

## Risk categorisation and graded approach to security measures

The UK's statutory regime for the security of radioactive sources has been in place since 01 January 2006, and voluntary arrangements preceded this. This history of UK experience (and its scope) probably exceeds that of any other state. In an iterative process, the UK has both contributed to the IAEA's library of technical guidance on these matters, (which will be described in the next section) and benefitted from it.

Implementing a comprehensive security scheme across a large, distributed industry requires a series of component parts. The first is a system for categorising the level of harm (or some other parameter, such as attractiveness of the item to an adversary). For radioactive sources, the potential for harm is well understood and the various types of radiations emitted from different sources can readily be normalised. It is straightforward to then arrange radioactive sources into categories, based on the risk they represent. Risk categories for radioactive sources were developed by the IAEA and, while they were published as non-binding guidance documents, they have become the reference for national regulatory regimes worldwide. The IAEA has defined two key ways to categorise sources:

"Security is required across the whole life-cycle of radioactive sources, and toxic chemicals. The level of protection needs to be similar during what may be multiple transportations; usage, storage and at end of life."

"In the chemical sector, categorisation frameworks for hazardous materials already exist at the national level and at the international level, for a range of purposes, such as environmental protection, waste management, and labelling and transport standards."

1. The primary way is to allocate a source to a "practice". A practice is defined in radiation safety circles as any activity that adds to the overall radiation exposure a person receives. So, medical radiotelethерapy and industrial radiography are both practices. This practice-based approach (the result of consensus building by a group of international experts) can be used for each of the five Categories, where Category 1 sources are the most dangerous and Category 5 sources are the least dangerous. Any radioactive source used for radioteletherapy is by definition a Category 1 source; similarly, any source used for industrial radiography is defined as a Category 2 source. This is summarised in Table 1, which includes examples for the other categories. This heuristic and pragmatic approach is normally sufficient to decide which Category a source (or a collection of sources) falls into.
2. The secondary approach is to refer to so called D-values (where D signifies "danger"). A D-value is the quantity of a specified radioactive material which is deemed to be a dangerous quantity if it is involved in a defined accident scenario. These values were calculated by the IAEA based on realistic (not overly conservative) assessments of the risk posed by the radioactive material if it becomes uncontrolled. The methodology deserves a detailed explanation that is beyond this paper, but the outcome is a list of D-values for a wide range of radionuclides. These are tabulated in IAEA Safety Guide RS-G-1.9, a document that has become a key reference for relevant security practitioners. All that remains is to compare the quantity ("A") of radioactive material in the source (or sources, if all held in close proximity) to the appropriate D-value. The magnitude of this A/D ratio is then compared to a Table. For example, if A/D exceeds 1000, then it is a Category 1 source; if A/D is less than 10 but greater than 1, it is Category 3; if less than 0.01, then it is Category 5.

These explanations are provided to show that whilst a categorisation system is fundamental, its precise nature is less important. It seems likely therefore that experts on the effects (and utility to an adversary) of toxic chemicals and precursors could arrive at a consensus of judgements (Approach 1), or perhaps a more calculational approach.

In the chemical sector, categorisation frameworks for hazardous materials already exist at the national level and at the international level, for a range of purposes, such as environmental protection, waste management, and labelling and transport standards. Some of the key resources,

**Table 1: Overview of exemplar usage contexts for radioactive sources**

| Category | Practice (explanation) |
|---|---|
| 1 | Radioisotope thermoelectric generators (free standing power supplies)<br>Irradiators (of patients, medical products, agricultural produce, research organisms)<br>Teletherapy sources (focussed radiation treatment of tumours) |
| 2 | Industrial radiography (safety-critical checks of welds) |
| 3 | High strength fixed industrial gauges (process control instruments in manufacturing)<br>Well logging gauges (geological study of boreholes for oil and gas exploration) |
| 4 | Lower strength fixed industrial gauges<br>Bone densitometers (medical checks of the skeleton) |
| 5 | Materials analysis devices (real time analysis of paintings or artefacts) |

in addition to the Chemical Weapons Convention, are the Basel, Rotterdam and Stockholm Conventions. These instruments, as well as national frameworks that have proved successful, could represent the ideal starting points for a categorisation system aimed at assessing the risk posed by potentially toxic chemicals in common industrial use. The aim might be to develop a form of categorisation for dangerous chemicals in common industrial and commercial uses, such as Schedule 3 or non-scheduled chemicals of concern that would be adopted essentially worldwide in the way that has been achieved for categorising radioactive sources. It is worth noting that while IAEA guidance on nuclear material was developed in two distinct series for safety and security, the IAEA's categorisation of radioactive sources is explicitly intended to form a basis for both safety and security considerations; this fits with the approach, pursued by the OPCW so far, to keep Safety and Security close.

Categorisation of risk is the basis for what practitioners call a "graded approach", based on assessment, and consequent mitigation of risk. A clear understanding of the risk presented by a specific type of radioactive source – or chemical substance – in a specific context and application informs decision-making about the disbursement of effort, money and technical measures for its protection. More resources will then be deployed to protect the most sensitive assets; fewer resources can be deployed to protect the less sensitive.

Guidelines and instruments centred on risk-based approaches exist in the chemical sector for the prevention of accidents. These include the Seveso Directives (now in their third version) and Registration, Evaluation, Authorisation & restriction of CHemicals (REACH), both parts of the EU framework, as well as several industry-led standards. The tools and approaches contained in these, as well as the lessons learned implementing them over the years, should be central to the development of risk-based security approaches for potentially toxic chemicals in common industrial use.

## Provision of security advice at the practitioner level

Just as making safety assessments is a professional skill, so is analysing security vulnerabilities and identifying appropriate security measures to address them. An industry whose core business relies on sustaining high levels of security (such as the nuclear industry) is necessarily funded to support either inhouse or high levels of consultant advisers. However, in the UK at least, for most industrial and educational/research users of radioactive sources, there is neither inhouse expertise nor sufficient funding to buy it in. Hospitals usually have security managers, but the special challenges of radioactive source security are usually deemed beyond their scope. This is likely to be the case for many industrial and commercial activities that employ or handle toxic chemicals.

In the radiological sector, a solution to this lack of internal expertise emerged in the UK during the post-9/11 period. Part of the UK's response to an increased threat level was the establishment of a National Counter-Terrorism Security Office. Its role is to coordinate the training, development and operations of a network of specialist police officers. Counter Terrorism Security Advisors (CTSAs) work within local UK police forces as officers and staff. Their primary role is to provide help, advice and guidance on all aspects of counter terrorism protective security to specified industry sectors. These include:

"These instruments, as well as national frameworks that have proved successful, could represent the ideal starting points for a categorisation system aimed at assessing the risk posed by potentially toxic chemicals in common industrial use."

"The operational principles underpinning the security of radioactive sources can be summarised as: 'deter, detect, delay'."

- crowded places throughout the UK
- hazardous sites and dangerous substances (which includes radioactive substances, pathogens and toxins and toxic chemicals, as well as dual use substances like ammonium nitrate fertilisers.
- the critical national infrastructure
- personal security

CTSAs develop considerable expertise in physical protection. In addition to supporting the regulatory authority with advice on physical protection they can assist in the development of an appreciation of the importance of acquiring external security expertise, as well as an understanding of the key goals and principles to pursue when doing so. They also each develop their own networks of security providers and this enables rapid communication when required, such as during periods of increased threat.

The operational principles underpinning the security of radioactive sources can be summarised as: "deter, detect, delay". (Security practitioners will recognise that "response" needs to be added to this list. In the UK, the latter is provided solely by the police and for this reason no further treatment of it will be provided in this paper).

What has been described so far is reasonably typical implementation of general physical security methods. However, the industrial/commercial/public service contexts of the facilities using radioactive sources have required the development of specialised solutions that are different in their implementation from more general security practice. For example, a large hospital may have several tens of exits/entrances: a perimeter fence will not be appropriate – it would hinder staff, patient and visitor access, not to mention emergency cases. A more nuanced approach is needed. Consider briefly each of deter, detect and delay:

**Deter**: deterrence is about dissuading adversaries from conducting an attack by emphasising the likelihood of failure and capture. This is done by projecting a sufficiently hostile view of the environment to an adversary so as to make an attack difficult or too unachievable to progress. To do this in a hospital or a university (both of which rely on an apparent culture of openness and public access) is a challenge. But engendering a whole hospital security culture (which can have collateral benefits for other security risks) can help in this regard. A similar approach could be taken in a chemical works where (for example) chlorine was used, or phosphorus oxychloride. Or a university lab using lectins such as ricin or abrin.

**Detect**: an effective response to an attack by a hostile adversary cannot be "on standby" continuously, and response forces will often cover multiple facilities – this is especially the case where the response is police-mediated. This means that a timely response can only be mobilised when an attack has been detected and an alarm has annunciated. If assessment of the alarm suggests that an attack is underway, action can be taken. If deterrence fails, then the earlier in the timeline of the attack that detection occurs, the more time there is to assess the alarm and mobilise a response before the attacker completes his task and escapes with the radioactive source/toxic chemical or precursor.

The adversary task time is the variable that can be manipulated by the use of appropriate security measures to give the

defending authorities an edge. If the task time can be extended, then there is more time for the alarm to be noticed and assessed, and for a response to be mobilised. The introduction of security measures that create delay is therefore essential.

**Delay** is created by the use of multiple barriers or technologies, each of which obstructs the adversary until they have been overcome. Different materials used in each delay barrier can be selected to require a range of tool-sets and thus create additional delays. As has already been explained, for radioactive sources delay measures usually have to be located very close to the asset being protected. This presents both advantages and disadvantages: Local or very local security measures create only a low profile for the location of the assets of concern; but they also mean that the physical distance between multiple delay measures may be very small. There is clearly a need to optimise these two effects and this usually comes down to expert judgement. In the UK, this judgement is provided by the CTSAs.

The main feature of CTSAs is not so much that they are police officers or staff, though this does create intelligence gathering opportunities. Instead, what matters is that there is a small centrally funded cadre of experts who *inter alia* can provide security expertise to industrial or commercial entities, most of whom are not equipped nor funded to develop or procure their own source of expertise. This approach has been key to improving security standards across the radiological field, and given that the same lack of security expertise and funding is shared by many entities that employ or trade in potentially dangerous chemicals, it could be adopted or adapted to apply to toxic chemicals and precursors, as is already the case in the UK.

Moreover, the OPCW has already recognised the importance of a security framework based on "prevent, detect, and respond": given this shared framework, lessons learned in implementing security measures for radiological sources on commercial or industrial premises, or in "open" settings like hospital and universities, could be more readily studied and adapted for application to toxic chemicals of concern.

A further component of the UK's approach to the security of radioactive sources is the use of prescribed standards for security equipment. The minimum performance of processes intended to support personnel, information, transport and physical protection can be designed and engineered by the use of appropriate standards. The UK has an extensive collection of security standards. (An example can be summarised as a "security rated class three door" will resist attack from hand and rechargeable tools for five minutes; another might be that all recruits to a company keeping and using toxic chemicals and precursors will have their identity, immigration status, employment history and criminal records checked prior to appointment). Similar national standards could be developed by states concerned to improve security of toxic chemicals and precursors, or standards from other states could be adopted. The UK, the USA and other states publish many such documents; then all that is required is to ensure that any security equipment bought locally or processes developed locally, meet these performance standards.

## The importance of security culture

The need for unimpaired operability in most of the practices for which radioactive

"The main feature of CTSAs is not so much that they are police officers or staff, though this does create intelligence gathering opportunities. Instead, what matters is that there is a small centrally funded cadre of experts who *inter alia* can provide security expertise to industrial or commercial entities."

"In order to help secure the world-wide chemical industry, and to tighten security standards around chemicals in common industrial uses, the OPCW can lead the way in formulating guidelines and disseminate best practices."

sources are used means that compromises have to be made: optimisation of layers of security measures inevitably means that there remains some risk that, despite all efforts the adversary may succeed in diverting the materials we wish to protect to some malicious use. Adding more technology is not only costly, but also is likely to hinder operability. Instead, with good management, a strong security culture can be engendered in all staff, each of whom can then act as "eyes and ears" to reinforce the physical security measures.

Clearly, an effective security culture alone will not stop an insider threat. To mitigate this risk, effective personnel security measures can be used. The UK's lessons learned in this area can minimise bureaucracy but provide high levels of confidence that the risk of an insider threat has been demonstrably minimised.

## The available guidance

The IAEA's Nuclear Security Series contains a wealth of international best practice and is couched at a level that is aimed at governments and regulators. These documents provide a process that enables governments and regulators to understand how they can identify and discharge their contributions to achieving suitable levels of security for radioactive sources. These are public domain documents that can be downloaded from the IAEA website, so the material is readily accessible to those that need it.

In addition, the World Institute or Nuclear Security (WINS), which collaborates closely with the IAEA has published a suite of documents on more operational issues, aimed at the level of practitioners. Details of both IAEA and WINS guidance documents are listed below.

The UK's detailed information on security requirements for radioactive sources is a classified document. It is therefore not in the public domain. The principles it follows are very similar to those of the IAEA. The classification of this document is due to the fact it contains information that would enable the adversary to understand the security measures that has to be defeated. However, experts in academia, NGOs and the private sector have a good understanding of the principles and lessons learned behind these requirements, and can share them in greater depth.

## Conclusions

Recent events in Syria and beyond have highlighted the danger that non-scheduled chemicals be put to malicious use by non-state actors, even as the OPCW verification system ensures strong controls on the most dangerous substances. The maturation of the field of radiological security in the almost two decades since the 9/11 attacks of 2001 can provide a blueprint for efforts to close this gap, by demonstrating how even materials in a wide range of common industrial applications can be covered by security measures. The IAEA has developed an extensive knowledge base on the security of radioactive sources. The UK has developed extensive knowledge and practical experience of implementing these arrangements, based on a thorough understanding of the threats and risks presented by various types of items and substances, and on a graded approach to introducing security measures.

### Recommendations

In order to help secure the worldwide chemical industry, and to tighten security standards around chemicals in common industrial uses, the OPCW can lead the way in formulating guidelines and disseminate best practices.

A useful measure the OPCW could take is to develop guidance on the categorisation of the danger posed by chemical substances, as well as a risk-based, graded approach to securing these substances. These could be based on existing international instruments and on good practices emerging at the national level. Several resources already exist for chemical safety protocols and procedures, and these could be built upon to develop security guidelines, in line with the OPCW approach of keeping Chemical Safety and Security in close synergy.

In order to develop these resources, the OPCW should leverage the expertise of its member states (possibly through in-kind contribution of expert staff), as well as engage with experts and industry. This will be crucial not only to ensure that the final product is comprehensive and accurate, but also to build a sense of ownership among key stakeholders, ensuring that the final guidelines are seen as authoritative and desirable.

This document (or documents) could be part of the "core" texts of an OPCW-led publication series of guidance documents for chemical security. Later texts should aim to provide specific advice for different levels of implementation, such as government, regulators and practitioners; organisations and expert individuals at the appropriate level should be involved in the drafting and reviewing of guidance. An issue of particular interest given the practitioners involved would be how to use existing national security expertise to provide advice to businesses in securing their premises and substances, based on lessons learned at the national level (such as with the UK CTSA model).

Given that this framework would focus on ordinary industrial and commercial applications, it is also important to recognise some specific needs that any OPCW-led framework would need to address. Firstly, the diverse industries that use these substances may initially lack "in-house" expertise on how to assess risks and implement security measures; so practices and procedures to enable transmission of advice to users will therefore be a priority. One area that should be investigated is the use of existing national security expertise and institutions to provide support to businesses (such as with the UK CTSA model). Secondly, facilities that are accessed by a range of publics have specific security requirements; often in these contexts, detection and delay technologies will need to be deployed very close to the locations where inventories are stored and used. Thirdly, first response organisations, including local law enforcement, need to understand how to safely intervene in the event that an unauthorised intrusion is detected; guidance and capacity-building material should be prepared for these audiences, too. Finally, security must be applied to the entire lifecycle of these substances, from manufacture, during transportation and during keeping and use, as well as during the accumulation and disposal of wastes.

This paper provided an initial overview of the principles underlying the security of radioactive sources. Further studies could usefully focus on analysing cases of industrial application, understanding regulatory approaches, and investigating the life cycle of key non-scheduled and Schedule 3 chemicals of concern to better understand and characterise use cases.

"A useful measure the OPCW could take is to develop guidance on the categorisation of the danger posed by chemical substances, as well as a risk-based, graded approach to securing these substances."

## Summary of recommendations and proposals

- A straightforward system that provides a graded approach to securing these substances is developed.

"Recognise that security must be applied to the entire life-cycle of these substances, from manufacture, during transportation and during keeping and use, as well as during the accumulation and disposal of wastes."

- Effort is invested in developing some form of categorisation of these substances so as to enable prioritisation to inform decision making on what to protect and how much to invest in doing so.
- Engagement with selected stakeholders in relevant industries is undertaken that will help to ensure a sense of ownership and to maintain the high level of credibility of OPCW documents.
- Consideration is given to whether a structure based on division into: governments; regulators and practitioners could usefully be adopted, by analogy with the IAEA/WINS model.
- Tiers of guidance for each division are developed, preferably involving organisations and/or consultants who have experienced the arrangements for radioactive sources as well as those familiar with relevant dangerous chemical substances and precursors that are the subject of this paper.
- A more or less prescriptive approach is adopted, recognising that in most cases, users of these substance will not have "inhouse" expertise on security methods.
- Advice is developed on how states might use existing security advisers (analogous to the UK's "CTSAs") to advise and support relevant premises.
- Recognise the need to enable transmission of relevant advice to relevant users.
- Recognise that the diverse industries that use these substances require the development of an understanding of how to implement deterrence, detection and delay technologies to secure their inventories.
- Recognise that where premises are accessed by a range of publics, this drives the use of detection and delay technologies very close to the locations where inventories are stored and used.
- Recognise that first response organisations need to understand how to safely intervene in the event that an unauthorised intrusion is detected.
- Recognise that security must be applied to the entire lifecycle of these substances, from manufacture, during transportation and during keeping and use, as well as during the accumulation and disposal of wastes.
- Adoption of relevant existing national (or in their absence: international) security standards are promoted to enable secure outcomes.

## References


IAEA Nuclear Security Series publications: http://www-ns.iaea.org/security/nss-publications.asp

WINS Best Practice Guides: https://wins.org/document-category/wins-best-practice-guides/

Both IAEA and WINS documents are available in a range of languages.

IAEA safety Guide No. RS-G-1.9 Categorization of Radioactive Sources. Vienna. 2005. Accessible from https://www-pub.iaea.org/books/iaeabooks/7237/Categorization-of-Radioactive-Sources


## Glossary

**A –** symbol for "activity". The strength of a radioactive source is called its activity, which is defined as the rate at which the isotope decays. Specifically, it is the number of atoms that decay and emit radiation in one second.

**Adversary** – "the enemy" who is trying to gain unauthorised access to specific assets for malicious purposes.

**D-value** - the radionuclide specific activity of a source which, if not under control, could cause severe deterministic effects for a range of scenarios that include both external exposure from an unshielded source and internal exposure following dispersal of the source material.

**HR** – Human Resources Management

**IAEA** – the international Atomic Energy Agency, headquartered in Vienna.

**Intelligent Customer** – The capability of the organisation to have a clear understanding and knowledge of the product or service being supplied by a contractor.

**Operability** – the ability to keep equipment, a system or a whole industrial installation in a safe and reliable functioning condition, according to pre-defined operational requirements. This ensures sustainable levels of productivity, such as patient throughput in a medical context.

**Physical protection** – security measures that are designed to deny unauthorised access to facilities, equipment and resources and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance,

security guards, protective barriers, locks, access control protocols, etc.

**Plutonium** – Usually isotope 239: fissile metal used in nuclear power and nuclear weapon applications.

**Practice** – a term used in radiological protection, meaning any process or use of radiation that results in an increase of exposure of a person. In contrast, an intervention is a measure that will reduce exposure.

**Radioactivity** – (1) the emission of ionizing radiation or particles caused by the spontaneous disintegration of atomic nuclei. (2) radioactive substances, or the radiation emitted by these.

**Radioteletherapy** – treatment of cancer by use of a focussed beam of radiation intended to preferentially kill tumour cells rather than healthy tissue.

**Radionuclides** – an atom that has excess nuclear energy, making it unstable. The instability results in the nucleus disintegrating into smaller fragments, which include the emission of various types of radiation. During those processes, the radionuclide is said to undergo radioactive decay. These emissions are considered ionising radiation because they are powerful enough to liberate an electron from another atom, thus creating a net charged ion.

**Special nuclear materials** – fissile isotopes of actinides that can be diverted to weapon manufacture involving a nuclear detonation.

**Statutory regime** – a system of legally enforced requirements which is subject to compliance assessment by a regulatory body, and enforcement action when appropriate.

**Uranium** – usually isotope 235: fissile metal used in nuclear power and nuclear weapon applications.

**Editors**
Larry Macfaul

**Design and layout**
Rick Jones

**ISSN**
1740-8083



## About this paper

This paper has been produced by VERTIC under a project funded by the Swedish Government. The project aims to contribute to the debate on the OPCW's role and initiatives in supporting chemical security and preventing non-state actors from employing chemical weapons. This initiative has analysed approaches and lessons learned from the IAEA experience in improving the global nuclear security regime. The paper presents a set of recommendations and proposals.

This paper forms a pair with VERTIC Brief 32 'The OPCW's role in chemical security: approaches and lessons learned from the IAEA's Nuclear Security Plans'.

Additional studies may be carried out in the future, dealing with topics outlined in this paper in more depth, or looking further afield for useful experiences and models as well as challenges overcome.

The authors would like to thank colleagues, including Yasemin Balci and Larry MacFaul among others, who provided helpful advice.

VERTIC
The Green House, 244–254
Cambridge Heath Road,
London E2 9DA,
United Kingdom

*Tel* +44 (0)20 3559 6146
*E-mail* vertic@vertic.org
*Website* www.vertic.org

Building trust through verification

**VERTIC** is an independent, not-for-profit, non-governmental organisation. Our mission is to support the development, implementation and effectiveness of international agreements and related regional and national initiatives, with particular attention to issues of monitoring, review, legislation and verification. We conduct research, analysis and provide expert advice and information to governments and other stakeholders. We also provide support for capacity building, training, legislative assistance and cooperation.