JAPAN SCENARIOS: VULNERABILITY TO TERRORISM OF NUCLEAR SPENT FUEL MANAGEMENT

Recommended Citation

JOAN DIAMOND, PETER HAYES, DAVID VON HIPPEL

August 11, 2017

I. INTRODUCTION

In this essay, the authors present three bold, creative stories about possible non-state nuclear terrorist attacks involving nuclear spent fuel in Japan. These were: a) Frustrated North Koreans attack spent nuclear fuel in Japan; b) Frustrated civil society actors instigate spent fuel terrorism in Japan; and c) Frustrated insiders. Based on these scenarios, fourteen critical questions were posed relevant to wherever spent fuel is found, not only in Japan, including: how to reset standards for spent fuel management and security, how to respond to insider threats, and how to determine which domestic, regional and global conditions militate against versus foster the risk that non-state actors will attack nuclear spent fuel and related fuel cycle facilities for terrorist purposes.

This Special Report was prepared for the *Project on Reducing Risk of Nuclear Terrorism and Spent Fuel Vulnerability In East Asia*. It is based on the scenarios group activity at a Nautilus Institute Workshop at International House, Tokyo, September 14-15, 2015, funded by The Macarthur Foundation. This workshop was conducted under Chatham House rules. Thus, the Nautilus Institute staff prepared this report and is completely responsible for its contents. The narratives in this report also depart in some minor respects from those created at the workshop.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

Banner image: a snarled knot signifying complex, interrelated global problems; created by Nautilus Institute, Beijing scenarios workshop, 2004

II. NAPSNET SPECIAL REPORT BY JOAN DIAMOND, PETER HAYES, DAVID VON HIPPEL

JAPAN SCENARIOS: VULNERABILITY TO TERRORISM OF NUCLEAR SPENT FUEL

MANAGEMENT

August 11, 2017

This report is the first publicly available in-depth scenaric exploration of the threat of terrorism against nuclear spent fuel in Japan.[1] Previous scenario workshops *have* visited the general topic of terrorist attacks in Japan, including against nuclear power plants. For example, in 2007, Japanese, Korean, and American military officials met to discuss pre-defined scenarios, which presented decision-makers with a "chain of regional crises for which they must analyze various possible measures to enhance tripartite collaboration in dealing with disaster, particularly centered on the military's role and capabilities in support of overall national objectives."[2]

One of these scenarios posited "Pirates Threatening to Detonate Hijacked Oil Rig near a Nuclear Power Plant" as it approaches Niigata port. According to the narrative, the pirates were from the "Martyr Brigade a follow-on, poorly organized group of the followers of a religious cult who were attempting to keep the organization functioning"—an obvious reference to residual elements of Japan's Aum Shinrikyo cult that launched terror attacks in Japan from 1990-95. The Brigade's leader broadcasts a radio message and "threatens to create havoc by detonating it in the vicinity of a nuclear power plant, or in Niigata Harbor, creating the "mother of all oil spills." His demands include "the closure of all nuclear power plants; and an apology of the government (for what was not clear)." The participants' task is to figure out how real is this threat, and what to do to defeat it. The initial response attributed to nuclear energy officials after only 35 minutes is "that any danger to a nuclear installation is highly unlikely."[3]

Since 2007, attitudes towards the threat of terrorist attack on nuclear facilities have shifted, both globally and in Japan. Much effort has gone into improving Japan's nuclear security organization and capacities, especially since the Great East Japan Earthquake and Fukushima catastrophe on March 11, 2011.[4] In 2015, Japanese, Chinese, and South Korean ministers met and re-committed to undertaking a regional counter-terrorism strategy.

Over the same period, the US-led campaign to eliminate terrorists with global reach and the actual capacity to launch attacks on defended sites such as nuclear facilities has continued, with mixed success. New organizations have emerged, some with proclaimed nuclear aspirations, substantial funding, and supported by global and local networks.[5] Home-grown terrorist actions have increased, often inspired by religious or nationalist ideologies propagated via the Internet. New technology has also emerged that enables distributed and devolved command-and-control of small group terrorist attacks across borders, including the use of drones, social media as a real-time situational awareness tool, precision targeting using GPS navigation, and improvised explosive devices, including suicide bombers.

Underlying global trends suggest that littoral or coastal cities suffering from extreme inequality and poverty may become transmission belts for global strikes, possibly more than one at a time.[6] The target of choice may be driven as much by practical and logistical considerations as by ideology, the goal being to cripple global flows of information, goods, services, or people as much as to strike a designated enemy. In this regard, the actual victims targeted by mass terror attacks are incidental means to a larger end, and their identity and beliefs are irrelevant to terrorist planning.[7]

Given this array of new and rapidly evolving factors that pertain to the risk of nuclear terrorism, it is

timely to revisit the global issue of the vulnerability of spent fuel and nuclear facilities to non-state attack.[8] Although we have chosen to do so in Japan because the issues of nuclear security are pronounced in the post-Fukushima period and Japan's choices with regard to reactor restart, plutonium reprocessing, recycling, and breeding may have global and regional impact on the risk of nuclear terrorism,[9] these issues are global and generic. That is, they apply to all countries because any country may be the target of nuclear terror using stolen nuclear material; and any country with nuclear facilities may be targeted directly, or be affected hugely by a nuclear terror attack, even in a distant country, just as the Fukushima disaster had global effects on nuclear power.

One way to determine how best to respond to the increasing uncertainty posed by these developments is to employ scenarios methodology—the subject of the rest of this report.

On September 14/15, 2015, The Nautilus Institute for Security and Sustainability convened a workshop in Tokyo. Day 1 was dedicated to a range of analytic, technical and political issues relevant to the vulnerability of spent fuel to terrorism in Japan; and, Day 2 to exploring the implications of that information, using narratives (also referred to as scenarios) to capture the relationship among human, political and technical factors.

Terrorism-Related Spent Fuel Vulnerability Scenarios

As mentioned earlier, the scenarios were based on the knowledge communicated in and the common ground established during the analytic/technical workshop of Day 1.

Nautilus refers to these narratives as "uncertainty" scenarios. Rather than predictive futures based on analytic variables and data models, such scenarios are based on a wide range of possible futures that include not only technical information but individual, social, political, and other non-quantifiable environmental factors.

The purpose of the process is to create courageous and stimulating narratives that will inspire policy makers to include a wider range of possible futures in their planning and foster more robust strategies designed to better "prepare" society for an uncertain future.

The scenarios workshop was led by Masahiro Kakuwa, one of Japan's leading scenarists and Chief Economist, Showa Shell.[10]

He opened the session by quoting Ged Davis of RD Shell:

> *"A scenario is a story that describes a possible future.*
>
> *It identifies some significant events, the main actors and their motivations, and it conveys how the world functions.*
> *Building and using scenarios can help us explore what the future might look like and the likely challenges of living in it."**[11]***

At the end of Day 1, Dr. Kakuwa reviewed and sorted over 100 notes made during the analytical presentations and discussions. He found that the fundamental theme was that terrorists deliberately terrorize and exploit fear to achieve their goals leading in turn to the following key questions for consideration on Day 2.

- *Who would be motivated to use spent nuclear fuel to terrorize Japan and its people?*
- *How close is ISIL to acquiring nuclear weapons?*
- *What, if any, are the implications of terrorists having 100% control of the timing and strategies for*

their attacks (planned human actions are not random), in contrast to naturally caused disasters and many technological failures?

- *Is it true that terrorists don't worry about their own death?*
- *Is Japan merely "lucky" that Islamic State (ISIL), Al Qaeda, and similar groups have not yet carried out an attack on Japanese soil, or is something else at play sparing Japan from such attacks?*

These questions led to the supposition that the types of terrorists most likely to attack Japanese targets were: frustrated North Koreans, possibly outside of the DPRK and not controlled by the DPRK state; frustrated groups from Japanese civil society; and, frustrated "insiders" working at a nuclear facility. Postulating attacks mounted by each of these three groups, respectively, became the basis for the three scenarios that were created during the session. Thus, participants were assigned to a group and given the following guidance by the scenarist.

All participants were charged, with respect to these three scenarios, to:

- *Create a scenario story (that) will identify and illustrate the actors and their motivations, the surrounding scenery, and the flow of time;*
- *Respect multiple possibilities;*
- *Remain open-minded and not reject ideas with immediate criticism.*

Japanese participants were asked to:

- *Explore with bold imagination;*
- *Identify vectors, signals and examples.*

Non-Japanese participants were asked to:

- *Propel stories toward end result(s);*
- *Be inquisitive about logic and flow of the scenarios;*
- *Provide a logical check and ensure consistency of scenario stories;*
- *Help less confident English speakers.*

The facilitator presented a range of techniques for developing the story in each scenario, including identifying drivers of events, causal relationships, and events before (upstream) and after (downstream) the defining terrorist attack in the scenario. The teams were free to use these or any other tools to create their narratives.

With this foundation, the teams set out to craft plausible yet bold stories.

SCENARIO 1

Frustrated North Koreans attack spent nuclear fuel in Japan

The group first reviewed notes and insights from the discussions on Day 1. These were not intended to limit scenaric thinking to what had been identified, but rather to fuel it. Topics included the possible collapse of North Korea; positing that a group of North Koreans occupied Fukuoka; and the possibility that North Korean non-state actors might exist, even outside the control of the North

Korean state. The core issue to be addressed was: “Why would North Koreans terrorize Japan?”

This question of plausibility of an attack originating somehow from North Korea immediately led to related questions, including what would motivate a North Korean terrorist attack. Two possible motivations were examined. The first was an actual war between Japan and North Korea. The second was the living memory of Korean survivors of the Nagasaki and Hiroshima nuclear bombings, now living in North and South Korea and its resonance with anti-Japanese views held by many Koreans.

After discussing the driver of an attack, the group tackled what means might be employed to effect such an attack in two circumstances. In the first, the North Korean state might facilitate non-state actors, North Korean or otherwise, to conduct a terrorist attack on spent fuel in Japan. In the second, the North Korean state might encourage a non-state actor to undertake insider sabotage at a nuclear site in Japan.

Relatedly, the group asked what strategy might be preferred to conduct such an attack originating from North Korea. A “complex” attack strategy seemed likely that would exploit cyber and poor network security, the potential to enter the site during evacuation after an initial attack, and choosing to attack nuclear materials site with relatively loose security (such as at Tokai). As instructed, the group then concluded that a terror attack happens due to a combination of the motivations and strategic considerations noted above, and set out to define the point of entry for the attack and the measures taken to attack in the scenario, by exploiting cyber insecurity.[12]

Narrative 1: Vulnerability of Spent Fuel Japan to Cyber Insecurity

Mr. Lee, a North Korean man born in Japan and recently returned after spending many years working in the North in their software export industry is the main and catalyzing actor behind this terrorist attack. Mr. Lee actually likes aspects of Japanese culture, and has fond memories of growing up in Japan and watching Disney movies in Japanese, including Mickey Mouse. Due to his childhood in Japan, he speaks fluent Japanese with no trace of a Korean accent. After working at the Pyongyang Informatics Center exporting software to Japanese clients, he was trained as a cyber warrior at the DPRK’s Unit 121 at Mirim University.[13] Here, he became proficient in the design and deployment of logic bombs or cyber munitions designed to trigger a nuclear plant meltdown, open dams above a populated area, or disable air traffic control services, resulting in airplane crashes.[14] He has been sent back to Japan posing as a Chinese businessman in the software business from Shen Yang where he had worked for the North Korean cyber force staying at the Chilbosan Hotel[15] that allegedly attacked the Sony Corporation in 2014.

His instructions are to cultivate a network of Japanese and pro-North Koreans living in Japan who are alienated from the increasingly revisionist Japanese state aiming to reject historical textbooks that accept that comfort women worked for the Japanese military in World War II, and suggesting that Japanese colonialism was beneficial for Koreans. He is gripped by a gnawing anger and joins and then becomes the controller of a shadowy group of North Korean and Japanese hackers who decide to hack the control system of a nuclear power plant at Sendei.[16] At the same time, they set out to hack and take over the controls of the Rokkasho spent fuel reprocessing facility. To do so, they spend considerable on-line time researching the engineering systems for these facilities, focused on regulatory agencies, industrial suppliers, and utilities, to obtain emergency procedures manuals, engineering design, and electronic controls systems.

In order to obtain the necessary codes to access the Sendai plant’s control systems, Lee, assisted by other North Korean agents resident in Japan, kidnaps the daughter (“Jo An”) of the Sendai nuclear plant manager. They threaten to kill her to force her father to provide them with the plants’ computer security access codes without informing the authorities or his colleagues. They also force

Lee to install a wireless-capable USB stick into a control room computer linked to a smart phone in anticipation that the plant will be cut off from Internet contact as soon as they launch their remotely controlled attack.[17]

Using these access codes, Lee's network launches a cyber-attack. The attack has two parts. The first uses dozens of distributed denial-of-service attacks using thousands of computers commandeered around the world to saturate the Internet connections to the Rokkasho and Tokai processing plants and the now five reactors that have been restarted by the Abe government. This leads to confusion and alarms that in turn flood into the five affected provinces as well as the central ministries and security agencies. At the same time, they attack the Sendai reactor by infiltrating the computers in the plant control rooms, using the codes secured from the manager. This is the main line of attack and it shuts down the whole power plant, including its spent fuel cooling pumps. It also degrades the monitoring systems of the reactor including the high level waste spent fuel cooling pool as well as the cooling system. The cyber-terrorists maintain control of the plants' cooling system defeating the frantic attempts by the primary and backup control room operators to shut them out and even the separation of the reactor site from the Internet—thought to be impossible before the attack. At the same time, the plant itself is held hostage by the terrorist group who threaten to sabotage it using auto-activating computer codes if their access is cut off.

Due to the slow response from the government to their demands, the hackers decide to shut down the reactor and its primary cooling cycle. While the demands were fragmented, multiple and unfocused, the desire to cause terror was clear. Emergency back-up cooling automatically cools the reactor core, but because monitoring systems are off-line, plant operators are not sure whether the reactor core has remained intact or has suffered from partial meltdown. Up until this time, there is no evidence of radiological release on or off-site from sensors accessible to the utility and the government, but thermal plumes observed with infrared cameras from a distance indicate that the core is extremely hot.

Now that the hackers have infiltrated the operating system, the control room operators find themselves disabled and distracted by a local denial-of-service-attack delivered by their own distributed network of computers in the reactor complex, thereby freezing their operating systems. This stratagem decoys the operators away from recognizing and overcoming the main line of cyber-attack. The collapse of their operational control is compounded by the loss of access to plant monitoring systems and sensors, and the apparent removal of the cooling systems for the reactor core and spent fuel pool from the operating system.

The response of security forces and back-up emergency capacities to provide make-up water to the spent fuel pools is delayed and confused. With strange things happening in the control room due to remote manipulation of the systems by terrorists, the operators were disoriented (rendering their communications to outside authorities to be a combination of mystifying and muddled). Coupled with a powerful public disinformation campaign via Twitter and other social media sent out by the attacker group, the terrorists were successful at achieving their primary goal: generalized panic and lack of confidence in Japanese authorities, particularly in the nuclear sector but not limited to it. Even as they struggle to regain control, they receive a terrorist Tweet that they have taken over the plants and threatening to cause a meltdown. The emergency response forces are located at nearby police stations and Self Defense Force bases, not on site. They move even more cautiously in response to this news until more information is available about who is in control of the operator room and plant site.

In the midst of the attack, news commentators speculate that in order to accomplish their attack, the hackers would require insider assistance. At this juncture, as the security forces enter the plants, the plant manager admits that his daughter has been kidnapped and that he facilitated virtual

takeover of the plant. This revelation inflames public anxiety and undermines trust in the nuclear industry.

Immediate Aftermath of Scenario 1

The Sendai and Rokkasho plant operators ascertain that the hackers have not managed to compromise these sites at all, just knock them off-line, but they have not had time to check all the operating systems. Thus, in case the hackers did manage to overcome firewalls and other security software, they treat the spent fuel pools at the two facilities as if their cooling systems have been compromised. They double-check that the manual cooling controls to stabilize the spent fuel pools are available and stand-by for further instruction. However, rapid-fire Tweets from the terrorist groups sow confusion among the public and even among political, military, and nuclear officials, as to the state of play, not only at the Sendai reactor where actual damage has been incurred, but at all the sites subject to the initial cyber-attacks. Indeed, neither the government nor the facilities operators know which plants have been affected. Social media reports of airborne radiation exposure from smart phone Geiger counters generate contagious panic and tens of thousands of people rush to evacuate from the Rokkasho and Sendai areas.

Medium and Long-Term Impacts of Scenario 1

Once the sites have been stabilized, the full policy implications of the attack sink in. Immediately, all nuclear operators are ordered to overhaul their cyber-security practices, which quickly extend to a Japan-wide review across all critical nuclear and non-nuclear infrastructures. The central government directs all reactor operators to speed up transfer of hot spent fuel to special dry cask storage units on site, and starts to develop multiple land and coastal-sea based dry cask storage sites, including on ships and on in-land islands, using emergency powers to overrule local provincial opposition to the locations and to the transport of dry casks full of spent fuel to these sites. This policy is extended not long afterward to the Rokkasho and Tokai plant operators. The central government instructs them to no longer use spent fuel pools for nuclear waste storage and to immediately transfer spent fuel to dry casks as soon as these can be ordered and delivered to the sites.

There are further delays to restarts of the remaining nuclear units in Japan, as plant host communities and the general public demand more stringent security measures in the wake of the cyber-attack scare.

Ultimately, Jo An uses Taekwondo to escape by taking her captor totally by surprise. Being an older North Korean man, he simply could not imagine that a demure Japanese young woman could have Olympic-level black belt skills in a Korean martial art. Indeed, she knocks out Mr. Lee, the lead abductor of the hacker gang, with a swirling head kick, and he is apprehended. But the rest of the hacker network remains at large because they only met on-line, not face-face, and not even Mr. Lee knows exactly who they are or where and when they might strike again. As a result, the Japanese nuclear communities and the general public remain apprehensive that the cyber-terrorists remain a threat to the nuclear power sector, which causes further delays in nuclear energy sector activities.

The event forces a high-level international dialogue on cyber-security at nuclear facilities well beyond the relaxed IAEA process under way at the time of the attack.[18] Whether to operate Rokkasho at all becomes a hot political issue in Japan and internationally. Across Japan in all sectors with critical infrastructure, emergency response plans are reviewed. A debate ensues as to the necessity to conduct in-depth background checks with regular updates on all employees in sensitive positions in all critical infrastructures, not just in the nuclear sector. An attempt is made to shore up public support for nuclear power by revising and publishing protocols for crisis communications, but

most people remain skeptical.

Terrorists everywhere also learn from the event. They see this attack as a success although the plants were not disabled. New and old groups set out to emulate the attack, and to enlist superior hacking capabilities on a global basis, deployable for any number of political and other motivations against critical infrastructure, including nuclear facilities.

In the long-term, nuclear security policies and practices are strengthened in Japan. Ironically, this takes place as nuclear power is slowly phased out due to its high cost, the vulnerabilities of the nuclear fuel cycle, including spent fuel sites, to new attacks as well as other technological and natural risks. Ultimately, policy makers decide that nuclear energy is simply too risky to retain as a means of obtaining energy for Japan's economy.

SCENARIO 2

Frustrated Civil Society Instigate Spent Fuel Terrorism in Japan

Like group 1, group 2 began by reviewing notes and insights from the discussions on Day 1. These were not intended to limit scenaric thinking to what had been identified, but rather to fuel it.

Topics that surfaced on Day 1 included a series of issues internal to Japan and civil society frustration with government (in)action on nuclear vulnerabilities. Such topics included the risk that the Okinawa situation might become extreme with some opponents of the US military base becoming radicalized—indeed, some wondered why this hadn't already happened and whether the situation might soon reach a sudden tipping point; whether the voice of civil society in Japan is increasing or decreasing in the formation of public policy and public opinion; the possibility that those in civil society concerned with nuclear security issues may be indifferent to a wider portfolio of civil society concerns; the possibility that civil society's role is impossible to predict and may even be a wildcard that could disrupt the status quo; the cultural differences between the United States and Japan over civil society's use of the Freedom of Information Act and whistleblowers; and whether Japan is culturally ready and able to establish sufficient means to deter and/or defeat terrorist attacks. Rather than limiting or directing scenaric thinking, these factors were noted as possible drivers or issues in the narrative.

Narrative 2: Green Politics or Police State? Civil Society as Frustrated Actors in a Terrorist Attack on Nuclear Spent Fuel

Japan has introduced a national identity system after much debate. On average, younger Japanese are much less well off than the older generation of parents and grandparents. Youth in general no longer have secure, well-paying jobs, perhaps as a failure of Abe-nomics. Although many youth vocally opposed the identity card system and protested against increasing inequality, they were just one more public voice largely ignored by the Japanese government.

One consequence of the income gap is the massive increase of *Otaku* or jobless young people who stay at home playing video games all day. Many *Otaku* live as much in the virtual as in the real-world; indeed, the two become blended in their minds and lifestyle such that real life is surreal and virtual life is for real. Many also acquire advanced technical skills with no productive outlet.

Prime Minister Shinzo Abe's push for Japan to play an active role in a US-led global and regional collective defense has increased the militarization of Japan, as many feared at the time it was pushed through the national assembly. Japan has also become an explicit target of the self-declared Islamic State calling on sympathetic individuals to act on their own to carry out attacks within their own

countries. Meanwhile, radical groups in Japan have formed to oppose the new militarism, and those in Okinawa are especially vigorous. Ex-Aum Shinrikyo cult members are still active although somewhat under the radar. Many worry that the combination of restarted nuclear power plants and the deep mistrust of the nuclear industry in Japan may motivate an anti-nuclear group to attack a nuclear plant. Others fret that Islamic State could attack Japan. An expert wrote in a national newspaper that any non-state group might choose to target spent nuclear fuel because of the combination of its particular vulnerabilities and their own dissatisfaction with growing social instability.

In this scenario, an *Otaku* is recruited by a Japan-based terrorist organization to launch a cyber-attack on a nuclear power plant.

Civil society groups and scholarly experts, including Green Peace, have long observed the vulnerability of nuclear facilities to cyber-attack and attempted to alert local and central authorities. However, their warnings are ignored by officials and utility managers alike due to the cost and difficulty of overcoming cyber-insecurity and the financial pressure to operate reactors after the Fukushima catastrophe and shutdown. Moreover, Japan's general cultural orientation based on rote learning in education and the general lack of free-thinking in education, obviates against institutional and individual learning and critical reasoning. As a result, the terrorists' frustration is growing in the face of bureaucratic inaction and a culture of NATO ("no action, talk only"). The *Otakus* are happy to support the effort since it expands their virtual world into the real world.

Also, the lack of free competition in the energy industry puts enormous pressure on utility managers to operate reactors to meet public and industrial needs for power. The general lack of transparency in nuclear regulation contributes to a myth that the nuclear fuel cycle is entirely safe. Job hierarchies are inflexible within industries, and cross-sector labor mobility is very limited, creating multiple barriers to transparency and understanding the risks of nuclear spent fuel management in Japan: fear of reprisal discourages workers from taking responsible professional risks and sharing their information and understanding of potential risks to the community. The "nuclear village"—perhaps better named "nuclear fortress" today--has stood intact for decades against many political, economic, and technological pressures. Also, there is no whistleblower protection for those in the know about the security shortfalls in safety protocols further discouraging those who might otherwise risk their jobs and families to go public with their concerns and knowledge. For all these reasons, in spite of the Fukushima disaster, Japan has continued to develop its nuclear program without sufficient attention and resolve to address the tough issues associated with spent fuel management.

The terrorist group which recruits the young *Otaku* gives him the on-line identity Deaf Ears to emphasize that his attacks are to be merciless. He executes a skillful cyber-attack on the Fukui nuclear power plant spent fuel storage area, causing a power outage. As a result, Biwako Lake is contaminated. Another *Otaku* ("Nerd") posts a notice on the Kyoto city government and police emergency websites instructing residents to evacuate due to an attack on a MOX shipment within the city and resulting radiological contamination over a wide area. He also turns on alarm sirens by hacking the emergency alert system; and makes road lights turn red to green haphazardly. This hoax and hacking causes mass hysteria and confusion and severe disruption to business-as-usual in Japan's ancient, sacred city.

Immediate and Medium-Term Aftermath of Scenario 2

The second team saw two possible extreme narratives unfold from the conditions created by these trigger events.

The first narrative is that a “Green Party” is born. Japanese politics becomes more influenced by the German model and related policies, and the government commits to phasing out nuclear power. Japan spearheads an international plutonium disposal project, as well as forming a coalition with South Korea to create an international convention on nuclear security (including fissile material control). The Freedom of Information Act is strengthened and more civil society groups take advantage of the information available. The Protection of Whistleblowers Act is enhanced. An independent peer review system is established. The Japan Atomic Energy Commission becomes an “independent” audit commission. The Diet also establishes an independent commission on nuclear technology.

Japan strengthens its nuclear disarmament campaign but brings the global rhetoric home to local and regional practice. Japan works with the United States and South Korea to establish a nuclear weapons-free zone in northeast Asia, starting with a six party summit of heads of state combined with a massive meeting of city mayors held in Hiroshima and Nagasaki. In a few years, this zone culminates in the denuclearization of North Korea. Japan strengthens its alliance with the liberal-internationalist leaders in the United States to promote a global and regional multilateral nuclear security framework. Japanese civil society also collaborates actively with counterparts in the United States, Europe, and elsewhere in East Asia who are concerned about nuclear fuel and risks.

In the alternative narrative, instead of a green party emerging, the “Japan National Party” is born. This party is heavily influenced by conservative and radical politicians in the United States and by radical nationalists at home. Japan not only restarts most of its nuclear power plants; it expands its program to separate and stockpile plutonium. It also adopts its own “Homeland Security Act” and begins to limit freedom and mobility of its own people. Japan joins the coalition against Islamic State and changes its constitution to allow offensive military operations overseas and high surveillance of the domestic population with curtailed civil liberties.

As this police state evolves, Japan also begins to develop its own nuclear weapons options although it is careful to do so in a way that does not rupture the US alliance but rather, provides useful political and even military leverage against China on regional security issues such as disputed territories. Thus, the Japan Atomic Energy Commission is moved into a new Japanese Department of Defense. South Korea quickly follows suit to pursue its own nuclear weapons option and an active northeast Asian nuclear balance of terror emerges. Under this police state, elements of Japanese civil society concerned about nuclear issues are forced to go completely underground and start to consider more extreme measures to push back against the national security police state, including attacks against nuclear materials processing facilities.

SCENARIO 3

Frustrated Insider(s) Instigate Terrorism at a Nuclear Facility

Like the first two groups, group 3 reviewed salient information from Day 1 that related to the specter of frustrated nuclear plant workers instigating a terrorist attack on the plant. Many possible reasons were raised for such potentially devastating action. These factors that would affect how insiders engage in terrorist activity in nuclear facilities in Japan include:

- *The use of temporary workers without in-depth or even any security clearance within the plant;*
- *Maintenance of sub-contractors without in-depth security clearances arriving in large numbers during maintenance shutdown, at which time the site personnel increases by a factor of three;*
- *Massive failures in the security of US personnel reliability system databases suggest that a system of formal background checks not only may not suffice to overcome the insider threat. Implemented*

poorly, it may exacerbate the problem;

- *Labor union structure inadvertently facilitates discontent, poor hiring, too many sub-contractors, has a vested interest in the status quo; and resists cultural change in the workplace;*
- *Vulnerabilities created by a large pool of young, insecure workers in Japan;*
- *The risk that moles or sleeper agents can slip into the system, as occurred when Aum Shinrikyo recruited members in the police, in Mitsubishi Heavy Industries, and in other related organizations;**[19]***
- *The risk that a plant manager's family could be kidnapped and the manager "forced" to do something devastating;*
- *Non-existence of a two man rule inside sensitive areas of nuclear facilities, leaving to too much latitude for individuals to act malevolently;*
- *Failure to recognize and act on the fact that good security is "20% equipment and 80% culture," as one participant put it.*

With these issues in mind the workshop team found that an insider attack[20] would be shaped by at least seven factors that determine what type of insider, what strategy, what targets, and what success or failure might result from an attempt to overcome the defenses maintained by Japanese nuclear facilities today against the threat of attack by a non-state actor.

1. ***Many possible insider motivations***: Insiders might attack a nuclear facility for multiple, possibly contradictory reasons. They may be angry that nuclear power is either imposed by the government without regard to risk, or are upset that nuclear power is insufficiently supported by the government. They may be frustrated with cost-cutting pressures from inside and outside the utility or plant operator that compromise safety. They may perceive nuclear power as being imposed by the government on society and even after Fukushima, unable to change to adopt safer practices. They may be upset over decreased wages or non-promotion. They may be individuals who are susceptible to psychological control by another insider, or an outsider. And they may have a basic anti-social personality not screened out at time of employment or afterwards. Japan's sector-wide utility restructuring in the last two decades put formal emphasis on safety at the management level, but led to many cost-cutting practices that undermined safety in the facility workplaces, leaving many workers highly frustrated. Also, many utility managers did not want to adopt nuclear power due to its cost and the likelihood of political contestation at the local level of constructing and operating reactors, and in effect, sent mixed messages to their own workforce about the desirability of nuclear power. Indeed, it is not overstating the situation to say that due to most of the workforce not being able to speak out about such issues when they were told that they were expected to speak, the potential source of alienated insiders is the *entire skilled workforce*.

2. Weak Personnel Security Checks: The legal obligations and organizational structure at nuclear plants or facilities and within utility management may create vulnerabilities to malevolent insiders. For example, for legal and privacy reasons, employees may have only cursory private background checks when hired, without periodic review. Japan has strong constitutional and legal protections over privacy, including personal medical information, and medical professionals are not allowed to share this information even if they are concerned about the individual's potential to do harm. Thus, Japanese nuclear organizations are unable to adopt one possible technical fix—the use of biometric sensors to be worn by individual employees to monitor their physical and mental stress—that might provide warning of pending insider attack.[21]

3. Deficits in safety culture: The organization itself may lack what is known as a safety culture,

where employees are encouraged to monitor and report attitudes and behaviors of other employees that could manifest psychological or other problems that are outside a normal range.[22] At particular times, the organization may rapidly bring large numbers of short-term and casual workers onto the site and into the plant for periodic shutdowns for fuel replacement and maintenance, at which time an insider could combine with outsiders to bring external supplementary capacity—both human and hardware—into a nuclear facility. A senior insider with long-term presence and knowledge of the plant, its layout, systems, and routines, might recruit a lower-level person with access to more significant areas such as the spent fuel pool or cooling systems or their backup; or to control room(s), and also enable outsiders to defeat entry control security systems, most likely by recruiting a guard.

4. Trade unions may provide de facto security screening: The trade unions in nuclear facilities are well-paid and have good benefits. The unions themselves may screen the union workforce and thereby control corruption and oppose infiltration by outsider groups, in order to protect their privileged position. However, they do not represent management employees and may not be a barrier against high-level insiders in nuclear plants, nor against the use of sub-contractors to introduce outsider agents of a terrorist group. Nonetheless, unions are an important bulwark against extremist attack on nuclear plants in Japan and should play an active role in developing and implementing a "security culture."

5. Long-term alienated insider is invisible: An alienated individual can maintain an extreme mindset for years, undetected even by close colleagues or direct supervisors; and by virtue of their long service, can gain high levels of access, insight, and trust that make the insider a powerful asset in a conducting an attack on a nuclear facility. Such an insider is extremely difficult, even impossible to detect with assurance in advance of an attack, and possibly not even after an attack has taken place.[23] It is possible to match faces and force levels with potential outsider attackers, and to prepare by conducting force-on-force exercises. Without a face and with no insight into the state of mind of the alienated insider, it is very difficult to prepare for an insider attack.

Possible attack strategies and targets within nuclear plant: Once inside the plant, an insider has multiple possible targets to take control of and to attack. The mostly likely modalities for terrorist attack include taking the plant hostage in the control room(s) and a significant area such as a spent fuel pool or reactor cooling system; and partially disabling the plant control room; an all-out, frontal attack on and inside the plant aimed at damaging it and causing a radiological release on a massive scale; or maintaining a sleeper capacity inside the plant for future use by an outsider group engaged in a range of terrorist activities in Japan. A well-informed insider and outsider with knowledge of nuclear engineering and nuclear systems would know the specific systems that could be quickly and relatively easily damaged or destroyed. Such a person might be a retired nuclear engineer who might be extorted or recruited into providing the requisite technical guidance on how to disable cooling systems with least effort. Considerable generic data on these engineering details is also in the public record and open source Internet documentation. Of a wide array of possible fuel cycle targets that an insider-outsider team could aim to occupy, control, and possibly damage or destroy, the team suggested that the most likely targets would be reactor core cooling, spent fuel pool cooling, and theft of special nuclear material from the Tokai or Rokkasho reprocessing plants for use outside the plant in some manner, possibly in a radiological dispersion device.

6. Political-ideological versus religious millenarian goals: The insider-outsider terrorist group could have one of two very different goals for their attack. The first is an attack motivated by a political-ideological goal and aiming to realize some objective in relation to a social grievance of the type discussed in scenarios 1 and 2. The second is an attack inspired by a religious-millenarian worldview that seeks to create an apocalyptic event accompanied by massive damage, without

regard to realization of a specific political or social objective.

These different goals and objectives might lead the insider-outsider terrorist group to design and calibrate their attacks differently. In the first case, for example, the attack might be aimed at disabling the cooling system of a spent fuel pool while exerting control over the site against external security forces, creating a timeline after which the fuel might lose coolant coverage sufficient to catch fire and cause a massive radiological release. This attack strategy would aim to exert leverage over the central government and may be described as a "hostage taking" strategy.

In the second case, the attackers would simply set out to destroy the cooling systems of the pool and reactor core as rapidly as possible, while holding external security forces at bay.

7. Who would be blamed? This distinction between political-ideological and apocalyptic types of attacks led directly to a key question, the answer to which would shape one of the major consequences to such an attack. If such an event occurs, who would be held accountable in the subsequent blame game?

With these seven factors in mind, the workshop team then explored plausible attack scenarios described in the next section.

Narrative 3: Frustrated Insiders

Unlike the first two scenarios which relied on outsiders who use cyber-attack from off-site to disable and damage nuclear facilities, the third group concluded that an insider attack would be designed to attack the site itself by physical means and occupation in the case of a reactor, or use physical means to remove materials in the case of a bulk processing site. The team considered it unlikely that an insider could introduce sufficient hardware to conduct an attack on his or her own; and even after recruitment, would need to enable supplementary and armed individuals to enter the plant in order to occupy and hold it long enough to conduct a disabling attack on the plant systems. Therefore, the key role of the insider, whether such an insider is that instigator or is a recruited agent of an external group, is to facilitate access at the time of the attack to armed outsiders; and before the attack, to obtain critical information on fastest route from entry point to significant sites such as the control room, the backup control room, the reactor cooling systems, emergency backup cooling systems, and the spent fuel pool and its cooling systems; and to monitor and understand the location and work routines of other staff, and in particular, security personnel at various phases of plant operation.

Such a premeditated and well prepared attack would take considerable time, at least months and possibly years, to gather the relevant information, conduct reconnaissance and gather logistical data, and to train, establish and position the attacking force in place. A reasonable analog is the time taken for Al Qaeda to emplace its agents and prepare the attack on the World Trade towers--roughly three years. Such a force requires considerable funds; secure communications; well trained and armed personnel; a command and control system combined with agile, secure communication and sensor systems; a publicity and mass communications presence; and the ability to identify and conduct simultaneous strikes, including on significant non-site infrastructure needed to operate a reactor such as power lines, access roads and bridges, etc., which may be targeted relatively easily to create distraction and emergency response delays. It might also employ hackers to conduct cyber-vandalism or cyber-attacks to prepare for or support its physical attack, but this would be ancillary to the primary force, not the main modality as in the first two scenarios.[24] Finally, it might recruit or place sleepers in response forces, including in security forces that might then be activated in order to create an actual emergency to mask a malicious act.[25]

For all these reasons, the insider is unlikely to be the instigator of such an attack, but rather, is likely to be the recruited facilitator who is either turned by political-ideological or religious reasons, depending on the type of external group engaged in the attack; or who is forced to cooperate by extortion or coercion over his or her family, his or her personal circumstances such as financial troubles, sexual identity, or criminal behavior. However, although nuclear engineers, scientists, technicians, and managers would not normally have the skills and backgrounds necessary to conceptualize and activate such a complex strategy, there is precedent for such positioning and disparate skill set in one person in the world of global terrorism; and such a person who envisions and orchestrates such a complex attack cannot be precluded from existing within the ranks of senior nuclear facility personnel.

Conversely, without such an insider, an external group is unlikely to choose a relatively highly defended and secure target such as nuclear facilities when other targets that also promise mass coverage, bargaining leverage with the central government, or mass damage are more easily accessed and attacked. Thus, the “lone” insider attack risk in Japan boils down to relatively random incidents, possibly separated in time, whereby an individual might do significant damage or cause an outage, but is unlikely to overcome the multiple barriers to loss of control, coolant, and cooling of reactor cores or spent fuel pools to lead to mass destruction.[26]

The team examined carefully whether the political-ideological hostage-taking versus religious apocalyptic motivation of the attacking group involving an insider, with possibly different attack strategies, would make any substantial difference to how the government would respond, once the attack began or was announced.

The key argument is that the hostage-taking reactor/spent fuel pool attack on one hand, and the apocalyptic attack on the other, would collapse into one type of event for the government. The government, it was suggested, would be forced to treat the hostage-taking attack as if it were an apocalyptic attack, no matter what the hostage taker attackers’ declared intention. In part, this logic emerges because to be credible, a hostage-taking attack likely would seek to seriously damage a significant area of the facility such as a spent fuel pool to create a relatively slow (for example, 48 hour coolant boil-off) timeline for negotiating with the threat that major damage would result unless demands are met; or to set a much shorter timeline for damage with serious risk at the reactor core by attacking certain valves and cooling systems, to force the government to bargain.

However, it is almost certain that the government would neither trust the hostage-taker’s authenticity in negotiating a safe outcome if it responded to a demand, assuming a coherent and specific demand were to be made, nor take the risk that irreversible damage wasn't already or wouldn't become catastrophic results, whatever the “hostage taking” attacker’s intention. In part, the government would be driven by the fact that no government agency keeps updated information on how much spent fuel is stored in spent fuel pools, including its age and burnup level. In Japan, as in the United States, this knowledge is kept only by the utility and if, for any reason, the utility cannot access this information immediately, officials must act without knowing the status and configuration of spent fuel in pools at reactors and spent fuel storage and processing sites. This information deficit might drive governments to act forcefully in case the spent fuel pool is densely packed with very hot, recently discharged spent fuel rods.

Indeed, the conjuncture between reactor shut-down for maintenance and discharge, the discharge of very hot spent fuel, and the influx of large numbers of maintenance personnel with the opportunity for attackers to enter via this influx undetected, suggests that shortly after reactor shutdown might be a particularly attractive time for an insider-outsider attack and that utilities and security personnel should be especially alert during such periods.

Moreover, no government could afford to be seen to be not taking decisive action to eliminate such the risk of catastrophic damage, even if there were no guarantee that catastrophe could be avoided in the course of retaking control of the plant by force. Indeed, even if they failed and significant radiological release occurred, the government might be rewarded politically by its voting public for trying to reassert decisive control. In short, it is almost certain that the government would move at maximum speed to retake the facility with police and military forces, in order to regain control, shut down the plant if necessary, or allow emergency response agencies to enter the site to deal with damage and cleanup such be required after an attack.

A mature terrorist organization, especially a "rational" actor with limited political-ideological objectives in conducting such an attack, would figure this logic out for itself in advance, and would expect to be attacked heavily at the outset. Therefore, it would likely try to create conditions of rapid escalation to stave off being overrun and removed or to create deep crisis very quickly, which implies direct attack on and disablement of cooling systems and the valves that control these systems for the reactor and the spent fuel pool. Thus, even with a limited political-ideological objective, the "hostage-taking" strategy of terrorist attack has an inherent tendency to veer over the edge into an apocalyptic, all-out attack, whatever its intent.

Immediate and Medium-Term Aftermath of Scenario 3

The immediate political impact of such an attack, successful or not, on the government is one thing. The medium-term impact of such an attack on the nuclear sector is another altogether. Even it were blocked at the gate, let alone resulted in meltdown and radiological release at the other end of the spectrum of attack, the public perception that such an attack was mounted with insider assistance could have extraordinary impact on the nuclear sector as a whole. This longer term outcome, it was suggested, would depend primarily on the public perception as to whether the terrorist insider, being Japanese, was a low-ranking, exploited worker or a high-level employee. The industrial hierarchy in the nuclear sector begins with the utility at the top, followed by tiers of sub-contractors. If the terrorist insider were from a lower tier subcontractor, then the public would blame this industrial hierarchy, which is theoretically re-formable against such insider penetration via reforms and security checks on personnel on the site, especially for sub-contractors.

In this case, the entire nuclear hierarchy (aka nuclear village) might be insulated and even gain public support due to swift decisive action, although if the reactor type attacked (assuming it was not a materials storage and processing facility) was a boiling water reactor, the attack might swing support behind pressurized water reactors while shutting down boiling water reactors. Conversely, as noted above, the demands of a long planning horizon and substantial preparation suggests that the insider would be a high-level person with knowledge and access to sensitive and significant areas of the plant, not a short-term contractor. Short-term contractors might be used as cover to infiltrate and supplement an attacking force, but would not be the lead force in a mature insider-outsider attack.

But if the key insider who made the attack possible was a high-level management type person on the utility's regular payroll, then the entire nuclear village might lose public support and the future on nuclear power itself might be put at question. The public would perceive vulnerability to terrorist insiders to be beyond remedy.

The team treated the insider threat to nuclear material storage and processing sites differently to that which might involve nuclear reactors. In this case, the current security measures at these facilities arguably preclude insiders from smuggling in arms and other hardware needed to take over such a facility. For this reason, the plausible roles of insiders would be limited to facilitating armed attackers from outside to enter the facility; or instead, to divert and walk out relatively small

amounts of radioactive material (although these could add up over time) from a bulk processing facility (such as Rokkasho and Tokai). Such an insider might then use or threaten to use or sell this material once it is outside of the facility.

However, the political and symbolic impact of such an attack on the nuclear village and the nuclear power project as a whole was not discussed by the team, although it is reasonable to conclude that such an event might lead to severe examination and the possible ending of attempts to create a plutonium-based fuel cycle in Japan.

As we noted at the outset of this section, this insider attack scenario differs substantially to that envisioned in the two scenarios, both of which are based on cyber-attack against nuclear facility. In the third scenario, the human insider is the critical variable on which a successful attack occurs. Furthermore, the main attack would be a physical takeover whereby the insider facilitates an outside armed group to take over the facility; or removes nuclear material from a facility for use in an attack outside the facility. In the third insider scenario, cyber-attacks might be launched on the nuclear facility or other critical infrastructure at the same time to confuse, distract, and diffuse responding security forces in order to facilitate the physical entry of the outside attack force; but the key to entry and to successful attack is the intimate knowledge of the insider of the facility, its technology and engineering, the organization's procedures, the security systems, the other staff, and their routines.

CONCLUSION

This workshop was not designed to produce specific policy recommendations or prescriptive actions for policy makers in Japan or elsewhere, whether they be government ministries, regulatory agencies, corporations such as utilities, civil society organizations, or managers of spent nuclear fuel.

The goal was to provide provocative stimulation for the parties responsible for public safety and security as they plan for an uncertain future, and to identify critical questions demanding answers wherever spent fuel is found, including but not limited to Japan.

These three scenario narratives suggest that it is urgent to tackle the following research agenda.

1. Who should establish global and national standards for spent fuel management and security? Who must be involved? Is establishing such minimum, universal standards a national or international imperative? Depending on the answer, who should take the lead in defining these standards?
2. Once these security standards are established, who exactly is responsible for implementing changes that realize the standards? Again, is this a national or international issue? Can guidelines be created for ascertaining and justifying the cost of these changes relative to alternative investments in societal risk reduction due to terrorist attack aimed at unleashing mass destruction?
3. Should government agencies maintain current information on the status and configuration of spent fuel stored in pools, not just authorize the shift from low to high density racking and then relying on the facility operator to maintain this data?
4. Should Japan and other countries consider reducing the density of racking in spent fuel pools to reduce the risk that loss of cooling and ultimately, loss of coolant, could result in catastrophic radiological release?
5. Every country and nuclear agency, civilian and non-civilian, faces the issue of insiders

facilitating or perpetrating a nuclear terror event. What are the implications for background checks, personnel reliability programs, and cross-sectoral and cross-border collaboration to share information related to individuals and organizations that might undertake an attack on a nuclear facility by responding to or recruiting, by whatever means an insider?

6. Is such a system, including parallel civilian surveillance schemes, consistent with domestic constitutional and international legal standards of human rights and privacy?
7. What means of deterrence, if any, exist to block or shape the linkage between the alienated insider individual and the outsider terrorist group? In particular, what are the potential roles of unions and local communities in surveilling and reporting threatening individuals and what are the possible resultant scapegoating and stereotyping behaviors that could create false positive and negative reporting that could controvert such a system?
8. How current and realistic are estimates of outsider and external (to Japan) versus internal (domestic to Japan) terrorist group threats when considered in combination with possible insider capabilities; and how are these reflected in the Design Basis Threats used in training and force-on-force exercises in Japan's nuclear facilities and related response forces?
9. What level of cyber-insecurity exists with regard to nuclear facilities in Japan? Can distributed means of terrorist command-and-control and related reconnaissance, surveillance, computer, and communication systems, including social media, such as those employed in the Mumbai attack in 2009, be identified in real-time and disrupted or blocked?
10. What are the links between global, regional, and domestic security conditions and the insider attack risk? Is there any correspondence between resolution of such multi-level and multi-dimensional insecurities, for example, an easing of antagonistic Japanese-North Korean relations, and the risk of an insider attack?
11. What are the implications for nuclear power (and other critical infrastructure) from recognizing the existence of completely home-grown terrorist threat, inspired by an "endogenous" political goal or ideology, or seeking to act on an apocalyptic vision?
12. What impact would an act of nuclear terror, in Japan or elsewhere, have on the central government's will and ability to resolve the social-contractual issues involved with provision of subsidies and jobs to nuclear-hosting communities (for reactors or bulk processing sites such as Rokkasho), and to implement rapidly a technical solution, such as dry cask storage, that of itself could substantially reduce the probability that an act of nuclear terror could be perpetrated by attacking spent fuel? For example, could the central government use emergency powers to move spent fuel into dry casks and store them on ships or on artificial islands in inland seas, pending adoption of long-term storage or disposal strategies?
13. What level of nuclear power in various permutations (the balance of PWRs to BWRs, once-through versus MOx-recycling fuel cycles, plutonium-fueled reactors) provides increased technological diversity to Japan's energy security index over time, and what level of nuclear power dependence increases susceptibility to supply disruption due to direct attack of the kind considered in these scenarios, or to the political and technological impact of such an event occurring in another country, for example, South Korea or China? How does this risk compare with the risk of loss of supply of renewable energy, energy efficiency, or fossil fuels?
14. What price is worth paying for Japan to maintain and use a "nuclear weapons technological deterrent" in its international relations, based on its plutonium stockpile and enrichment capacity, as against its retention of an inactive, latent nuclear weapons proliferation potential? If such a pro-active technological deterrent is sustained and used in Japan's international relations, and starts to inflect its relations with the United States, other security partners, and third parties with which Japan has security conflicts for historical or contemporary reasons, what level

of spent fuel and stockpiled plutonium is required to maintain this stance? Does maintaining a larger stockpile of spent fuel and separated plutonium than the minimum necessary for a credible technological deterrence affect the probability of a non-state actor outsider or insider attack on Japanese spent fuel?

III. ENDNOTES

[1] Such an open source study has been done at a purely technical level in China. See Zheng Qiyan, Shi Zhongqi, Wang Xingyu, "Consequence Assessment of Attacking Nuclear Spent Fuel Pool by Terrorist," Institute of Nuclear Energy Technology, Tsinghua University, Beijing, 2003.

[2] See COD Scenario 140, at Open Scenarios Repository, US Institute for Defense Analyses, downloadable Excel database with links to over 250 scenarios, at: http://openscenarios.ida.org/docs/Open-Scenario-Repository-06-25-2010-2.pdf The scenarios exercise involved IDA, Korean Institute of Defense Analysis (Seoul), National Institute of Defense Analysis (Tokyo) and the Office of the Secretary of Defense, US Department of Defense. The description of the scenario cited here is drawn from the link in this spreadsheet to "Pirates Threatening to Detonate Hijacked Oil Rig Near a Nuclear Power Plant" at: http://openscenarios.ida.org/scenarios/107-Nuclear_Plant_Crisis.ppt

[3] The description of the scenario cited here is drawn from the link in this spreadsheet referred to in *op cit*, "Pirates Threatening to Detonate Hijacked Oil Rig Near a Nuclear Power Plant" at: http://openscenarios.ida.org/scenarios/107-Nuclear_Plant_Crisis.ppt

[4] Advisory Committee on Nuclear Security, *Strengthening of Japan's Nuclear Security Measures*, Japan Atomic Energy Commission, March 9, 2012, at: http://www.nsr.go.jp/archive/nc/kettei120309.pdf.

[5] See Albert J. Jongman, "Introduction To The World Directory Of Extremist, Terrorist And Other Organisations Associated With Guerrilla Warfare, Political Violence, Protest, Organised Crime And Cyber-Crime," in A. Schmid, edited, *The Routledge Handbook of Terrorism Research*, Taylor and Francis, Kindle Edition, 2011. The "Big, Allied and Dangerous (BAAD)" database maintained at University of Maryland provides a listing of 100 such organizations that may have global reach and a proclivity to engage in terror attacks, at: http://www.start.umd.edu/baad/database Top of Form

[6] This trend is described convincingly by David Killcullen *Out of the Mountains: The Coming Age of the Urban Guerrilla*. New York: Oxford University Press. 2013

[7] Robert Ayson provides an excellent typology of possible nuclear terrorist threats, attacks, and outcomes in Robert Ayson, "After a Terrorist Nuclear Attack: Envisaging Catalytic Effects," *Studies in Conflict and Terrorism*, 33, 2010, pp. 571-593.

[8] "Nuclear Power Plant Security and Vulnerabilities" Mark Holt and Anthony Andrews, January 3, 2014 Congressional Research Service

[9] An excellent account of this state of affairs is summarized in D. Birch, R. Jeffrey Smith, J. Adelstein, "Japan could be building an irresistible terrorist target, experts say, The country has balked at U.S. security advice for its nuclear plants," Center for Public Integrity, March 11, 2014, at: https://www.publicintegrity.org/2014/03/11/14366/japan-could-be-building-irresistible-terrorist-target-experts-say

See also: “Japan Conducts Nuclear Terrorism Drill at Plant on Sea of Japan Coast,” Embassy Cable, January 27, 2006, at: http://www.wikileaks.org/plusd/cables/06TOKYO442_a.html and “Nuclear Terrorism Convention: “Nudge” could help Japan Ratify; Physical Protection Concerns Remain,” Embassy cable, February 26, 2007, at: http://www.wikileaks.org/plusd/cables/07TOKYO805_a.html

[10] Masahiro Kakuwa, Scenarios projects in Japanese government: Twenty years of experience, five tales from the front-line, GRASPP Discussion Paper E-15-001, Graduate School of Public Policy, University of Tokyo, March, 2015, at:
http://www.pp.u-tokyo.ac.jp/research/dp/documents/GraSPP-DP-E-15-001.pdf

[11] Shell International, *Scenarios: An Explorer’s Guide*, 2008, p. 8., at:

http://www.shell.com/energy-and-innovation/the-energy-future/scenarios/new-lenses-on-the-future/earlier-scenarios/_jcr_content/par/tabbedcontent/tab_1646782241/textimage.stream/1447230877395/5ab112e96191fa79e1d30c31dc6e5cd2ce19ed518a4c1445ab32aa4c4b5c7ec5/shell-scenario--explorersguide.pdf

[12] “The Vulnerability of Nuclear Facilities to Cyber Attack,” Brent Kesler, *Strategic Insights* Spring 2011 Vol.10 Issue 1,
at: http://calhoun.nps.edu/bitstream/handle/10945/25465/The_Vulnerability_of_Nuclear_Facilities_to_Cyber_Attack.pdf?sequence=1

[13] David Sanger, Martin Fackler, “Tracking the Cyberattack on Sony to North Koreans,”

New York Times, 19 Jan 2015: p. A1, at:
http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0

[14] These three types of cyber-munitions are listed as use of cyber force justifying a military response by the US Department of Defense, Law of War Manual, June 2015, p. 997, at:
http://archive.defense.gov/pubs/law-of-war-manual-june-2015.pdf Many states are creating and arming themselves with such cyber warfare capabilities. See Aliya Sternstein, “The Secret Pentagon Push for Lethal Cyber Weapons,” Defense One, November 5, 2015, at:
http://www.defenseone.com/technology/2015/11/secret-pentagon-push-lethal-cyber-weapons/123435/?oref=defenseone_today_nl

[15] Michael Daly, “Inside the ‘Surprisingly Great’ North Korean Hacker Hotel,” The Daily Beast, December 20, 2014 at:
http://www.thedailybeast.com/articles/2014/12/20/inside-the-surprisingly-great-north-korean-hacker-hotel.html

[16] In 2014, hackers, allegedly from North Korea, hacked into the operating systems of two Korean nuclear power plants. Later, extortion threats were received. S. Shankar, “Hacker Who Posted South Korean Nuclear Plants’ Information Online Demands Money,” *International Business Times*, March 13, 2015, at:

http://www.ibtimes.com/hacker-who-posted-south-korean-nuclear-plants-information-online-demands-money-1845838

[17] On the general issue of reactor cyber-vulnerability, see R. Blunt, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks,* Chatham House , October 5, 2015, at:

https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks

[18] See IAEA, International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, June 1-5, 2015, Vienna, at: http://www-pub.iaea.org/iaeameetings/46530/International-Conference-on-Computer-Security-in-a-Nuclear-World-Expert-Discussion-and-Exchange

[19] Detailed by John Sopko, "Global Proliferation of Weapons of Mass Destruction: A Case Study On The Aum Shinrikyo," *Global Proliferation of Weapons of Mass Destruction,* Part 1, Hearings Before the Permanent Subcommittee on Investigations, US Senate Committee on Governmental Affairs, 104th Congress 1st Session, 31 October and 1, November 1995, p. 48, at: https://ia601407.us.archive.org/7/items/globalproliferat01unit/globalproliferat01unit.pdf

[20] The team did not define precisely what it meant by "insider" or "insider threat." The IAEA provides the following which is consistent with the usage by team 3 in this report: "The term 'adversary' is used to describe any individual performing or attempting to perform a malicious act. An adversary may be an insider or an outsider. The term 'insider' is used to describe an adversary with authorized access to a nuclear facility, a transport operation, or sensitive information. The term 'outsider' is used to describe an adversary other than an insider." See International Atomic Energy Agency, *Preventive and Protective Measures Against Insider Threats*, IAEA Nuclear Security Series 8, Vienna, 2008, p. 4, at: http://www-pub.iaea.org/books/IAEABooks/7969/Preventive-and-Protect-ve-Measures-against-Insider-Threats

[21] Such a system would monitor heart rate and pressure, sweat, skin temperature, metabolic rate, etc., and would stream data to a central data bank. Algorithms would create a profile for each individual, and would track work location at different times, types of work normally encountered such as heavy labor, desk work, long distances walked, etc. When these parameters are exceeded, could set off an alarm and instantly locate the individual. Japanese nuclear managers have considered such systems but believe them to be unusable due to privacy considerations in Japan. It is also possible that well-trained individuals can spoof such a monitoring system. Such a system is already deployed by Samsung in various research domains. See Karissa Bell, "First look at Simband, Samsung's health-tracking wearable of the future," Mashable blog, November 12, 2014, at: http://mashable.com/2014/11/12/samsungs-simband/#.ZE06M1ev8qn

and "Samsung-Simbad, Documentation," at:

https://www.simband.io/documentation/simband-documentation/

The US Defense Science Board on Avoiding Strategic Surprise also suggested in 2015 that a system that tracks these stress indicators and integrates biometric with information obtained from big data sets be considered in the United States: "All defense information systems should continuously monitor cleared personnel with sensitive accesses. Continuous monitoring can be accomplished through the use of big data and creative analytics that combine physical and cyber security information with personnel security information. Insider actions often generate suspicious indicators in multiple and organizationally separate domains-physical, personnel, and cyber security. The use of big data and creative analytics can be carefully tuned to the style and workflow of the particular organization and can help to audit for integrity as well as individual user legitimacy. Software that learns over time may also be used to increase detection and decrease false alarms. Leveraging more open source data is also a sound approach to maintain a more complete picture of personnel with sensitive accesses." See Defense Science Board on Avoiding Strategic Surprise, *DSB Summer Study Report on Strategic Surprise*, July 2015, pp. 9-10, at: http://fas.org/irp/agency/dod/dsb/surprise.pdf

[22] The US Nuclear Regulatory Commission requires that utilities maintain a safety culture; if well run, all employees see something wrong or strange behavior, they are supposed to report it, and the utility is required to ensure that it is safe to do so for the employee, without reprisal. After the September 11, 2001 attack on the United States, the NRC added security to safety in this cultural requirement. See US NRC, "Safety Culture and Nuclear Security," March 26, 2014, at: https://www.nrc.gov/about-nrc/safety-culture/sc-nuclear-security.html

[23] See Gary A. Ackerman and James Halverson, "Attacking Nuclear Facilities: Hype or Genuine Threat?" in Brecht Volders, Tom Sauer, edited, *Nuclear Terrorism: Countering the Threat*, Routledge, forthcoming, 2016; and the 80 malicious and activist attacks and invasion incidents on nuclear facilities described in the "Nuclear Facilities Incident Tool," at: http://www.start.umd.edu/news/new-online-tool-reveals-terrorist-networks-and-behavior-over-time

[24] See M. Bunn, Matthew, S. Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes*, Occasional Paper, American Academy of Arts & Sciences, Cambridge, April 4, 2014, at: http://belfercenter.ksg.harvard.edu/publication/24088/worst_practices_guide_to_insider_threats.html

[25] International Atomic Energy Agency, *Preventive and Protective Measures Against Insider Threats*, IAEA Nuclear Security Series 8, Vienna, 2008, p. 20, at: http://www-pub.iaea.org/books/IAEABooks/7969/Preventive-and-Protective-Measures-against-Insider-Threats

[26] Such as the August 5, 2015 attack on the Doel Nuclear Power Station, Doel, Belgium in which a saboteur released the oil to an underground storage tank, causing the overheating and shutdown of the Doel 4 turbine and ultimately the reactor.

IV. NAUTILUS INVITES YOUR RESPONSE

The Nautilus Asia Peace and Security Network invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent in the response.

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/japan-scenar-os-vulnerability-to-terrorism-of-nuclear-spent-fuel-management/