DETERRING NUCLEAR TERRORISM: INSIDER THREATS TO NUCLEAR FACILITIES

Recommended Citation

Martha Crenshaw, "DETERRING NUCLEAR TERRORISM: INSIDER THREATS TO NUCLEAR FACILITIES", NAPSNet Special Reports, October 06, 2017, https://nautilus.org/napsnet/napsnet-special-reports/deterring-nuclear-terrorism-insider-threats-to-nuclear-facilities/

MARTHA CRENSHAW

October 6, 2017

I. INTRODUCTION

In this essay, Martha Crewshaw concludes that “the difficulties associated with meeting the

requirements for a successful strategy of deterrence suggest that governments and the nuclear power industry would be wise to emphasize prevention of the full range of insider, outsider, and combined insider-outsider terrorist threats from non-state actors."

Martha Crenshaw is Senior Fellow at Center for International Security and Cooperation, Freeman Spogli Institute for International Studies, Stanford University

Paper prepared for Workshop *Reducing Risk of Nuclear Terrorism and Spent Fuel Vulnerability in East Asia* co-sponsored by Nautilus Institute and Research Center for the Abolition of Nuclear Weapons, Nagasaki University, Nagasaki, January 20-22, 2017

Banner image: Excavation of fused soil, rocks and debris under hypocenter of Nagasaki nuclear explosion. Photo credit: Nautilus Institute

II. NAPSNET SPECIAL REPORT BY MARTHA CRENSHAW

DETERRING NUCLEAR TERRORISM: INSIDER THREATS TO NUCLEAR FACILITIES

October 6, 2017

This paper addresses the issue of the threat posed by terrorists to civilian nuclear facilities, with particular attention to insider threats to the nuclear fuel cycle. The question is whether or not deterrence is an effective answer to the problem posed by the possibility that terrorist non-state actors could possess both motivation and capability to exploit vulnerabilities in this area. This analysis begins by explaining what deterrence is and what the target of a deterrent strategy should be, since the concept is often poorly understood. It then considers the range of ideological objectives and social contexts that characterize contemporary terrorist organizations and movements and that would affect their reactions to a deterrent strategy. Next the paper evaluates the different purposes of terrorist attacks (the specific tactical or short-term objectives that an attack on nuclear facilities might serve). It then asks how vulnerable the nuclear fuel cycle, especially spent fuel, is to insider threats, based on the historical record as well as expert judgments. Last, the paper considers the particular case of Japan. The conclusion of this analysis is that deterrence is a difficult strategy to implement and that its results are uncertain.

Deterrence

Deterrence takes two basic forms: retaliation and denial. Both types are ways of influencing how adversaries think. Typically studies of deterrence assume that the state is the primary defender against terrorist challengers. The government trying to deter a terrorist attack attempts to alter the decision-making calculus of the opponent. If deterrence is successful, the terrorist does not act. This expectation makes it difficult to judge the success of a deterrent strategy. It is hard enough to know why such adversaries take action, and even harder to understand why they might not act or even whether or not they intended to act. In general, studies of terrorism lack a clear understanding of terrorist decision-making processes, which is understandable considering the nature of the clandestine underground organizations that are usually the subject of analysis.

Deterrence by retaliation, or punishment, means that the state communicates a clear and credible threat of unacceptable harm to the threatening non-state actor. The message must be explicit and definitive concerning the "red line" that must not be crossed. The terrorist actor must be convinced that crossing this line (which could, for example, mean acquiring nuclear materials, never mind constructing an explosive or other device) will trigger the activation of the threat, or at least terrorists should be sufficiently uncertain about the possibility of retaliation that the risk is not worth taking. Thus the threat has to consist of some proposed infliction of pain that the state is both willing and able to carry out, even if the threat leaves something to chance. Willingness is often hampered by domestic political constraints and international norms; for example, an American threat to destroy Muslim holy places in order to deter Al Qa'ida or the Islamic State might not be convincing. Even issuing such a threat would be controversial and provocative, never mind the consequences of carrying it out.

Capability also depends on being able to attribute responsibility for an attack in order to identify and then retaliate against the offending actor. There are numerous barriers to accurate and timely attribution. For example, terrorist actors may not claim credit and may deliberately obfuscate responsibility. There can be multiple competing claims. The capacity to respond also depends on having not just general superiority in the means of using force (asymmetry between defender and challenger can be assumed) but having exactly the right sort of retaliatory capabilities ready for timely deployment. For example, one of the reasons that India did not retaliate in 2008 when civilian targets in Mumbai were attacked by Islamist militants was lack of the type of specific precision military capabilities required to hit terrorist strongholds in Pakistan without causing so much damage as to provoke inter-state war. The situation was complicated by Pakistan's connections to extremist groups and by the nuclear rivalry between the two states, leading to fears of escalation. As a consequence there was pressure on India, at least from the United States, to exercise restraint. If terrorists can anticipate these constraints on retaliation, deterrence is weakened.

Deterrence by denial is usually thought to be somewhat less complicated and more likely to be effective in discouraging an adversary. It means making the commission of the act of terrorism so physically difficult and costly and unlikely to succeed that the adversary chooses not to undertake it. In effect, deterrence by denial usually involves target-hardening, and it is difficult to distinguish denial from simple prevention. The terrorist adversary knows in advance that the state's defenses are so strong that it is not worthwhile to attack. It is not impossible to do so, but too costly. In this case, the defending government confronts something of a dilemma, in that publicizing the strength of one's defenses might provide useful information about how to subvert, evade, or design around them. This dilemma can encourage secrecy. Advertising one's strength might also provoke some terrorists. And governments must consider the issue of cost. Will the public accept the argument that strong protective defenses are needed, particularly if they are expensive and/or undermine civil liberties and invade privacy? Publics will be especially reluctant to pay high costs and inclined to think that the government is exaggerating the threat when defenses have not been directly challenged, which is the case with nuclear terrorism in general. The seriousness of the threat has been debated among experts for many years.[1]

Deterrence by denial can also be particularly costly if there is an abundance of possible targets for terrorist attack (Powell 2007). In addition, in a target-rich environment effective deterrence of attack against one particular class of target might create a substitution effect, whereby the terrorists are simply deflected onto an easier less well-defended target.

Social resilience and effective consequence management can be considered variants of deterrence by denial. If the terrorist knows or even suspects that the attack will not create an extreme public

reaction, the anticipated result might not seem worth the cost, especially if the cost is certain and the reward is not. Again, what is important is that the terrorist not even attempt an action that is contemplated.

Clearly the effectiveness of deterrence in either form, retaliation or denial, depends on the "rationality" of the adversary. However, rationality cannot be assumed. An adversary may be insensitive to cost, and if there are no costs to terrorism that outweigh the perceived benefits, then deterrence cannot succeed. If the adversary does not make reasonable decisions then calculations of cost versus benefit are not possible. If there is no unitary actor the situation is complicated, and terrorist actors are often extremely elusive and fluid in organizational terms. Actors range from disgruntled and inspired individuals ("homegrown" extremists acting without operational direction, essentially volunteers) to small groups or social networks to hierarchical and structured complex organizations.

Who should deterrent threats be addressed to? Discussions of the subject differ in terms of the appropriate level of targeting. Even if an organization or entity as a whole could be considered irrational in terms of objectives (they may think that gaining the end is worth any cost no matter how high) or impervious to cost-benefit calculations, the individuals who make up the organization may still be susceptible to influence. The government can threaten things they value. Thus targeting individual leaders might at least deter other aspiring leaders and degrade organizational effectiveness. These targets can be top leadership or mid-level operators, such as financiers, planners, or bomb-makers. Drone strikes or targeted killings may perform this role (although if deterrence is successful the threat alone suffices to deter), although it appears more likely that such attacks are meant to remove dangerous individuals rather than influence the willingness of replacements to serve. The rationale is apparently that there is a limited supply of talent for any terrorist organization, and it will eventually be exhausted if the government is persistent. The idea proposed from time to time that governments target family members of suspected terrorists may follow the same logic, although it is critical to remember that such a policy would be contrary to international law and norms of noncombatant immunity.

This type of individual-level deterrence figures prominently in the field of criminal justice. Central questions are whether or not stiff prison sentences deter crime. Severe penalties must be meaningful to the potential individual criminal, whether or not a member of an organized gang, and he or she must also be reasonably sure of being caught and punished.

The Terrorist Adversary

A strategy of deterrence has to be tailored to specific adversaries. Groups and individuals using terrorism can and have pursued a variety of ideological objectives, from revolutionary socialism to right-wing reactionary causes to jihadism, and passing through single-issue motivations such as environmental or animal rights activism. Possibly these ideologies could be classified as "reconcilable" versus "irreconcilable." When jihadist groups such as Al Qaida first came to the attention of experts and scholars in the late 1990s some political analysts distinguished terrorists as "old" versus "new" types: the "old" pragmatic terrorists were presumably willing to negotiate, to sit at the table and bargain with the authorities, and their methods were limited. In contrast the "new" terrorists seemed only to want to destroy the table; their ends and their means were unbounded (for a review of these arguments see Crenshaw 2011.) Aum Shinrikyo was typically placed in the category of "new" and apocalyptic and thus beyond influence. Often the "new" was associated with religious motivations and flat decentralized organizational structures. This binary interpretation between "old" and "new" is somewhat simplistic even if superficially persuasive. In reality, the response to terrorism has to proceed on a case-by-case basis, and an effective response requires deep and detailed understanding of specifics. Even apparently absolutist groups with excessively

ambitious goals can make cost-benefit calculations, and there may be limits to the risks they are willing to undertake and the costs they are willing to incur. It is essential to understand each group's perception of risk and its definition of what constitutes cost as well as benefit. What does "success" mean to them? The government's conception of these factors probably does not match the terrorist's.

Three operational characteristics of terrorist strategies could be important to ascertaining how such actors think and how they might respond to deterrent threats. One factor is the group's willingness or intent to cause mass casualties.[2] Typically such intent is associated with the "new" terrorism, but in practice this association does not always hold up. Sendero Luminoso in Peru, for example, was an extremely deadly organization despite lacking an apocalyptic or millenarian ideology. So too was the Secret Army Organization (OAS) during the last stages of the Algerian war (1954-1962), which offers a historical precedent worth thinking about. The OAS was composed of French settlers and former military officers who opposed the French government's plan to offer Algeria independence after years of costly struggle. They determined on a destructive "scorched earth" strategy; if the French could not stay in Algeria there would be nothing left for the Algerians. More recently, jihadist groups such as the Islamic State are justifiably infamous for killing large numbers of fellow Muslims simply because they are regarded as apostate. It could be argued that willingness to kill indiscriminately is linked to high risk tolerance, since there is a high possibility of popular backlash in the constituency the group aspires to represent. There is also a strong likelihood that opposing governments will be provoked to respond in force. As the above examples indicate, indiscriminate killing of civilians is not necessarily associated with religion or millenarianism.

Another possible strategic consideration is degree of reliance on suicide missions. Suicide attacks (defined as those acts that require the death of the perpetrator in order to succeed tactically) can be interpreted as a form of costly signaling of resolve and commitment ("our resolve is so strong that we do not fear death"). As in the case of killing civilians, suicide missions are often associated with "religionist" groups such as jihadists and with ideologies of martyrdom and sacrifice. However, the LTTE, a secular ethno-nationalist group in Sri Lanka, elevated suicide attacks to a central strategy. (The LTTE also fought to the death without compromise after negotiations failed repeatedly.) Reliance on suicide attacks certainly indicates that some individual members of organizations are not just willing but eager to give their lives, and thus that retaliatory deterrence at an individual level is unlikely to work. Deterrence by defense might also be problematic. Suicide attacks can be tactically successful in breaching the first line of defenses so that squads of armed attackers can enter facilities (a tactic used in Afghanistan and Iraq). That is, suicide attackers can overcome the defensive barriers that might deter other types of attackers. This knowledge is easily available to terrorists. In this discussion, however, it is essential to account for role differentiation within organizations. Not everyone in an organization is willing to become a suicide attacker nor will the organization want to deploy them. Indeed in civil wars such as Syria foreign fighters who possess limited fighting skills are used to fill the ranks of suicide bombers.

A third characteristic that might be relevant to terrorists' risk perception, cost-benefit calculation, and capability is transnational reach. Some groups are content to restrict their actions to the local theatre of conflict, whereas others extend the scope of their ambitions to the global or at least regional scale. The latter expansiveness is often associated with jihadist groups attempting to strike the "far enemy," which could be any ally of the United States. ISIS, for example, killed Japanese nationals in Syria. However, groups such as Al Shabaab in Somalia and Boko Haram in Nigeria strike across national borders in their regional neighborhoods. It is difficult (although not impossible) for a state to retaliate against or punish a group that is located outside its boundaries, possibly in a "safe haven" in a failed state or one immersed in the chaos of civil war. Israeli policy has consistently relied on cross-border retaliation for terrorist attacks from Palestinian groups.

Alternatively, the group might have found asylum in a hostile neighboring state that would retaliate in turn if the group were struck within its borders.

Another possible variable is the terrorist actor's ability to organize complex attacks. However, it would be unwise to assume that an attack on nuclear facilities would necessarily be complex or involve complicated and lengthy planning.

The Vulnerability of Nuclear Facilities

Ackerman and Halverson (2016) collected and analyzed a Nuclear Facility Attack Database, which contains 80 cases of intrusions and attempted intrusions into nuclear facilities worldwide from 1961 to 2015. Approximately half of the cases were regarded as reliably "high threat." The authors noted that a wave of attempts to breach security from the outside began in about 2010, indicating a possible upward trajectory in attack occurrence. Nuclear power plants are the most common target (being the most common type of nuclear facility). The most common attack type is armed assault, followed by theft, usually by an insider. Ackerman and Halverson caution, however, that no type of attack should be ignored.

Insiders were involved in a quarter of all incidents and close to half of those defined as higher threat. The insider threat was also associated with an anti-nuclear power ideology – that is, these activists were apparently more likely than others to be able to get into nuclear facilities. (Criminals are also extensively involved, interestingly enough.) Ackerman and Halverson describe in detail the fairly recent case of the Pelindaba Nuclear Facility near Pretoria, South Africa, an attack that occurred in 2007. Two teams of attackers penetrated the secure perimeter of the facility, which contained 1000 pounds of HEU, even though it was supposed to be well-protected. Although details are lacking, it seems that insiders were probably involved. Certainly the attackers had good knowledge of the layout of the facility, so they could have been former insiders. The identities and motivations of the attackers are not known, so it is impossible to say whether or not they could have been deterred. The case also shows that if the government does not expect attack it will not have issued a deterrent threat or communicated a posture of deterrence by denial.

The authors conclude that the human component of security systems is critical. Poor security culture – resulting in complacency, carelessness, lack of training, and glitches and oversights such as security cameras or sensors that are not working – is often at fault. Even though many attacks over the years have involved insiders, the administrators of security systems seem to neglect the importance of their role. The authors urge more attention to personnel reliability programs. In a public presentation (Halverson 2016), Halverson noted that the easiest terrorist assault is disruption or shut-down of a nuclear facility, rather than theft or release of radioactive material (e.g., through breach of spent nuclear fuel storage). He also called attention to two possible insider options; action by someone already inside the facility who later becomes "radicalized" versus the deliberate insertion of an operative from the outside, someone who is already a member of the organization and who procures employment or access.

In another research study, Hegghammer and Daehli (2017) focused specifically on insider versus outsider threats. They found that terrorists have shown less interest in using insiders to attack nuclear facilities than might have been expected, and they suggest that the reason is the difficulty of recruiting insiders. Where there is interest in recruiting insiders, it is more likely to come from far-right than jihadist groups. Furthermore, infiltration of a nuclear facility is more likely to happen when someone already inside reaches out to a terrorist group ("outreach"). Second to that possibility is what the authors call "autonomous action," essentially a variant of self-radicalization or "lone wolf" terrorism without operational direction from the outside. Their findings were based on careful examination of terrorist communications about nuclear attacks. Jihadist groups rarely

mentioned nuclear facilities, with the exception of past Chechen groups, who threatened Russia. The authors found little explicit discussion of recruiting insiders, leaving aside general calls for inspirational terrorism by anybody, anywhere, mostly from Al Qa'ida in the Arabian Peninsula and ISIS. Another prominent exception to the pattern of not discussing insiders is Aum Shinrikyo, the leaders of which not only wrote about using nuclear weapons but took steps to acquire them, including recruitment. Aum Shinrikyo abandoned the plan because it was too difficult, and feasible alternatives such as the use of sarin gas were easier.

Like Ackerman and Halverson, Hegghammer and Daehli created a dataset that covered 1960 to 2013. They found three insider attacks, two of which were potentially serious. In 1982 the African National Congress exploded four bombs in a nuclear power plant, and in 1995 there was a Chechen plot against a Russian nuclear submarine. They regarded the Pelindaba South Africa attack as uncertain in terms of an insider role. In the end they concluded that the 1982 ANC bombings were the only confirmed serious case, and the scope of the attack was limited although it is a clear case of outreach by someone already inside. There were, however, other suspected plots, most significantly the Belgian case in late 2015 and early 2016, when investigations following the November Paris attacks discovered indications that the jihadist cell linked to the Islamic State meant to kidnap an official who could help them get materials to build a dirty bomb. Later authorities learned that the groups also had photographs of a nuclear storage facility.[3] There were also close-call cases of individuals who radicalized while working at nuclear facilities but who left that employment before becoming active participants in jihadist groups. Apparently it did not occur to them that their insider knowledge and experience could be beneficial to the cause they aspired to support.

How to explain the rarity of nuclear attacks and plots? According to Hegghammer and Daehli, despite a general image of complete ruthlessness and indifference to norms, terrorists do face ideological constraints about using such weapons. In addition, opportunities are limited. There are few nuclear facilities worldwide, and most of those are located in countries largely free of terrorism. Trying to recruit someone already on the inside is prohibitively costly and difficult, especially since there are easier alternatives to the nuclear option. The authors concluded nevertheless that it would be unwise not to protect nuclear facilities from insider threats, and that one way of doing this is to encourage terrorist groups to believe that insider volunteers are actually clandestine intelligence agents trying to trap them. That is, the projected use of informants and double-agents could constitute a deterrent threat if appropriately communicated to would-be recruiters. This measure would constitute a strategy of deception.

Japan and Nuclear Terrorism

The 2016 report of the Nuclear Threat Initiative listed Japan as one of the countries that was increasing its stock of weapons-usable nuclear materials.[4] Japan had, however, improved in terms of theft ranking (now number 12 out of 24 countries). Japan ranked fifth in terms of sabotage and number two in terms of risk environment. The NTI report observed that the factor of culture "particularly affects the threat posed by malevolent insiders. In cultures where trust is high or where privacy is highly valued, the concept of intrusive personnel vetting through background checks that include drug testing and psychological tests may be unpopular or considered unnecessary" (p. 32). The report also emphasized that nuclear terrorism could be combined with a cyberattack, an area where the critical infrastructure of most countries is vulnerable and a subject of intense security concern in the United States and elsewhere. Thus vulnerability is real and growing, but the conditions that would promote effective deterrence, especially deterrence by denial, may be weak or absent.

According to NTI, Japan is increasing the quantities used in the civilian nuclear energy sector – producing or receiving plutonium faster than the reactors can consume it. Restarting the Rokkasho

Reprocessing Plant as planned is expected to further increase the stock of separated plutonium. The Center for Public Integrity warned in March 2016 that

Already, Japan has 9.3 metric tons of plutonium stored at Rokkasho and nine other sites in the island nation; about 35 tons of plutonium are stored in France and the United Kingdom. Once Rokkasho opens, the size of its stockpile could easily double in five and a half years, because by the government's own forecast Japan is at least 20 years from completing the first of the commercial reactors designed to burn the plutonium that Rokkasho will produce.

Building such large factories for nuclear materials poses special risks. Experts say the International Atomic Energy Agency will likely be able to track 99 percent of the plutonium as it moves through the Rokkasho plant. While 99 percent might sound good, the plant's annual output will be so high that a one-percent error rate means roughly eighty kilograms of plutonium a year could be untraceable — enough for 26 bombs. Critics worry as a result that the sizable uncertainties will open the door to diversion attempts by insiders.[5]

There is international concern that Japan needs more capable and extensive security forces (armed as opposed to unarmed guards on site and more training exercises at the least, quicker response time by armed units, and probably more involvement of official police or military forces) and more widespread and thorough background checks of employees. However, robust norms of privacy and expectations of a non-threatening environment impede initiatives to bring about policy change. Moreover, the public-private partnership in nuclear facility operation makes it difficult to reform, in terms of both capabilities and resolve or will. Yet such changes leading to enhanced state control would be essential to a strategy of deterrence by denial or retaliation. Improved levels of protection would also have to be communicated to potential terrorist insiders, which requires some transparency. That is, potential terrorists would have to be sure that they could not succeed and possibly that they would be apprehended and punished.

Some of these recommendations might encounter obstacles. For instance, background checks of workers would not necessarily be effective if the insider threat is actually based on self-radicalization or recruitment by an outside organization of an existing employee rather than insertion of a sleeper agent by an outside adversary. It is extremely difficult if not impossible to ascertain who might be likely to become radicalized and either act on his or her own or accept a recruiting offer. Similarly, background checks upon hiring would not solve the kidnapping and blackmail problem (referred to in the 2015-16 Belgium case). The use of biometric sensors to measure stress might help alleviate this threat but the reliability of such systems is unproven. A safety culture that encourages employees to report unusual attitudes or behavior might also help, but it is instructive to recall the case of Omar Mateen, who was responsible for the Orlando, Florida shooting in June 2016. He was reported by fellow workers to the FBI, which deployed an informant to check on Mateen's security risk, but after investigation the authorities concluded that he was not a threat. Their assessment may have been wrong, but it is also possible that his attitudes changed over time.

A critical problem for deterring insider attacks or insider-outsider combined attacks relates to the short-term goals of the group (thinking of the adversary as a collective entity is reasonable since the self-radicalized individual thinks of himself as acting in the name of an ideological cause). If simply creating public fear and distrust of government or of nuclear power is the largely symbolic objective, this is relatively easily accomplished without much actual destruction or mass casualties. Such attacks might be especially hard to deter since they do not have to "succeed" in a physical or material sense. For example, Al Qaida in the Arabian Peninsula (AQAP) was quite satisfied with the accomplishments of the 2009 Christmas bomber even though he did not succeed in blowing up the aircraft and was arrested by the American government. The fact that he had penetrated American

aviation defenses was reward enough. It is also possible that such "weak" symbolic attacks are more attractive to groups that do not actually wish to cause mass casualties (or to take a lot of time in planning, which increases the likelihood of discovery of the plot) and thus that the lowered normative threshold might make such attacks that much more likely. As Hegghammer and Daehli concluded, some terrorist groups are sensitive to normative constraints. On the other hand, what was intended by sensitive terrorists as a simple demonstration could accidentally evolve into catastrophe. Yet governments might not wish to emphasize the likelihood that minor incidents in a nuclear facility might spin out of control because of the danger of sparking public fears about nuclear power. This reticence would complicate a strategy of deterrence.

Deterrence by threat of retaliation or punishment may not succeed against adversaries bent on suicide missions. It is hard to tell if such threats would work to deter the insider who radicalizes, but the prospect of severe punishment should one be apprehended (and the likelihood that one would be caught) could be a strong influence. If the threat is an insider-outsider combined attack and all the outside attacking team plan to die in the attack, then threats of individual punishment will be ineffective, of course. But if the team is sent by a larger outside organization that is vulnerable to reprisals (e.g., a major crackdown that removes or incapacitates all their members) then credible threats of retaliation could work. The credibility requirement should be stressed here. If the organization is located within Japan, it could be rolled up as the Japanese Red Army and Aum Shinrikyo were. However, if the adversary's operational center is located outside of Japan, it will be hard to make threats of retaliation credible. Outside centers might be jihadist groups headquartered abroad or state-sponsored groups associated with North Korea, generally considered a less than optimally rational adversary and which a crisis might derange entirely. An outside terrorist group would be well aware that the government would react strongly in both short and long terms even to an attack that was not extremely destructive in a material sense. Provocation is often one of the central aims of terrorism. A nuclear terrorist attack of any sort would be highly provocative, to say the least. Threats of retaliation might simply play into the hands of non-state or state-sponsored terrorists who intend to provoke over-reaction.

In conclusion, the difficulties associated with meeting the requirements for a successful strategy of deterrence suggest that governments and the nuclear power industry would be wise to emphasize prevention of the full range of insider, outsider, and combined insider-outsider terrorist threats from non-state actors. As noted earlier, prevention is often hard to distinguish from deterrence by denial. Either way, prevention or denial, the strategy is costly on many levels, and in Japan it seems that deterrence would require social, economic, and political adjustments that have so far proved difficult and slow to accomplish. Unfortunately it often takes a disastrous terrorist attack to produce policy change. The 2011 Fukushima disaster was an immense safety lapse with profound implications for nuclear security that may not yet be entirely realized. The American government's reaction to the 9/11 attacks showed that when the rare catastrophic terrorist event happens, the state is likely to undertake a quick and massive response that is rife with unintended consequences and difficult to roll back or adapt to changing circumstances as the threat shifts over time (Crenshaw and LaFree, 2017).

III. ENDNOTES

[1] See the debate between Brian M. Jenkins and John Lauder, *The Nuclear Terrorism Threat: How Real Is It?* Nonproliferation Policy Education Center Working Paper 1602, September 2016. Editor Henry D. Sokolski.

[2] Note that I am not arguing that attacks on nuclear facilities or the use of radiological dispersion devices made from stolen material would necessarily cause mass casualties.

[3]Patrick Malone and R. Jeffrey Smith, “A Terrorist Group’s Plot to Create a Radioactive ‘Dirty Bomb’,” The Center for Public Integrity, February 29, 2016. (https://www.publicintegrity.org/2016/02/29/19376/terrorist-group-s-plot-create-radioactive-dirty-bomb)

[4] *Building a Framework for Assurance, Accountability and Action*, January, 2016. (http://www.ntiindex.org/wp-content/uploads/2013/12/NTI_2016-Index_FINAL.pdf)

[5] R. Jeffrey Smith, “Nuclear Security: A Vital Goal but a Distant Prospect” (https://www.publicintegrity.org/2016/03/28/19447/nuclear-security-vital-goal-distant-prospect). Also Douglas Birch and R. Jeffrey Smith, “Japan Could be Building an Irresistible Terrorist Target, Experts Say,” November 20, 2015 update (https://www.publicintegrity.org/2014/03/11/14366/japan-could-be-building-irresistible-terrorist-target-experts-say). See also Peter Hayes, "Nuclear terrorism risks in Northeast Asia: Japan’s reactor restart and spent fuel", NAPSNet Special Reports, March 23, 2015 (https://nautilus.org/napsnet/napsnet-special-reports/nuclear-terrorism-risks-in-northea-t-asia-japans-reactor-restart-and-spent-fuel/).

IV. REFERENCES

Gary A. Ackerman and James Halverson, “Attacking Nuclear Facilities: Hype or Genuine Threat?” in Brecht Volders and Tom Sauer (eds.), *Nuclear Terrorism: Countering the Threat* (New York: Routledge, 2016).

Martha Crenshaw, “The Debate over ‘Old’ vs ‘New’ Terrorism,” in Rik Coolsaet (ed.), *Jihadi Terrorism and the Radicalisation Challenge: European and American Experiences* (Second Edition), (London: Ashgate, 2011).

Martha Crenshaw, “Will Threats Deter Nuclear Terrorism?” in Andreas Wenger and Alex Wilner (eds.), *Deterring Terrorism: Theory and Practice* (Stanford: Stanford University Press, 2012).

Martha Crenshaw and Gary LaFree, *Countering Terrorism* (Washington: Brookings Institution Press, 2017).

James Halverson,”Radicalization as a Threat to Nuclear Facilities,” presentation to the Workshop on Countering Homegrown Violent Extremism in the Nuclear Sector, London, May 25, 2016.

Thomas Hegghammer and Andreas Hoelstad Dæhli, "Insiders and Outsiders: A Survey of Terrorist Threats to Nuclear Facilities," in Matt Bunn and Scott Sagan (eds.), *Insider Threats* (Ithaca, NY: Cornell University Press, 2017).

Robert Powell, “Defending against terrorist attacks with limited resources,” *American Political Science Review* 101, 3 (2007), pp. 527-541.

V. 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.
