THE NEED FOR CREATIVE AND EFFECTIVE NUCLEAR SECURITY VULNERABILITY ASSESSMENT AND TESTING

M. BUNN
Project on Managing the Atom, Harvard Kennedy School
Cambridge, Mass., USA
E-mail: matthew_bunn@harvard.edu

Abstract

Realistic, creative vulnerability assessment and testing are critical to finding and fixing nuclear security weaknesses and avoiding over-confidence. Both vulnerability assessment and realistic testing are needed to ensure that nuclear security systems are providing the level of protection required. Systems must be challenged by experts thinking like adversaries, trying to find ways to overcome them. Effective vulnerability assessment and realistic testing are more difficult in the case of insider threats, and special attention is needed. Organizations need to find ways to give people the mission and the incentives to find nuclear security weaknesses and suggest ways they might be fixed. With the right approaches and incentives in place, effective vulnerability assessment and testing can be a key part of achieving and sustaining high levels of nuclear security.

1. INTRODUCTION

Realistic, creative vulnerability assessment and testing are critical to finding and fixing nuclear security weaknesses and avoiding over-confidence. In the U.S. experience, nuclear security systems that looked great on paper have sometimes failed, in evaluations or tests, to protect against mock adversaries who had found a clever approach to defeating the defenses. Around the world, there have been numerous non-nuclear cases in recent years where thieves managed to defeat apparently formidable security systems, exploiting previously unnoticed vulnerabilities [1].

Both vulnerability assessment and realistic testing are needed to ensure that nuclear security systems are providing the level of protection required. A checklist approach that simply asks whether the system has all the particular elements required by regulations is not sufficient. Instead, nuclear security systems must be challenged by experts thinking like adversaries, trying to find ways to overcome them.

The need for realistic vulnerability assessment and performance testing is already the subject of IAEA recommendations. INFCIRC/225/Rev. 5 recommends that nuclear operators have quality assurance programs to ensure that security systems can provide the level of protection required by the state. Further, it recommends that these programs should include exercises to test security performance at least annually [2]. Because these steps are recommended in INFIRC/225/Rev. 5, they are included in the commitments of the Strengthening Nuclear Security Implementation Initiative (INFCIRC 869), for the dozens of states participating in that effort [3].

This paper will discuss vulnerability assessment and performance testing in turn, discussing steps that can help ensure that such efforts contribute effectively to improved nuclear security. It will then briefly explore the special challenges of assessing nuclear security systems' effectiveness against threats that include insiders, and then it will offer a few conclusions. Before doing so, however, it is worth considering a brief history of problems that have arisen in implementing such assessments and tests in the United States and lessons that can be learned from them.

2. HISTORY IN THE UNITED STATES

In the United States, the shift from a checklist approach that simply sought to ensure that facilities and transports complied with designated requirements to an approach that included initial steps toward ensuring that security systems were actually effective in protecting against specified types of threats began in the 1970s. The U.S. nuclear security system had been alerted to potentially serious vulnerabilities by the apparent loss of hundreds of kilograms of highly enriched uranium (HEU) at the Nuclear Materials and Equipment Corporation (NUMEC) in Apollo, Pennsylvania in the mid-1960s; by experts within the Atomic Energy Commission raising concerns about the potential danger of nuclear terrorism; and by the terrorist attack on the 1972 Munich Olympics, which made clear that a well-trained, well-armed terrorist team striking without warning in the middle of a major developed country was a realistic threat that had to be addressed [4].

Experts at Sandia National Laboratories, which the Atomic Energy Commission (AEC) designated as the lead laboratory for physical protection, developed the first systems-engineering approaches to assessing the vulnerability of facilities, based on probabilities of detection, delay times, and response times along various plausible adversary pathways. This required generating data on the actual probability of detection of various types of sensors, the actual delay times provided by various barrier types, and so on. Hence, the U.S. government sponsored a large program of barrier and sensor testing, including tests of breaching barriers with explosives. At the same time, engineers developed early software programs to help analysts estimate the probability of interception along various paths into the facility, the forerunners of widely used modern programs such as Simajin and Avert. Already, however, issues began to arise: a security assessment based on a few obvious potential adversary paths might suggest a security system was highly effective, while a more creative set of assessors might invent a different adversary strategy that would readily defeat the system (though then there were often debates as to how credible the creative strategies were). People who were especially successful in finding vulnerabilities were sometimes ostracized as troublemakers.

After the AEC was split into the Nuclear Regulatory Commission (NRC) and what became the Department of Energy (DOE) in 1974, both organizations began exploring approaches to testing the actual performance of complete nuclear security systems. Both established the first versions of a design basis threat (DBT) that they required nuclear power reactors and facilities handling Category I nuclear materials to protect against.

In the late 1970s, to see if these requirements were being met, DOE established the "Independent Assessment Program" (IAP), which included both in-depth inspections by a team of experts in different security fields and early versions of force-on-force exercises designed to test whether a group of attackers like that described in the DBT would be able to overcome a site's security system. These exercises were aggressive, led by current or retired military experts with training in tactics for overcoming security systems. At that time, few procedures for or constraints on the tests were in place, and when the tests found a wide range of vulnerabilities that would be expensive to fix, the operators complained that the tests were unfair and reflected an excessive level of adversary skill and knowledge (as well as being expensive to prepare for and implement, inconvenient, and embarrassing).

When the new Reagan team came to office in 1981, they terminated the IAP. But canceling the test and inspection program provoked outrage among nuclear security critics in Congress, leading to a similar program being relaunched in 1982 – and continuing to find troubling weaknesses in DOE's security systems thereafter [5]. Both at DOE and at the Department of Defense, creative testers continued to find important vulnerabilities. In one test at a nuclear weapon storage facility in Europe, for example, the testers noticed in test preparations that the guard force's armament was stored in a separate building across a road from the guard force. During the exercise, the adversary team came careening into the facility at high speed with a dump truck filled with sand, which they deposited in front of the door of the armament building, thereby disarming the defenders [6]. Today, DOE requires such force-on-force exercises at all of its major nuclear facilities on a regular basis, although such tests continue to generate controversy over issues ranging from cost to alleged lack of realism to operator cheating.

The newly created NRC first established DBTs in new security rules approved in 1977-1979 [7, 8]. In 1981, NRC began to try to check the actual performance of licensees' security systems (as opposed to only going through a checklist of whether each site was meeting specified requirements). It began with simple tests of whether particular tactics could allow adversaries to enter a site without detection, which identified major weaknesses at almost every site [4]. Once those initial weaknesses had been corrected, in 1991 NRC moved to force-on-force exercises. This effort was known as the Operational Safeguards Response Exercises (OSRE) [4].

In the OSRE program, plants knew when a test was coming 6-12 months ahead of time and made major security improvements to get ready – assessing their own vulnerability, changing their security plans, installing new barriers, and training their guard forces. Plants were allowed to have a more substantial guard force for the test than they normally had day-to-day. Nevertheless, in the first eight years of the effort, in 40 of the drills at 27 plants (of 58 plants reviewed by that time), the mock "terrorists" managed to break in and get to the targets which, if destroyed, could have caused a meltdown. The weaknesses identified were subsequently corrected, leading to significant security improvements. The NRC staff in charge of the program argued that the lists of requirements in the NRC's rules had proved insufficient in themselves to ensure that plants were effectively protected, and that with pressures in the industry to cut security costs, it was essential for rigorous NRC-led tests of real security performance to exert "countervailing pressure."[9]

Nevertheless, operators objected to the expense, inconvenience, and embarrassments of the tests and argued that they exaggerated the likely capabilities of attackers, ignored what plants might be able to do to prevent a

radioactive disaster even if their key safety equipment was destroyed, and exceeded NRC's legal authority. In 1998, the NRC canceled the OSRE program (with no notice or public announcement). But the leader of the effort, David Orrik (a retired Navy SEAL), objected, using the NRC's formal system for handling "Differing Professional Views," and ultimately worked with the non-government Nuclear Control Institute to make the cancellation public. After unfavorable press stories and pressure from both the White House and Congress, the NRC reversed itself and relaunched the OSRE program [10].

The nuclear industry then convinced the NRC to approve a modified approach to the testing program in which the industry would evaluate and test its own performance, with NRC staff observing. That decision was reversed after the 9/11 attacks in 2001, though the NRC agreed to allow the contractor who provided many of the guards for nuclear power plants to also provide the adversaries to test those guards [11]. Congress acted in 2005 to require force-on-force exercises at NRC-regulated nuclear power plants and Category I facilities at least once every three years. Nevertheless, there is an ongoing discussion between the NRC and industry over how many scenarios will be tested, what types of capabilities and skills adversaries will be permitted to use, and how independent the test program will be of the operators. The NRC has agreed to several steps that appear to reduce the stringency of the test program [12].

The U.S. experience makes clear that effective vulnerability assessment and testing are essential to find and fix vulnerabilities. But it also makes clear that getting these efforts right is not easy. Approaches that are not sufficiently creative and probing are likely to miss important vulnerabilities; but approaches that are seen as excessively aggressive and unfair are not likely to be sustainable.

3. VULNERABILITY ASSESSMENT

As noted at the outset, the IAEA recommends that nuclear security programs should include an element of quality assurance to ensure that nuclear security systems are performing properly and reaching their objectives. To ensure quality really requires nuclear operators to carry out in-depth vulnerability assessments regularly, with effective oversight of the assessment process by regulators. The IAEA has not yet offered implementation guidance for assessing the performance and remaining vulnerabilities of nuclear security systems, though it has published the report of a cooperative research program outlining a variety of current approaches to nuclear security system assessment, including computer modeling and simulation [13]. The World Institute for Nuclear Security (WINS) has also offered guidance on using modeling and simulation to assist in evaluating nuclear security systems [14].

Tools ranging from expert judgment to tabletop exercises to large computer simulations can be helpful in performing a vulnerability assessment for a nuclear facility or transport operation. Depending on the level of detail desired, the process can be laborious and resource-intensive. Getting reliable data is key – and in most cases, it is important for the data to be from real testing at the facility or transport operation being assessed, rather than, for example, "standard" data on equipment performance provided by a vendor (which tends to be optimistic).

Computer modeling and simulation, in particular, can be extraordinarily valuable tools. They can allow the operator to explore many different adversary scenarios; they can make it possible to assess a variety of potential modifications to the security system or strategy, to find ways to get more effectiveness for less money; and they can be very helpful in training nuclear security personnel and strengthening exercise programs. In recent years, as computing power available to operators has increased, computer modeling has become significantly more robust. An exercise, however realistic, provides data on one scenario at one moment in time; modeling and simulation can provide at least some information on thousands of variations [14].

There are, however, limitations and challenges to nuclear security modeling and simulation which practitioners should remember [15]. First, there are large and largely irreducible unknowns. We do not really know what numbers, capabilities, and tactics the adversary will use, what system weaknesses they will try to exploit, how the guard force will react in the moment, or what the full scope of consequences of adversary success might be.

Second, we can only model what we can think of. As noted earlier, in major non-nuclear heists from guarded facilities, the security systems were typically defeated through vulnerabilities that the operators had not noticed. The security system for the Antwerp Diamond Center, for example, seemed essentially impregnable, with multiple, substantial layers of defense and detection; yet in 2003 a gang of thieves with specialized skills collected intelligence on the system for over a year and found ways to beat each layer, making off with tens of millions of dollars in gems [16].

Third, security systems are complex, exhibiting emergent behavior that is not just the sum of the parts. Changing one part of the system may lead to unexpected and difficult-to-model results elsewhere. A new system setting off increased false alarms, for example, can affect the willingness of the guard force to spend time constantly checking the alarms, as occurred at the U.S. Y-12 nuclear facility before the 2012 protester intrusion. Fourth, and relatedly, effective nuclear security is highly dependent on strong performance from the *people* in the system, and models are not especially good at modeling human and organizational behavior. Not only will intelligent adversaries adapt to the defenses and try approaches the defenders have not thought of, but intelligent employees will seek to avoid doing things that are inconvenient, boring, that they perceive as unimportant, and that distract from other activities more likely to be rewarded or to bring them pleasure. When the Superbowl is on, some guards are likely to be watching the television rather than the fences. People will often disregard security rules they see as excessive or useless – so the day-to-day implementation of security often looks quite different from what is written down in the rulebook and incorporated in a model.

Fifth, as discussed in more detail below, assessing and modeling threats from insiders – who may be among those designing, implementing, and assessing the security system – is particularly challenging. Finally, models have a tendency to distract us from everything that is not in the model. Daniel Kahneman, Nobel Prize winner in economics for his work on human behavior, calls this phenomenon WYSIATI, for the assumption that "what you see is all there is." [17] In a classic experiment in the 1970s, when shown a fault tree of reasons a car did not start, people assumed it included nearly all of the possible reasons – *regardless of what fraction of the possible reasons were actually included.* This was true even of trained mechanics [18]. In particular, the focus of most modeling on overt, violent outsider attack may lead to security managers thinking less about other adversary strategies that may be more likely, including deception, stealth, and insider conspiracies.

The issue of unnoticed vulnerabilities is particularly important. Consider, for example the Kryptonite bike lock. For years, these locks with their circular keys were considered among the most secure and difficult-to-defeat types commonly available. Then some creative person discovered that they could be easily picked by inserting a Bic pen. The apparently secure system had a gaping vulnerability – that had not been discovered in earlier vulnerability assessments. (The company redesigned the lock, so its products are no longer vulnerable to this attack.)

Vulnerability assessors will never find every vulnerability. Indeed, Roger Johnston, formerly the head of the Vulnerability Assessment Team at Argonne National Laboratory, offers what he calls the "infinity maxim": "there are an unlimited number of vulnerabilities for a given security device, system, or program, most of which will never be discovered (by the good guys or the bad guys)." He argues that this is true because whenever his team looks at a system a second time, they find vulnerabilities they did not find before; whenever they look at a system someone else has looked at, they find vulnerabilities the other team did not find; and whenever another team looks at a system his team looked at, they find vulnerabilities his team missed [19].

Nevertheless, by employing "red teams" with a creative, "hacker" mentality whose job is to find security vulnerabilities and propose solutions, organizations can find and fix many vulnerabilities and greatly strengthen their security programs. (Johnston and his colleague Anthony Garcia offer suggestions for how organizations should implement such "adversarial vulnerability assessments" in [20].) This approach is common in cybersecurity, where major conferences such as DefCon are focused on discussions of newly discovered vulnerabilities and how they should be addressed. "White hat" hackers who find vulnerabilities are rewarded with fame and "bug bounties" offered by major software providers. Nuclear organizations need to find ways to give assessors real incentives for finding vulnerabilities (though clearly it would not be a good idea to publicize the vulnerabilities they find – at least until after they have been fixed). Operators need to protect vulnerability assessment teams from organizational backlash. Johnston, again, offers a "troublemaker maxim": "the probability that a security professional has been marginalized by his or her organization is proportional to his/her skill, creativity, knowledge, competence, and eagerness to provide effective security." [19]. Doing vulnerability assessment right requires buy-in and commitment from the organization's leadership; ultimately, the effort to proactively look for vulnerabilities is driven by, and helps to drive, the organization's security culture. Finding vulnerabilities should not be seen as a sign of failure or a reason to punish security designers, managers, or implementers (unless the vulnerabilities really are the result of someone's shoddy performance), but as a sign of an organization proactively pursuing continuous improvement.

4. REALISTIC TESTING OF SECURITY SYSTEM PERFORMANCE

In addition to in-depth vulnerability assessments, operators and regulators should carry out a variety of forms of performance testing, from testing whether particular pieces of equipment are functional or whether guards respond to a particular signal appropriately to testing whether the entire system can defend against intelligent adversaries (insiders and outsiders) trying to find ways to defeat it.

Realistic performance testing is a particularly important tool at nuclear facilities, where guards can go their entire career without witnessing an actual threat. Such tests can expose weaknesses, combat complacency, strengthen security culture, and foster better understanding of threats. The results of realistic testing are often more convincing to organizational leaders and policymakers deciding on security requirements and budgets than any amount of paper or computer analysis. Both the IAEA and WINS have offered guidance on implementation of exercises and tests for security forces, which also discuss the purposes these tests can fulfill [21, 22].

There are many ways to conduct performance tests. For example, table-top exercises using "battle boards" are sometimes used to evaluate security plans and help security officers think through how they would respond to different types of threats. Table-tops or computer simulations are particularly appealing because they are less expensive and time-consuming and make it easier to examine scenarios that go beyond a facility's DBT.

But table-top exercises are not an effective method of testing how guards would react in a realistic situation. For that and other reasons, as INFIRC/225 suggests, full-scale force-on-force exercises, in which groups pretending to be adversaries attempt to defeat the security system, are also needed. A realistic force-on-force exercise is an opportunity to see how a security system would actually respond to an intelligent, well-equipped, insider or outsider threat employing a range of tactics.

Unlike table-tops, a force-on-force exercise can be expensive and time consuming to plan, require dozens of people, and interfere with normal facility operations. Force-on-force exercises can also expose embarrassing security deficiencies. As a result, some nuclear operators argue against requirements for regular, realistic force-on-force exercises, or try to make them less realistic or intensive. It was not until 2011, in the fifth revision, that INFCIRC/225 recommended regular force-on-force exercises, and some countries have been slow to adopt the recommendation. China, for example, has included force-on-force exercises in draft revised security regulations, but has not yet implemented a full-scale program.

Vulnerability assessment and performance testing are closely related. Possible adversary scenarios developed in vulnerability assessment can be tested in force-on-force exercises. Force-on-force exercises and other testing can provide data for use in vulnerability assessments and can help check the validity of assumptions and the plausibility of proposed tactics. Ultimately, both are seeking to contribute to a better understanding of the strengths and weaknesses of a nuclear security system (along with other objectives). For testing, as for vulnerability assessment, it is key to ensure that the testers are creative and thinking like adversaries, imagining and testing clever ways adversaries might attempt to defeat the security system. With the expense and inconvenience of full exercises, strong leadership commitment and buy-in is essential. As with vulnerability assessment, a strong testing program is both driven by and helps to drive a strong organizational security culture.

5. THE CHALLENGES OF INSIDER THREATS

Both effective vulnerability assessment and realistic testing are more difficult in the case of adversary threats involving one or more insiders. Insiders, who might be in any position within a facility, pass daily through layers of the security system, and may be gathering experience with the operation's security arrangements and the people who implement them for months or years at a time. They are known, trusted individuals who are often not suspected until it is too late [23].

Envisioning all the vulnerabilities insiders might exploit is an extraordinary challenge. Insiders may have more time than vulnerability assessors do to think through possible approaches to accomplishing their objectives. Assessors can certainly evaluate individual elements of the security system – such as the probability that the material control and accounting system would detect a loss, and how rapidly that detection might occur. But it is difficult to evaluate how all the individual elements fit together, especially since many of them are based on how people and the organization behave (such as reporting of concerning behavior). That is particularly the case since the insider may be actively confusing efforts to detect their activity (such as falsifying the accounting records to reduce the

probability that a loss of material would be detected, for example). Much of the software that has been developed for vulnerability assessment simulation is significantly stronger for outsider threats than for insider threats; while it may be able to model an insider participating in an attack, it is unlikely to be able to help with the kind of confusion and delay an insider may be able to create inside the facility.

The matter of what capabilities the insider should be assumed to have, or not to have, is always problematic. For example, assessors should not envision superhuman insiders who know everything there is to know about a facility and its security system – but on the other hand, an insider with friends and acquaintances on the staff may end up knowing a good deal more than his or her job description would suggest. And then there is always the possibility that there will be more than one insider, as there often are in non-nuclear heists [1].

Finding realistic ways to test insiders' ability to exploit their trusted access to conduct adversary actions without compromising safety and security is also difficult. Individual elements can be tested – such as whether nuclear material could be removed from a particular process area without setting off an alarm – but even that requires considerable work to find test methods that preserve safety and security during the test. But testing the many layers of the security system – including the personnel reliability and behavior reporting systems – to see how well they would work in complicating an insider theft or sabotage is extraordinarily difficult.

Recognizing these challenges, nuclear organizations should task their vulnerability assessors and testers to develop means to assess and test what they can, using expert judgment for whatever cannot be more formally addressed. Tabletop exercises in which staff envision what steps they would take if they wanted to steal material or conduct a sabotage, and then work together to strengthen the measures in place to block or detect those steps, can both strengthen the technical security system and develop a broader understanding of security among the staff. Being unable to do complete and rigorous tests of protection against the insider threat does *not* mean organizations can turn their attention away from the insider problem.

6. CONCLUSIONS

Creative, effective approaches to vulnerability assessment and performance testing are fundamental to effective and sustainable nuclear security systems. When done well, vulnerability assessment and performance testing contribute to a strong organizational security culture and to finding and fixing vulnerabilities – a central element of continuous improvement in security. They help managers and policymakers understand the strengths and weaknesses of the security systems in place and help to justify necessary investments in security. All nuclear organizations need to make ongoing vulnerability assessment and testing a priority for their nuclear security programs.

REFERENCES

[1] LAFLEUR, J.M., PURVIS, L.K., and ROESLER, A.W., The Perfect Heist: Recipes From Around the World, SAND-2014-1790, Sandia National Laboratories, Albuquerque, N.M. (2014).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.5, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Communication Received From the Netherlands Concerning the Strengthening of Nuclear Security Implementation, INFCIRC/869, IAEA, Vienna (2014).

[4] BUNN, M., "Beyond Crises: The Unending Challenge of Controlling Nuclear Weapons and Materials," in Sokolski, H.D. and Tertrais, B., eds., Nuclear Weapons Security Crises: What Does History Teach?, U.S. Army Strategic Studies Institute, Carlisle, Penn. (2013).

[5] BUKHARIN, O., Physical Protection Performance Testing: Assessing U.S. NRC Experience, Journal of Nuclear Materials Management, **28** 4 (2000) 21-27.

[6] Personal communication with U.S. vulnerability assessor, June 2013.

[7] U.S. NUCLEAR REGULATORY COMMISSION, Rulemaking for Enhanced Security of Special Nuclear Material: Regulatory Basis Document, 3150-AJ41, NRC, Rockville, Md. (2015).

[8] WALKER, J.S., Regulating Against Nuclear Terrorism: The Domestic Safeguards Issue, 1970-1979, Technology and Culture, **42** 1 (2001) 107-132.

[9] ORRIK, D.N., Differing Professional View Regarding NRC Abandoning its Only Counter-Terrorism Program, Nuclear Regulatory Commission, Rockville, Md. (1998).

[10] LYMAN, E.S., "Radiological Sabotage at Nuclear Power Plants: A Moving Target Set," Proceedings of the 41st Annual Meeting of the Institute for Nuclear Materials Management, New Orleans, Louisiana, 16-20 July 2000. INMM, Northbrook, Ill. (2000).
[11] LYMAN, E.S., Security Since September 11th, Nuclear Engineering International (March 2010), 14-19.
[12] LYMAN, E.S., "Update on the Decline of the NRC's Security Inspection Program," Proceedings of the 60th Annual Meeting of the Institute for Nuclear Materials Management, Palm Desert, California, July 14-18. INMM, Mount Laurel, N.J. (2019).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA-TECDOC-1868, IAEA, Vienna (2019).
[14] WORLD INSTITUTE FOR NUCLEAR SECURITY, Modeling and Simulation for Nuclear Security, WINS, Vienna (2013).
[15] BUNN, M., Modeling of Nuclear Security: Use the Tool, But Remember its Limits (presentation), in Workshop on Emerging Issues in Nuclear Security, Project on Managing the Atom, Harvard Kennedy School, Cambridge, Mass. (2019).
[16] SELBY, S.A. and CAMPBELL, G., Flawless: Inside the Largest Diamond Heist in History, Union Square Press, New York (2010).
[17] KAHNEMAN, D., Thinking, Fast and Slow, Farrar, Straus, Giroux, New York (2011).
[18] SLOVIC, P., FISCHHOFF, B., and LICHTENSTEIN, S., Accident Probabilities in Seat Belt Usage: A Psychological Perspective, Accident Analysis and Prevention, **10** (1978) 281-285.
[19] JOHNSTON, R., Security Maxims. Rightbrain Sekurity, Argonne, Ill. (2018).
[20] JOHNSTON, R.G. and GARCIA, A.R.E., Effective Vulnerability Assessments for Physical Security Devices, Systems, and Programs, LA-UR-03-0269, Los Alamos National Laboratory, Los Alamos, N.M. (2002).
[21] WORLD INSTITUTE FOR NUCLEAR SECURITY, Security Exercises, WINS, Vienna (2014).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparation, Conduct, and Evaluation of Exercises to Test Security Contingency Plans at Nuclear Facilities, IAEA, Vienna (2018).
[23] BUNN, M. and SAGAN, S.D., eds., Insider Threats, Cornell University Press, Ithaca, N.Y. (2017).