UPGRADING SECURITY AT NUCLEAR POWER PLANTS IN THE NEWLY INDEPENDENT STATES

by Oleg Bukharin

Dr. Oleg Bukharin is a research staff member of Princeton University's Center for Energy and Environmental Studies.

As of 1996, 48 nuclear power reactors were operating in five newly independent states (NIS) of the former Soviet Union: 29 units at nine sites in Russia,[1] 15 units at five sites in Ukraine, a double unit plant in Lithuania, and one unit each in Armenia and Kazakstan. These nuclear power facilities need to be reliably protected against possible radiological sabotage or terrorism. The post-Soviet transition in the NIS has been marked by ethnic and political conflicts, crime, and societal instabilities. Nuclear power facilities are not immune from these maladies and face a broad range of threats. Indeed, potentially catastrophic releases of radioactivity and resultant global societal dislocations make the NIS nuclear industry a particularly attractive target for industrial sabotage.

The 1986 Chernobyl accident, the worst reactor accident in the history of nuclear power, is a useful benchmark for examining the potential consequences of nuclear sabotage. The number of deaths directly attributed to the accident was 31, far less than in a typical airliner bombing. Chernobyl, however, has caused many additional health, economic, and societal effects. As of 1996, there were approximately 800 thyroid cancers in children; and the long-term health effects, such as leukemia and genetic deformities, are not yet known but may affect thousands of people.[2] The accident has caused heavy economic losses associated with mitigation and environmental clean-up, resettlement of hundreds of thousands of people, and global damage to agriculture. The economic toll of the accident continues to rise: the estimated cost of closure and decommissioning of the Chernobyl plant, site clean-up, erection of a new sarcophagus around the damaged reactor, and construction of replacement generation capacity is estimated at $4.5 billion. (Even if no radioactivity were released as a result of some future incidence of sabotage, loss of a reactor could be an economic disaster of national proportions.[3])

Psychological and social consequences are also very serious. Many Chernobyl victims suffer from post-traumatic stress syndrome and related diseases. The handling of the Chernobyl disaster by the Soviet government greatly undermined its credibility and, arguably, contributed to the collapse of the Soviet system.

Finally, the Chernobyl accident has caused a lasting depression in the development of nuclear power. In the former Soviet Union, dozens of nuclear power projects planned and under construction have been brought to a halt. No new reactors have been ordered in Western Europe or the United States, and several countries are leaning towards phasing out nuclear power.

This article discusses the technical aspects of reactor sabotage and analyzes the safety threats posed to NIS nuclear power industries. It then suggests a range of possible reactor security upgrades to meet these new threats in the NIS.

REACTOR SABOTAGE: TECHNICAL ASPECTS

Production of heat and its effective conversion to useful forms of energy (electricity and hot steam) are the main functions of a commercial nuclear power reactor. Production of heat via a nuclear chain reaction takes place inside a thick-walled reactor vessel in a reactor core, which is composed of zirconium-clad uranium-oxide fuel assemblies and support elements. Released heat is removed by water pumped through the core by the main circulation pumps. In a boiling water reactor (BWR), water is allowed to boil inside the core, and the resulting steam is routed directly to a turbine generator to produce electricity. In a pressurized water reactor (PWR), heated water in the primary coolant circuit is prevented from boiling by increased pressure; steam is produced in a steam-generator in the secondary coolant circuit. The chain reaction is regulated by control rods and can be quickly brought to a halt by a scram (shutdown) system. Reliable and safe operation of the front-line control and coolant systems depends on power, cooling, and water services provided by various support and auxiliary equipment.

The possibility of a catastrophic release of radioactivity from a power reactor is due to two fundamental factors. First, the reactor core contains a very large inventory of fission products (approximately 15 billion curies for a typically-sized 1000-MWe reactor).[4] Second, the intensive generation of heat inside the core provides a mechanism for the violent release and dispersal of radioactivity.

Overheating and melting of the reactor fuel—a situation known as "core meltdown"—is a prerequisite for a massive release of radioactivity.[5] As overheating progresses, the following chain of events can be expected. The initial surge in fuel temperature would rupture the cladding thereby allowing volatile fission products (iodine, cesium, and noble gases) to escape.[6] As fuel began to melt, fission products would be ejected from the core region by rising gas flows. Subsequently, the interaction of the molten core materials with the concrete base of the reactor cavity would produce steam and hot gases that would sparge the fission product melt. Finally, a steam or hydrogen explosion could oxidize and disperse fine particles and aerosols of radioactive fuel.[7]

An explosion would likely trigger multiple fires, hot water floods, and other massive failures that would contribute to the dispersion of radioactivity and would complicate mitigation activities. The 1986 core explosion at Chernobyl-4 provides a graphic example of such a breakdown:

> Jets of hot water were gushing from the damaged pipes in various directions and landing on electrical equipment. There was steam everywhere, and the sharp reports of shorting in the electrical circuits sounded like gunfire. Near the No 7 turbogenerator, oil that had leaked out of some damaged pipes was burning....[8]

Extensive core damage would likely create a pressure build-up substantial enough to breach the containment of all but the most recent generations of reactors, potentially releasing fission products into the environment.[9]

Reactor sabotage, however, is not a straightforward task. Modern plants are built to very high safety standards and have redundancy of all important safety functions. This built-in safety factor can be defeated only by careful, plant-specific selection of vital equipment, the destruction of which is both feasible and could result in core damage. A detailed knowledge of a plant's layout and equipment is required to locate and identify the selected targets. Finally, reactor machinery and equipment are mechanically robust and designed to operate with a wide safety margin, even under the most unfavorable conditions. A working knowledge of explosives and demolition techniques is, therefore, required to destroy nuclear power plant equipment.

Reactor sabotage, at the same time, is not impossible. There are several ways to cause a core meltdown. All of them flow from general reactor safety principles and involve attempts to cause a failure to cool reactor fuel. In particular, severe core damage could result from one of several situations: loss-of-coolant,[10] station black-out, interference with the reactor controls, or elimination of the capability to cool the core of a shut-down reactor (loss of the heat sink).[11]

Let us consider, for example, an attack directed against a plant's power supply. Alternating current (AC) power is required to operate various coolant pumps and safety equipment. A sufficiently prolonged loss of power (station black-out) could lead to severe core damage. Elimination of a plant's power supply is one possible approach to causing a station black-out. Typically, a plant power supply consists of off-site power lines, the main turbine-generator, and back-up diesel generators. The off-site power lines

are located outside of the plant's perimeter and are virtually impossible to protect. At most plants, when the connection to off-site power is lost, the turbine must be shut down. Thus, if a terrorist succeeds in sabotaging the diesel generators as well, a dangerous station black-out would occur. A diesel generator can be destroyed easily and quickly, for example, by a relatively small explosive charge.

To prevent an adversary from causing reactor core damage, the U.S. Nuclear Regulatory Commission (NRC) recommends: "to protect as vital the reactor coolant pressure boundary and one train of equipment—with the associated piping, water sources, power supplies, controls, and instrumentation—that provide for the capability to achieve and maintain hot shutdown."[12] For example, for a typical PWR, this requires protection of the nuclear power plant functions and equipment listed in Table 1.

On a practical level, it is often more useful to talk in terms of "target sets." A target set is a combination of plant systems and components, such that destruction of each element of the set would cause core damage. For example, the off-site power lines and back-up diesel generators would make a complete target set for most plants. An individual plant may have as many as 10 or more various target sets. A knowledgeable adversary would attempt to "hit" at least one complete set of targets (as opposed to destroying at random equipment listed on Table 1). Accordingly, the reactor security force must protect at least one element in every target set of the plant.

Target sets are plant specific and might differ substantially from one plant to another. For example, Soviet-designed reactors have unique strengths and weaknesses that affect their vulnerability to sabotage, and make their target sets different from those typical of Western plants.

Most of the installed nuclear capacity in the NIS is represented by RBMK-1000/1500, VVER-440, and VVER-1000 reactors. Several design features make these reactors resistant to sabotage. The VVER-440 design, in particular, has a number of unique, built-in safety features. (The VVER-1000 design, by contrast, is in many respects closer to that of Western PWRs and thus has lost many advantages offered by the VVER-440 design.[13])

The coolant-to-power ratio for the primary coolant circuit in a VVER-440 reactor is twice that in a Western PWR. (The RBMK's coolant inventory is also twice that in a Western BWR.[14]) The large volume of coolant is important because it could delay core damage in case of a station black-out or a loss of the heat-sink.[15] Indeed, according to Finnish experts, "VVER-440's core conditions resemble a hot shutdown 3 hours after the loss of power; and after 6 hours the situation could still be recovered with no damage to the core."[16]

There are, however, safety deficiencies and vulnerabilities that make NIS plants more difficult to protect, and more susceptible to sabotage. For example, despite recent efforts to improve fire safety, virtually all plants remain vulnerable to fire. Combustible materials (e.g., floor covers and cable coating) are widely used; separation between individual fire zones is insufficient; and fire detection and fire-fighting

Table 1: PWR Vital Functions and Equipment

Function	Equipment
reactivity control	scram components and systems
decay heat removal	turbine-driven auxiliary feedwater pump, including control and water source
process monitori	temperature and pressure monitoring systems
reactor coolant makeup and reactor coolant pump seal cooli	charging pump, including water source and motor control center
support	- diesel generators, including switchgear, cooling, startup, and controls - batteries - service water pump and motor control center, including cooling components

equipment is often inadequate. Metal-frame turbine halls containing reactor control rooms, auxiliary feedwater components, electrical switch-gear systems, and steam generators are particularly vulnerable: exposure of the interior of a steel-framed building to high temperatures (greater than 550° C.) for approximately 10 minutes would cause a failure of its structural steel members.[17] Generally, a sabotage attack resulting in a fire or flooding could completely disable reactor safety systems and result in severe core damage.[18]

NIS ADVERSARIES

Prior to discussing reactor security systems, it is useful to take a look at potential adversaries who have the capability and, possibly, the motivation to attack a nuclear power plant. A comprehensive threat characterization cannot be accomplished without a thorough assessment of law-enforcement information. A tentative, media-based analysis, however, indicates that reactor security in the NIS countries could be challenged by adversaries of the following four broad classes.[19]

Paramilitary terrorist groups. Hostage-taking, kidnappings, assassinations, bombings, industrial sabotage, and guerrilla warfare have become widespread in the NIS. In many cases, attacks are executed by highly capable, experienced, and dedicated paramilitary organizations. Ethnic, religious, and political groups capable of staging an attack against heavily protected targets have emerged in several post-Soviet states. In particular, many paramilitary organizations operate in conflict areas ("hot spots") in the Russian Caucasus, Georgia, Armenia, Azerbaijan, Pridnestrovye, and Central Asia. Motives for a paramilitary attack against a nuclear power plant might vary from extortion schemes to political demands to revenge or to intimidation of a population (especially if perpetuated by ethnic- or religious-based terrorist groups).

Currently in Russia, the conflict and instability in the break-away republic of Chechnya pose the most serious terrorist threat. The June 1995 raid by Shamil Basayev's guerrillas against Budennovsk provided a glimpse of possible strategies and operational characteristics of a Chechen terrorist group. Over 70 heavily armed gunmen infiltrated the supposedly sealed Chechen-Russian border and drove in three "Kamaz" trucks and a police car over 200 kilometers (km) to Budennovsk, a small town in southern Russia. There they assaulted several targets (including the police headquarters), took over 1,000 civilian hostages, barricaded themselves in a local hospital, and made political demands, including withdrawal of Russian troops from Chechnya. After unsuccessful attempts to free the hostages by Russian anti-terrorist forces, the crisis was resolved by negotiation, and the gunmen returned to Chechnya.

Arguably, an attack of this magnitude is not feasible deep inside Russia, where nuclear power plants are located.[20] However, a smaller-scale attack by undercover agents cannot be ruled out. The Metzamor plant in Armenia is relatively vulnerable: it is located approximately 200 km away from the Stepanokert war zone in Azerbaijan (and only 14 km from the Turkish border) and, thus, is within striking range by adversaries.

A paramilitary attack could also be staged by a political group in a time of governmental instability. The assault by extremists on the Ostankino television center and other installations in Moscow in October 1993, during the showdown between the Yeltsin government and the Russian parliament, is an example of such an attack. In contrast to ethnic or religious groups, political extremists would have no difficulty operating in nuclear power plant areas or recruiting insider assistance.

Professional criminals. There are an estimated 3,000 to 4,000 organized criminal groups in the NIS. Many of them are highly complex and hierarchical organizations. According to a senior official in the Russian Ministry of Internal Affairs:

> The trend of growing professionalization of criminals has become apparent. Criminals seek to commit sophisticated profit-oriented crimes, and, in attaining their criminal goals, demonstrate particular impudence, aggressiveness, and negligence regarding not only rights, but also the lives of citizens and officials.... More and more crimes are committed with the use of firearms. The armed actions are often connected with terrorism, thus becoming a tool of pressure on officials, a method of intimidating business competitors, and a means of settling conflicts in the criminal underground.[21]

Blackmailing the authorities and extortion are the likely motives for organized crime threats against nuclear targets. For example, in 1994 the Ignalina plant in Lithuania received two bomb threats.[22] A Lithuanian national in Sweden made the first threat and demanded that the Swedish authorities pay him $8 million. This individual was subsequently

detained, tried, and convicted. On a second occasion, the Lithuanian authorities received information about an alleged bomb placed at the plant on behalf of a local organized crime boss whose son had been sentenced to death. This threat was taken seriously and the plant was shut down and searched. No bomb, however, was discovered.

Professional criminals are likely to rely on insider assistance and use bomb or arson threats. However, violent attacks against protected targets (for example, army depots) have been reported and, therefore, similar attacks against nuclear facilities cannot be ruled out in the future.[23]

Extremist protesters. Nuclear safety could be endangered by anti-nuclear or environmental movements engaged in vandalism, picketing, or demonstrations. Massive anti-nuclear protests could be violent and could involve site or building takeovers, bombings, or fights with security forces.[24]

In the NIS, the anti-nuclear and environmental movements (which were often separatist and nationalist in nature) reached their peak in the late 1980s and early 1990s. Most of the environmental protests were peaceful in nature. However, direct actions (pickets and demonstrations) against the construction of new reactors took place, for example, at the Khmelnitsky plant in Ukraine in the early 1990s. Environmentalists were largely behind the closure of the Metzamor plant in Armenia as well. Generally, violent environmental activities appear unlikely, but they cannot be ruled out (especially if linked to broader political or nationalist actions).

Insiders. NIS nuclear industries are experiencing great hardships, and many nuclear facilities are on the verge of bankruptcy. Salary delays and unpaid leaves have become common. The social prestige of the nuclear profession, already undermined by the Chernobyl disaster, has plummeted. Distressed social and economic conditions subject nuclear workers to powerful psychological stresses and create an environment conducive to malevolent acts by insiders.

An insider, with unrestricted access to the plant and possibly intimate knowledge of reactor targets and/or security vulnerabilities, could represent a very serious threat. (Indeed, one NIS reactor technician observed in a conversation that no one would be able to save the reactor had he decided to sabotage it.) Some insiders also make good potential recruits for professional criminal or terrorist organizations. There are three major groups of insiders that are of concern: disgruntled employees, people with mental disturbances, and minor criminals.

Disgruntled employees could stage a protest or demonstration on-site which, if it escalated to violence, could endanger reactor safety. (Peaceful protests have already taken place at nuclear facilities in Russia.) They also could engage in vandalism or actual sabotage of reactor equipment. In 1995, a worker at the Severodvinsk submarine production complex, who had his salary delayed by several months, posted a note with a threat to blow up a shop containing two reactors.

A mentally disturbed employee could be the most dangerous of all because he or she might seek to cause a full-scale accident. Idiosyncratic individuals, engaged in irresponsible activities out of curiosity or adventurism, also represent a considerable danger. For example, in 1992, a worker at the Ignalina plant planted a virus in a computer system controlling the plant's auxiliary systems.[25]

Finally, a small-time criminal could be a security and safety threat if his or her criminal actions involved damage or theft of safety- or security-related equipment. Most security arrangements at Soviet nuclear facilities in the past were designed to prevent property theft.

DESIGN-BASIS THREAT

A design-basis threat postulates the capabilities of a potential adversary and serves as a benchmark to design and implement a reactor security system. In real life, a design basis threat must be developed and maintained on the basis of comprehensive law enforcement and intelligence information regarding nuclear-related crimes, terrorist attacks, significant criminal activities against high-value or well-protected targets, and major events involving theft or use of weapons and explosives.[26]

Public information about criminal and terrorist activities in the NIS suggests that the NIS design basis threat for reactor sabotage would be similar in structure to that used by the NRC, and thus would include: a) a paramilitary violent assault; b) a sabotage by a single insider in any position; and, possibly, c) a car-bomb attack. Two points should be made regarding to the car-bomb and paramilitary threats.

First, no car-bomb attack against a protected fixed target has been reported so far in the NIS. However,

car bombs have been widely used by professional criminals and terrorists as an assassination device.[27] The effectiveness with which car bombs have been employed against buildings in foreign countries (especially, in the Middle East and the United States) could inspire NIS adversaries as well.

Second, the paramilitary threat to nuclear power facilities in the NIS countries is considerably greater than in the United States; it is also more credible. Indeed, the NIS design basis threat of a violent assault is driven by the conflict in Chechnya. Accordingly, NIS plants are facing a threat of a commando raid, carried out by a fairly large group of trained, combat-tested, and motivated gunmen, armed with high-powered, hand-held weapons (including machine guns and rocket-propelled grenades) and explosives.[28] Terrorists would be able to operate in more than one team.[29] A truck would be used for transportation of the men and equipment. Terrorists could coerce or bribe a nuclear power plant worker to provide plant and security information. (Insider assistance would likely be a critical element for a successful attack because of nuclear power plant complexity and because no detailed technical information related to nuclear power facilities has ever been made public in the former Soviet Union.)

NIS REACTOR SECURITY

A reactor security system must ensure reliable protection of a nuclear power plant against all threats postulated in the design basis threat. The details of reactor security designs may vary from one plant to another. Security systems, however, are expected to have the following general elements: a) a vehicle barrier; b) a perimeter fence with cleared areas on both sides of it; c) a perimeter intrusion detection system coupled with a closed-circuit television (CCT) system or other assessment system; d) a central and a secondary alarm station; e) armed guards (which in certain contingencies could be supported by a local law enforcement agency or the military); f) perimeter access control equipment; and g) measures to control access to vital areas. Regulatory oversight by an independent national agency is important to ensure that nuclear power plants comply with regulations and have functional and effective security.

In the Soviet Union, reactor security was designed to defend nuclear plants against a war-time attack by NATO commandos, as well as to provide for common, day-to-day industrial security. The idea that someone would want to damage a reactor intentionally during peacetime probably did not emerge until after the Chernobyl disaster in the late 1980s. Accordingly, nuclear power plants in the Soviet Union were not designed to accommodate physical security requirements and, generally, were not prepared to confront post-Soviet sabotage threats. For example, guards at nuclear facilities were vulnerable to small-arms fire; communication systems were inadequate; and physical protection equipment was obsolete (especially alarm assessment systems).[30]

NIS operators and security personnel are working to improve reactor security. Many weaknesses, however, remain. Upgrades have been stalled largely because of insufficient funding. It also appears that NIS security managers often seek to implement isolated technical fixes and overlook the need for a systematic, performance-based approach to security. With this in mind, we need to review the general requirements for reliable and cost-effective reactor protection against paramilitary or insider threats and discuss the need for security upgrades at NIS plants.

PROTECTION AGAINST A PARAMILITARY ATTACK

The key factor in planning a defense against paramilitary attacks is the speed with which a trained adversary could reach and destroy its targets. A fence line could be blown up by explosives or jumped in a matter of seconds.[31] Breaching locked doors to gain access to vital areas would require the same or less time. It may take an adversary only a little longer to run to and blow up the intended targets. All in all, only few minutes may elapse between the beginning of an assault and the destruction of the reactor.

There are several fundamental implications inherent in such a high-speed attack. First, at least during the initial stage of the assault, off-site assistance is not realistic and the reactor security system must be self-sufficient. (For example, during the major fires at Metzamor (1982) and Beloyarsk (1978), the arrival of the off-site fire brigades was delayed by one and two hours, respectively.[32]) Second, fences, doors and other physical obstacles do not offer significant resistance nor slow down an adversary equipped with explosives. Third, timely interdiction and containment of an adversary by the armed security force are the keys to countering an external violent attack. As discussed below, a timely and effec-

tive response is not possible without a defensive strategy, a trained response force, reliable detection, and an accurate assessment of an attack.

Defensive strategy

According to the defensive strategy adopted by nuclear power plants in the United States, the principal objective of the response force is to interdict and contain (or neutralize) an adversary before it destroys any single set of targets. This strategy means that, after the alarm sounds, a sufficient number of response officers must move to prearranged defensive positions in a timely manner.[33] The response force must be properly armed and trained to engage and stop an adversary. If an adversary destroys an element(s) of a particular target set, the response force must regroup to defend the rest of the set.

Identification of all target sets (target set analysis) is a cornerstone of the defensive strategy because it provides the security force with a knowledge of the location and nature of the targets.[34] (Target set analysis participation also provides useful training for operators in developing contingency mitigation plans in the event management of a severe accident is required. Operators are typically not trained in mitigating accidents created by sabotage.) Armed with target information, security force supervisors must identify likely assault avenues and determine the time intervals required for terrorists to reach target locations. The analysis then becomes a basis for determining response parameters (for example, the number, weapons, and location of response officers) and for selecting delaying barriers, contingency defensive positions, and interdiction routes.

Soviet (and now NIS) security planners exercise a totally different approach to reactor security; they have no target set analysis. In its absence, the traditional Soviet defensive strategy was to protect the site perimeter.[35] Little priority has been given to protecting buildings and facilities inside the site protected area. This strategy has a number of serious shortfalls. First, considering the speed with which barriers can be penetrated, the response force would likely be too late in interdicting an adversary at the fence-line. Chasing the threat inside the plant would in all probability be a recipe for disaster. Second, a response to the perimeter, as opposed to prearranged defensive positions, may expose the response force to hostile fire. Third, the response capability could be easily fragmented and overwhelmed if alarms (some of them diversions) occurred in several perimeter zones nearly simultaneously. (This problem is often compounded by inadequate assessment capabilities at many NIS plants.) Generally speaking, the outer perimeter probably cannot be protected without multiple, heavily manned, armored guard posts and roving patrols.

Detection and assessment

Reliable detection of a perimeter intrusion is absolutely critical for a timely and effective response. The detection system must also be coupled with a CCT or watchmen: an accurate assessment of an adversary's capabilities and intentions could make the difference between success and failure of the response operation.

Many NIS plants have recently improved their perimeter intrusion detection capabilities.[36] Some plants even employ two systems based on different physical principles. Assessment systems, however, are lagging behind. CCT systems are expensive and usually must be imported. Bullet-resistant guard towers are viewed by many NIS security managers as outmoded or obsolete; they are also not inexpensive. Thus, the problem persists, and upgrading intrusion detection and assessment capability should be a priority at least at some NIS plants.

Security personnel

Training and preparedness of security personnel are the cornerstones of reactor security. Accordingly, personnel problems caused, for example, by poor morale, boredom, lack of threat awareness, or a negative attitude by the plant management towards security are the most serious and could have devastating consequences.[37] Steve Hartman, a former member of an elite counter-terrorism unit in the U.S. Navy observes:[38]

> The easiest thing to defeat is the human factor. You can have the best, high-tech equipment that you want. You can still defeat the human factor because somebody has to monitor that equipment, to watch that CCT cameras, the screen. Someone has to watch the alarm board. You can wear them down. I can give you an example. Some places have microwave alarm systems with a dual perimeter, like the President's helicopter pad. Those systems can be defeated and all you need are a cat and a couple of rabbits. You start at one in the morning and you wear them out. They think it is misalignment...and they don't show up. It is easy. You have all the time in the world. Time is on your side.

> You can sit out there in the bush and throw cats, dogs, or rabbits all night long.

In the NIS, nuclear security forces, including armed guards and the response force, are provided by the national Ministries of Internal Affairs (MVD) under a contract with the plant. (As a result, the MVD troops have their own chain of command.) The plant also has its own security staff and may hire semi-private unarmed watchmen.

MVD nuclear security forces are regular military units and appear well-trained and equipped (although the level of training has decreased recently). Their capability, however, could be further improved by practical, site-specific (target set-based) training, including table-top and force-on-force exercises.[39] There is also a need for better coordination between the MVD troops, the plant's security organization and reactor operators. Finally, although most security officers are disciplined and motivated, low salaries and general deterioration of the armed forces have created serious morale problems, which must be addressed and resolved.[40]

PROTECTION AGAINST THE INSIDER THREAT

Reactor defense against an insider threat relies on access control and human reliability measures. The perimeter access control measures are intended to prevent unauthorized personnel and contraband, such as explosives and weapons from entering the plant protected area. To enter the protected area, personnel should use a limited number of entry portals where identification and search procedures (including the use of metal and explosive detectors, X-ray radiography of packages, and physical search) can take place. Access to internal vital areas, where critical equipment is located, should be restricted to authorized personnel by locked (key-carded) and alarmed doors.[41]

NIS plants are facing considerable difficulties in organizing effective access control procedures. There is a lack of experience and equipment. Access control is further complicated by very large numbers of support and maintenance personnel working on-site.[42] Vital areas (and critical equipment) are not defined and are easily accessible via a large number of entrances. In the opinion of security experts working with the VVER-440 Lovisia plant in Finland[43]:

> ...access control to an area is not meaningful if access must be granted to a large number of the plant staff. For example, the turbine hall is an important but large building with plenty of different equipment requiring access by a large number of people. [....] In general, the layout of a VVER-plant does not support meaningful access control, and expensive electrical access control systems don't, without backfitting some parts of the layout, serve the purpose.

Eventually, NIS plants will have to introduce modern, full-scope access-control systems. In the near-term, several relatively low-cost steps to improve the situation appear feasible. In particular, plant managers should reduce the number of personnel with access inside the protected area by relocating non-essential support services (such as, mechanical workshops) off-site. It is also important to begin work on managing access to vital areas.

Personnel reliability measures (such as drug and alcohol tests, background investigations, psychological evaluations, and behavioral observations) are also important in countering the insider threat in the nuclear power industry. In the former Soviet Union, nuclear industry personnel were closely monitored by the KGB and by the Communist Party.[44] Nuclear industry workers enjoyed social prestige and high living standards and had no motivation to engage in malevolent activities.

The situation has changed. NIS nuclear industries continue to employ background investigations and medical checks, but these have only limited utility. Party controls are gone, and the role of internal security may have decreased. More significantly, nuclear personnel have become impoverished and desperate.

Thus, NIS plants must improve their personnel reliability programs (for example, by practicing behavioral observation). However, achieving an acceptable level of reactor security against the insider threat would likely require fundamental improvements in professional discipline and resolution of broader economic and social problems.

SUPPORT PROGRAMS

Regulatory oversight, coordination with law enforcement agencies, and development and maintenance of physical security equipment (and other support programs) are important to ensure the effectiveness of reactor security systems, both at individual plants and across the industry. Only Russia, which after the break-up of the Soviet Union in 1991 inherited most of the Soviet physical security infrastructure, has a network

of organizations and agencies specializing in the security of nuclear installations.[45] The research and production center "Eleron" of the Ministry of Atomic Energy (Minatom) performs site-specific system analysis and provides physical security equipment. Special research institutes of Eleron, the MVD, and the Federal Security Service assist nuclear facilities in developing design-basis threats.[46] Gosatomnadzor is responsible for overseeing and regulating civilian nuclear activities, although its inspection and enforcement capabilities remain limited. In contrast, the non-Russian NIS have yet to introduce the concept of a design-basis threat, and their regulatory authorities and technical infrastructure are still in a much earlier stage of development.

INTERNATIONAL COOPERATION

The possibility of a catastrophic reactor accident in the former Soviet Union or Eastern Europe remains a fundamental concern of the international community. In the post-Chernobyl years, the Soviet Union and, later, the NIS countries have undertaken a range of technical measures to upgrade nuclear power plant safety. The internal effort has been complemented by multilateral and bilateral international safety initiatives. The International Atomic Energy Agency (IAEA), in particular, has been playing an important role in coordinating the RBMK and VVER safety programs and consolidating their results. The IAEA programs are designed to assist both the regulatory and operating organizations and to provide a basis for technical solutions. These programs include plant-specific safety reviews to assess the adequacy of design and operations, reviews of plant design, and reviews of topical issues (e.g., fire safety). The U.S. Department of Energy (DOE) also has been working with Russia, Ukraine, and the East European countries to improve their national capabilities in the areas of reactor management, operational safety, engineering, technology, and plant safety evaluations.

Nuclear material protection, control, and accounting (MPC&A) is another area of cooperation between the NIS and the West. Particularly intensive is the cooperation between the United States and Russia. Under the government-to-government agreement (now merged with the laboratory-to-laboratory program, discussed below), the partners are upgrading nuclear safeguards and security at Minatom's civilian facilities that process and store weapon-usable, highly enriched uranium and plutonium.

The MPC&A laboratory-to-laboratory program involves cooperation between the U.S. national laboratories and Russian weapon design institutes and focuses on both safeguards upgrades at individual facilities (including those of Minatom's defense complex) and research and development in the area of safeguards. The United States also is assisting Russia in improving transportation security, establishing a safeguards training center, and developing nuclear regulations. Safeguards cooperation, though much smaller in scope, also is under way in Kazakstan, Ukraine, and other NIS.

Physical security of nuclear installations and materials is an important aspect of the MPC&A cooperation. Security upgrades at individual facilities include a security survey, vulnerability assessment, technology transfer (including perimeter and interior intrusion detection systems, CCTs, alarm stations, locks, doors, etc.), and personnel training. Much of the required physical protection equipment is produced by Eleron. In addition, the U.S. national laboratories have cooperative projects with Eleron in the area of physical protection equipment and technologies.

In contrast to the reactor safety and MPC&A initiatives, however, little cooperation has occurred in the area of reactor security. Under the Nunn-Lugar Cooperative Threat Reduction (CTR) program, the DOE is helping to upgrade physical security at the South Ukraine plant in Ukraine, the BN-350 complex in Kazakstan, and the Ignalina plant in Lithuania. The U.S. NRC is working with the national regulatory authorities in the NIS to develop regulations and to establish national licensing and inspection capabilities. Assistance to selected plants in Ukraine, Kazakstan, and Lithuania is also provided by European countries (mainly Finland and Sweden) and Japan.[47] Very little reactor security work has been done in Russia.

The narrow scope of the reactor security cooperation is unfortunate because, if expanded, it could enhance the effectiveness of both the reactor safety and MPC&A efforts.

First, a successful act of sabotage against a nuclear power reactor would lead to a catastrophic reactor accident. Therefore, nuclear power plant protection against sabotage should be viewed as an integral part of the overall reactor safety measures. Second, reactor security cooperation would strengthen the

national nuclear safeguards systems. Indeed, physical security equipment, procedures, response tactics, and regulatory requirements necessary to protect a power plant are, in many respects, identical to those used to safeguard weapons-usable fissile materials.[48] Thus, improving the NIS capability of the NIS to secure nuclear power facilities would strengthen their MPC&A capabilities as well.

A reactor security cooperative initiative could be built upon and integrated with the existing nuclear safety and safeguards programs. Such an initiative should include a number of efforts:

1. Cooperation among reactor operators and plant designers regarding target set analysis.
2. Cooperation among the Ministries of Internal Affairs regarding tactical training and response strategies of the nuclear security force. (This effort could greatly enhance the effectiveness of the MPC&A cooperation, as existing nuclear material safeguards programs are technology-oriented and generally not designed to increase the effectiveness of nuclear security force response.)
3. Physical protection technology transfer. (As in the MPC&A programs, this would include a site survey, definition of security upgrade requirements, procurement of equipment and personnel training. In order to encourage the development of domestic equipment manufacturing and maintenance capabilities, equipment, and services should be sought from local sources. Interregional cooperation, mainly with Russia's Eleron, should also be encouraged.)
4. Assistance to the national regulatory authorities to develop licensing and inspection capabilities, legislation, and specialized programs to conduct performance evaluation of reactor security programs.

CONCLUSIONS

NIS nuclear power industries face a wide range of security threats and must be reliably protected against radiological sabotage. In particular, NIS nuclear power facilities need to enhance their armed response capability, the key to countering an external violent attack by an adversary armed with explosives. A timely and effective response is not possible without a defensive strategy that is based on a target-set analysis, trained response force, and reliable detection and assessment of an attack. Defenses against the insider threat need improvement as well. Reactor security upgrades could be undertaken in cooperation with Western nations. Such an initiative could be built upon and integrated with the existing nuclear safety and safeguards programs.

[1] In addition, there are three dual-use plutonium production reactors still in operation in the closed cities of Tomsk-7 and Krasnoyarsk-26, and two tritium production reactors in Chelyabinsk-65. There are also tens of smaller-power research and propulsion reactors. Sabotage of these reactors, however, would be less damaging because of their much smaller inventories of radioactivity and lower power.

[2] Abel Gonzales "Chernobyl—Ten Years After," *IAEA Bulletin*, 3/1996, p. 9.

[3] In the West, a shutdown of a plant could cost the operating utility up to one million dollars a day; replacing a plant would require billions in investment. Nuclear power is an important component of the NIS energy sector. Nuclear-generated electricity accounts for approximately 13 and 33 percent of total generation in Russia and Ukraine, respectively (up to 40 percent in Russia's north-west). Lithuania's Ignalina nuclear power plant (NPP) produces over 85 percent of that nation's electricity (over half of which is exported). The Metzamor-2 reactor, restarted in October 1995 (after the shutdown in 1989), is virtually the only source of electricity in Armenia. In Kazakstan, the BN-350 reactor in Actau provides fresh water and electricity to the Mangyshlak peninsula, an industrialized region on the Caspian sea.

[4] Sources of tens of curies of radioactivity represent a significant hazard to human health.

[5] Destruction of a reactor and its containment from outside (e.g., in an air raid) would also release radioactivity. Such a threat, however, is outside of the scope of the design- basis threat. Defense of a plant against an external military threat is the responsibility of the national government.

[6] In the Chernobyl accident, damage and heating of the reactor fuel (up to 2000° C.) resulted in complete or partial evaporation of volatile nuclides: 100 percent inert gases, 50 to 60 percent Iodine-131 (45 MCi), 50 percent cesium. ("*Chernobyl and Its Consequences*," Project Polyn database, RSC Kurchatov Institute, 1996.)

[7] Hydrogen would be produced in zirconium-water (steam) reactions ($Zr + 2\ H_2O \longrightarrow ZrO_2 + 2H_2$ + 140 kCa/mole). Oxidation of zirconium (20 t in a typical core) would release 10 kg/sec of hydrogen and large amounts of heat.

[8] Anatoli Dyatlov, "26 April 1986," *Nuclear Engineering International* (April 1996), pp. 18-22.

[9] Of all Soviet-designed power reactors, only VVER-1000 reactors have Western-type containment; VVER-440/230 and RBMK reactors do not have a structure designed to contain an accident; and VVER-440/213 reactors have a pressure suppression structure.

[10] A loss-of-coolant accident (LOCA), which could potentially result in a complete de-watering of the core, is the principal concern of reactor safety experts. The possibility of a LOCA is minimized by the use of redundant and highly-reliable front-line systems and equipment. Dedicated safety systems, such as the emergency core cooling system, are employed to mitigate a LOCA should it occur. These defenses, however, would fail if an adversary equipped with explosives had access inside the reactor containment where both the primary and emergency cooling equipment (piping, pumps, tanks, etc.) could be easily destroyed.

[11] Even if a reactor were shut down successfully, core damage still could occur over time if a long-term heat removal capability were lost (this situation is known as "loss of the heat-sink"). Indeed, approximately 200 MWt heat is produced in a 1,000-MWe reactor by the decay of fission products immediately after

the shutdown, and several hours may elapse until the heat production rate drops to a safe level of a fraction of a percent of the full power rate.

[12] U.S. Nuclear Regulatory Commission (NRC), "*Vital Equipment/Area Guidelines Study: Vital Area Committee Report*," NUREG-1178 (Washington, D.C.: NRC, February 1988), p. 6-1.

[13] Jukka Laaksonen, "VVER-1000: Considering its strengths and weaknesses," *Nuclear Engineering International* (May 1994), pp. 21-23.

[14] Allen Brown, "International RBMK Project: Engineering and Analysis Aspect," *Nuclear Engineering International* (October 1994), pp. 41-43.

[15] For example, the core of the Metzamor-1 unit in Armenia survived a five-hour long blackout during the 1982 fire.

[16] In a Babcock & Wilcox reactor, the core temperature would become unacceptable after less than one hour; in a Westinghouse reactor, there would be severe core damage in less than three hours. (Jukka Laaksonen, "It ain't necessarily so: reassessing VVER-440 safety," *Nuclear Engineering International* (September 1992), pp. 22-25.)

[17] "*Explosives and Demolitions*," Field Manual 5-25 (Washington, D.C.: Department of the Army, 1967).

[18] Tero Varjoranta and Kristian Maunula, "Reassessing VVER-440 Physical Protection; Strengths and Challenges," paper presented at the conference "Nonproliferation and Control of Nuclear Materials in Russia," Moscow, May 1996.

[19] John Stewart, John Davidson, Cynthia Fulwiler, Harvey Jones, and Sarah Mullen, "*Generic Adversary Characteristics Summary Report*," NUREG-0459 (Washington, D.C.: NRC, March 1979).

[20] Budennovsk is located approximately 200 km from Chechnya's capital Grozny. The distance between Grozny and the nearest nuclear power plants (the Zaporozhye and Novovoronezh NPP in Ukraine and Russia) is approximately 1,000 km.

[21] Gennady L. Lezhikov, head of the Main Information Center of Russia's Ministry of Internal Affairs, "Statistical Information on Crime and its Use in Crime Control," presented at 9th U.N. Congress on the Prevention of Crime and the Treatment of Officers, Cairo, April 29-May 8, 1995.

[22] Author's correspondence with Lithuanian nuclear experts in September 1996 (names withheld by request).

[23] Graham H. Turbiville, Jr., "*Mafia in Uniform: The 'Criminalization' of the Russian Armed Forces*" (Fort Leavenworth, KS: Foreign Military Studies Office, July 1995).

[24] In a May 1996 example, a transport of vitrified high-level waste to the Gorleben repository in Germany took place "under conditions analogous to civil war." The shipment required protection by 20,000 riot police at a cost of $33 million. The property damage totaled $66 million. Some of the violent tactics used by the protesters were the destruction and bombing of railways, setting fires, blocking roads, cutting power lines, and fighting with police and firefighters. (*Nuclear Fuel*, May 20, 1996, p. 10.)

[25] Radio Baltica (8:50 AM, Moscow time, 14 February 1992).

[26] John Davidson and Roberta Warren, "*Development and Maintenance of a Design Basis Threat for Use in Designing Nuclear Safeguards*" (Washington, D.C.: NRC, November 1994).

[27] An example at hand is the assassination attempt on the President of Georgia Eduard Shevarnadze in which terrorists detonated a car-bomb near Shevarnadze's motorcade on August 29, 1995. ("*Patterns of Global Terrorism 1995*," (Washington, D.C.: U.S. Department of State, April 1996), p. 10.)

[28] The assumed number of adversaries is almost arbitrary. Potential NIS adversaries appear to have no manpower constraints. However, the larger the group size the more difficult it would be to maintain operational security.

[29] The capability of the group to operate in more than one team is very important. Ideally, the adversary would want to have an assault/demolition unit(s) to get to and destroy the targets, and a security team(s) to create diversions, delay re-enforcement, and neutralize the reactor security force.

[30] *Report on Activities of the Federal Regulator of Russia on Nuclear and Radiation Safety in 1993*, RD-03-02-93 (Moscow: Gosatomnadzor, 1993), pp. 60-61.

[31] According to a U.S. counter-terrorism expert "You can go over the fences, both fences, in under 30 seconds, set the alarm off and still not get detected." ("Red Cell," documentary film, S. C. Cranford and John Wieseman, eds., L.O.T.I. Group Production, 1993.) It should be noted that an assessment would be assured with a digital video-capture system that allows an alarm station operator to freeze frames one second before the alarm, at the moment of the alarm, and one second after; author's communication with Michael Warren, U.S. Nuclear Regulatory Commission, September 1996.)

[32] Heikki Aulamo, Jouko Marttila, Heikki Reponen, "The full stories on Armenia and Beloyarsk," *Nuclear Engineering International* (July 1995), pp. 32-33.

[33] Whenever possible, engagement should occur at choke or hard points located inside buildings but outside of vital areas.(Author's communication with Bryan Dettman and Michael Warren, B. A. Dettman & Associates, January 1997.)

[34] Initial sets of targets could be determined by evaluating a range of sabotage scenarios and plant responses. The analysis could be further refined on the basis of statistical models such as the probabilistic safety analysis.

[35] *Report on Activities of the Federal Regulator...*, pp. 60-61.

[36] A wide variety of sensors are manufactured domestically. In Russia, Eleron is a major producers of intrusion detection systems of various types. In Ukraine, manufacturing of microwave detectors was started in Kharkiv.

[37] G. Spies, *et al.*, "*People-Related Problems Affecting Security in the Licensed Nuclear Industry*", NUREG-0768 (Washington, D.C.: NRC, March 1981).

[38] See "Red Cell."

[39] A table-top exercise for a given attack scenario is an analytical game in which refereed "adversaries" and "responders" use floor plans and actual time-lines to simulate maneuvers and engagements. A force-on-force exercise is a realistic war-game at the actual plant site. Typically, a force-on-force exercise is preceded by a table-top exercise.

[40] There is considerable corruption and crime in the Russian armed forces, including MVD and other security forces. (Graham H.Turbiville, Jr., *Mafia in Uniform...*, p. 5.)

[41] It should be noted that at some sites not all potential targets are inside vital areas.

[42] For example, the three-PWR-unit Palo Verde plant in the United States is run by 2,400 personnel and uses 600 contractors. In the future, these numbers will be reduced to 1,800 and 100 respectively. In contrast, at a similar NIS plant approximately 6000 people have access to the protected area. (Janet Wood, "Palo Verde," *Nuclear Engineering International* (May 1996), pp. 43-46.)

[43] Tero Varjoranta and Kristian Maunula, "Reassessing VVER-440 Physical Protection; Strengths and Challenges." Finnish experts also observe that access control is particularly difficult for a plant with two reactors sharing much of their auxiliary equipment. During reloading, a large number of support personnel have access to the shut-down unit. The other unit continues to operate and is more vulnerable to insider sabotage.

[44] In addition to managing background investigations, the KGB had a network of informants. For example, as indicated in a KGB memo (February 21, 1979, No. 346-a) to the CPSU Central Committee, the KGB was fully informed about construction flaws at the Chernobyl 4 unit. (As presented in "Chernobyl Bibliography. Construction Flaws" (http://www.spu.edu/depts/library/third/chernobyl-bib.html).)

[45] The plant's management and Rosatomenergo (Minatom's utility organization) are directly responsible for reactor security. The Ministry of Internal Affairs provides armed guards. Organization of reactor security also is coordinated with Minatom's Second Main Directorate (Physical Protection) and the Federal Security Service.

[46] It appears that individual facilities may have different design basis threats. Whether such a practice assures consistency of design basis threats across the nuclear industry and their timely upgrades is not known. The arrangement for development, maintenance and validation of the design basis threat appears very different from that for the nuclear power industry in the United States, where these functions are imple-

mented by the U.S. NRC.

[47] Assistance activities are conducted according to a "Coordinated Technical Support Plan" prepared by the donor countries under the auspices of the IAEA.

[48] In fact, the task of fissile materials protection might be in many respects easier. At a nuclear power plant adversaries would achieve their goals by reaching the intended targets. At a fissile material facility, they would also have to escape. Accordingly, the security forces and law-enforcement agencies could be able to prevent an adversary from escaping by mounting a cordon operation or by conducting a hot pursuit and recovery of stolen materials.