Nuclear Free Local Authorities
briefing

Date: 23rd May 2016 **No.145**

Subject: Nuclear security concerns – how secure is the UK civil nuclear sector?

1. Overview of report

This report has been developed by Dr David Lowry, former Director of the European Proliferation Information Centre in London and a senior research fellow with the Institute for Resource and Security Studies in Cambridge, USA; in full conjunction with the NFLA Secretary. It considers one of the most sensitive areas of nuclear policy – the security around nuclear sites, nuclear material transports and the protection of nuclear materials in the UK and at the international level. Due to its sensitivity and issues around national security, this is one of the more difficult and delicate areas with which to have significant public engagement with government at the national and international level. Recent meetings of the DECC NGO Forum Nuclear Security sub-group have reiterated how difficult it can be to have an in-depth and wide-ranging discussion on nuclear security matters.

This Policy Briefing attempts to bring forward a number of strands to the nuclear security debate in order to inform NFLA member authorities, nuclear policy NGOs and nuclear regulatory agencies. It also provides an analysis of some of the perceived risks within this area of policy. The aim of this report is to highlight some of the key security threats, and provide more detail to them. NFLA also seeks to directly engage with government and nuclear regulatory agencies on such issues, as far as it is practical to do so. Although nuclear security is a sensitive issue, NFLA considers that the UK Government should engage in greater dialogue in some areas without jeopardising security.

2. Introduction

> *"More than 10 years after the 9/11 hijackers considered flying a fully loaded passenger jet into a Manhattan area nuclear reactor, U.S. commercial and research nuclear facilities remain inadequately protected against two credible terrorist threats – the theft of bomb-grade material to make a nuclear weapon, and sabotage attacks intended to cause a reactor meltdown." (1) **

This briefing focuses on a selection of key and emerging nuclear security threats in the civil sector, and it then considers the responses that are being made to these threats. The NFLA also make a number of conclusions and recommendations for government and the nuclear sector to consider and act upon. A separate briefing on defence nuclear safety and security is in preparation.

The threats that are considered include:

- the risks to a nuclear site from an 'insider' attack;
- the risks from the loss of sensitive information on nuclear facilities;
- the risks from a 'cyber attack' and attacks on information security at a nuclear site;
- the risks and potential damage from an aircraft attack;
- the risks from a malicious attack on a nuclear material transport;
- the risks from a 'drone' type device on a nuclear site.

** This briefing relies considerably on primary sources from the United States, which, although it has been the subject of the most destructive international terrorist attack in history, is a nation substantially more open and transparent in publishing key studies on nuclear security than the UK.*

C/o NFLA Secretariat, Nuclear Policy, City Policy, Level 5, Town Hall Extension, Manchester, M60 3NY
Tel: 0161 234 3244 E-Mail: s.morris4@manchester.gov.uk Website: http://www.nuclearpolicy.info

The nuclear security threats:

3. Potential for a malicious attack from a nuclear insider

Insider threats have been described as "perhaps the most serious challenges that nuclear security systems face". (2) Operators of nuclear facilities are well aware of the potential security threat posed by insiders, be they disgruntled employees, individuals who have been coerced into helping others, or people who have infiltrated an organisation with the express intention of causing harm. Due to this potential threat, a vetting system is operated for all those inside the security fence at nuclear facilities, although there have been reported (in the annual reports of the US nuclear security regulator) difficulties in the efficient operation of vetting procedures, including insufficient resources and staffing.

A similar vetting system is operated in the UK, and a recent example of the risks from an insider threat occurred at the Hunterston site in October 2015. In this case a nuclear plant worker was found reading information on-site about how to make bombs. A fellow worker alerted authorities and the worker was removed forthwith from the site, pending a Police investigation. (3)

In the US, the Federal Bureau of Investigation (FBI) operates a "Watch List" to unmask suspected malevolent actors. Immediately following September 11, 2001 - and for several weeks afterwards - the US Nuclear Regulatory Commission (NRC) worked with the FBI, the Nuclear Energy Institute (a private organization that represents the nuclear industry), and licensees to review access authorisation lists of employees working at nuclear power plants and other licensed facilities to identify any individual whose name also appeared on the FBI 'Watch List'. Based on this extensive review, the NRC and FBI determined that there were no positive matches between the licensees' and the FBI's access authorisation lists. However, the NRC continues to receive a steady flow of information from the intelligence community, law enforcement authorities, and licensees that is evaluated promptly for any possible action. (4) It can be assumed similar procedures exist in the UK.

Dr Matthew Bunn, a Professor at Harvard University's John F. Kennedy School of Government and Co-Principle Investigator with the 'Project on Managing the Atom' at Harvard Kennedy School's Belfer Center for Science and International Affairs, has led a study of Insider threats, along with his co-author, Dr Scott Sagan, a Senior Fellow at the Freeman Spogli Institute for International Studies. They have published a research paper offering a "worst practices" guide on protecting against insider threats. This has real utility for the global nuclear industry. (5)

In it, they considered past disasters caused by insiders, from the assassination of Indira Gandhi to the mass shooting by a US soldier at the Fort Hood military base in Texas, and drew from them ten lessons about what *not* to do in designing protections against insiders. The key point they assert is *'don't assume'*. Assess, test, and always look to find and fix any vulnerabilities that are found.

Lessons learned: don't assume -

In their paper, Bunn and Sagan offer some key advice and insights based on lessons learned from past insider incidents:

- Don't assume that serious insider threats are NIMO (not in my organization).
- Don't assume that background checks will solve the insider problem.
- Don't assume that red flags will be read properly.
- Don't assume that insider conspiracies are impossible.
- Don't assume that organisational culture and employee disgruntlement don't matter.
- Don't forget that insiders may know about security measures and how to work around them.
- Don't assume that security rules are followed.
- Don't assume that only consciously malicious insider actions matter.
- Don't focus only on prevention and miss opportunities for mitigation. (6)

This seems to the NFLA a very sensible and practical strategy to be considered for the UK context.

4. Security threats from the loss of sensitive nuclear information

The loss or theft of documents or information relating to sensitive nuclear systems also represents a security risk. Such information could assist in the proliferation of nuclear weapons, allow security

systems at a nuclear site to be side-stepped, or provide details of vulnerable points in a nuclear design.

Infiltration of civil nuclear facilities is a critical threat. In recent years there have been several instances reported, including many discussed in a contemporary analysis by Allison Macfarlane, Professor of Science and Technology Policy at George Washington University. Professor Macfarlane recently served as Chairman of the U.S. Nuclear Regulatory Commission from July, 2012 until December, 2014. (7)

Professor Macfarlane argues that nuclear states need to follow the tight security model developed in the United States over the past decade. She remains concerned that there are no global standards for physical protection at civil nuclear facilities, meaning that there is a lack of consistency in protecting sites from the loss of sensitive nuclear information. Professor Macfarlane recommends that security forces at nuclear facilities (in the UK this is undertaken by the Civil Nuclear Constabulary) should be required to practice attack scenarios regularly under the oversight of independent observers. NFLA would recommend such a practice in the UK.

Such concerns have become particularly relevant after disturbing information has come to light in the activity of the cell members responsible for the Paris and Brussels terror attacks in November 2015 and February 2016 respectively. Reports have emerged that some of the suspects had a number of files on nuclear facilities and had been monitoring the activity of nuclear plant workers. (8)

It would appear that one of the consequences of these security revelations is that the Belgian Government has decided to issue the entire population of Belgium with iodine tablets, which are essential in limiting the effects of radiation on the body in the event of a radiation release. The Netherlands Government has followed suit with a similar policy.

NFLA poses the question as to why the UK Government is also not following suit. NFLA understands there are stocks of iodine tablets at regional centres ready for swift deployment. Given the increased threat arising from these types of incidents NFLA urges the Government to reconsider the need for a national release of iodine tablets to cover not just existing nuclear sites but from the potential for an attack by a malevolent group on a nuclear material transport. (9)

5. Cyber security concerns

Computer systems that help operate nuclear reactors and their safety equipment are isolated from the internet to protect against outside intrusion. However, the nuclear industry does take additional measures to ensure that its nuclear plants are protected from ‘cyber’ attacks, which in this context can be defined as all efforts to disrupt, deny, degrade, distort or destroy electronic information that organisations rely upon, store, process and generate.

Although the September 11 terrorist attacks had no cyber component, the global nuclear energy industry took the initiative following those events to implement a cyber security program. The industry formed a task force, which developed comprehensive guidelines for protecting against cyber vulnerabilities. In the US for example, the NRC endorsed the industry guidelines in 2005. By May 2008, all operating nuclear plants had implemented the guidelines voluntarily.

The NRC security rule issued in 2009 required enhancements to cyber security at nuclear power plants. All companies that operate nuclear plants or seek to license new plants have developed and submitted plans for cyber security, including requirements pertaining to individuals who have electronic means to interfere with plant safety, security or emergency preparedness functions or critical equipment that supports those functions. (10)

To give a recent and highly relevant example of how cyber attacks can be used against the global nuclear industry is that of ‘Stuxnet’. This was a malware program widely believed to have been created by the US and Israel which infected a Russian nuclear power plant, according to cyber security expert Eugene Kaspersky. The virus is believed to have been introduced to the Natanz plant using an infected memory stick, demonstrating that isolation from external networks is no guarantee of protection against cyber ‘infection’ in the nuclear industry.

Speaking at the Canberra Press Club in Australia in 2013, Kaspersky criticised the government departments responsible for engineering such cyber-attacks, saying: “They don’t understand that in cyberspace, everything you do - it’s a boomerang: it will get back to you.”

The ‘Stuxnet’ virus was also found to specifically target industrial control systems manufactured by Siemens. The initial target of the virus is widely thought to have been the centrifuges used in Iran’s uranium enrichment program. The country’s then-President, Mahmoud Ahmadinejad, confirmed in November 2010 that ‘Stuxnet’ had “managed to create problems for a limited number of our centrifuges.” (11)

One of the most concerning issues with the ‘Stuxnet’ virus is that its method of proliferation has been indiscriminate and the code has since been found on computers across the world – many not even connected to the nuclear industry. In a 2012 report, the New York Times suggested that the US Government chose to continue cyber-attacks against Iran even after the existence of ‘Stuxnet’ became public. (12)

In reference to the use of cyber-warfare by national governments, Kaspersky has said: “They don’t understand that it’s possible to shut down power plants, power grids, even the international space station. They don’t know what to do.”

The scale of the problem with cyber security and the nuclear industry is also laid bare in a January 2016 report published by the Nuclear Threat Initiative. The study notes that as many as twenty countries with significant atomic stockpiles or nuclear power plants have no government regulations requiring minimal protection of those facilities against cyber attacks.

The study considered whether any cyber-protections are required by law or regulation at nuclear facilities, and whether cyber attacks are included in the assessments of potential threats to the security of those installations. One question asked whether there were mandated drills and tests to assess responses to a cyber assault, rather than just a physical attack on the facilities. Amongst the twenty countries of concern were Argentina, China, Egypt, Israel, Mexico and North Korea.

Because of the secrecy surrounding military nuclear facilities, the report found it impossible to determine the levels of cyber protection used to protect nuclear weapons in the nine countries known to possess them. The report concluded that President Obama’s global initiative to sweep up loose nuclear material, which was the subject of the fourth and final nuclear security summit meeting in March (noted below), has slowed substantially. (13)

The CEO and former Chairman of the US Committee on Armed Service, Sam Nunn, commented:
“I believe it is fair to say that today we are at a crossroads on nuclear security. When the 2016 Nuclear Security Summit opens, leaders will have important questions to answer: Will they take the difficult steps needed to better protect against nuclear theft, attack, and sabotage? Will they work together to build the global architecture needed to protect against catastrophic nuclear terrorism? Will they sustain the momentum that the summit process created? Because the consequences of an act of nuclear terrorism would reverberate around the globe, leaders also have an obligation to work together. We are in a race between cooperation and catastrophe, and the world’s leaders must run faster”. (14)

In considering the United States ‘perfect’ cyber security score in the NTI report, Dr Edwin Lyman, Senior Scientist of the Union of Concerned Scientists commented that the US NRC does not require nuclear fuel production facilities, some possessing weapon-usable materials, to have comprehensive programs to protect against cyber attack. The NRC is working on such a rule, but it may not be in place for years. Meanwhile, the Nuclear Energy Institute, the United States nuclear industry’s chief trade association, questions the need for such a requirement, maintaining that voluntary industry efforts will suffice. The institute has also petitioned the NRC to weaken cyber security rules already on the books for nuclear power plants. Dr Layman argues the US Government cannot lecture other nuclear states on such matters unless it resolves this issue. (15) NFLA would suggest the UK Government and UK nuclear regulators also need to consider such matters in much more detail as well.

The spring 2016 issue of 'Cyber Security Review' also discusses how the Israeli government remotely disabled the radar system that protected a secret Syrian nuclear facility using a cyber attack in Operation Orchid. This example shows how truly effective cyber attacks can be on nuclear facilities. (16)

6. Aircraft Crashes and Nuclear Sites – the key effects of the 9/11 attacks

In the immediate aftermath of the devastating September 11th 2001 terrorist attacks the US Nuclear Regulatory Commission (NRC) activated its Incident Response Centre at NRC Headquarters and in its regional offices, staffed the centres with teams of top officials and technical experts. It maintained this staffing for several months afterwards. The NRC advised its licensees to go to the highest level of security and the agency established communications with the FBI, the federal Department of Energy, and the Federal Emergency Management Agency, among others. It is highly likely similar arrangements were established in other nuclear states, like the UK.

On 21st September 2001 the NRC admitted it:
"…*did not specifically contemplate attacks by aircraft such as Boeing 757s or 767s and nuclear power plants were not designed to withstand such crashes*." (17)

UK-based consultant nuclear engineer, Dr John Large, in a public presentation of a confidential report on forecasting the 'Possible Outcome and Consequences of a Terrorist Attack' says:
"…if it is acknowledged that an accidental aircraft crash could lead to a very severe radioactive release then, however remote the probability of this event, there is a requirement that the consequences be identified and assessed. Put another way, this is a consequence analysis approach that disregards any offset from the probabilistic value of a foreseeable event happening. If the aircraft crash is an act of sabotage then the probability must be assumed at unity and the event considered only in terms of its consequence mitigation." (18)

His main conclusions are that:

a) None of the UK's nuclear reactors has a containment which has been specifically designed to resist aircraft attack, other than at Sizewell B where the reactor secondary containment dome is designed to resist an accidental impact of a light aircraft.
b) None of the radioactive waste and spent fuel facilities, at the nuclear power plants and at Sellafield, could withstand the directed impact of a fully loaded commercial airliner.
c) Many of the radioactive waste and fuel storage facilities, again at the nuclear power plants and at Sellafield, contain massive amounts of radioactive material available for suspension and dispersal in the aftermath of a terrorist attack.

Immediately after the terrorist attacks in the United States, the IAEA Board of Governors and the General Conference endorsed recommendations on 'Physical Protection Objectives and Fundamental Principles' as an important step to strengthen the international physical protection framework. The main principle set out in this framework is that *"responsibility for the establishment, implementation and maintenance of a physical protection regime within a State rests entirely with that State."* (19)

Dr Gordon Thompson of the Institute of Resource and Security Studies has also presented similar analysis to a NFLA UK and Irish Conference on Nuclear Hazards of the disastrous damage and wider risks that could take place from an aircraft attack on spent fuel ponds – such as at Sellafield – by a small aircraft loaded with explosives. In the presentation he noted that defence policies needed to recognise nuclear power stations as potential 'pre-deployed radiological weapons'. It should be noted also that a partial drainage of a spent fuel pond is much more dangerous than a complete failure due to reduced air cooling. Dr Thompson has regularly called for a new paradigm on international and homeland security. (20)

Obviously, a calculated professional attack on a nuclear station using an aircraft could be devastating. However, as lethal technology gets ever more destructive, the likes of small drones, automatic weapons, rocket propelled grenades, and/or demolition charges, are becoming of increasing concern. The technology of some modern missiles, for example hidden on board a passing yacht, motor boat or truck, can potentially penetrate several metres of concrete (it may

take two missiles a few seconds apart) and the thickest practical armour plate. (21) (22) For example, the sinking of an Israeli destroyer as long ago as 1967 by a missile-carrying motor boat, or the much more recent attack on the USS Cole in Aden, Yemen in October 2000, which killed 18 crew members and nearly sank the ship. (23)

7. Risks from an attack on a nuclear material transport

One of the key issues for UK nuclear regulators and policy makers is around security with the transportation of radioactive materials and their protection from a malicious attack. Many transports of radioactive materials involve mildly radioactive material such as pharmaceuticals, ores, low-level radioactive waste, and consumer products containing radionuclides (e.g., watches, smoke detectors). However, increasing quantities of much more radioactive - and thus hazardous - nuclear materials such as irradiated ("spent") nuclear fuel and fresh, un-irradiated nuclear fuel, including some containing plutonium (in so-called MOX or a mixed oxide plutonium-uranium mix), is beginning to be transported around the UK as the existing nuclear programme is wound down and decommissioned; and a new build programme of over a dozen new reactors distributed around the country is planned.

High-level nuclear waste materials, such as spent nuclear fuel, are transported in very heavy, robust containers, which must meet extremely demanding standards to ensure their integrity in the most severe conditions, including sabotage.

International assessments of risk to transportation casks -

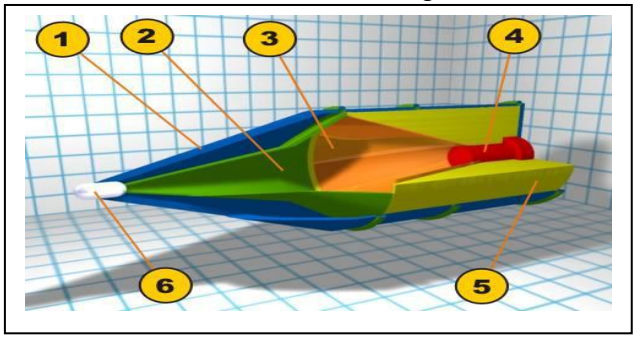
After September 11, 2001, the US NRC issued to licensees special new orders to increase security in the transportation of specific types of radioactive materials, including spent fuel shipments. (24)

The September 11, 2001 terrorist attacks on the US caused the German government to reassess the security of its nuclear power plants and spent fuel storage facilities. The German Nuclear Safety Commission issued a statement recommending that an analysis be carried out on each plant to assess its vulnerability to September 11-type attacks. Plant operators assert that terrorist attacks are a general risk of society and should be treated like attacks on other infrastructure (e.g., chemical facilities). Moreover, general analysis of the impact of the different civilian aircraft on commercial nuclear plants was requested by the German Environment Ministry and has been carried out by a nuclear industry consortium. (25)

A series of tests simulating terrorist attacks on transportation casks were undertaken in Germany, France, the United States (for the German Government), and Switzerland (for the Swiss Government). Additional tests may have been done that are not publicly acknowledged. As long ago as 1979–1980, at the German Army facility in Meppen, a hollow charge (i.e., shaped charge) weapon was fired at a ductile cast iron plate and fuel assembly dummy to simulate a CASTOR cask. The cask plate was perforated but release fractions from the fuel assembly were not examined. From this experiment, the German government concluded that the wall thickness of the cask should not be less than 300 millimetres. (26) (27)

Other tests were carried out at the Centre d'Etude de Gramat in France in 1992 on behalf of the BMU involving shaped charges directed at a CASTOR cask filled with nine fuel element dummies with depleted uranium. The shaped charge perforated the cask and penetrated fuel elements. *This damaged the fuel and resulted in the release of fuel particles from the cask.*

The photographs below show the lethal force though of new missile technology:



January 2008 Test of a Raytheon Shaped Charge, Intended as the Penetration (Precursor) Stage of a Tandem Warhead System

Before test

After test (viewed from the attacked face)

Notes:

(a) These photographs are from: Raytheon, 2008 - Raytheon Company, "Raytheon Unveils New Record-Breaking Bunker Busting Technology", 12 March 2008, accessed at: http://www.raytheon.com/newsroom/feature/bb 03-10/ and cited in Nuclear Regulatory Commission document 'Comments on Draft Consequence Study, **NRC-2013-013ý'** http://www.nrc.gov/docs/ML1322/ML13225A397.pdf

(b) The shaped-charge jet penetrated about 5.9 m into a steel-reinforced concrete block with a thickness of 6.1 metres. Although penetration was incomplete, the block was largely destroyed, as shown. Compressive strength of the concrete was 870 bar.

(c) The shaped charge had a diameter of 61 cm and contained 230 kg of high explosive. It was sized to fit inside the US Air Force's AGM-129 Advanced Cruise Missile.

Such research leaves the NFLA concerned that there may be ways for a determined terrorist group to use weaponry that could be able to pierce nuclear material storage containers transported around the country and the globe. NFLA calls on the Government to make further checks of the structural integrity of storage containers used in the transport of nuclear materials by road, rail, sea and air.

UK issues around the transportation of radioactive materials -

Looking more closely at these issues for the UK, regulations covering the safety and security of transport of nuclear materials are based on the recommendations of the IAEA. (28)

The UK nuclear regulator, ONR states of its responsibilities and mission: "ONR Transport carries out a range of regulatory activities to assure the safe transport of radioactive materials. Approval is granted for the designs of packages used to carry high-hazard radioactive materials to ensure they meet exacting international safety standards, and the packages are built to robust quality assurance plans, and are correctly used and maintained. Regulation is also carried out through a programme of targeted, risk-informed inspections and engagement with duty holders which may lead to interventions. Inspections examine the management systems utilised by duty holders, as well as compliance with safety and security legal requirements. ONR Transport inspects duty holders across nuclear; non-nuclear; and industrial, medical and carrier sectors." (29)

But groups like CND, CORE and the local pressure group Highland Against Nuclear Transport have been critical about the robustness of the ONR oversight of such transports in practice. (30) NFLA have also consistently been raising concerns over the safety of nuclear material transports for a number of years, whether they be of radioactive waste material transports or nuclear weapon convoys (which is being considered in a parallel briefing on the defence nuclear sector).

Of particular recent concern has been the transport of highly radioactive materials from Dounreay to Sellafield. These 'exotic' fuels have been to date sent on rail transports, but the Nuclear Decommissioning Authority (NDA) has also commenced sea transports. NFLA's concern relates to the occurrence of a malicious incident or an accident taking place on a remoter part of the rail network or close to one of Scotland's large towns or cities. Much of the rail network in the Highland region is single-track and could be a considerable distance away from an effective emergency

response. NFLA is also concerned about sea transports which will go through - in the Minches - one of the most treacherous shipping channels in the British Isles, at a time when there is now only one emergency towing vehicle for Scotland, based at Orkney. (31)

NFLA has met twice now with Dounreay and NDA staff on these matters and has tabled a number of detailed questions. It remains unconvinced with the responses so far, and it is awaiting a longer response to its questions from the NDA.

Additional concerns now relate to the potential of using air transport of these materials, in a significant change of UK Government / NDA policy, for on-site management and reprocessing in the United States, as is noted in more detail in Section 9 below.

In a recent Parliamentary answer, it has been confirmed that there have been 23 air transports of nuclear materials from the UK to the United States in recent years. NFLA notes comments made to 'The Guardian' by the independent nuclear engineer, John Large, that such transports may not comply with international safety regulations for civil nuclear transports. He argued that a crash could *"contaminate large tracts of land with potential radiological consequences for unprotected members of the public."* (32)

The UK Energy Minister Andrea Leadsom also informed Parliament in April 2016 of a relevant new report by the Office of Nuclear Regulation (ONR) - "Details of safety events involving the transport of nuclear material both by rail and on the strategic road network".

This report noted that there have been 3866 noteworthy 'events' relating to health and safety and security recorded either at civil sites or with the transport of nuclear materials between the 1st April 2001 and 31st March 2015 (a list which also includes conventional health and safety events). Of these, 3141 were rated on the INES scale as being of 'no nuclear safety significance' (INES level 0 or not rated), and 716 were rated at INES 'level 1 (anomaly), being the lowest level of nuclear safety significance on the INES scale. There were eight events rated at INES Level 2 (incident), and a single event rated at INES level 3 (serious incident), which was in 2005. No events occurred that merited a higher INES rating during this period, and none were designated as 'accidents'. (33)

NFLA welcomes the publication of this report as a serious attempt to develop a culture of openness and transparency between the nuclear regulator and nuclear policy groups on such matters. It also welcomes the steady reduction of incidents in recent years. NFLA still remains to be convinced that the large and increasing amount of nuclear transports taking place in the UK is best practice for the future, despite a good safety record. NFLA would rather see transportation of nuclear materials limited as much as is practical, with safe on-site storage facilities developed instead.

This comment of Dr John Large lay at the heart of NFLA's concerns:
"Movement of nuclear materials is inherently risky both in terms of severe accident and terrorist attack. Not all accident scenarios and accident severities can be foreseen; it is only possible to maintain a limited security cordon around the flask and its consignment; the transportation route will invariably pass through or nearby centres of population; terrorists are able to seek out and exploit vulnerabilities in the transport arrangements and localities on the route; and emergency planning is difficult to maintain over the entire route." (34)

8. The fast emerging threat from drones

The first innovative, small drone attack by a malicious / radical group will inevitably be a wake-up call to public and politicians. This new security threat was not present when the Government's National Policy Statement (NPS) on nuclear power facilities was published in 2011. In 2015, drones were flown close to a number of French nuclear facilities and the security agencies were not clear in the initial phase the identity of those actually using them. This is a perfect example of how unexpected nuclear security threats from drones could be. (35)

The fast emerging 'drones' threat, and the enhanced threat from malicious groups more generally, would suggest that the size of the site area should be reviewed in terms of 'defence-in-depth' security and public safety in any review of the UK Government's national policy statement on nuclear generation. An increase of the in-site area, potentially clear-felled to facilitate the safe

elimination of drones threatening a site, may have significant implications for sites adjacent to populated urban areas, (e.g. Hartlepool), proposed sites for decentralised Small Modular Reactors (SMRs), and sites near or constrained by protected areas e.g. Sites of Special Scientific Interest (SSSIs).

The Government's Nuclear National Policy Statement (using ONR guidelines) currently recommends a site area of 30-50 hectares per (around 1.6 GW) reactor/store with regard to defence-in-depth site security (defined by IAEA), decommissioning area, etc. So a new nuclear reactor - 2.8-3.4 GW twin / triple project - might require a site area (enclosed by the perimeter fence) to be around 60-100 hectares or more. The actual buildings area footprint of a twin / triple reactor project might be around 10 hectares of the perimeter site area. Presumably coastal sites with no public beach access and a (marked) seaward exclusion zone might require a smaller secure land area.

The average drones available at present could potentially carry a few kilograms of shaped demolition charges, shrapnel, poison gas, petrol, chaff, glue, booby-traps, decoys, distraction devices, and so on. One heavily-ladened small drone could probably travel at least 20 mph (9 meters per second) with a load of 5-10 kg. Just one 5 kg shaped charge can penetrate 0.75 meters (30 inches) of reinforced concrete, or 0.25 meters (10 inches) of steel. (36)

Lone, several or mass drone attacks, some pre-programmed and perhaps controlled from remote locations, could be potentially staged against nuclear stations, fuel and waste transports or other sites such as reprocessing and surface waste repository facilities. Other drones could video the proceedings for download to the internet for the use of malicious groups. It may also be possible that multiple or mass drone attacks could precede, be a distraction, or form part of an attack by malicious groups or individuals with heavier demolition charges. It should be noted that just one 20 kg demolition charge can punch a hole through 1.5 meters of concrete. (37) The proposed Hinkley Point C double dome concrete containment walls (dome over reactor and other critical areas) are between 1.3 and 1.8 meters thick. (38) The spent fuel ponds and diesel back-ups proposed at the site are behind a 1.3 to 1.8 metre wall. (39)

It is foreseeable that drones could be launched from vehicles parked close to perimeter fences and could travel quickly, and or possibly stealthily, to a target. Site defence response times (i.e. target acquisition-assessment-decision-action) would be minimal. In 20 to 40 seconds a drone travelling at just 20 mph could cover between 180 to 360 meters. Some currently available drones can now reach 50 mph (40) and are highly controllable and manoeuvrable at speed. (41) It could be very difficult for on-site security forces to be able to stop such a threat from a single or multiple drone attacks.

Drones have the potential to become a major weapon in asymmetric warfare in the 21st Century. The unidentified flights over French nuclear stations in summer 2015 should be seen as a major wake-up call for the nuclear industry. Military drones have been used to considerable effect by the US, UK and Russia in Yemen, Syria, Iraq, Afghanistan and other countries, and by Israel above Gaza.

Another important analysis of the threat from drones was published in March 2015 by Dr David Lochbaum, currently the director of the Nuclear Safety Project for the Union of Concerned Scientists. It argues drones can have positive utility for nuclear power plant safety, by carrying out authorised aerial surveillance; but it also identifies malevolent drone hazards.

Dr Lochbaum writes: *"But drones have a potential dark side. Reports of drones buzzing around French nuclear plants prompted considerable discussion about whether drones carrying explosives could wreak damage. The short answer is yes. The longer answer is that the steps mandated by the US NRC after the 9/11 tragedy, to reduce nuclear plant vulnerabilities to damage inflicted by a piloted aircraft on a suicide mission, also protect against explosive-laden drones. The NRC's post-9/11 upgrades did not eliminate the suicide aircraft threat entirely, however, and multiple explosive-laden drones might be able to overwhelm the upgrades."* (42)

In addition, drones could distract the plant's security responders. Similar to how military pilots use countermeasures to confuse incoming missiles, ground-based attackers could employ drones to lure security responders away from an attack route. In the 'force-on-force' exercises conducted periodically to test nuclear plant security capabilities, mock attackers penetrate fences and proceed rapidly through the plant, simulating the destruction of equipment needed to cool the reactor core.

Security personnel respond to intrusion-detection alarms and to indications that locked doors have been blown open by rushing to take defensive positions behind bullet-resistant enclosures—located between the intruders and the remaining equipment that could trigger a meltdown if sufficiently damaged

The exercises have demonstrated that the responders need not be delayed long to tilt the advantage in favor of the attackers. Drones broadcasting loud sounds of explosions and gunfire, for example, could confuse and slow down the responders. Likewise, collisions with the perimeter fence—activating the intrusion-detection system—could send responders on time-consuming 'wild drone' chases. (43)

In a paper by the 'Remote Control' project of the Network for Social Change, hosted by the Oxford Research Group, they acknowledge that no single countermeasure is completely effective at limiting the hostile use of drones by non-state actors. They therefore suggest that: *"…the United Kingdom adopts a hierarchy of countermeasures encompassing regulatory, passive and active countermeasures, which provides a layered defence. Regulatory countermeasures include point of sale regulations, civil aviation rules and manufacturing standards and restrictions. Passive countermeasures include early warning systems and signal jamming. Active countermeasures include kinetic defence systems, such as missiles, rockets and bullets, and less-lethal systems, such as projectile weapons and net guns. Each stage of the hierarchy of countermeasures requires government action, but it is the regulatory countermeasures upon which it can affect the greatest change."* (44)

NFLA agree with the paper's conclusion that any changes to the law surrounding the use of drones have to be achieved in proportion to the risks. There is also a need to fairly balance interests relating to privacy, individual freedoms and safety with the commercial interest of the nuclear industry.

Global responses to the threat:

9. Global Nuclear Security Summits

In April 2009, President Obama warned that terrorist groups were trying to get nuclear weapons or the materials needed to make them, a danger he called "the most immediate and extreme threat to global security." He called for the international community to join in an effort:
"…*to secure all vulnerable nuclear material around the world in four years*." (45)

Through President Obama's leadership, a series of 'Global Nuclear Security Summits' have taken place over the past five years seeking to increase international co-operation and consensus on the control of vulnerable nuclear material and increasing security for such material. The inaugural Global Nuclear Security Summit in 2010 agreed on the goal of securing all vulnerable nuclear material in four years. This goal implied that many countries would change their nuclear security policies. But the factors that drive changes in nuclear security policies, and that constrain those changes, are not well understood.

The Belfer Centre for Science and International Affairs at Harvard University undertook a survey of nuclear security experts in countries with weapons-usable nuclear material to examine whether countries have made significant changes in their nuclear security and accounting practices in the previous 15 years (to 2014); and what the major drivers of change and the major constraints on change have been, such as through the Nuclear Security Summits. Unsurprisingly, the 9/11 attacks in the United States in 2001 appear to have been the most important single factor in the nuclear security changes over the past 15 years. (46)

However, President Obama's aim of securing all nuclear material within four years appears to be dashed, despite the US Government spending as much as $5 billion on the project. As the US Government prepared for the final summit in Washington DC in March 2016, it appeared that the main hope is for 'modest' achievements rather than broad measures protecting the world from a nuclear terrorist attack. An analysis by Douglas Birch and R. Jeffrey Smith for Politico magazine notes: *"The US administration's focus on what its officials depict as the art of the possible has provoked grumbling from outsiders that progress achieved so far could be undermined after Obama departs in 2017, unless the government mounts a last-minute push for a more sweeping agreement—even one involving only a few dozen like-minded nations instead of a global pact."* (47)

President Obama has taken a very personal interest in these events by leading summit meetings in the US in 2010, South Korea in 2012 and the Netherlands in 2014. Over the course of these summits 53 states have attended them, with 46 of them led by sitting Presidents, Prime Ministers or other heads of state. Some of those leaders brought what the US administration called "gift baskets" meant to highlight their commitment to nuclear security, including offers to ship nuclear explosive materials to the United States or Russia for destruction.

But the meetings left "gaps and fissures" in the patchwork of domestic regulations and international agreements designed to protect nuclear materials from falling into the wrong hands. There now appears a need for Obama to lead an effort to transform the current system before his term of office ends, where it is up to individual countries to decide how seriously to take the protection of their nuclear materials, into one with enforceable international standards. It looks unlikely that will take place at present as there appears to be no international consensus to do so.

Despite some 'incremental success' there also remains serious threats that require urgent attention. Of real concern to governments is the possibility that international terrorist groups like Isis / Daesh or Al-Qaeda may be able to obtain the materials necessary to build an improvised nuclear or radiological weapon. (48)

A 2014 US Government report prepared for the summit acknowledged that there are also hundreds of pounds of weapon-usable uranium at civilian sites in countries like South Africa and Belarus, which do not have the level of security desired for control of such material. There also remains scores of research reactors around the world – as many as 60 alone in Russia for example – where security would be lower than for military sites.

Global plutonium stocks are increasing at the same time, with more than 100 metric tons produced since 1998 – enough material to build 20,000 nuclear weapons. The UK plays a significant part in this increase, with the reprocessing of plutonium at Sellafield. The urgency of this issue has led to the creation of a coalition of over 80 arms control, academic and philanthropic organisations under the banner of the 'Fissile Materials Working Group'. This coalition calls for bold new action by the Obama Administration and other leading nuclear states to create a pathway for agreeing international standards. It also calls on nuclear weapons states to share more information about security practice and expenditures and to fund independent external reviews of them. NFLA supports such a holistic approach. (49)

The 2016 Global Nuclear Security Summit put the threat of ISIL / Daesh using some sort of fissile and/or radioactive material right at the top of the international media terror spotlight, according to CBRN expert, Hamish de Bretton-Gordon, managing director at Avon Protection and a former experienced British Army security officer. The Summit provoked a flood of comment and analysis across the world, except in the UK, where the media almost entirely ignored it. (50)

Only one story - heavily briefed by the UK Government - made the British media. The US and UK Government announced a deal under which 700kg of un-irradiated Highly Enriched Uranium (HEU) - categorised by the NDA as 'exotic fuels' and safely stored at Dounreay - would be transported to the United States in exchange for US nuclear material being sent to Europe for conversion into medical isotopes for diagnosing cancer. As the NFLA noted in an article published by 'The Ecologist', the deal was trumpeted as a 'win-win' for both parties - the United States has more capacity to store and process the HEU, while France and Belgium get 'beneficial' nuclear materials that will help save lives

in the fight against cancer. In digging a little deeper, it would appear to the NFLA that the deal actually looks like a purely commercial decision suiting the UK, US and European nuclear industries - and one that creates a real and serious security risk. It would appear to be a dangerous irony that the main contribution of the UK government from this Global Nuclear Security Summit could be to actually contribute to an increase in nuclear insecurity with new air flights or shipments of radioactive materials potentially going from the UK to the US. (51)

With President Obama's term of office concluding later this year, a key concern remains as to whether some of the positive momentum from these summits will be continued by his successor. Real concerns must remain that a weak international consensus to deal with nuclear security could unravel quickly after Obama stands down.

This threat remains very real. For example, it has recently emerged in February 2016 that the group known as ISIL / Daesh had stolen a laptop-sized case kept in a safe near Basra, which contained a small quantity of iridium-92 used in the oil industry. The group has also captured the facility in Mosul in northern Iraq which houses radioactive isotopes that can potentially be converted into 'dirty bombs' (52)

10. Other global initiatives to combat malicious attacks from terrorist groupings

In February 2014 at Lancaster House in London, the Home Office - supported by the Atomic Weapons Establishment, the Ministry of Defence and the Foreign and Commonwealth Office - hosted a major international gathering of concerned parties to the *Global Initiative to Combat Nuclear Terrorism*, which the UK co-chairs.

In his speech to open the conference, James Brokenshire, the then Home Office Minister responsible for co-ordinating UK counter terrorism policy, focused on how nuclear forensics can help the UK to tackle nuclear terrorism. He stressed that: "*The impact of a terrorist attack involving chemical, biological, radiological or nuclear materials would be potentially catastrophic. Our focus is to ensure that the UK remains a hard target for any terrorist with ambitions to use these materials against us. The UK's national security is the first priority of this government*."

Mr Brokenshire went on to claim that: "…*the likelihood of terrorists obtaining a functioning radiological or nuclear device to attack the UK is low*."

He did however concede: "*The International Atomic Energy Agency's Incident Tracking Database records incidents of radiological and nuclear materials being found outside of regulatory control – and between 1993 and 2012, the IAEA's Trafficking Database recorded 419 incidents of unauthorised possession and criminal activity relating to radiological or nuclear material. And the availability of nuclear material could increase as more nations adopt nuclear energy*." (53)

The Home Office plays a significant role in combating nuclear terrorism, through its border detection system that prevents terrorists from trying to move material in the first place and seeking to catch them if they do. This system is known as 'Cyclamen', and it aims to detect "the illicit importation of radioactive or nuclear materials by terrorists or criminals." It operates across the UK, on a 24/7 basis. It also forms a key part of the strategy to protect the UK from a terrorist attack, being within the Government's 'Contest' counter-terrorism policy. 'Cyclamen' uses a combination of fixed and mobile equipment to screen vehicles, containers, freight and pedestrians for the presence of radioactive and nuclear material at UK points of entry. (54)

The dilemma for the Home Office though is this – whilst it has been pursuing various ways to minimise the dangers from, and impact of failures in nuclear security, other government departments, notably the Department of Energy and Climate Change (DECC) and the Department for Business, Innovation & Skills (BIS) are promoting respectively the indigenous development of a new nuclear programme and the attendant plutonium-based nuclear fuel cycle; and the potential export of nuclear materials, as has been seen with the Dounreay example noted above.

For example, in early 2013, BIS, in taking forward this initiative published a suite of documents supporting the expansion of civil nuclear power in the UK and the nuclear export trade abroad. One key document was: *Nuclear Energy Research and Development Roadmap: Future Pathways.* (55)

This 128 -page document: "…*assesses the needs and opportunities for nuclear energy R&D in the UK in the context of new build of nuclear generation capacity to levels required in a range of scenarios that Government considers plausible. It sets out future R&D pathways that encompass the full range of technologies and capabilities considered capable of delivering a nuclear contribution to electricity generation capacity of up to 75 gigawatts (GW) by around the middle of the 21st century."*

This is equivalent to approximately ***seven*** times the current level of installed nuclear power capacity. Nowhere does the document explicitly recognise the need for complementary research into the implications of this for a robust nuclear security regime.

As far as BIS is concerned this is principally about the commercial opportunity:
"*The global nuclear renaissance provides a multi-billion pound opportunity for those industries involved in the supply of goods and services required for the construction, operation and maintenance, as well as decommissioning, of nuclear power stations and fuel cycle infrastructure*."

This apparent contradiction in policy between, on the one hand seeking to expand and export nuclear power programmes and, on the other, maintaining nuclear security by controlling the movement of nuclear materials and know-how, represents to the NFLA a real challenge for efforts to manage the global proliferation of nuclear technology, with its attendant security risks.

11. NTI research on international nuclear security controls

In early January each year, the respected Washington DC-based Nuclear Threat Initiative (NTI) publishes its annual report assessing the success of such international initiatives. Its report covered factors like national laws, participation in international treaties and security, including whether a state has armed guards protecting its facilities.

Using the data from NTI, the New York Times commented on the 2014 edition:
"There is some rare good news on the issue of securing and containing deadly nuclear materials. In the last two years, seven countries have forsaken their uranium and plutonium stockpiles, bringing the number of nations still possessing appreciable quantities of nuclear fuel usable for bomb-making down to 25. In 1991, the number was 52." (56)

In the report, the countries deserving special praise — Austria, the Czech Republic, Hungary, Mexico, Sweden, Ukraine and Vietnam — effectively gave up their bomb-making capability and now have less than one kilogram (2.2 pounds) of material that can fuel nuclear weapons. Of the countries that still have weapons-usable nuclear material, Australia placed first on the security ranking, because it reduced its supply of nuclear materials and ratified a treaty that commits countries to criminalize acts of nuclear terrorism and to bring nuclear criminals to justice. The United States fell from 10th to joint 11th in part because it failed to ratify two nuclear accords.

Of the 25 states with weapons-usable nuclear materials, the UK is ranked joint 11th with the US. Their relatively low ranking comes out of being bottom of the list for the quantity and amount of sites with such material – the UK has the largest stockpile of plutonium in the world, most of it at Sellafield, where a long-term decision has still to be made as to what to do with it. The UK is though joint second for security and control measures of this material. (57) NFLA welcomes the strong security and control measures that appear to be evident from this analysis but encourages the UK Government to amend their policy on plutonium management by developing, through the Nuclear Decommissioning Authority, strategies to immobile and safely store plutonium on-site.

12. Official UK concerns on nuclear security matters

In early June 2015, the Office for Nuclear Regulation (ONR) issued two documents of relevance to the issue of aerial threats to nuclear facilities and materials in transport: one was the final report of the Chief Nuclear Inspector's Technical Advisory Panel on accidental aircraft crash hazard assessment; the other was a technical appraisal undertaken by avionics experts at Loughborough University.

The Chief Nuclear Inspector concluded in his report that full consideration should be given to hot-air balloons, gyrocopters, gliders, airships and unmanned aerial vehicles being used for a malicious attack on nuclear facilities.

Previously, ONR reported in July 2012 that the then Chief Nuclear Inspector took a decision to convene a Technical Advisory Panel (TAP) on the topic of accidental aircraft crash hazard assessment, because, while he considered that there was confidence in existing methodologies, there would be value in exploring potential improvements to the methods for calculating accidental aircraft crash frequency. The TAP was convened in order for its members to provide independent, objective, authoritative, professional scientific and technical advice to the Chief Nuclear Inspector in the area of accidental aircraft crash hazard assessment. (58)

NFLA welcome this updated study and encourages a full consideration being made as promptly as possible and published, if it is practical to do so.

13. Chatham House study on cyber security and recommendations for dealing with the threat

The independent UK think-tank Chatham House published a detailed study on international cyber security and nuclear security at civil nuclear facilities in October 2015. It concluded that the risk of a serious cyber attack on civil nuclear infrastructure is growing, as facilities become ever more reliant on digital systems and make increasing use of commercial 'off-the-shelf' software.

The report found that the trend to digitization, when combined with a lack of executive-level awareness of the wider risks involved, could lead to nuclear plant personnel being unaware of the full extent of their cyber vulnerability. They could then be inadequately prepared to deal with potential attacks.

Specific findings included:

- The conventional belief that all nuclear facilities are 'air gapped' (isolated from the public internet) is a myth. The commercial benefits of internet connectivity mean that a number of nuclear facilities now have VPN (virtual private network) connections installed, which facility operators are sometimes unaware of.
- Search engines can readily identify critical infrastructure components with such connections.
- Even where facilities are air gapped, this safeguard can be breached with nothing more than a flash drive.
- Supply chain vulnerabilities could mean that equipment used at a nuclear facility risks compromise at any stage.
- A lack of training, combined with communication breakdowns between engineers and security personnel, means that nuclear plant personnel often lack an understanding of key cyber security procedures.
- Reactive rather than proactive approaches to cyber security contribute to the possibility that a nuclear facility might not know of a cyber attack until it is already substantially under way.

In the light of these risks, the report outlines a blend of policy and technical measures that will be required to counter the threats and meet the challenges:

- Developing guidelines to measure cyber security risk in the nuclear industry, including an integrated risk assessment that takes both security and safety measures into account.
- Engaging in robust dialogue with engineers and contractors to raise awareness of the cyber security risk, including the dangers of setting up unauthorized internet connections.
- Implementing rules, where not already in place, to promote good IT hygiene in nuclear facilities (for example to forbid the use of personal devices) and enforcing rules where they do exist.
- Improving disclosure by encouraging anonymous information sharing and the establishment of industrial CERTs (Computer Emergency Response Team).
- Encouraging universal adoption of regulatory standards. (59)

NFLA is alarmed by these specific findings and strongly encourages the UK and international nuclear industry, with support from government and the nuclear regulators, to urgently implement the recommendations of the Chatham House report. As noted above, it appears to NFLA that there remains a lack of clarity in the nuclear sector to the threats from cyber systems.

14. Conclusions and recommendations

NFLA is concerned that the UK Government may be underestimating the serious threat to nuclear operations from determined malevolent actions of radicalised groups or individuals. A key reason why NFLA remains concerned over new nuclear power reactors being promoted and potentially built is the contradiction between a Government policy that is looking to enhance energy security through new nuclear reactors whilst simultaneously asserting nuclear terrorism threats are growing.

This briefing has been developed using publicly available resources to summarise some of the genuine nuclear security concerns that exist.

Following the latest Global Nuclear Summit, NFLA urges the UK Government to continue to work with President Obama and US authorities to transform the current global nuclear security system, where it is up to individual countries to decide how seriously to take the protection of their nuclear materials, into one with enforceable international standards. NFLA are concerned the momentum in this area may significantly reduce as President Obama's terms of office concludes later this year.

NFLA call on a review of nuclear transport guidelines in relation to the structural integrity of transport containers. As local authorities would be involved as a supporting agency to an accident or malicious attack involving such transports, NFLA calls for their full involvement in such discussion.

In light of this, NFLA also urges that real discussion should be taking place between the Government and local authorities and emergency services on how all agencies would need to plan for the aftermath of a nuclear security incident, which could involve substantial amounts of people being evacuated, and medical services being potentially overwhelmed by the numbers of people contaminated by radioactive fallout. NFLA is fully aware of the real sensitivity in such discussion and has been acutely aware of trying as much as possible to not be overly alarmist with this briefing. It does believe it is useful though to highlight in this briefing some of these key issues, given the major emergency response issues that a nuclear security incident could lead to from the emergency services, supported by local authorities.

NFLA will forward this briefing to the UK Government and appropriate nuclear regulatory agencies for comment and sensitive and constructive engagement.

**This briefing is based on a substantially longer (20,000 word) analysis by Dr Lowry, which may be requested from him at: drdavidlowry@hotmail.com.

15. References

(1) Independent Study: U.S. nuclear reactors vulnerable to terrorist attack, University of Texas, 15th August 2013 http://sites.utexas.edu/nppp/files/2013/08/Hastings-PR-2013-Aug-14-rev5.pdf

(2) A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes, Matthew Bunn and Scot D.Sagan, American Academy of Arts and Sciences, 2014.

(3) Daily Record, October 27, 2015. http://www.dailyrecord.co.uk/news/scottish-news/scots-nuclear-plant-worker-6716601#jUzBx7HwqyCF73X.97

(4) Taken from NRC information sheet, April 16, 2014.

(5) See reference (2).

(6) Protecting Against Insider Threats – Lessons of Past Disasters; April 4, 2014; http://nuclearsecuritymatters.belfercenter.org/blog/protecting-against-insider-threats-%E2%80%93-lessons-past-disasters; "When it comes to security at nuclear facilities, danger likely lurks from within, Stanford scholar says Stanford Report," April 24, 2014; http://news.stanford.edu/news/2014/april/nuclear-security-risks-042414.html

(7) Energy Post, "How to protect nuclear plants from terrorists", April 26, 2016; http://www.energypost.eu/protect-nuclear-plants-terrorists/

(8) The Guardian, April 14, 2016, "Paris attacks suspect Salah Abdeslam had German nuclear files: Documents about Juelich centre, used to store atomic waste, were discovered in Abdeslam's flat, say German newspapers"; reuters in Berlin; Guardian, 14 April 2016 http://www.theguardian.com/world/2016/apr/14/paris-attacks-suspect-salah-abdeslam-had-german-nuclear-files
Independent, March 25, 2016 **"**Brussels attacks: Belgium fears Isis seeking to make 'dirty' nuclear bomb: A senior Belgian nuclear official was secretly monitored by suspects linked to the Paris attacks in November,

report claims"; http://www.independent.co.uk/news/world/europe/brussels-attacks-belgium-fears-isis-seeking-to-make-dirty-nuclear-bomb-a6951661.html
(9) Zero Hedge, April 29, 2016 "Amid Rising Fears Of Nuclear Terrorism, Belgium Hands Out Iodine Pills To Entire Population," www.zerohedge.com/news/2016-04-29/amid-rising-fears-nuclear-power-plant-sabotage-terrorism-belgium-hands-out-iodine-pi
(10) Cyber Security in Digital Instrumentation and Controls NRC briefing http://www.nrc.gov/about-nrc/regulatory/research/digital/key-issues/cyber-security.html
(11) Russian nuclear power plant infected by 'Stuxnet' malware says cyber-security expert,' Independent, 12 November 2013; http://www.independent.co.uk/life-style/gadgets-and-tech/news/russian-nuclear-power-plant-infected-by-stuxnet-malware-says-cybersecurity-expert-8935529.html
Also: http://www.independent.co.uk/life-style/gadgets-and-tech/news/russian-nuclear-power-plant-infected-by-stuxnet-malware-says-cybersecurity-expert-8935529.html
(12) New York Times, January 6, 2012 http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyber-attacks-against-iran.html
(13) 'Nuclear Facilities in 20 Countries May Be Easy Targets for Cyber attacks'; David Sanger, New York Times, January 14, 2016 http://www.nytimes.com/2016/01/15/world/nuclear-threat-initiative-cyberattack-study.html
(14) Foreword to NTI Index 2016 by Sam Nunn, January 2016, http://www.ntiindex.org/wp-content/uploads/2013/12/NTI_2016-Index_Foreword_ExecSummary.pdf
(15) 'Nuclear Cybersecurity: Why We Should Worry,' Dr Edwin Lyman, Senior Scientist, Union of Concerned Scientists, Washington DC, letters, New York Times, January 25, 2016 http://www.nytimes.com/2016/01/25/opinion/nuclear-cybersecurity-why-we-should-worry.html?_r=0
(16) The New Yorker, September 17, 2012 Apoc@lypse: the end of the antivirus. When the antivirus *is* the threat - How Israel bombed a Syrian nuclear installation and kept it secret http://www.newyorker.com/magazine/2012/09/17/the-silent-strike
(17) US Nuclear Regulatory Commission, 21st September 2001 http://pbadupws.nrc.gov/docs/ML0201/ML020100489.pdf
(18) Information provided directly by Dr Large to Dr Lowry
(19) International Atomic Energy Authority, 14th September 2001 https://www.iaea.org/About/Policy/GC/GC45/Documents/gc45inf-14.pdf
(20) Dr Gordon Thompson, IRSS, 'Are Nuclear Installations Terrorist Targets?', presentation to UK and Ireland NFLA Conference on Nuclear Hazards, Drogheda, 10th March 2005 – a copy of the presentation is available from the NFLA Secretariat by emailing the NFLA Secretary – s.morris4@manchester.gov.uk
Also see 'Risks and Risk-Reducing Options Associated with Pool Storage of Spent Nuclear Fuel at the Pilgrim and Vermont Yankee Nuclear Power Plants' by Gordon Thompson, Section 8, Institute for Resource and Security Studies, May 2016 http://capedwonwinders.org/wp-content/uploads/pdf/GThompsonForAGO_060525.pdf
(21) See Wikipedia http://en.wikipedia/org/wiki/M203_grenade_launcher
(22) Navweaps.com http://www.navweaps.com/index_tech/tech-103.htm
(23) Ynetnews.com http://www.ynetnews.com/articles/0,7340,L-4198560,00.html
(24) NRC briefing - April 16, 2014; http://www.nrc.gov/security/faq-911.html
(25) Federal Ministry for the Environment, Nature Conservation and Nuclear Safety Summary of GRS study - Protection of German nuclear power plants against the background of the terrorist attacks in the USA on 11 September 2001, English version: http://www.greenpeace.org/raw/content/international/press/reports/protection-ofgerman-nuclear-p-2.pdf
(26) F. Large, G.Pretzsch, J.Döhler, E.Hörmann, H.Busch, and W.Koch. 1994. 'Experimental Determination of UO_2-Release from a Spent Fuel Transport Cask after Shaped Charge Attack'. 35th INMM Annual Meeting Proceedings (Naples, Florida). Vol. 23, pp. 408–413.
(27) RSK (Reaktorsicherheitskommission). 2001. Safety-Related Guidelines for the Dry Interim Storage of Spent Fuel Elements in Storage Casks. Recommendation of the Commission on Reactor Safety. April 5. Available at http://www.rskonline.de/Download/Leitlinien/English/RSK-GUIDELINES-DRY-INTERIM-STORAGE.pdff
(28) Regulations for the Safe Transport of Radioactive Material 2012 Edition; IAEA, Vienna, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1570_web.pdf
(29) Office for Nuclear Regulation http://www.onr.org.uk/transport/
(30) See for example: **"**Pleas made to end the transport of toxic waste through Paisley," Daily Record, 4 March 2016 http://www.dailyrecord.co.uk/news/local-news/pleas-made-end-transport-toxic-7491820#ruc5eTZY2VWqKKqu.97);
"Openness on transportation of uranium in the Highlands is essential," The National, 23 December 2015; http://www.thenational.scot/comment/letters-to-the-national-december-23-openness-on-transportation-of-uranium-in-the-highlands-is-essential.11563
"Public safety compromised and security risks taken," CORE Briefing, 12 December 2015; http://corecumbria.co.uk/news/core-condemns-transport-of-plutonium-fuel-from-scotland-to-sellafield-via-a-storm-damaged-and-flooded-rail-network-public-safety-compromised-and-security-risks-taken/
(31) NFLA Media Release, December 14 2016 http://www.nuclearpolicy.info/news/nfla-calls-for-complete-review-of-nuclear-waste-transports-going-out-from-dounreay-by-rail-sea-road-and-air

(32) The Guardian, March 1, 2016 http://www.theguardian.com/uk-news/2016/mar/01/mod-admits-flyinf-nuclear-materials-between-uk-and-us
(33) Office for Nuclear Regulation, April 2, 2016 http://news.onr.org.uk/2016/02/events-reported-to-nuclear-safety-regulator-2001-15/
(34) Dr John Large, Briefing on the safety of transports of radioactive material transports for Greenpeace UK, 2006 http://www.greenpeace.org.uk/MultimediaFiles/Live/FullReport7848.pdf
(35) The Guardian, 'Drones spotted over seven nuclear sites, says EDF', October 30, 2014 http://www.theguardian.com/environment/2014/oct/30/drones-spotted-over-seven-french-nuclear-sites-says-edf
(36) Global security.org http://www.globalsecurity.org/military/systems/munitions/bullets2-shaped-charge.htm
(37) Federal Business Opportunities.gov https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=8a5b5351149086437c6b80c5a284794a
(38) Areva design for EPR at Hinkley Point http://www.areva.com/EN/operations-5345/epr-reactor-prepared-for-every-situation.html#tab=tab5
(39) Areva EPR design, page 5: http://pbadupws.nrc.gov/docs/ML0522/ML052280176.pdf
(40) Sensefly.com https://www.sensefly.com/drones/ebee.html
(41) You Tube https://www.youtube.com/watch?v=6zDDsX5xYcA
(42) Drones at nuclear power plants: enemies or helpers? See Bulletin of the Atomic Scientists, March23, 2015; http://thebulletin.org/drones-nuclear-power-plants-enemies-or-helpers8132
(43) "Most French Nuclear Plants 'Should Be Shut Down' Over Drone Threat," Newsweek, 24 February 2015.
(44) Oxford Research Group, Network for Social Change's 'Remote Control' project https://sustainablesecurity.org/2016/03/04/how-to-respond-to-the-threat-from-hostile-drones-in-the-uk/
(45) "Remarks by President Barack Obama, Hradcany Square" (Prague, Czech Republic: The White House, Office of the Press Secretary April 5, 2009; http://www.whitehouse.gov/the_press_office/Remarks-by-President-Barack-Obama-In-Prague-As-Delivered/
(46) The Belfer Centre Project on Managing the Atom, Matthew Bunn and Eben Harrell, Threat Perceptions and Drivers of Change in Nuclear Security - Around the World, University of Harvard, March 2014 http://belfercenter.ksg.harvard.edu/files/surveypaperfulltext.pdf
(47) Politico Magazine, Obama's Nuclear Dream Fizzles, June 2015 http://www.politico.com/magazine/story/2015/06/obama-nuclear-wmd-weapons-uranium-regulations-119022.html#ixzz3dK89J5yZ
(48) See for example, The Independent, 23rd May 2015 http://www.independent.co.uk/news/world/middle-east/isis-claims-it-could-buy-its-first-nuclear-weapon-from-pakistan-within-12-months-10270525.html
(49) See reference (44)
(50) "Should we be concerned about the ISIL nuclear and dirty bomb threat; Crisis Response Journal, 13 April 2016; https://www.crisis-response.com/comment/blogpost.php?post=241)
"We Need to Speak Honestly About Nuclear Threats, "*War on the Rocks,* April 11, 2016; http://warontherocks.com/2016/04/we-need-to-speak-honestly-about-nuclear-threats/
"Enhancing nuclear security" Japan Times, 4 April 2016; www.japantimes.co.jp/opinion/2016/04/04/editorials/enhancing-nuclear-security/#.VwwS1uT2aM9; "Obama: The Anti-Anti-Nuke President, by Alan J. Kuperman, New York Times, Op-ed, 25 March 2016; http://www.nytimes.com/2016/03/26/opinion/obama-the-anti-anti-nuke-president.html
(51) "UK-US air transports of high enriched uranium: global security at risk for commercial gain; *The Ecologist*, 3 May 2016; http://www.theecologist.org/News/news_analysis/2987643/ukus_air_transports_of_high_enriched_uranium_global_security_at_risk_for_commercial_gain.html;
"Britain is sending a huge nuclear waste consignment to America – why?"; by Gordon MacKerron, Sussex Energy Group, 6 April 2016; http://blogs.sussex.ac.uk/sussexenergygroup/2016/04/06/britain-is-sending-a-huge-nuclear-waste-consignment-to-america-why/
(52) Radiation dispersal devices, (RDDs) ("Damage Limitation: CBRNE defence in the age of ISIS: Safety & Security International, 2/2016, pp 21-24
(53) Speech by James Brokenshaw, "How nuclear forensics can help us to tackle nuclear terrorism", Home Office, February 2014 https://www.gov.uk/government/speeches/how-nuclear-forensics-can-help-us-to-tackle-nuclear-terrorism
(54) HMRC, The Control and Facilitation of Imports, Supplementary Memorandum from the UK Border Agency, 24th March 2009 http://www.publications.parliament.uk/pc/cm200809/cmselect/cmpubacc/336/9030910.htm
(55) Department of Business, Innovation and Skills, February 2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/168043/bis-13-632-nuclear-energy-research-and-development-roadmap-future-pathway.pdf
(56) New York Times, 11th January 2011 http://www.nytimes.com/2014/01/11/opinion/increasing-nuclear-security.html
(57) Nuclear Threat Initiative, NTI Nuclear Materials Index, 2014 http://ntiindex.org/wp-content/uploads/2014/01/2014-NTI-Index-Report.pdf

(58) A Review and Statistical Modelling of Accidental Aircraft Crashes within Great Britain - Loughborough University, dated 12 September 2014; http://www.onr.org.uk/documents/2015/tap-research-report.pdf
(59) Chatham House study, 'Cyber Security at Civil Nuclear Facilities: Understanding the Risks', October 2015 http://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks