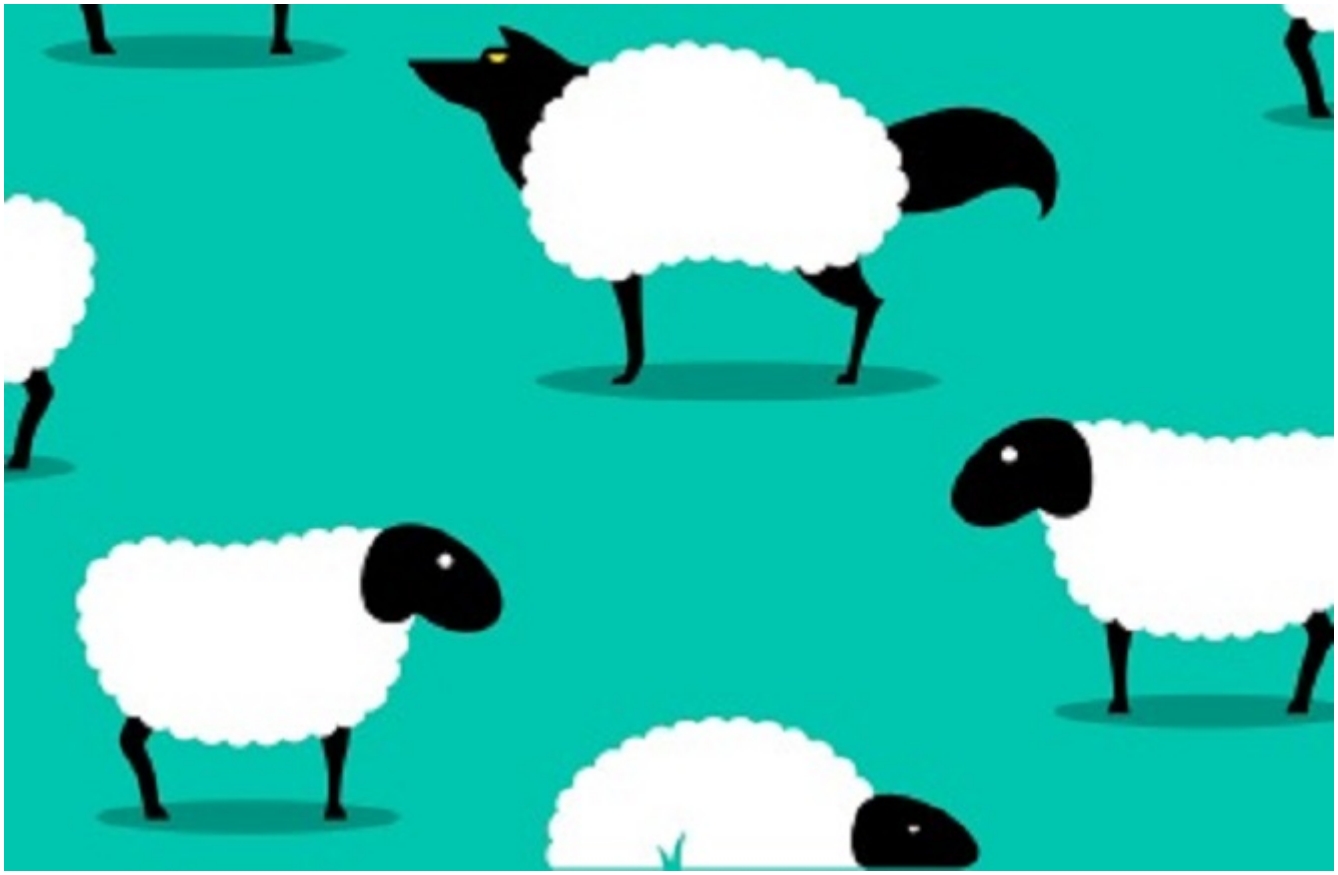
SCENARIOS OF INSIDER THREATS TO JAPAN’S NUCLEAR FACILITIES AND MATERIALS – AND STEPS TO STRENGTHEN PROTECTION



Recommended Citation

Matthew Bunn, "SCENARIOS OF INSIDER THREATS TO JAPAN’S NUCLEAR FACILITIES AND MATERIALS – AND STEPS TO STRENGTHEN PROTECTION", NAPSNet Special Reports, November 02, 2017, https://nautilus.org/napsnet/napsnet-special-reports/scenarios-of-insider-threats-to-japans-nuclear-facilities-and-materials-and-steps-to-strengthen-protection/

SCENARIOS OF INSIDER THREATS TO JAPAN’S NUCLEAR FACILITIES AND MATERIALS – AND STEPS TO STRENGTHEN PROTECTION

MATTHEW BUNN

NOVEMBER 2, 2017

I. INTRODUCTION

In this essay, Matthew Bunn reviews scenarios of insider threats to Japan's nuclear facilities and materials, and measures to strengthen protection. He concludes: "No one has all the answers about how best to do it. Hence, there is a need to keep trying, keep assessing, keep testing, and keep exchanging ideas – including among the countries in Northeast Asia. There is no room for complacency – which is always the enemy of effective security."

Matthew Bunn is an American nuclear and energy policy analyst, currently a professor of practice at the Harvard Kennedy School at Harvard 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

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: from Office of Homeland Security & Emergency Coordination
Insider Threat Program, here.

II. NAPSNET SPECIAL REPORT BY MATTHEW BUNN

SCENARIOS OF INSIDER THREATS TO JAPAN'S NUCLEAR FACILITIES AND MATERIALS – AND STEPS TO STRENGTHEN PROTECTION

NOVEMBER 2, 2017

Introduction: The Insider Challenge

Many people in nuclear organizations do not like to believe that any of their colleagues could ever pose a threat to their organization or their country. Nevertheless, the evidence suggests that while major nuclear incidents involving insiders are rare, insiders pose the most serious and challenging security threats to nuclear facilities. Nearly all of the nuclear theft and sabotage incidents that have occurred in which the circumstances are known were perpetrated by insiders in nuclear organizations, or with the help of insiders.[1] Most recently, in 2014, an insider at the Doel-4 nuclear power plant in Belgium (as yet unidentified) drained all the lubricant for the turbine, shutting the plant for months and causing hundreds of millions of dollars in economic damage. Investigations revealed that almost two years earlier, an insider named Ilyass Boughalab, cleared for access to the plant's vital areas, had left to fight for the Islamic State; while Boughalab had nothing to do with the sabotage, his clearance raised serious questions about the screening processes in place at the time.[2] Subsequently, Belgium substantially strengthened its protection against insider nuclear threats – while also beefing up physical protection against outsiders.[3]

Truly effective protection against insiders is difficult to achieve – particularly if the possibility of

multiple insiders conspiring together is considered (something that occurs regularly in non-nuclear thefts).[4] Insiders are known and trusted by other employees; they may have detailed knowledge of the security system and its weaknesses; and they can take months or even years to plan their activities. In some organizations, even the most alarming "red flags" can go unreported and unaddressed.[5]

Because of the difficulty of coping with the potential for insider adversaries, it is a mistake to assume that any particular measure (such as background checks) will be sufficient. Instead, protecting against insider threats requires a comprehensive approach including many elements – from programs to deal with employee disgruntlement to careful monitoring of critical materials and equipment. Insider protections are particularly important at HEU or plutonium bulk-processing facilities, which appear to have been the source of nearly all of the known cases of seizure of stolen weapons-usable nuclear material. When material is being handled regularly and is in the form of powders or liquids, it is significantly easier for insiders to remove small amounts without being detected.

This paper will draw on a number of real-world incidents to explore categories of potential insider motivations; types of possible insider actions; and some examples of insider scenarios that could pose a threat to nuclear facilities in Japan, in particular.[6] In a concluding section, the paper then suggests some potential solutions for reducing the risks posed by insider threats.

Categories of Insider motivations

Damaging insider incidents have taken place in many high-security organizations all around the world. Insiders commit their actions for a wide variety of reasons, from inadvertence to devotion to the cause of a terrorist group.

The radicalized insider

In some cases, insiders take their actions because of a fervent belief in a radical cause, such as that of a terrorist organization. This can occur if a participant in a terrorist group manages to infiltrate a high-security organization, or because they become radicalized after they have been employed.

Consider, for example, the case of Ilyass Boughalab, mentioned earlier. He was employed by a contractor to the nuclear plant, not on the plant's staff itself. Part of his job – which he reportedly did very well – was checking the quality of welds. This required access to the plant's vital areas – those areas from which a sabotage could potentially cause a major radioactive release – and he successfully passed a screening process and received a clearance for access to those areas. His family reports that he was radicalized after the clearance was approved. If that is true, the initial clearance process could not have been expected to turn up his radical tendencies.[7] Indeed, even the common practice of re-investigation every few years may not be sufficient, as in many recent cases of radicalization (including that of Boughalab), the change in views and behaviors happens over a period of months, rather than years. Hence, ongoing monitoring of all relevant staff – including programs to encourage staff to report any concerning behavior – must be a part of a comprehensive program to protect against insider threats.

It is worth noting that Boughalab, as far as is known, took no action against the reactor where he worked; rather than attacking in Belgium, he left to fight in Syria, where he was reportedly killed (after having been convicted in absentia of terrorist activities). The sabotage at the reactor was carried out by someone else – as yet unidentified – and may have been intended more to send a message to management than for terrorist purposes (since the particular sabotage that occurred could not have led to a radioactive release). Indeed, a detailed recent examination found few actions

and little writing by jihadi terrorist groups related to insider attacks on nuclear facilities – though the authors make clear that the threat cannot be dismissed.[8]

Arguably, as relatively homogeneous societies, countries such as Japan, the Republic of Korea, China, and Taiwan face smaller threats of Islamic radicalization than many other countries do. There are reported, however, to be at least nine Japanese citizens fighting for terrorist groups in Syria and Iraq, along with hundreds of Chinese citizens, primarily Uigurs.[9]

The Aum Shinrikyo experience in Japan provides a more troubling example. A group that originated in Japan – but could as easily have started in Korea, China, or elsewhere – was able to recruit thousands of people in Japan, including dozens of active or retired police and military personnel. Two members of an elite National Defense Force paratroop unit, for example, were charged with warning Aum before the March 22, 1995 raid on a key Aum facility; one of them also attacked Aum headquarters with a Molotov cocktail in an effort to build up sympathy for Aum and throw police off the scent.[10] After the sarin attacks, Aum member Yoshiyuki Kosugi, who was an active-duty policeman, asked to be transferred to the police unit investigating the attacks, apparently to help suppress, inform on, or misdirect the investigation. Kosugi was later accused of shooting National Police Agency chief Takaji Kunimatsu, who had taken personal charge of the investigation of the subway sarin attacks. (He was shot three times and severely wounded outside his home, whose location was secret.) Kosugi confessed more than once, but later retracted his confessions; the allegation was never proved and the shooting remains unsolved. A senior Aum member reported that Kosugi had leaked confidential information about the investigation to him, but Kosugi was never prosecuted on that charge, either.[11] Another member of the National Defense Force worked with Aum to steal confidential documents from Mitsubishi Heavy Industries, while another provided the head of Aum's chemical weapons effort with a textbook on protection against chemical weapons.[12]

While Aum as it was is no longer active, other groups could arise in the future. Unfortunately, the bottom line is that Japanese, Korean, Chinese, and Taiwanese nuclear managers cannot assume that the threat of radicalized insiders in their organizations can be ignored.[13]

The coerced insider

Even if all the members of an organization are highly reliable and loyal, one of them may be coerced to participate in a theft or sabotage attempt. In a case in Northern Ireland in 2004, for example, thieves allegedly linked to the Provisional Irish Republican Army made off with £26 million from the Northern Bank. The bank's security system was designed so that the vault could be opened only if two managers worked together, but the thieves kidnapped the families of two bank managers and blackmailed them into helping the thieves carry out the crime.[14] (The thieves also used deception in this case, appearing at the managers' homes dressed as policemen.) No background check or ongoing employee monitoring system can prevent insiders from acting to protect their families.

Terrorists (as the Northern Bank thieves may have been) also make use of such coercion tactics, and might do so to enlist help in a theft of nuclear material or sabotage of a nuclear facility. For example, kidnapping in order to blackmail family members into carrying out certain actions has been a common Chechen terrorist tactic.[15] A 2014 study from Sandia National Laboratories concluded that in a database of major non-nuclear crimes involving thefts of valuables worth millions of dollars from guarded facilities or transports, coerced insiders were "by far the most common type."[16]

In November 2015, terrorists linked to the Islamic State carried out roughly 10 hours of video monitoring of the home of a senior official of SCK-CEN, Belgium's largest nuclear R&D facility. Among many other things, tens of kilograms of highly enriched uranium (HEU) are located there. The purpose of this monitoring remains unknown – but it is certainly possible that the monitoring

was part of a plot to kidnap family members and coerce the official.[17]

Similarly, if agents of the Democratic People's Republic of Korea (DPRK) sought to damage a nuclear facility in, for example, Japan or the Republic of Korea (ROK), they might use coercion to get help from an insider. Such coerced insider assistance could, for example, facilitate an outsider attack by providing details of the security system and the defenders' planned tactics.

The lesson here is clear: while it is important to have programs that screen employees for trustworthiness and monitor their behavior once employed, no one should ever assume that these programs will be 100 percent effective. Measures to prevent insider theft are needed even when a manager believes all of his employees are likely to be completely trustworthy.

The greedy or desperate insider

For better or for worse, the world over, people sometimes betray their organizations for money. Leonid Smirnov, for example, who stole 1.5 kilograms of weapon-grade HEU from the Luch Production Association in 1992 (in small amounts at a time over a period of months), was motivated entirely by money – inflation in Russia was out of control, his salary was not keeping up, and he wanted to be able to buy his family a refrigerator. (It is worth noting that Smirnov was a known and trusted employee who had worked at the facility and held security clearances for many years.)[18]

Japan, Korea, China, and Taiwan are not likely to have nuclear workers suffering similar desperation in the near term. But all have suffered major cases of financially motivated insider betrayal. In 2007, for example, Hirofumi Yokoyama, an employee at Dai Nippon Printing Company, was charged with leaking personal data on 8.6 million consumers. Prosecutors reported that he smuggled the data out on an optical disk, and sold data on 150,000 accounts to a credit card fraud ring, leading to frauds amounting to millions of yen.[19] Similarly, in 2014 prosecutors revealed that an insider at Korea Credit Bureau had stolen personal data on 20 million people (out of a Korean population of 50 million), copying the data onto USB drives over a period of more than a year. The episode was severe enough that the Korean Prime Minister Chung Hong-won intervened to call for stiff punishment, and leaders of Korea's major credit firms resigned.[20] In China in 2016, two insiders at the Beijing branch of the Agricultural Bank of China were charged with stealing bills of exchange worth 3.9 billion yuan (almost $600 million at then-current rates of exchange); the pair had reportedly planned to invest their ill-gotten gains, make a huge profit, and then replace the stolen money before anyone noticed, but were foiled when the stock market went down rather than up.[21] Here, too, nuclear managers cannot assume that their employees would be immune to such temptations, if terrorists, DPRK agents, or others offered substantial sums for stolen nuclear material or information on a facility's nuclear security system.

The disgruntled insider

Employees who are unhappy with their organization and the way they are being treated are much more likely to become insiders – and much less likely to proactively help to improve security by reporting odd or suspicious behavior or by creatively looking for security vulnerabilities and ways to fix them. Hence, employee satisfaction is actually a security-related part of organizational culture. In an important study of cyber sabotage cases, for example, Andrew P. Moore, Dawn M. Capelli, and Randall F. Trzeciak found that 92 percent of the cases examined occurred "following a negative work-related event such as termination, dispute with a current or former employer, demotion, or transfer." Well over half of the insiders in these cases were already perceived by others in the organization to be disgruntled.[22]

Chelsea (then Bradley) Manning's decision to provide a vast trove of classified documents to

Wikileaks is a classic example of the importance of disgruntlement. On deployment in Iraq, as a person dealing with gender identity issues in the days of "Don't Ask, Don't Tell," Manning reportedly felt isolated and alone. After being told at a "counseling" session that she would lose his one day off a week as a result of her persistent lateness, Manning flipped over a table, damaging the computer that was on it, and had to be restrained from going for the gun rack in the room. Three weeks later, she began systematically downloading classified documents.[23]

In addition to disgruntlement, organizations need to be on the lookout for signs of mental illness or severe emotional strain – primarily to help employees who may need it, but also because such issues can contribute to insider threats. Countless employees suffer from such problems and never consider taking actions against their organizations, so insider threats and mental illness should not be lumped in one basket. But it is clear that Bruce Ivins, a scientist at the U.S. Army biological weapons defense laboratory who is believed to have carried out the anthrax attacks in 2001, was driven by deep and long-standing mental illness, which got catastrophically worse in the months leading up to the anthrax attacks. Had the organization recognized Ivins' illness and gotten him the help he needed, it seems likely that the attacks never would have happened. Organizations need processes for encouraging people to report issues related to emotional strains and mental illness, and for addressing such issues sensitively and appropriately. It is crucial not to create an environment in which people fear they will be punished or excluded from meaningful work if they have any troubles for which they seek help; but if the response to a report is, instead, that a person who needs help receives it, that may increase employees' incentive to report concerning behavior.

Categories of insider actions

The last section described a few of the many possible motivations insiders may have. But there are also a wide variety of particular roles insiders may play in nuclear theft or sabotage attempts. An insider might be the sole perpetrator of an incident, or an insider may work with outsiders, or seek to conspire with other insiders.

The passive insider

Often, insiders play only a passive role, providing information about a facility or a transport and their security arrangements. But that information can be crucial, providing insights into where critical materials are located, what the security arrangements in place are and how they might be beaten, and more. Such a "passive" role can also extend to helping to plan a theft or attack, without personally taking an active part.

Officials at the Nuclear Energy Corporation of South Africa (NECSA), for example, believe that insiders at the Pelindaba nuclear facility provided information that contributed to the 2007 intrusion at that facility (where hundreds of kilograms of HEU are stored). An armed group of intruders went through a 10,000-volt security fence, disabled the intrusion detection system, proceeded to the site emergency control center (through which many of the other site alarm systems were routed), used a ladder attached to an emergency vehicle to access a second story window, and struggled with a worker at the emergency control center, shooting him in the chest before departing.[24] Another armed team assaulted a different part of the facility the same night. This suggests that attack by a modest group of well-armed, well-trained outsiders, capable of operating as more than one team, with help from well-informed insiders, is a plausible threat that nuclear facilities must protect against. Information that an insider might provide could include details on getting through security fences, defeating intrusion detectors, and more.

In some cases, passive insiders can be entirely inadvertent, providing information to adversaries by clicking on a link in an e-mail, inadvertently leaving papers where they can be taken, posting on

social media, or talking too much at a bar. For example, John Deutch, while serving as Director of the CIA, connected a laptop at his home to the internet, even though the laptop contained highly classified information.[25] Similarly, in 1994, the author personally caused what was then considered the second worst virus infestation in the history of the U.S. State Department by putting a floppy disk into the computer at the business center in a Russian hotel without flipping the switch to prevent any information from being written to the disk. Hence, insider threat protection programs must focus not only on detecting and stopping malicious insider adversaries but on educating and motivating employees (and organizational leaders) to minimize the incidence of such inadvertent compromises of key information.

The active, non-violent insider

Insiders may also play an active part in a plot against a nuclear organization, without being willing to take violent actions. An insider might directly carry out a nuclear theft or sabotage, or might take critical enabling actions. The list of possibilities is long – a guard disabling or ignoring alarms, a worker opening a security door, an accountancy official falsifying nuclear material accounting records to prevent or delay detection of a nuclear theft, and more.

The recent sabotage of the Doel-4 reactor in Belgium provides one of many examples. An insider at the plant opened a locked valve, allowing the lubricant for the turbine to drain out. The turbine overheated and had to be replaced. The plant was down for months, requiring purchase of replacement power. At this writing (late 2016), no one knows who perpetrated this sabotage or why; one possibility is that it was a disgruntled employee, and may have related to a labor-management dispute. Given the particular nature of the sabotage – and the lack of any effort to publicize it – it does not appear to have been related to any terrorist intent.[26]

As in the Doel-4 case, both passive and active insiders usually seek to keep their actions covert and unnoticed. When they succeed, site response forces never swing into action. On-site armed response forces are absolutely critical in coping with armed outsiders, and would be critical to an insider-outsider collusion scenario, or an overt insider scenario. But none of the known cases of plutonium or HEU theft engaged the response force before the theft was completed, and the same can be said of insider sabotage cases such as Doel-4.

Even active insiders can act without any malicious intent. For example, Oleg Savchuk allegedly placed a virus in the computer system of the Ignalina Nuclear Power Plant in order to call attention to the need for increased security and to be rewarded for his diligence.[27]

In short, active insiders pose a very challenging threat to nuclear security, even if they are not prepared to take violent action or take action that would run much risk of provoking violent action against them.

The active, violent insider

Insider adversaries who are willing not only to play an active part in a plot to steal nuclear material or sabotage the facility, but to threaten or use violence in doing so, pose a particular challenge. Because other employees (including security staff) are not expecting threats from them, they have the advantage of surprise. In some cases, one insider might be able to render multiple guards ineffective, for example.

Guards, in particular, can pose a serious threat to an organization. In one database, guards were responsible for 41 percent of insider thefts at non-nuclear guarded facilities.[28] With their knowledge of the security system and access to weapons, members of the response force at a facility

can be “the most dangerous internal adversaries,” as one senior Russian nuclear security manager put it in a remarkable 2003 account of guard force issues at his site.[29]

Cybersecurity and the insider threat

In the 21st century, the combination of insider threats and potential weaknesses in cybersecurity poses a particular concern.[30] Nuclear control systems are increasingly digital, increasing their cyber vulnerability. Indeed, industrial control systems (ICS) generally, including nuclear control systems, are typically designed in ways that render them more vulnerable than many computer systems are. Physical protection and nuclear material control and accounting systems also increasingly rely on digital systems that might be hacked. Often these systems are “air-gapped” – not physically connected to external networks – but this disconnection from external sources of threats is often compromised (for example, when staff or contractors connect portable computers to internal networks as part of testing, maintenance, or upgrades). And if an insider is involved, the gap between the internal network and the outside world can potentially be breached. It appears, for example, that the industrial control systems at Iran’s Natanz enrichment facility were air-gapped from external networks – but it appears that an employee either intentionally or inadvertently brought the Stuxnet malware into the facility, in one of the first cyberattacks ever to cause physical damage to a nuclear facility.

Three main forms of cyberattack are particularly significant for nuclear security. First, a cyberattack might be used to sabotage a nuclear facility by itself, as Stuxnet reportedly did. Second, a cyberattack might contribute to a physical theft or sabotage attempt—for example, by confusing or disabling alarm and assessment systems, unlocking doors, or altering material accounting systems. Third, adversaries might use cyber weaknesses to get access to sensitive nuclear information. Cyber intruders might acquire items ranging from facility blueprints to details on nuclear security systems and response force defense tactics.

Insiders could play a central role in all three of these kinds of cyber incidents, potentially compromising a wide range of critical functions played by digital technology in nuclear organizations. Insider cyber incidents are, unfortunately, fairly common across a broad range of industries and organizations. The CERT Insider Threat Center at Carnegie-Mellon University has compiled an anonymized database with details on over 1,000 cases, and has done analysis and modeling based on that data to develop recommendations for organizations to protect against insider cyber threats.[31] One striking regularity they have found was that nearly all of the perpetrators (97 percent) “came to the attention of supervisors or coworkers for concerning behavior prior to the attack,” but the observed behavioral precursors were “ignored by the organization.”[32]

The current social media environment can also be helpful to adversaries in a number of ways. Through postings on social media, adversaries can identify people who serve in critical roles at nuclear facilities, from security guards to control room operators; where they live who their family members are; which ones are going through painful personal issues or financial problems that might be exploited; and more.

Similarly, “phishing” attacks that encourage employees to click on a link or a file that installs malware on their computer can turn loyal employees into inadvertent insiders, opening gateways into networks. Such attacks are becoming more and more sophisticated and tailored to the targeted individual (which can be done with increasing ease with the use of personal information from social media postings).

Unfortunately, many organizations still have weak cybersecurity protections in place, and it is

notoriously difficult to get employees to pay attention to good cybersecurity practices. A recent survey of executives found that 29 percent of Japanese respondents said that their companies had experienced a data breach or failed a cyber compliance audit in the past year. But while 56 percent of survey respondents globally were planning to increase spending on cybersecurity, only 26 percent of Japanese respondents were planning such increases – and the study identified a "lack of focus" that was "worrying" in that most Japanese respondents did not identify insiders with privileged access as the biggest insider threat they faced, as other global respondents did.[33]

In short, the possibility that insiders might participate in cyber intrusions – intentionally or inadvertently – vastly complicates an already very challenging cyber threat to nuclear organizations. The cyber threat must be included in design basis threats against which nuclear facilities must protect.

A particular problem: multiple insiders

The possibility of conspiracies involving two or more insiders poses an especially difficult challenge for nuclear security systems to address. With two or three insiders working together, a wide range of security systems and approaches can potentially be defeated. Two-person rule, for example, is designed to address the possibility that one of the two people present might pose an insider threat – but if both are involved in the conspiracy, the approach no longer provides protection.

In many countries (including the United States) nuclear security systems are mainly designed to cope with a single insider; insider conspiracies are beyond the design basis threat (DBT). In a survey of nuclear security experts from the majority of countries where plutonium or HEU exists, most of the participants expressed the view that multiple insiders were not a credible threat in their country.[34]

But in a wide range of non-nuclear thefts from or attacks on guarded facilities, participation by more than one insider is not at all unusual. In one recent study of major non-nuclear thefts, cases with more than one insider were somewhat more common than cases with only a single insider.[35] Even in nuclear cases, it appears that multiple insiders are a real threat. In 1998, for example, the Russian Federal Security Service announced that it had foiled an attempt by a conspiracy of insiders at a major nuclear facility in Chelyabinsk oblast to steal 18.5 kilograms of HEU.[36] While no one knows for sure, it appears more likely than not, given the range of information apparently available to the intruders, that more than one insider was involved in the 2007 intrusion at the Pelindaba facility in South Africa. In short, nuclear security systems should be designed to have at least some capability to protect against more than one insider.

Two Example Scenarios

Consider, for example, two scenarios in which insiders might pose a threat to Japanese nuclear facilities, one involving the spent fuel pool at a power reactor, and one involving plutonium at the planned mixed oxide (MOX) fuel fabrication facility. Similar scenarios could occur in the ROK, China, or Taiwan.

Scenario 1: Sabotaging a spent fuel pool

In this scenario, a radicalized insider at a nuclear power plant decides to take action by sabotaging the spent fuel pool, in hopes of causing a major radioactive release. The insider waits until hot, fresh fuel has recently been unloaded into the pool, with many of the hot assemblies in one area of the pool. Using tools that he had brought into the plant and hidden over the preceding weeks, he then damages the pump that would be used to add water to the pool, and also damages pool gaskets,

causing a rapid leak. Previously, he had disabled the pool level sensor, so that it would keep providing a constant reading even as the water drained. The pool water begins to drain, and the fuel is exposed. The water still in the bottom of the pool blocks air circulation, limiting air cooling of the exposed assemblies, and the assemblies overheat. With no cool water being added, the remaining water begins to boil. The hot steam reacts with the melting zirconium on the hottest assemblies, and a spent fuel fire begins. The zirconium-steam reactions release a substantial amount of hydrogen, which builds up in the spent fuel building and ultimately detonates, damaging the building. Much of the radioactivity released in the spent fuel fire is therefore released into the environment.[37]

Scenario 2: Stealing Plutonium from a MOX Facility

In this scenario, an insider works with outsiders to steal plutonium from a MOX fuel fabrication plant. The insider removes small amounts of plutonium at a time from the powder processing area, hiding the material in the facility. The insider also brings in a USB drive which he plugs into the plant's computer network, which installs malware that alters the facility's nuclear material accounting data, introducing larger elements of noise than usual and thereby hiding the losses in the accounting uncertainties. The insider and the outsiders arrange for the outsiders to pose as contractors entering the plant to do maintenance on heavy equipment. Since the maintenance occurs when the plant is not operating, in an area that does not normally contain nuclear material, detailed inspection of the contractor's equipment is not performed and the outsiders remove the plutonium without detection.

These scenarios are intended only as illustrations of possibilities to be prevented, to provoke thought and debate. As one long-time vulnerability assessment expert argues, "even wildly implausible scenarios get people thinking creatively about security."[38] Anyone attempting to steal from or sabotage a real facility would require a detailed knowledge of its security systems, and would likely encounter difficulties beyond those mentioned in these scenarios. But as noted earlier, insiders may have weeks or months to develop their understanding of the security system and the ways it might be defeated. (In a theft of millions of dollars of diamonds and other precious goods from the Antwerp Diamond Center in 2003, the thieves spent some two years collecting intelligence on the security systems they had to defeat and developing their plan.[39]) Organizations need to find ways of thinking through such possibilities creatively and fixing any vulnerabilities they can identify.

Solutions: Steps to Strengthen Protection Against Insider Threats

Protecting against insider threats while maintaining a culture of teamwork and trust likely to be necessary for an organization to be successful is an inherently difficult challenge. Organizations must balance operational and security imperatives, and balance between responding rapidly and effectively to real threats while avoiding ruining people's careers over false accusations. An examination of past cases makes clear, in particular, that people in many organizations are extremely reluctant to report potentially concerning behavior; even the most extreme "red flags" will sometimes go unreported and unremarked. Bruce Ivins, for example, the likely perpetrator of the 2001 anthrax attacks, sent an e-mail to one of his staff complaining about his own increasingly dangerous paranoia and speculating about ending up in the newspaper with a headline of "Paranoid Man Works with Deadly Anthrax" – but the staffer did not report that e-mail, and no one took action.[40]

Protection against insiders is already the subject of IAEA recommendations (and hence part of the commitment states make in joining the Strengthening Nuclear Security Implementation initiative, now enshrined in INFCIRC/869).[41] In particular, INFCIRC/225/Rev. 5 calls for physical protection systems to protect against both insider and external adversaries, and warns that insiders pose

special challenges because they "could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures."[42] The IAEA also offers more detailed technical guidance on steps to protect against insider threats, as does the World Institute for Nuclear Security (WINS).[43] The author and Scott Sagan have offered a "worst practices" guide to help organizations learn from the disasters caused by past mistakes in managing insider threats.[44]

Fundamentally, organizations need a comprehensive approach, rather than relying on only one or a few steps as sufficient to cope with the insider threat problem. Such an approach should include action to minimize the opportunities available to insiders; to screen and monitor staff; to train and motivate staff; to control, monitor, and account for protected materials, information, and areas; to limit and monitor insider access to those protected materials, information, and areas; to conduct investigations when needed; and to assess, test, and learn over time.[45]

Minimizing opportunities for insider adversaries to succeed – including minimizing plutonium reprocessing

A variety of steps can minimize the opportunities insiders have to succeed in a theft or sabotage attempt. Increased reliance on passive safety, for example, makes it more difficult for either accidental events or intentional actions (including cyberattacks) to cause a major radioactive release. Locating backup safety systems far from the systems they are backing up makes it more difficult for either an accident or a saboteur to disable both systems.

Minimizing the number of places where plutonium or HEU exist makes it possible to achieve higher security at lower cost by defending fewer locations, and minimizes the number of groups of insiders with potential access to the material or who might be able to assist in a theft attempt. Japan's action, for example, in eliminating the plutonium and HEU from the Fast Critical Assembly – all of which was in forms that would have been highly attractive to potential thieves – was a major contribution to reducing risk, and the ongoing reduction in the use of HEU in Japan (and in many other countries) also reduces risk.

Minimizing large-scale bulk processing of nuclear materials – and ensuring the highest standards of security, control, and accounting for it wherever it occurs – is particularly important, as nearly all of the known cases of theft of plutonium or HEU have been bulk materials, presumably in most cases stolen from bulk processing facilities. It is much easier to remove material without being detected when the material is in bulk forms such as powders than when it is in easily-counted items such as fuel assemblies. For Japan, in particular, plutonium reprocessing and MOX fabrication inevitably create more risk of insider theft than would exist if spent fuel were simply stored. Japan could reduce the risks of insider theft it faces by minimizing the quantity of plutonium it reprocesses, and by exploring approaches to disposition of already-separated plutonium that involve less processing, less transport (and, potentially, lower costs) than fabrication into MOX fuels.[46] China and the ROK, too, should consider this issue carefully in considering whether to move toward large-scale reprocessing of spent nuclear fuel; at a minimum, such bulk processing should only proceed under the very highest attainable standards of security, control, and accounting.

Where materials such as plutonium and HEU will still exist, ensuring that they are kept in secure vaults when not in use and minimizing both the number of people with access to those vaults and the frequency of that access will minimize opportunities for potential insider adversaries. Processing systems that are highly automated and involve little or no direct human access to the material can also reduce the opportunities for insider adversaries to remove material.

Keeping material in difficult-to-steal forms is also an important step for minimizing insider

opportunities. Material in fabricated fuel assemblies too big and heavy for a person to carry, for example, poses a quite different risk than material in powders or pocket-sized fuel elements. Mixing plutonium with uranium can multiply several-fold the amount of material that would have to be stolen to get the same amount of plutonium – and require another processing step after the theft took place. In general, security and operations approaches should be designed to ensure that the difficulties insider thieves and saboteurs would face are as numerous and difficult to get past as possible.

Screening and monitoring staff

Next, it is crucial for organizations to establish effective systems for screening employees for trustworthiness before giving them access to highly sensitive information, areas, or materials. Japan is working to introduce such trustworthiness checks. But managers should not rely on such initial checks too heavily, because (a) such checks are highly imperfect; (b) people change after the initial screening (as in the cases of radicalization within a few months, discussed above); and (c) even trustworthy employees can be coerced. Hence, organizations should have ongoing programs for monitoring employees and encouraging staff to report concerning behavior.

Getting such ongoing monitoring programs to work effectively is difficult. Employees often resist reporting on friends and colleagues, even if they are acting in a suspicious manner; moreover, each individual incident, not combined with others, often appears too harmless to report. Moreover, in many organizations, employees often choose not to report problems because of the headaches involved, or they pass troublesome employees off to someone else to deal with. Indeed, U.S. Defense Department research suggests that indicators of insider security problems are systematically underreported.[47] As noted earlier, one study study of information-technology sabotage found that almost all of the insider perpetrators had exhibited concerning behavior the organization had ignored.

Putting in place processes to increase the chances of noticing and acting on such signals is crucial to reducing insider dangers.[48] Organizations should provide training with real stories of disasters that reporting could have prevented and should make the process of reporting easy and known to all employees (including the possibility of anonymous reporting). They should take steps to give employees incentives to report and to prevent retaliation against those who do. It is crucial to establish a process for responding to reports that employees understand and that is considered fair and reasonable. Training should include the possibility that reporting could lead to troubled individuals getting the help they need. Organizations should make counseling and other services available to employees whose unusual behavior is caused by stress, distressing life events, or mental health issues—and publicize (if employees permit) cases of employees who benefit from and are grateful for such assistance. Organizations should make it relatively easy and routine for employees to be excluded (or exclude themselves) from the most sensitive work if they are facing unusual stress or emotional issues, and relatively easy and routine for them to return to that work when those issues are addressed.

Another fundamental element of monitoring staff is making sure that no one is bringing contraband into or out of the facility – for example, bringing guns or explosives into the facility, or bringing nuclear material out. This typically requires searches and monitoring equipment as people are entering and exiting. It is important to think through all the potential pathways that something could be brought in or out, such as being passed through a window or sent through a pipe. Even emergency evacuations should be planned to make it possible to ensure that no nuclear material is removed in the emergency.

Training and motivating staff

Nuclear organizations need to build organizational cultures in which all staff take nuclear security seriously, including the insider threat, and are always on the lookout for potential issues and vulnerabilities that should be addressed. As with safety, the focus must be on constant vigilance and continuous improvement, in a never-ending quest for excellence. The culture should be one in which everyone understands that security is everyone's responsibility, not something only the security team has to worry about.[49]

Building such cultures requires committed and effective leadership from the top of the organization. Establishing clear incentives that make employees understand that they will be rewarded for good security performance is one key element of building such a culture, and of making clear the priority that management places on security.[50]

Training should make the reality of the threat clear and vivid – and, as just noted, should include real stories of insider threats. The security systems and rules should be clearly designed to address the threat, and training should make clear why each key element of the security system is important, and should not be ignored or bypassed.

Workshops in which staff imagine how insiders might accomplish various types of thefts or attacks and then envision better ways to prevent such events represent one important approach to training on the insider threat; they highlight the threat and the relevance of security measures for addressing it, make staff feel included and involved, and help motivate staff to suggest improvements.[51]

Employee satisfaction is another critical aspect of organizational culture. As noted earlier, disgruntled employees are far more likely to pose insider threats. Nuclear managers should strive to build strong, performance-oriented cultures in which employees believe that they are respected and treated well, in which they have avenues for their complaints and ideas to be heard, and in which they expect the organization to be helpful rather than punishing when issues of mental illness or emotional difficulties arise. Fortunately, organizations have found that it is not very difficult or expensive to combat employee disgruntlement. Providing complaint and ombudsman processes that are perceived to result in actions to address the issues; complimenting and rewarding employees for good work; and addressing the problem of bullying bosses: these and other steps can go a long way toward reducing disgruntlement and its contribution to the insider threat.[52]

Controlling, monitoring, and accounting for protected material, information, and areas

Keeping a constant watch and effective control over the items and areas to be protected is, of course, another crucial element of an effective insider protection program. In the case of nuclear material, this includes the full suite of nuclear material control and accounting (MC&A) approaches. It should be noted, however, that the MC&A for international safeguards and for protecting against insider threats are not identical. For international safeguards, for example, it might not matter much how many people had access to a vault, whether the vault was monitored when people were inside, or whether nuclear material in use was left out in working spaces at night rather than being returned to the vault; for protection against insider theft, all of those factors might be quite important.[53]

As part of this effort, nuclear material access areas, vaults, and nuclear facility vital areas should be continuously monitored with security cameras and alarm systems, and two-person or three-person rule should be followed at all times, so that no one is ever alone with nuclear material or in a vital area of nuclear facility.

Limiting and monitoring insider access to protected material, information, and areas

In addition to routine monitoring of staff and sensitive items and areas, organizations should limit and closely monitor those occasions when employees do access the protected items and areas. The use of cameras, two- or three-person rule, and accounting and control systems that keep track of who had access when (and where and when losses of nuclear material occur) are key elements of an effective insider threat protection program.

Conducting investigations

The monitoring and reporting mechanisms just described will sometimes produce information that raises a concern. Hence organizations need to have effective processes for conducting investigations to clarify whether there is a real problem or not. As noted earlier, these processes have to be seen by employees as fair and reasonable, or employees will not be likely to report on issues they observe.

Assessment, testing, and learning

Finally, an effective insider protection program requires an ongoing effort to assess and test the program's effectiveness, to make corrections, and to learn from experience. Performance tests should go well beyond simply testing whether a particular security component such as a camera is functioning as intended, to exploring the ability of intelligent insiders to find ways to defeat the security system.

The same is even more true of vulnerability assessments. Security managers need to find creative people with a hacker's mindset to come up with a wide range of ways that insiders might try to beat the security system–and then develop security measures that will be effective against a broad range of possibilities. A security system adequate to defend against the first few pathways thought of by an unimaginative committee is not likely to be good enough against the real threat. Such uncreative vulnerability assessments were the target for Roger Johnston and his colleagues in the Vulnerability Assessment Team at Argonne National Laboratory. In their instructive and amusing set of "Security Maxims," they offer the "Thanks for Nothin'" maxim: "Any vulnerability assessment which finds no vulnerabilities or only a few is worthless and wrong."[54] At the same time, those with the most detailed information about how the organization protects itself against insider threats and the vulnerabilities in that system should be subject to especially strong background checks and reviews and monitoring to ensure that the organization is appropriately "guarding the guardians."

Rather than leaving their security system largely static until some crisis occurs – a major incident, a new regulation – organizations need to find ways to learn and adapt as they go. As with safety, each incident or new-found issue should be examined for root causes and lessons learned, and treated as an opportunity to improve.

Conclusion – Northeast Asian states have come a long way but needs to do more

Japan's approaches to nuclear security – including to protection against the insider threat – have come a long way in the last two decades. So have those in the ROK, China, and Taiwan. Many of the elements of an effective insider threat protection program described above are already in place at Northeast Asian facilities, and others (such as trustworthiness checks in Japan) are moving toward implementation. But because of insiders' ability to bypass many elements of the physical protection system with their authorized access; the trust other employees have in them; and their knowledge of the organization, the security system, and its weak points, protecting against insiders is an inherently difficult challenge.

No one has all the answers about how best to do it. Hence, there is a need to keep trying, keep

assessing, keep testing, and keep exchanging ideas – including among the countries in Northeast Asia. There is no room for complacency – which is always the enemy of effective security.

III. END NOTES

[1] For discussion, see Matthew Bunn and Scott D. Sagan, eds., *Insider Threats* (Ithaca, N.Y.: Cornell University Press, 2017). This paper draws in part on that book. For an earlier account, see Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge, Mass.: American Academy of Arts and Sciences, 2014), https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf.

[2] Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey, *Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?* (Cambridge, Mass.: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, March 2016), http://belfercenter.ksg.harvard.edu/files/PreventingNuclearTerrorism-Web.pdf.

[3] See Matthew Bunn, "Belgium Highlights the Nuclear Terrorism Threat and Security Measures to Stop it," *The World Post,* March 29, 2016, http://www.huffingtonpost.com/matthew-bunn/belgium-nuclear-terrorism_b_9559006.html.

[4] For examples from major non-nuclear thefts, see Jarret M. Lafleur, Liston K. Purvis, and Alex W. Roesler, *The Perfect Heist: Recipes From Around the World*, Vol. SAND-2014-1790 (Albuquerque, N.M.: Sandia National Laboratories, 2014).

[5] See Bunn and Sagan, *Insider Threats.*

[6] For an excellent summary of several incidents of real or attempted nuclear thefts involving insiders, see Noah G. Pope and Christopher Hobbs, "Insider Case Studies at Radiological and Nuclear Facilities," LA-UR-15-22642 (Los Alamos, N.M.: Los Alamos National Laboratory, 2015), http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-15-22642.

[7] For a discussion of Boughalab, see Thomas Hegghammer and Andreas Hoelstad Daehli, "Insiders and Outsiders: A Survey of Terrorist Threats," in Bunn and Sagan, *Insider Threats,* pp. 10-41.

[8] See Hegghammer and Daehli, "Insiders and Outsiders."

[9] See, for example, The Soufran Group, *Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq* (New York: The Soufran Group, December 2015), http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate_FINAL.pdf. See also Nate Rosenblatt, *All Jihad is Local: What ISIS' Files Tell Us About Its Fighters* (Washington, D.C.: New America Foundation, July 2016), https://na-production.s3.amazonaws.com/documents/ISIS-Files.pdf.

[10] Michelle Magee, "Japan Says Soldiers Warned Cult of Raid," *San Francisco Chronicle,* April 29, 1995.

[11] See, for example, "Cultist's Confession Crucial," *Daily Yomiuri,* July 8, 2004; "'95 NPA Shooting Probe Wild Goose Chase," *Daily Yomiuri,* March 30, 2010. I am grateful to Bobby Kim for research support on this and other cases in Japan.

[12] "Arrests of SDF Troops Spur Review of Anti-Spy Capabilities," *Nikkei Weekly,* May 29, 1995;

"GSDF Officer Gave Weapons Text to Aum Commando Chief," *Daily Yomiuri,* May 19, 1995.

[13] For a discussion of the dangers of assuming that insiders are "Not in My Organization" (NIMO), see Bunn and Sagan, "A Worst Practices Guide to Insider Threats," in Bunn and Sagan, *Insider Threats,* pp. 145-174.

[14] For a good introduction to the Northern Bank case, see Chris Moore, "Anatomy of a £26.5 Million Heist," *Sunday Life*, May 21, 2006. One of the managers, Chris Ward, was subsequently charged with being a willing participant in the crime, and the kidnapping of his family a sham. Ward denied the charges and was subsequently acquitted. See Henry McDonald, "Employee Cleared of £26.5 Million Northern Bank Robbery," *Guardian*, October 9, 2008.

[15] Robyn Dixon, "Chechnya's Grimmest Industry: Thousands of People Have Been Abducted by the War-Torn Republic's Kidnapping Machine," *Los Angeles Times*, September 18, 2000.

[16] Lafleur, Purvis, and Roesler, *The Perfect Heist*, p. 9. Similarly, a much earlier study found that coercion tactics were relatively common and often successful. See Robert Reinstedt and Judith Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs*, N-149--SL (Santa Monica, Calif.: RAND, 1980).

[17] Bunn, "Belgium Highlights the Nuclear Terrorism Threat."

[18] For an interview with Smirnov about his crime, see "Frontline: Loose Nukes: Interviews" (Public Broadcasting System, 1996), http://www.pbs.org/wgbh/pages/frontline/shows/nukes/interviews/.

[19] See "Japan Needs Stiff Punishment for Data Theft," *China Daily* (from the *Asahi Shimbun*), March 20, 2007, http://www.chinadaily.com.cn/cndy/2007-03/20/content_831538.htm.

[20] Choe Sang-Hun, "Theft of Data Fuels Worries in South Korea," *New York Times,* January 20, 2014.

[21] "Bank Duo's Theft Scheme Fails When Stock Markets Crash," *Shanghai Daily,* January 26, 2016.

[22] Andrew P. Moore, Dawn M. Capelli, and Randall F. Trzeciak, *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures*, CMU/SEI-2008-TR-2009 (Pittsburgh: Software Engineering Institute, Carnegie Mellon University, May 2008).

[23] Paul Lewis, "Bradley Manning Flipped a Table During Counseling, Defence Tells Hearing," *The Guardian,* August 12, 2013. This and other episodes also reflect red flags that went unreported to higher officers and were not acted upon.

[24] For discussions of the Pelindaba intrusion, see, for example, Douglas Birch and R. Jeffrey Smith, "How Armed Intruders Stormed Their Way Into a South African Nuclear Plant," *Washington Post,* March 14, 2014, and Matthew Bunn, *Securing the Bomb 2008* (Cambridge, MA Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative 2008), http://www.nti.org/media/pdfs/Securing_The_Bomb_2008.pdf, pp. 3-4.

[25] Central Intelligence Agency Inspector General, *Report of Investigation: Improper Handling of Classified Information by John M. Deutch*, 1998-0028-IG (Washington, D.C.: CIA, February 18, 2000).

[26] For a useful summary of this incident, with photographs, see Pope and Hobbs, "Insider Case Studies."

[27] William Potter and Charles Ferguson, with Amy Sands, Leonard S. Spector, Fred L. Wehling, *The Four Faces of Nuclear Terrorism* (New York: Routledge, 2005), p. 224.

[28] Bruce Hoffman, Christina Meyer, Benjamin Schwarz, and Jennifer Duncan, *Insider Crime: The Threat to Nuclear Facilities and Programs* (Santa Monica, CA: RAND Corporation, 1990): http://www.rand.org/content/dam/rand/pubs/reports/2007/R3782.pdf.

[29] Igor Goloskokov, "Refomirovanie Voisk MVD Po Okhrane Yadernikh Obektov Rossii [Reforming MVD Troops to Guard Russian Nuclear Facilities]," trans. Foreign Broadcast Information Service, *Yaderny Kontrol*, Vol. 9, No. 4 (Winter 2003).

[30] For a useful summary of the issues, see Caroline Baylon, with Roger Brunt and David Livingstone, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks* (London: Chatham House, September 2015), https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf.

[31] Matthew Collins, Michael C. Theis, Randall F. Trzeciak, Jeremy R. Strozer, Jason W. Clark, Daniel L. Costa, Tracy Cassidy, Michael J. Albrethesen, and Andrew P. Moore, *Common Sense Guide to Mitigating Insider Threats,* 5th Ed., CMU/SEI-2016-TR-015 (Pittsburgh: Software Engineering Institute, Carnegie-Mellon University, December 2016), http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.

[32] Moore, Capelli, and Trzeciak, *The "Big Picture" of Insider IT Sabotage*.

[33] Andrew Kellett, *2015 Vormetric Insider Threat Report: Trends and Future Directions in Data Security: Japan and ASEAN Edition* (San Jose, Calif.: Vormetric Data Security, 2015).

[34] Matthew Bunn and Eben Harrell, *Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, 2014), http://belfercenter.ksg.harvard.edu/files/surveypaperfulltext.pdf, p. 24.

[35] Lafleur, Purvis, and Roesler, *The Perfect Heist*, p. 68.

[36] This cases is discussed, for example, in "Interview: Victor Yerastov: MINATOM Has All Conditions for Providing Safety and Security of Nuclear Material," *Yaderny Kontrol Digest*, Vol. 5, No. 1 (Winter 2000). The fact that the material in question was HEU comes from an interview with a Ministry of Atomic Energy official by the author.

[37] For a recent discussion of the risks of fuel overheating in spent fuel pools, see U.S. National Academies of Science, Engineering, and Medicine, *Lessons Learned from the Fukushima Nuclear Accident for Improving Safety*

and Security of U.S. Nuclear Plants: Phase 2 (Washington, DC: National Academies Press, 2016). For more detailed calculations, particularly on the potential consequences of such an event, see Frank von Hippel and Michael Schoeppner, "Reducing the Danger from Fires in Spent Fuel Pools," *Science & Global Security,* Vol. 24, No. 13 (2016), pp. 141-173.

[38] Roger Johnston, "Some Unconventional Security Metrics," *Asia-Pacific Security Magazine,* November 2016, http://www.asiapacificsecuritymagazine.com/some-unconventional-security-metrics/.

[39] For a book-length treatment of this remarkable incident, in which many seemingly impenetrable

layers of security were defeated, see Scott Andrew Selby and Greg Campbell, *Flawless: Inside the Largest Diamond Heist in History* (New York: Union Square Press, 2010). This heist is also among the many discussed in Lafleur, Purvis, and Roesler, *The Perfect Heist*.

[40] This was one of a very large number of other worrisome indicators that were written off as eccentricity. For an account of the Ivins case, see Jessica Stern and Ronald Schouten, "Lessons from the Anthrax Letters," in Bunn and Sagan, eds., *Insider Threats,* pp. 74-102. For a broader discussion of organizations' failures to notice and address "red flags," see Matthew Bunn and Scott Sagan, "A Worst Practices Guide to Insider Threats," in Bunn and Sagan, *Insider Threats,* pp. 145-174.

[41] International Atomic Energy Agency, *Communication Received from the Netherlands Concerning the Strengthening of Nuclear Security Implementation*, INFCIRC/869 (Vienna: IAEA, 2014).

[42] International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.5 (Vienna: IAEA, 2011), http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf.

[43] International Atomic Energy Agency, *Preventive and Protective Measures Against Insider Threats*, Vol. IAEA Nuclear Security Series No. 8 (Vienna: IAEA, 2008); World Institute for Nuclear Security, *WINS International Best Practice Guide 3.4: Managing Internal Threats*, Rev. 2.0 (Vienna: WINS, 2015).

[44] Bunn and Sagan, *Insider Threats,* pp. 145-174.

[45] For a similar framework, and questions to ask about how the insider protection program works in any organization, see Matthew Bunn and Kathryn M. Glynn, "Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries," in Bunn and Sagan, eds., *Insider Threats,* pp. 121-144.

[46] For discussion of relevant dilemmas, see, for example, Masafumi Takubo and Frank von Hippel, *Ending Reprocessing in Japan: An Alternative Approach to Managing Japan's Spent Nuclear Fuel and Separated Plutonium* (Princeton, N.J.: International Panel on Fissile Materials, 2015), http://fissilematerials.org/library/rr12.pdf. See also James M. Acton, *Wagging the Plutonium Dog: Japanese Domestic Politics and its International Security Implications* (Washington, D.C.: Carnegie Endowment for International Peace, 2015), http://carnegieendowment.org/files/Plutonium_Dog_final.pdf.

[47] Suzanne Wood and Joanne C. Marshall-Mies, *Improving Supervisor and Co-Worker Reporting of Information of Security Concern* (Monterey, Calif.: Defense Personnel Security Research Center, January 2003). Subsequently, researchers from the same center developed an improved reporting system now used in the Department of Defense, which may be of interest to nuclear security managers. See Suzanne Wood, Kent S. Crawford, and Eric L. Lang, *Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers* (Monterey, Calif.: Defense Personnel Security Research Center, May 2005).

[48] See Wood, Crawford, and Lang, *Reporting of Counterintelligence and Security Indicators.* For examples of programs to encourage incident reporting with respect to safety, see "Engineering a Reporting Culture" and "Engineering a Just Culture," in James Reason, *Managing the Risks of Organizational Accidents* (Aldershot, U.K: Ashgate, 1997), pp. 196-213.

[49] On the importance of this point, see World Institute for Nuclear Security, *Nuclear Security*

Culture: A WINS Best Practice Guide for Your Organization, revision 1.4 (Vienna: WINS, September 2009).

[50] Matthew Bunn, "Incentives for Nuclear Security," *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., July 10–14, 2005* (Northbrook, Ill.: INMM, 2005); available at http://belfercenter.ksg.harvard.edu/files/inmm-incentives2-05.pdf.

[51] The U.S. State Department's Partnership for Nuclear Security has sponsored such workshops in several countries.

[52] Roger G. Johnston, "Mitigating the Insider Threat (and Other Security Issues)," http://www.ne.anl.gov/capabilities/vat/pdfs/Insider%20Threat%20and%20Other%20Security%20Issues.pdf.

[53] The IAEA has offered guidance on the somewhat different implementation of MC&A needed for nuclear security. See International Atomic Energy Agency, *Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities*, Nuclear Security Series No. 25-G (Vienna: IAEA, 2015), http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1685web-43244937.pdf.

[54] See Roger G. Johnston, "Security Maxims," Right-Brain Sekurity, September 2016, http://rbsekurity.com/Papers/security%20maxims%20(dec%202016).pdf.

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.
