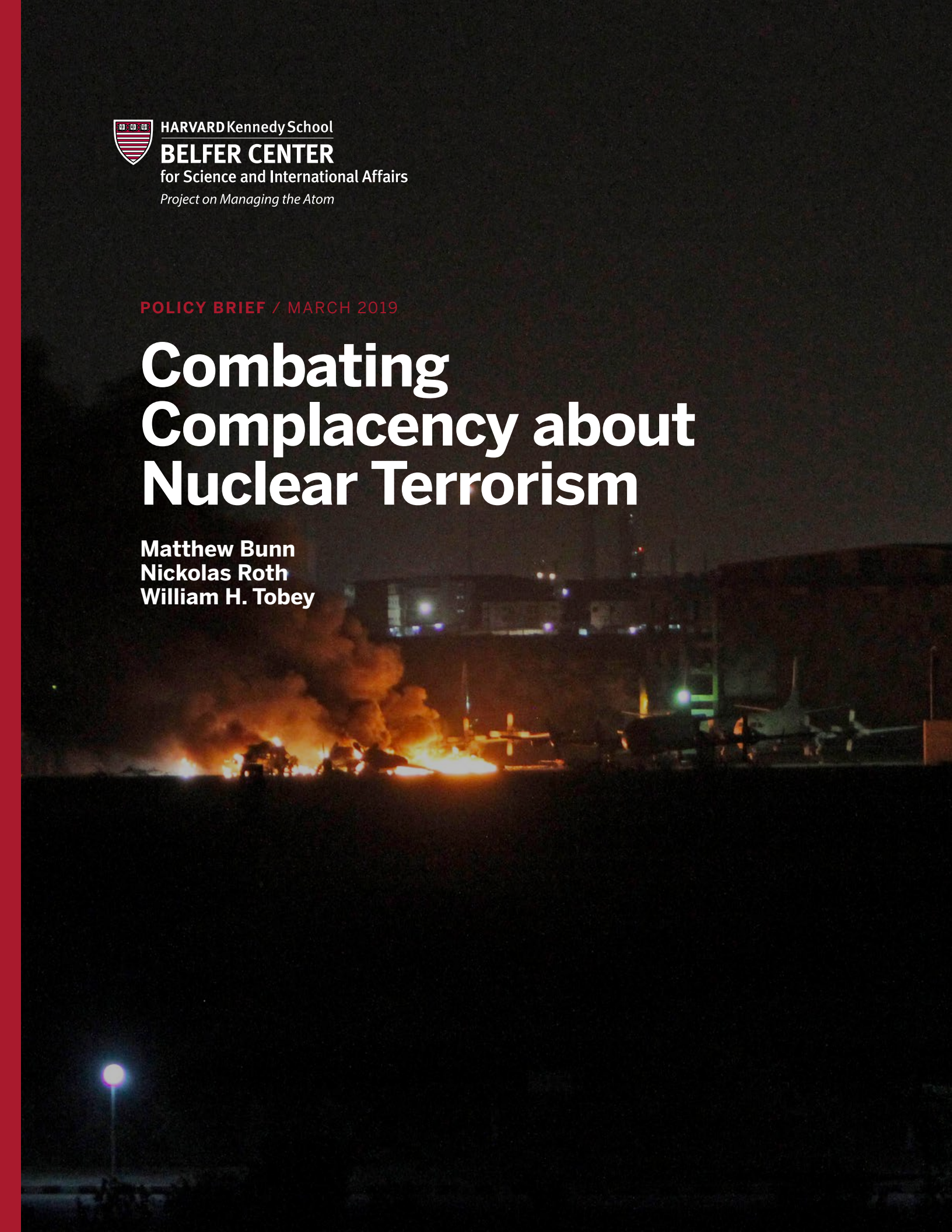
HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs
Project on Managing the Atom

POLICY BRIEF / MARCH 2019

Combating Complacency about Nuclear Terrorism

Matthew Bunn
Nickolas Roth
William H. Tobey



Combating Complacency about Nuclear Terrorism

Complacency about the threat of nuclear terrorism—the belief that nuclear and radiological terrorism threats are minimal and existing security measures are sufficient to address them—is the fundamental barrier to strengthening nuclear security.

Many factors can lead to complacency, but the most significant contributors are lack of knowledge about: events related to nuclear terrorism; weaknesses of nuclear security systems; and the capabilities demonstrated by thieves around the world. People will be more likely to take action to strengthen nuclear security if they believe that nuclear terrorism poses a real threat to their own country's interests and their actions can significantly reduce the threat. There have been many incidents in recent years that demonstrate the need for strong and sustainable security at both military and civilian nuclear facilities.

Have terrorists pursued nuclear weapons?[1]

Yes. Ambitious, well-financed, sophisticated terrorist groups employing apocalyptic rhetoric have sought nuclear weapons. The terrorist cult Aum Shinrikyo released sarin nerve gas in Matsumoto and in the Tokyo subway in 1995 and attempted to acquire both nuclear and biological weapons. Al Qaeda, whose leader declared acquisition of nuclear and chemical weapons to be a "religious duty," had a focused nuclear weapons effort that reported directly to Ayman al-Zawahiri (now the group's leader). This effort included repeated attempts to get nuclear material and recruit nuclear expertise and progressed as far as carrying out crude but sensible tests of conventional explosives in the Afghan desert. Chechen terrorists planted a stolen radiological source in a Moscow park as a warning, repeatedly threatened to sabotage nuclear reactors, and reportedly carried out reconnaissance on both nuclear weapon storage sites and nuclear weapon transport trains. So far, there is no public evidence of a focused Islamic State effort to acquire nuclear weapons, despite some hints, including video monitoring of the home of a top official of a Belgian nuclear research center.

Are nuclear theft or sabotage dangers hypothetical or real?[2]

There are over 20 publicly documented cases from 1992-2019 in which stolen plutonium or HEU has been seized. While none of these incidents involved quantities large enough to make a nuclear weapon, they constitute empirical confirmation of nuclear security failures resulting in loss of control of fissile material. Moreover, because in all but one of the cases the site from which the material was stolen has not been publicly confirmed, there can be no independent certainty that the leaks have been plugged (indeed in almost all of these cases it is not clear that the missing material was even noticed at the facilities from whence it came).

In some cases, the smugglers claimed the seized material was a sample of a larger quantity for sale. While many of these cases occurred in the 1990s, when nuclear security was undermined by the dissolution of the Soviet Union, governments in Europe also seized stolen HEU or plutonium in 2003, 2006, 2010, and 2011. The absence of publicly disclosed seizures for nearly eight years is encouraging, but it is too early to infer that the problem is solved.

There have also been cases of nuclear sabotage. Most recently, in August 2014, at the Doel-4 nuclear power reactor in Belgium, an unknown insider drained lubricant for the turbine and then rigged the valve so that it appeared to still be closed.[3] The turbine overheated and failed. There was never any danger of a radioactive release, but the cost of replacing the turbine and replacement power while the plant was shut down amounted to $100-$200 million, one of the largest acts of economic sabotage ever. A variety of other cases have occurred in the past—including a case where an insider brought explosives into a plant and detonated them on the steel pressure vessel head, and a case where armed terrorists overwhelmed site security guards.

Are nuclear security incidents still occurring?[4]

There have been many incidents in recent years demonstrating the need for strong and sustainable security at both military and civilian nuclear facilities.

- In 2012, explosives were found under a truck at the Ringhals nuclear power plant, the largest in Sweden. Fortunately, the explosives were not connected to a detonator.
- In 2014, a computer in the control room (though not one actually controlling the reactor) at Japan's Monju nuclear reactors was hacked.
- In October 2014 at the Madras Atomic Power Station in India, a nuclear security officer shot and killed three men and wounded two others using a sub-machine gun obtained from the facility's armory.
- In 2016, at Incirlik Air Base in Turkey, 70 miles from Syria, where U.S. nuclear weapons are reportedly stored, local authorities cut off power to the base and arrested the base commander and others for alleged participation in a coup attempt. Security concerns there are so high that spouses and children of U.S. personnel were ordered to leave, but the nuclear weapons remain.
- In 2017, the commander of U.S. Strategic Command, Gen. John Hyten, told Congress that recent incidents of unauthorized drones overflying both Navy and Air Force nuclear facilities "represent a growing threat to the safety and security of nuclear weapons and personnel."
- In 2017, the deputy director and Chief Engineer of Elektroprimbhor, one of the two remaining Russian nuclear weapon assembly and disassembly plants, were arrested for taking bribes amounting to millions of dollars.

What adversary capabilities should nuclear security systems protect against?[5]

Thieves and terrorists have used a wide range of tactics and capabilities in non-nuclear thefts and attacks around the world, including:

- Well-armed, well-equipped teams with military-style training and tactics and access to aerial vehicles such as drones or helicopters (e.g., the 2009 Vastberga cash depot heist in Sweden);

- Employing deception with fake uniforms, identification cards, or vehicles intended to resemble police or security vehicles (e.g., the 2017 Tambo Airport heist in South Africa, where a group of armed robbers wearing police uniforms, driving a car disguised as a police vehicle, and carrying "Airports Company South Africa" identification cards stole millions of dollars from the airport's "highly secure" cargo area);
- Use of prolonged intelligence collection, planning, and specialized tools and skills to overcome layered security (e.g., the 2003 Antwerp Diamond Center heist in Belgium and the 2015 Hatton Garden theft in London);
- Insider-outsider and insider-insider conspiracies (e.g., the 2004 Swissport Heathrow heist);
- Tunneling to bypass security systems (e.g., multiple prison breaks and bank robberies); and
- Cyber-attacks (including on nuclear facilities), including some in conjunction with physical thefts (e.g., a case in which pirates hacked a system to get data on which specific shipping containers on which ships they should steal from).

Recommendations to combat complacency[6]

Expose the threat. The U.S. government should prepare detailed reports and briefings on the threats of nuclear and radiological terrorism. (Other countries may want to prepare similar reports and briefings, to make clear that this is not an American-only concern.) These reports would include analyses of real terrorist efforts to get nuclear or radiological weapons; descriptions of real incidents of nuclear theft, smuggling, and sabotage; assessments of how difficult it would be for terrorists to overcome the key barriers to these types of terrorism; and descriptions of types of nuclear security vulnerabilities that must be addressed. Such reports and briefings should be prepared in varying levels of classification, for different audiences.

Establish regular sharing of incidents and lessons learned. Several steps should be taken to improve information-sharing about incidents relevant to nuclear security. First, as a pilot initiative, the U.S. government should prepare (or contract for) detailed open-source information on a set of incidents and lessons learned relevant to nuclear security policymakers and operators, which could be shared internationally. Second, each government with nuclear power plants or facilities handling HEU or separated plutonium should establish a mechanism for confidential sharing of incident information within its own country. Third, governments and the nuclear industry should work together to find an effective means for sharing this incident information internationally; each country should establish a means for reviewing the confidential reports developed for sharing within the country and editing for international sharing.

To the extent practical, each incident should be explored in depth, with analyses of the vulnerabilities that adversaries exploited to defeat security systems, and strengthened security measures that could prevent such incidents. Non-nuclear incidents that offer important lessons about the types of capabilities and tactics against which nuclear materials and facilities must be protected should also be included.

In nuclear safety, sharing of information on incidents and lessons learned is routine, and contributes enormously to ongoing improvement. For example, if there is a safety "near miss" at a U.S. nuclear power plant, the plant operator will analyze the incident, exploring its root causes and lessons learned from it. This information is shared through an industry group, the Institute for Nuclear Power Operations (INPO). Compiling information from many facilities, INPO analyzes trends and issues. It sends lessons learned reports to U.S. operators—and then inspects to see how well the facilities are implementing them. Nothing remotely comparable exists in nuclear security, nationally or internationally.

Secrecy makes sharing detailed security information more difficult than is the case for safety. But a great deal of information about incidents can be shared—particularly after the vulnerabilities that adversaries exploited have been fixed—without in any way compromising security. Secrecy has not prevented several industries from putting in place regular mechanisms for sharing detailed information on security incidents and lessons learned from them. Civil aviation, for example, has extensive measures for sharing such information. In the United States, for cybersecurity, in response to presidential Executive Orders, various industries have established "Information Sharing and Analysis Centers."

Conduct creative, realistic vulnerability assessment and testing. Few things do more to convince policymakers or managers that security needs improvement than seeing their security systems defeated—either in a vulnerability assessment in which analysts identify plausible ways to beat the system, or in a realistic test by mock adversaries. As major non-nuclear heists around the world repeatedly demonstrate, security systems that *look* quite impressive—thus contributing to complacency—can often be defeated by intelligent adversaries who find and exploit unnoticed weaknesses.

Conduct intelligence agency dialogues. States usually rely on their intelligence agencies to inform them about security threats. Hence, convincing intelligence agencies that nuclear and radiological terrorism are real dangers, and that existing nuclear security measures are not fully sufficient to address the threat, would be a major step toward combating complacency. The United States and other interested countries should direct knowledgeable teams from their intelligence agencies to conduct dialogues with other countries' intelligence agencies to build common understandings about the threat—and, where practicable, to undertake cooperative actions against the threat.

Notes:

1. See Matthew Bunn, Nickolas Roth, and William H. Tobey, *Revitalizing Nuclear Security in an Era of Uncertainty* (Cambridge, Mass: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, January 2019), www.belfercenter.org/NuclearSecurity2019, p. 33.
2. For more, see *Revitalizing Nuclear Security*, p. 26.
3. Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey, *Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?* (Cambridge, MA: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2016), p. 29.
4. For more, see *Revitalizing Nuclear Security*, pp. 27-28, 30, 60, 73.
5. For more, see *Revitalizing Nuclear Security*, p. 52.
6. For more, see *Revitalizing Nuclear Security*, pp. 158-166.

READ THE FULL REPORT:

"Revitalizing Nuclear Security in an Era of Uncertainty"

belfercenter.org/NuclearSecurity2019

READ THE FULL REPORT:

Revitalizing Nuclear Security in an Era of Uncertainty

belfercenter.org/NuclearSecurity2019

Project on Managing the Atom
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/MTA

Cover photo: A building at a Pakistani naval aviation base burns during an attack by a substantial group of well-armed, well-trained militants, apparently with insider help, in May 2011. Nuclear weapons and materials must be protected against comparable adversary capabilities and tactics.
(AP Photo/Shakil Adil)