The future of nuclear security: Commitments and actions – Power generation and stewardship in the 21st century

P.G. Martin⁎, N.G. Tomkinson, T.B. Scott
Interface Analysis Centre, HH Wills Physics Laboratory, University of Bristol, BS8 1TL, UK

A R T I C L E   I N F O
Keywords:
Nuclear
Drones
Technology
Security
Terrorism
Safety

A B S T R A C T
Since the terrorist events of the 11th September 2001, the world as it was once known was changed forever. It was these catastrophic terrorist actions over fifteen years ago that saw the dawn of a new era with heightened security across many everyday areas of society that had not previously witnessed such scrutiny or control. Coupling this elevated risk of physical and technical aggression with the ever-increasing global per capita energy demand – there has been witnessed a continually growing reliance on nuclear energy for baseline power generation, a form of electricity production that requires both the necessary international safeguards and controls for its safe use. As more and more of the global energy budget is provided by low-carbon sources (over highly-polluting fossil fuels), the volume of nuclear material in existence will grow substantially – requiring considerable attention and policy to ensure its long-term safety and security.

This commentary describes the vast range of policy challenges faced by the nuclear industry resulting from the rapid technological advancements being made across society, and how these directly (and indirectly) affect global nuclear security, as well as providing a thorough discussion on how best these challenges may be overcome.

1. Introduction – A changing global energy budget

With 2011 marking the year in which the world population first exceeded 7 billion, current estimates place 2021 as the year when 8 billion people will inhabit our planet (The World Bank, 2017a; United Nations Department of Economic and Social Affairs - Population Division, 2015). It may seem logical to conceive that the global energy requirement is a direct consequence of the total global population – with more people requiring access to electricity. Whilst the global population explosion is in-part responsible for our total energy requirements, a form of electricity production that requires both the necessary international safeguards and controls for its safe use. As more and more of the global energy budget is provided by low-carbon sources (over highly-polluting fossil fuels), the volume of nuclear material in existence will grow substantially – requiring considerable attention and policy to ensure its long-term safety and security.

This commentary describes the vast range of policy challenges faced by the nuclear industry resulting from the rapid technological advancements being made across society, and how these directly (and indirectly) affect global nuclear security, as well as providing a thorough discussion on how best these challenges may be overcome.

Through these means, and what is viewed by many as a “renaissance” in nuclear power (Grimes and Nuttall, 2010; Marcus and Levin, 2002; Nuttall, 2005). Because of this increasing drive to liberate the vast quantities of energy stored within the atom, after a brief recession from 2010, the per capita proportion of nuclear power contributing to the global energy budget is increasing (Fig. 1(b)). This resurgence in nuclear energy (albeit later that many foresaw) is similarly paired with a corresponding reduction in the proportion of fossil fuels consumed. As shown graphically within Fig. 1(c), global fossil fuel consumption (per capita) has begun to decline – with this reduction enhanced further if China (the world’s largest consumer of fossil fuels) is excluded (Fig. 1(d)) (The Shift Project Data Portal, 2017a).

However, despite this observed growth within the sector, is it the opinion of many that such a renaissance has not occurred and that any upturn in nuclear growth is considerably smaller than was once envisaged (or widely-sold). This is often ascribed to the fact that the building of new nuclear power plants is not economically viable via private investment, given the vast initial facility construction costs and the extended time for payback on such investment (Bradford, 2004; Brown, 2008; van de Graaff, 2016). Works including these also cite the lack of large-scale facilities globally to deal with the wastes that are produced by the nuclear fuel cycle, in spite of the technological...
progress and new facilities witnessed in northern Europe (Sweden and Finland) (Darst and Dawson, 2010).

Such resurgence in nuclear is further demonstrated by not only the total number of nuclear facilities operating globally, but also the total number of plants undergoing construction as well as those at the planning or initial design (proposal) stage, as shown graphically within Fig. 2. Following the 2011 Fukushima Daiichi Nuclear Power Plant accident in Japan, several countries elected to halt their nuclear programs, including Japan and Germany. Whilst this represented a significant number of facilities to enter shutdown – as is shown in Fig. 2, this was balanced by many reactors entering service in other countries. It is estimated that by 2035, approximately 130 reactors will enter retirement, however these will be replaced by nearly 300 new units – many of which will provide a considerably larger power-generating capacity (IAEA, 2016; World Nuclear Association, 2017a).

2. More material, more risk?

Consequently, with more nuclear reactors located in ever more countries, there exists (and will rise still further), a record amount of nuclear material of varying types (e.g. enrichment, form and radioactivity) distributed globally (World Nuclear Association, 2017a). This presents considerable security, transport and health risks associated with all stages of the materials lifecycle; from fuel precursors through to spent fuel reprocessing, to wastes and final disposal. A plot illustrating the global uranium production directed into the fabrication of fresh nuclear fuel for use in reactors is shown within Fig. 3. Despite annual fluctuations in the volume of material entering fabrication, there is still evident a steady increase in material entering the nuclear fuel cycle. Recent advancements in nuclear fission technology towards Small Modular Reactor (SMR) systems, arising principally from their lower projected construction costs and reduced proliferation risk makes them (for the first time) viable for private investment (World Nuclear Association, 2017b). These perceived benefits of SMR technology have led many to speculate that the number of such units will increase rapidly, to constitute a considerable component of many countries total nuclear reactor inventory (Fig. 4).

Unlike “traditional” fission reactors which generate power in the order of 1000 Mega Watt Electric (MWe), these off-site manufactured reactors are designed to be brought on-site fully-constructed and produce an electrical output of less than 300 MWe during peak operation. Whilst it may be the viewpoint of many that the wider distribution of smaller volumes of radiological material represents an improvement for safeguarding material from those wishing harm – with any potential attack yielding access to only a comparatively small volume of nuclear material, these reactors will still need to be kept highly-secure and therefore require an effective Nuclear Site Security Plan, following INFCIRC/225/Rev.5 recommendations (IAEA, 2011), as for any other nuclear installation.

Accentuated by this portended rapid and extensive growth in SMR’s around the world due in no small part to the differing systems produced by a large number of vendors detailed in a recent publication by the National Nuclear Laboratory (2014a), several key challenges and threats to current (as well as future) nuclear security are apparent. As previously alluded to – the possibility of direct violent physical terrorism on nuclear infrastructure is considered the most obvious risk,
and in the aftermath of recent global events, the threat of nuclear terrorism is now viewed by many international organisations to be as great as ever, as detailed in a number of summative works such as that of the (Nuclear Threat Initiative (NTI), 2016). This “nuclear terrorism” can occur through actions such as direct physical attacks on nuclear power facilities, its transport network or the sites in which material is stored, potentially alongside co-ordinated cyber-attacks on the networks and systems that are utilised in the sector. Despite intensive screening, the additional threat posed by insiders within these facilities cannot also be excluded. With terrorism defined not only as the use of violence, but also the threat of its use, suitable fear and anxiety exists even without any such acts ever occurring (North Atlantic Treaty Organisation (NATO), 2014).

3. Keeping stock is keeping safe

Due to greater volumes of radiological material disseminated worldwide across the entire nuclear fuel cycle (from initial mining through to final waste reprocessing and storage), it becomes imperative for countries as well as regulatory organisations (such as the IAEA and Euratom) to accurately monitor radiological material, its location, form and enrichment state. Two related, yet contrasting aspects arising from this to impact future nuclear security are (i) smuggling: the act of moving material for monetary gain to criminal gangs and terrorist groups and (ii) proliferation: the spreading on nuclear material for weapons (typically clandestine) programmes. The IAEA Incident and Trafficking Database (ITDB) (IAEA, 2015) has reported a total of 2889 confirmed unauthorised possession and criminal activity incidents between 1993 and 2015 where material had been moved without authorisation and was intercepted by controlling authorities. Incidences where material has successfully been trafficked are obviously unreported, but it is highly likely that international policing efforts to prevent or intercept illicit trafficking of nuclear materials are not always successful. Such is evidenced by the regional variation in reported incidents made within the ITDB (IAEA, 2015). Whilst despite containing less nuclear material as a region (IAEA, 2016), the total incidents of theft and loss within Asia is one-fiftieth of that of the USA, a disproportionality low amount.

With such growing risks associated with our future divestment in fossil fuel power; a central aim for the future of global nuclear security will be a strong commitment and requirement for (i) the physical and technical protection of nuclear materials, (ii) the meticulous accounting of nuclear materials, and (iii) the highly-accurate monitoring of nuclear sites and borders – incorporating a strong focus on evolving technologies, automation, robotics and the Internet of Things (IoT). However, whilst representing a key opportunity for improved safeguarding and monitoring, there lies a range of potential threats from each of these technologies (as is the case with any such system) if not employed for the correct means by those wishing harm through co-ordinated terrorist acts.

4. Threats and opportunities posed by new technologies

The rapid development of small but computationally powerful devices for a variety of industrial, domestic and recreational uses provides a rapidly evolving opportunity and threat register for nuclear facilities worldwide. As such, the topic of nuclear security is rarely out of the global media spotlight (BBC News, 2017).

One such opportunity, but also a potential threat in the future of global nuclear security, is the rapidly evolving field of drone or unmanned aerial vehicle (UAV) technology. Accelerated markedly by the events at the Fukushima Daiichi Nuclear Power Plant in Japan, lightweight systems have been developed by a number of authors (Kurvinen et al., 2005; Martin et al., 2015; Sanada et al., 2012), each capable of achieving substantial flight durations and distances (> 30 min and 10’s of km). When combined with the range of existing available detection options, UAVs represent a means by which to gather large volumes of valuable data over nuclear sites or in response to radiological incidents. However, the availability of these systems to the public, coupled with the ease at which they are operated (using a combination of conventional hand-held remote controls and GPS waypoints) has already been seen to impact upon operations surrounding airports – with numerous reports of unidentified aircraft or airspace incursions around the world (Federal Aviation Authority (FAA), 2016).

The potential use of these systems for physical attacks (not only on nuclear institutions) has been viewed as significant by a UK thinktank (The Remote Control Project, 2016), with a number of media articles also documenting recent global events (Nicas, 2015; Warrick, 2017). Possible scenarios range from (i) utilising drones to carry explosive materials into a nuclear site, potentially producing a criticality incident in the acquisition of radioactive material – using unmanned aerial systems to disperse this contaminant material over a wide area, or population centre.

Considerable recent advancements in artificial intelligence (AI) technology could prove beneficial for improving site monitoring using these UAVs and without the need for operator input and guidance. Conversely UAVs could also be employed in physical attacks (Clark, 2015). In these cases, the UAV operator need not be in direct communication with the system during the attack with the drone targeting pre-defined positions on the ground. Whilst a lone, well targeted UAV system could cause moderate disruption and damage to a single item of nuclear infrastructure, a coordinated ‘swarm’ could pose a much more substantial threat. The term ‘swarm’ technology, was a concept introduced by Beni and Wang (1993), whereby multiple robotic systems can operate as a group independent of a human operator. UAV ‘swarms’ could facilitate simultaneous co-ordinated attacks of a site / sites, using a significant number of airborne systems inbound from different heights, directions and at different speeds; in sufficient numbers such that existing defences would be overwhelmed.

The last ten years has also seen the accelerated advancement of battery technology with which to power these unmanned aerial platforms. As a result of considerable research effort from both industry and academia, the amount of electrical charge that can be stored within the same physical volume and weight has increased enormously (Scrosati and Garche, 2010). Because of this, the typical survey duration possible with a UAV has grown, and hence accordingly, the distance from which attacks can take place has also increased.
4.1. Development of dynamic monitoring networks for nuclear monitoring

In addition to this remotely operated airborne technology, the use of other robotic systems, within advanced monitoring capabilities, contributes positively to the wider field of dynamic radiation monitoring. As a direct result of the extensive advancements that have occurred in radiation detectors and their miniaturisation, a powerful suite of technology now exists to enhance the current strength of nuclear security. This enhanced detection capability has enabled the production of “dynamic sensor networks”, whereby a range of sensors can be deployed using a range of mobile platforms, all feeding back autonomously in near real-time to produce an extensive data network of a site or incident. The use of AI to process the numerous coincident data streams, much like the human brain manages inputs from the body’s nervous system, means that temporal anomalies recorded by the sensors in the network representing a divergence from a known and calibrated baseline for the site can be rapidly verified and enacted upon.

As well as UAVs, mobile platforms able to carry these increasingly more capable radiation detection devices include humans and cars, however other (less mainstream) systems for dynamically monitoring radiation include hovercraft (Jones et al., 1999) and pipe-crawlers (Roman et al., 1993). Current work to advance the scope of dynamic monitoring networks for nuclear security is investigating other remotely operated vehicles (ROVs) such as inflatable airships and miniaturised underwater subsimmers.

Whereas dynamic sensor networks represent a means to actively “search” for radiation anomalies, their inherent complexity, with the required upkeep of the physical carrier platform, as well as the potential challenges in referencing their position over the duration of their survey means that static (fixed position) systems will always exist as a backbone within the future of nuclear site security onto which dynamic ones are incorporated. Again, with the recent progression in detector technology, numerous static systems that can be placed strategically around nuclear sites or dispersed within a public setting, for continual monitoring – typically based on gamma-ray detection (Lin et al., 2004; Nabeshima et al., 1996). Typical examples of such systems include “portals” (typically large archways) and “pads” (everyday objects such as road cones, speed-humps and safety barriers) within both large arrays of highly-sensitive gamma-ray detectors can be installed to monitor for activity above normal background levels. Stemming from work at CERN (Large Hadron Collider), the application of muon tomography and scattering (utilising naturally occurring sub-atomic particles incident from space) for the detection as well as determination of the type of any radioactive source material, is a further detection method that now exists as part of the global nuclear security portfolio, most commonly for the scanning of entire shipping containers or large transport vehicles (Baesso et al., 2012; Borozdin et al., 2003; Thomay et al., 2016).

All of the detectors employed as part of dynamic systems are hence required to be both small and highly-portable, being widely dispersed via the aforementioned range of potential carriers to provide a wide spatial coverage. This distribution of hundreds, if not thousands (or hypothetically tens of thousands), of various sensor types and their real-time feedback to a single command point from where all of the information converges, is dependent on mass-network connectivity, the ability to stream (securely) data wirelessly at a sufficiently rate and subsequently reprocess it efficiently (Hart and Martinez, 2006). Data acquired from static sensors presents less of an issue with regards to data transmission due to their fixed position over time, and hence less of a need for high-end data infrastructure and extensive coverage in the case of continually moving, dynamic systems. Through deploying this wide range of sensor options for monitoring, a ‘hub’ from which all the platforms are capable from being dispersed and collating incoming data steam is required. This hub would typically act as a ‘node’ via which data acquired by the systems would be collated before transmission to a central data facility. There is also the potential for this technology to be used in a more covert method, to deliver a counter-proliferation capability, in identifying illicit nuclear weapons sites and materials.

4.2. Deployment of passive versus active sensors

Each of the detectors mentioned in the previous section may be referred to as “passive”, whereby there is no external input of energy in order to stimulate the detection of any potential radioactive material (Knoll, 2010; Tsoulfanidis and Landsberger, 2015). The contrasting type of system is what is termed “active”. Unlike the smaller, cheaper and more readily transportable passive detectors, active type detectors require the production of highly penetrating beams to determine the internal structure of a large volume. Such systems include the use of neutrons, electron / neutron-induced gamma-flash or laser scanning to examine the contents of objects such as barrels and large containers (Estre et al., 2013; Jones et al., 2016).

Like any electronic device; to enable it to function even for short periods it is required to receive power. For large, “active” devices this demand is considerable – with vast quantities needed for their operation, supplied through dedicated power networks. On the other hand, smaller “passive” devices which do not need to produce an activating source to detect radioactive material, call for markedly less power. As a result, potential exists for such low-power (static) devices (that remain stationary indefinitely) to benefit from advancements in long-term power supply for applications such as radiation store monitoring. Using natural radioactive decay; such as that associated with $^{239}$Pu, $^{241}$Am or more recently the β-decay of $^{14}$C, a small but sufficient current can be produced to provide power to devices – acting as a “nuclear battery” to trickle-charge systems (EPSRC, 2013) (Patent Applications 17074485.6 and 62/504,012). The system (Fig. 5), using a diamond tri-layer surrounded by metallic contacts, has been invited to be able to provide thousands of hours of current from materials otherwise considered as costly waste following power generation.

Current detector technology and the mechanisms by which to deploy it for continued nuclear security into the future have witnessed extensive progression over recent years, with great advancements in detector crystal production, miniaturisation and spectral resolution (Carchon et al., 2007; Zhang et al., 2013). With the explosion in the number of these detectors and limitless potential locations where they could be installed, the future will likely not lie in the detection hardware itself, but in their connectivity, automation, combined sensitivity and ultimately how best to utilise the “big data” generated by such a network of assorted sensor technology. Additional sensors can be incorporated alongside the radiation sensor in order to provide greater situational awareness around any detection incident. This enables a more detailed understand of what was in the area at the time of detection to help focus appropriate responses.

Fig. 5. Schematic of the proposed diamond battery, consisting of the multi-layer setup with differing forms of diamond (radioactive and stable) encased within metallic contacts (EPSRC, 2013).
5. Data security and access

One of the fundamental questions to arise whenever nuclear site data is accumulated is how securely it is held, and who maintains a responsibility for its long-term security (stewardship). There are also additional issues centred on the correct data access and its presentation; making sure that those who require the data at varying levels are given the best and most complete access to it.

To produce high spatial resolution radiation monitoring with the greatest coverage achievable, data will be sourced from a range of not only different sensor types, but also different organisations / bodies. These organisations would typically include private companies such as power plants, reprocessing facilities and the operators of large indoor/outdoor event spaces in addition to public and law-enforcement groups. While the data derived from these sources would constitute part of a combined data-map; certain data obtained from specific sites or found to constitute “interesting” or “abnormal” results may not be fully disclosed, representing issues surrounding data ownership and how information pertinent to nuclear security should be shared. To provide data into this combined system, complications arise surrounding its transmission and processing. Whilst the Internet of Things (IoT) is beginning to facilitate greater connectivity than ever before – revolutionising the data demand, questions need to be asked of how securely the considerable quantity of data originating from the extensive sensor network will be communicated back to locations where it is collected and monitored. Recent high-profile data hacks and system intrusions of large companies have highlighted the vulnerability of many of what were assumed to be highly secure and well defended systems – comprising high-end encryption and cutting-edge software (BBC News, 2016). With the production of a shared repository into which different groups and organisations deposit their data as part of a larger collective, issues regarding the responsibility to protect and manage this data need to be addressed. Through “Quantum Encryption” over traditionally employed mathematical encryption forms, this future form of data-handling will permit large data volumes to be transmitted securely with clear knowledge of whether any data had been intercepted on route (Boykin and Roychoudhury, 2000; Chen et al., 2008).

Attacks on computer networks as a result of the connected system are only a small portion of the negatives, however, that result from the IoT – with the 2015 Dell Annual Threat Report concluding that the number of attacks on corporate and industrial networks has been increasing by 100% year-on-year from 2013 (Dell, 2015).

Due to the range of differing sensors and carrier platforms that exist in addition to its transfer via the IoT, the data that is produced will vary considerably in its resolution and granularity. Relating back to the issue of data access and roles in future safeguarding; whereas the data may be collected at high resolution in many areas (and lower, more commonly at others), there represents the need to control (and streamline) what data is either seen by certain individuals and groups as well as the resolution at which they meet. For example, those interested in the continual routine monitoring of buildings and individual sites such as plant operators will demand data at increased resolution than emergency response groups such as the UK’s Cabinet Office Briefing Rooms (COBR) – where a wider overview of the data is demanded.

Indeed, The Sendai Framework argues that to ‘understand disaster risk’ it is necessary to ‘promote real time access to reliable data, make use of spatial and local sensors, including geographic information systems (GIS), and use information and communications technology innovations to enhance measurement tools and the collection, analysis and dissemination of data’. Risk mitigation must be built upon an empirically grounded understanding of the nature of the hazards, requiring an improvement of the integration of scientific knowledge into government and community decision-making (United Nations Office for Disaster Risk Reduction, 2015).

6. Conclusion

In conclusion, whilst future risks to national and international nuclear security will still be posed by groups or individuals wanting to undertake direct physical violence or destruction, there will be a growing threat posed directly or in conjunction with physical attacks by more technologically-advanced methods. Whilst there still exists a credible threat from physical attacks on nuclear infrastructure or from groups dispersing acquired radioactive material within populated environments, the likelihood of an attack is considered to be low and the threat level remains relatively constant. However, as a deterrent and a representative illustration of capacity to prevent such attacks, a traditional armed and physical security presence will continue to be required on nuclear sites.

By contrast, the global evolution of smart technologies is unabated, with the world having evolved unrecognisably over the past half a century, mostly for good – with the invention and accessibility of the internet recognised as pivotal in our history. Despite the immense benefits that these technologies have brought to society, including quantifiable benefits for the nuclear sector, the IoT and smart technologies more widely may also be viewed as one of the greatest potential threats to global nuclear security over the foreseeable future. A comprehensive and joined up physical and cyber security plan (both covering the threat from an insider) is essential to counter the current threats to the global nuclear sector. Some arising technologies will present both a threat and an opportunity, e.g. the application of UAVs in routine nuclear/security monitoring and emergency/security assessment are of considerable promise, but at the same time present a security threat, as many nuclear sites are not currently fully prepared for the detection or prevention of co-ordinated incursions.

Ultimately, organisations responsible for nuclear safety and security must be obliged to stay up to date with both emerging physical and digital technologies that could enhance or pose a threat with respect to nuclear monitoring, security and safeguards. The further development of outcome based security regulation, placing the onus on the nuclear site to demonstrate security/system effectiveness, should encourage a more innovative approach to tackling the threat. Instead of the historical prescriptive approach to security regulation, a change in this methodology will encourage a stronger uptake of emerging beneficial technologies and stimulate the faster development of countermeasures against those which pose a threat. This will likely necessitate close liaison and resource sharing between defence and intelligence agencies, delivering further tangential benefits in other areas of national and international security outside of nuclear.

Author contributions and interests

All authors (PGM, NGT and TBS) contributed equally to the content of the article. PGM produced the figures included within the manuscript.

The authors report no competing financial interests.

References
