



Volume 3

Number 1 *International Journal of Nuclear Security*

---

12-15-2017

# The Future of Nuclear Security: A Medical Physicist's Perspective

Katharine E. Thomson

*Plymouth Hospitals NHS Trust*

Follow this and additional works at: <https://trace.tennessee.edu/ijns>

 Part of the [Defense and Security Studies Commons](#), [Engineering Education Commons](#), [International Relations Commons](#), [National Security Law Commons](#), [Nuclear Commons](#), [Nuclear Engineering Commons](#), [Other Medical Sciences Commons](#), and the [Training and Development Commons](#)

---

### Recommended Citation

Thomson, Katharine E. (2017) "The Future of Nuclear Security: A Medical Physicist's Perspective," *International Journal of Nuclear Security*: Vol. 3: No. 1, Article 9.

Available at: <http://dx.doi.org/10.7290/ijns030109>

This Special Opinion Editorial is brought to you for free and open access by Trace: Tennessee Research and Creative Exchange. It has been accepted for inclusion in *International Journal of Nuclear Security* by an authorized editor of Trace: Tennessee Research and Creative Exchange. For more information, please contact [trace@utk.edu](mailto:trace@utk.edu).

---

# The Future of Nuclear Security: A Medical Physicist's Perspective

## **Cover Page Footnote**

This essay was one of three winners of the International Atomic Energy Agency's inaugural International Essay Competition on Nuclear Security for Students and Early Career Professionals, awarded in Vienna in December 2016.

# **The Future of Nuclear Security: A Medical Physicist's Perspective**

Katharine E. Thomson  
Plymouth Hospitals NHS Trust

*This essay was one of three winners of the International Atomic Energy Agency's inaugural International Essay Competition on Nuclear Security for Students and Early Career Professionals, awarded in Vienna in December 2016 as a side event of the 2016 International Conference on Nuclear Security: Commitments and Actions.*

## **Abstract**

Medical physicists, of whom the author is one, oversee all aspects of small-scale radiation use. This paper discusses three key areas increasingly important to both medical and nuclear uses of radioactive materials: public engagement, prevention of nuclear and radiological terrorism and cyber security. It compares and parallels practices in both industries and suggests strategies both can take for the future.

## **I. Introduction**

On the 5<sup>th</sup> April 2009, Barack Obama addressed a huge crowd in Hradcanske Square, Prague, in one of the first major foreign policy speeches of his presidency. He spoke of a post-Cold War world in which the threat of global nuclear war had receded, but the risk of nuclear attack had not. He described the Cold War's legacy of thousands nuclear weapons, and warned of the menace of nuclear terrorism, and the ultimate threat "to our global safety, our security, our society, our economy, to our ultimate survival" [1].

The future of nuclear security is not addressed easily. International, multi-professional conferences are vital precisely because of the scale of the challenges and the diversity of expertise required. As a medical physicist, I am no expert in international diplomacy or nuclear smuggling. Instead, as someone who oversees all aspects of small-scale radiation use, I hope to draw some parallels between medical and nuclear uses of radiation, and make some suggestions for both their futures.

The challenges both communities face are the same: controlling access to dangerous material, creating a strong security culture, cooperating with the wider world and engaging the public.

I would like to focus on three challenges for the future of nuclear security: public engagement, nuclear terrorism and cyber security. The medical sector has benefited greatly from the nuclear community's expertise; perhaps we can contribute some suggestions in return.

## **II. The Current Situation**

In the seven years since President Obama spoke of “dangers that recognize no borders”, much has happened globally. We have experienced the Fukushima disaster and a series of North Korean weapons tests. Syria has descended into bloody civil war, the government has collapsed in Libya, and ISIS, or Da’esh, has taken control of vast swathes of territory. We have endured terrorist attacks in Pakistan, Kenya, France, and throughout the Middle East. Diplomatic tensions have been heightened and populist movements have grown in popularity [2–4].

There has also been tremendous progress. The USA and Russia signed the New START arms treaty, a historic nuclear deal was struck with Iran, the Amendment to the Convention on the Physical Protection of Nuclear Materials (CPPNM) came into force, and four Nuclear Security Summits have been held, the latest this year.

These Summits have been hugely valuable in reducing nuclear material worldwide and improving security practices. As they finish in their current form, it would be easy to fall into either despondency, as a period of great progress ends, or complacency, congratulating us on a job well done.

Our responsibility is to do neither. We find ourselves in a critical period in global affairs and in nuclear security in particular. As the Nuclear Security Summit process ends, we must reflect on its achievements, consolidate its successes and plan our next steps.

## **III. Public Engagement**

2016 has been an interesting year to be British. I have followed the events of the past few months with near obsession and occasional alarm. From the renewal of the Trident nuclear deterrent to strained relations with China over delays to the Hinkley Point C nuclear power station, nuclear issues have been in the public eye to an unusual degree.

However, the story dominating the headlines is not obviously nuclear-related: the referendum on membership of the European Union, and the shock decision to leave: Brexit.

Analysis of the motivations, which led to the leave vote, will continue for years. It seems clear, however, that one key factor was the feeling, justified or not, that ordinary people were being left behind by a “political elite” [5] who neither understood nor cared about their concerns. Appeals by the government fell on deaf ears. The International Monetary Fund, the Bank of England, security experts, business leaders, ten Nobel-prize winning economists, 5000 scientists and 1000 academics collectively extolled the virtues of the EU and warned of the consequences of leaving; to no avail. As the then Justice Secretary, Michael Gove, said, “People in this country have had enough of experts” [6].

This poses a problem to we who fall into that much-maligned category, “so-called experts”. As discontent with traditional politics increases, evidenced by the rise of populist movements across Europe and the USA [2], we need to make sure that reasoned and coherent messages are getting through.

Public engagement is sometimes viewed as an optional extra after the technical matters are arranged. Whatever our nationality or political persuasion, recent events should have taught us the danger of this way of thinking. This is particularly true in nuclear security and medical physics, where the focus of our expertise is primarily on advising and supporting governments, hospital boards and industries. These groups become the prism through which the public is kept informed, and sometimes messages are lost in translation.

There is a discrepancy between reality and public perception that is not challenged enough. In 2011, the BBC reported that support for nuclear power had dropped considerably worldwide, with only

around 22% of respondents in countries with nuclear programs confident of its benefit and safety [7]. In a 2013 report from the UK Energy Research Centre, only 33% of Britons thought their government adequately regulated nuclear power [8]. An acquaintance of mine, a veterinarian with years of education and professional training, is convinced that the nuclear-powered submarines docking in our nearest port has given most of the inhabitants leukemia.

In my work as a medical physicist, I often speak to patients who are anxious about their exposure to radiation from x-rays or nuclear medicine procedures. Their level of understanding of the risks is often low, and the fear for themselves or their families correspondingly high. A proper discussion, where they are not only told the facts but also given a chance to express their concerns and ask questions, usually allays most fears and puts the risks and benefits in perspective. This does not normally alter whether or not a procedure goes ahead, but it makes things go much more smoothly, relieves unnecessary worries and gives the patient a better picture of the hospital's work. These patients, and the wider public, are not only capable of understanding the facts; they have a right to, and it is the fault of we "so-called experts" when they do not.

There are many ways of tackling public engagement. In the UK, professionals in a range of industries are encouraged to sign up to the Science, Technology, Engineering and Maths (STEM) Ambassadors scheme, running workshops in schools and talking about careers in science. The UK Institute of Physics and Engineering in Medicine recently launched a "Science for Patient Benefit" campaign, displaying posters and leaflets in hospital waiting rooms describing the uses of radiation in medicine. Professional bodies and learned societies have a key role in influencing school syllabuses and engaging teachers.

An emphasis on education will not only pay dividends in public support and democratic mandate. It will also produce the next generation of scientists, engineers and policy makers. The medical profession has already seen the benefits of better public education and engagement; the nuclear industry might gain in the same way.

Who, then, should be involved in nuclear security? The answer, surely, is everyone, even only by understanding what is done in his or her name. From a brutally financial perspective, it is contributions from member states that form the budgets of the IAEA, INTERPOL and other key bodies. Our taxes fund our nuclear security, and our security is on the line.

Of course, this is not just about money. Our governments represent us and act on our behalf. We must not lose sight at large international meetings of whom it is we are protecting: first and foremost, nuclear security is there to defend the world's 7.4 billion ordinary citizens.

#### **IV. Nuclear Terrorism**

Since the IAEA's creation in 1957, the global nuclear security situation has changed radically. As the Institute on Global Conflict and Cooperation note [9], "International security in the 21<sup>st</sup> century has been transformed from a starkly bipolar confrontation of states and their surrogates, characteristic of the Cold War, to interactions among a wide variety of actors and institutions."

Huge progress has been made at a state level, but the threat from non-state actors such as terrorist groups has been increasing. The prospect of ISIS obtaining nuclear weapons would keep even the most hardened security expert awake at night; in President Obama's words, it presents "the most immediate and extreme threat to global security." It is hard to disagree: ISIS has shown no scruples over causing large-scale loss of life, and there are reports of them using chemical weapons against military and civilian targets.

It would be naïve to expect ISIS not to aim for the ultimate symbol of power: a nuclear weapon. Their forebears Al Qaeda claimed "acquiring weapons of mass destruction for the defense of Muslims is a religious duty" [10]. It would be just as naïve to assume they would not use it if acquired. The

traditional deterrence strategy of Mutually Assured Destruction holds no sway; they “lack the minimum degree of risk-adversity to be capable of being deterred; religious fanaticism has made them immune from fear of death” [11].

ISIS could either steal a complete weapon or aim to produce one itself, requiring accurate blueprints, scientific expertise and fissile material [12]. We need to ensure all sources are under regulatory control, reduce reliance on highly enriched uranium, and support schemes such as INTERPOL’s “Fail Safe” and “Conduit” operations and the IAEA’s Incident and Trafficking Database. Poor national nuclear security, as well as proliferation, increases the chance of material falling into the wrong hands. We must also counter the false but effective propaganda that brings ISIS recruits, some with scientific expertise.

Instead of acquiring or producing nuclear capabilities, acquiring non-fissile radioactive material for use in dirty bombs or large-scale contamination would be relatively easy, and must be a tempting choice for terrorists. Although the threat to the public is lower in terms of casualties, the psychological impact on a population from a dirty bomb incident would be huge. This is, of course, one of the key aims of terrorism.

Medical and nuclear uses of radioactive material overlap in this area. Hospitals have relatively weak security, particularly for radioactive materials in transit, and use highly radioactive objects such as molybdenum generators or iridium brachytherapy seeds. Guidance such as the IAEA’s “Security of Radioactive Sources” provides a valuable resource for keeping sources safe, but this must be implemented within a strong security culture.

However, attitudes are changing. UK hospitals now include in their departmental rules contingency plans for theft or loss of radioactive sources. This has been valuable, not only in planning for the worst, but also in creating a security-conscious mindset in staff not used to seeing themselves as a target. Many medical physicists now train as responders under the “National Arrangements for Incidents Involving Radioactivity” scheme, which provides assistance to the police after a radioactive incident. On the nuclear side, the Berlin workshop in September on the security of sealed sources provides a valuable opportunity to focus on implementing and improving the IAEA’s Code of Conduct on the Safety and Security of Radioactive Sources. I suggest that the Code should cover unsealed sources as well as sealed, as they often have weaker security, particularly in medicine. We should not neglect the personal side of nuclear security. A poorly paid, overworked employee, or one who is vulnerable to radicalization, is the weakest link in a nuclear facility’s security; a well-trained one might be its strongest. Similarly, a hospital physicist competent to restrict access and control disposal of radioactive waste might be the difference between a failed theft and a dirty bomb.

## V. Cyber Security

Cyber security must be urgently developed. The best physical security is useless if it is not matched by equally strong cyber security, in any type of facility. As global infrastructure becomes inseparable from the computer systems that govern it, the importance of cyber security grows.

This is an area of particular weakness in hospitals. Radiology staff is traditionally drawn from academia and medicine and are not natural computer scientists. I suspect this is mirrored in the nuclear world. We need to focus on recruiting brilliant engineers, scientists and policy makers, but computer scientists and cyber security experts. The US government agencies including the FBI and NSA hire so-called “white hat hackers” to spot weaknesses in security systems [13, 14]. Despite the challenges involved, including background checks and competing with the private sector, this is a strategy that could be replicated in the nuclear industry, creating the balanced workforce required.

As this balance tips ever more towards computerization, the nuclear industry is well ahead of medicine. Our staff is scientific professionals and computer literate, but they are not capable of

building or maintaining a cyber security system. We outsource this task to computer experts and then misuse, or fail to understand, the results. An acquaintance of mine worked in a facility handling sensitive radioactive sources. The computer security system required all staff to change their passwords daily. The result was that workers would write each new password on a sticky note fixed to the computer monitor.

Just as a physical security system is let down by a careless employee, the weakest point of a cyber security system is the members of staff using it, and seniority is no guarantee of compliance. Cyber security systems need to be comprehensive, usable and respected. The Stuxnet attacks are an indication of the damage that can be wrought on nuclear facilities. Cyber security is the weakest point of hospital systems; the same must not be true of nuclear facilities.

## VI. Conclusion

As the Nuclear Security Summit process ends, we must ensure its strengths are harnessed for the future: the focus on tangible outcomes, the attention of national leaders and the emphasis on building relationships. Action Plans must be followed and the Amendment to the CPPNM universalized. We must address the current threats of nuclear terrorism and smuggling, and plan for the future by building strong cybersecurity systems and training upcoming experts.

We should also consider the consequences of failure. It will be ordinary, vulnerable people who suffer from nuclear security lapses: families in bombed out Syrian cities fleeing before ISIS's nuclear capabilities; tourists and commuters in Western cities contaminated by dirty bombs; populations living in fear of a threat they can't see and barely understand.

The global community needs to grasp this, and commit to working across borders; reaching out diplomatically to countries we have little in common with. If we can work with scientists and police forces, industrialists and diplomats, governments and international agencies, in dialogue with the public and remembering that our efforts are all for their safety – then, truly, we will have Atoms for Peace.

## VII. Works Cited

1. Remarks By President Barack Obama In Prague As Delivered. *whitehouse.gov* (2009), (available at <https://obamawhitehouse.archives.gov/the-press-office/remarks-president-barack-obama-prague-delivered>).
2. R. Inglehart, P. Norris, Trump, Brexit, and the Rise of Populism: Economic Have-Nots and Cultural Backlash. *Harv. Kennedy Sch.* (available at <https://www.hks.harvard.edu/publications/trump-brexit-and-rise-populism-economic-have-nots-and-cultural-backlash>).
3. J. Staufenberg, Rise of right-wing populist threat in Europe can only be tackled by greater EU co-operation, says German philosopher. *The Independent* (2016), (available at <http://www.independent.co.uk/news/world/europe/german-philosopher-jurgen-habermas-right-wing-populist-parties-grow-eu-integrates-brexit-a7132936.html>).
4. A. Osborn, P. Devitt, Germany urges Russia and Ukraine to ease tension over Crimea, keep talking. *Reuters* (2016), (available at <https://www.reuters.com/article/us-ukraine-crisis-russia-germany/germany-to-russia-minsk-deal-must-stay-focus-of-ukraine-peace-process-ria-idUSKCN10Q0H4>).
5. I. Jack, In this Brexit vote, the poor turned on an elite who ignored them (2016), (available at <http://www.theguardian.com/commentisfree/2016/jun/25/brexit-vote-poor-elite>).

6. H. Mance, Britain has had enough of experts, says Gove. *Financ. Times* (2016), (available at <http://global.factiva.com/redir/default.aspx?P=sa&an=FTCOM00020160603ec6300bcd&cat=a&ep=ASE>).
7. R. Black, Nuclear power “gets little public support worldwide” (2011), (available at <http://www.bbc.com/news/science-environment-15864806>).
8. W. Poortinga, S. Capstick, N. F. Pidgeon, M. Aoyagi, Public Attitudes to Nuclear Power and Climate Change in Britain Two Years after the Fukushima Accident. *UK Energy Res. Cent.* (2017) (available at <http://www.ukerc.ac.uk/publications/public-attitudes-to-nuclear-power-and-climate-change-in-britain-two-years-after-the-fukushima-accident-summary-findings-of-a-survey-conducted-in-march-2013-working-paper.html>).
9. Institute on Global Conflict and Cooperation, “International Security” (UC San Diego, 2016), (available at <https://igcc.ucsd.edu/research-and-programs/research/international-security/index.html>).
10. R. Mowatt-Larssen, “Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?” (Harvard Kennedy School, Belfer Center for Science and International Affairs, Cambridge, MA, 2010), (available at <https://www.belfercenter.org/publication/al-qaeda-weapons-mass-destruction-threat-hype-or-reality>).
11. G. Verdirame, The “Sinews of Peace”: International Law, Strategy, and the Prevention of War. *Br. Yearb. Int. Law.* **77**, 83–162 (2007).
12. N. Eweiss, Non-state actors & WMD: Does ISIS have a pathway to a nuclear weapon? *Br. Am. Secur. Inf. Counc.* (2016).
13. Most Wanted Talent: Seeking Tech Experts to Become Cyber Special Agents. *Fed. Bur. Investig.* (2014), (available at <https://www.fbi.gov/news/stories/fbi-seeking-tech-experts-to-become-cyber-special-agents>).
14. D. Samuelsohn, Inside the NSA’s hunt for hackers (2015), (available at <https://www.politico.com/agenda/story/2015/12/federal-government-cyber-security-technology-worker-recruiting-000330>).