PROTECTING NUCLEAR MATERIALS AND FACILITIES AGAINST THE FULL SPECTRUM OF PLAUSIBLE THREATS

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

N. ROTH
Project on Managing the Atom, Harvard Kennedy School
Cambridge, Mass., USA

W. H. TOBEY
Belfer Center for Science and International Affairs, Harvard Kennedy School
Cambridge, Mass., USA

Abstract

Reducing the risk of theft of nuclear materials or sabotage of nuclear facilities to an acceptable level requires protecting them against the full spectrum of capabilities and tactics that adversaries might plausibly use to accomplish their objectives. International recommendations and requirements call for nuclear security systems to provide appropriate and effective protection against the state's evaluation of the threat. This inevitably requires a balance. On the one hand, states must ensure that all weapons-usable nuclear material and high-consequence nuclear facilities are effectively protected against real threats, but on the other, no one wants to waste money or impose undue inconvenience in protecting against unrealistic dangers. The problem is complicated by the fact that adversaries learn, adapt, and change, making the past a less reliable guide to the future. The paper proposes two complementary approaches to address this problem. First, states should examine real incidents of theft from or attacks on secured facilities, both nuclear and non-nuclear, to learn lessons about the types of capabilities and tactics adversaries have shown they can use. Intelligence information, information provided by other states or by international organizations, and open-source information can all be helpful in such an examination. Second, a strong case can be made that no state is so safe that it can afford not to protect against a common baseline level of threat that includes a modest group of well-armed and well-trained outsiders, capable of operating as more than one team; a well-placed insider; and both the outsiders and the insider working together. Having put such requirements in place, states should also put in place effective mechanisms for assessment and realistic testing to ensure that their security systems can defend against intelligent adversaries determined to defeat them.

1. INTRODUCTION

Reducing the risk of theft of nuclear materials or sabotage of nuclear facilities to an acceptable level requires protecting them against the full spectrum of capabilities and tactics that adversaries might plausibly use to accomplish their objectives. This inevitably requires a balance. On the one hand, states must ensure that all weapons-usable nuclear material and high-consequence nuclear facilities are effectively protected against real threats, but on the other, no one wants to waste money or impose undue inconvenience in protecting against unrealistic dangers. The problem is complicated by the fact that adversaries learn, adapt, and change, making the past a less reliable guide to the future.

The paper reviews international legal obligations and recommendations that highlight the need to provide effective protection against the state's evaluation of the threat; outlines approaches states can use to develop that evaluation, learning lessons about potential adversary capabilities and tactics from real incidents of theft from or attacks on secured facilities, both nuclear and non-nuclear; proposes a common baseline level of threat that all nuclear weapons, weapons-usable nuclear materials, and high-consequence nuclear facilities should be protected against; outlines approaches for assessing and testing whether nuclear security systems are effective enough to counter such threats; and describes approaches to international cooperation to strengthen the effort to put in place security systems intended to protect against the full spectrum of plausible adversary threats. Overall, the paper provides a more detailed analysis of one of five key areas of nuclear security outlined in a previous paper [1].

2. EXISTING INTERNATIONAL RECOMMENDATIONS AND REQUIREMENTS

Both legally binding international requirements and international recommendations address the issue of protecting nuclear materials and facilities against plausible adversary capabilities and tactics. At the broadest level, UN Security Council Resolution 1540 obligates all states to provide "appropriate effective" security, physical protection, and accounting for all nuclear weapons and related materials [2]. To truly be "appropriate" and "effective," a security system should provide effective protection against all the various types of adversary theft attempts that might plausibly occur in the country where a particular stock of nuclear weapons or related materials are located.

The amended Convention on the Physical Protection of Nuclear Materials and Facilities is somewhat more specific. In Fundamental Principle G, the Convention obligates states to provide protection against nuclear theft and sabotage based "on the State's current evaluation of the threat" [3]. This presumably means that the security systems should be able to protect against the full set of adversary threats that the relevant state believes exist and that this assessment should be kept up to date. Elaborating further on this thought, INFCIRC/225/Rev. 5 recommends that states establish a "design basis threat" (DBT) to be used for designing and evaluating systems to prevent nuclear theft and sabotage; that states base this DBT on a regularly updated assessment of the threat, using all available credible information; and that they design and maintain their physical protection systems to provide enough protection against the adversaries included in the DBT to maintain acceptable levels of risk [4]. As this is a fundamental element of the IAEA's nuclear security recommendations, it is part of the commitment states make in joining the Strengthening Nuclear Security Implementation Initiative (INFCIRC/869) [5].

3. LESSONS ON ADVERSARY CAPABILITIES AND TACTICS FROM INCIDENT INFORMATION

How can states judge what particular types of capabilities and tactics to include in their DBTs (or in their threat assessments, if that is what they use for activities such as protection of radiological material)?

As a first step, states should examine real incidents of theft from or attacks on secured facilities, both nuclear and non-nuclear, to learn lessons about the types of capabilities and tactics adversaries have shown they can use. Intelligence information, information provided by other states or by international organizations, and open-source information can all be helpful in such an examination. States should consider developing a regularly updated database of such incidents and lessons learned from them. First priority in such an examination should go to incidents within the state itself, but incidents in nearby countries and elsewhere in the world should not be ignored.

Real incidents can offer hard data on a wide range of factors. How many attackers have been involved? What kind of skills and training have they had? To what extent do insiders work with outsiders? What kind of tactics have adversaries used to defeat security systems? What kinds of skills, weaponry, vehicles, and equipment have adversaries used? Have the adversaries been willing to use violence? Have they been willing (or even eager) to die themselves, as in the case of suicide bombers?

Consider, for example, the 2009 Västberga cash depot heist in Sweden [6]. A gang with automatic weapons, specialty equipment, and explosives landed on the top of the building in a helicopter. They smashed through the ceiling window, came down by ladder, overpowered the employees on duty, opened the vault with explosives, removed the cash, returned to their helicopter, and flew away. They had spread metal spikes known as "caltrops" on the road around the building to delay the arrival of police vehicles, and placed a package that appeared to be a bomb (though it was not an explosive) at the police heliport to delay the arrival of police helicopters. In short, the gang included a substantial number of attackers; military-style tactics, training, and weaponry; a helicopter to fly over security measures and to escape; apparently some intelligence on the facility and its security arrangements; and actions to impede off-site response forces.

This is quite a challenging level of adversary capability for security systems to protect against. Yet Sweden would certainly not be on anyone's list of especially high-threat countries. Indeed, in this case, much of the gang traveled to Sweden from Serbia, nearly a continent away. Hence, in preparing their assessments of potential adversary capabilities, states need to look beyond events that have occurred in their own country.

The Västberga case is not known to have involved insiders within the facility. But many thefts from heavily guarded facilities (and terrorist attacks) do involve help from insiders [6]. Insider threats are particularly challenging for organizations to address, as insiders are trusted, may have authorized access to the secure areas of a

facility, may know the facility's security system and its weaknesses, can induce others unwitting of the threat to bend or circumvent rules, and could potentially spend months or years planning. Nearly all real cases of theft of weapons-usable nuclear materials or sabotage of nuclear facilities where the circumstances of the incident are known involved insiders [7]. Indeed, examination of insider thefts from secured non-nuclear facilities in recent years suggests that multiple insiders working together is also a plausible threat; states should give increased attention to the difficult problem of protecting against multiple insiders [6].

Deception – used to get through the initial layers of security, or delay or confuse the security response – is also often a key element of major thefts from or attacks on heavily guarded facilities. The recent theft of millions of dollars from Tambo airport in South Africa, for example, reportedly involved a dozen or more attackers dressed as police officers and driving fake police vehicles [8]. (Though the investigation is still underway, this theft apparently also involved insider help.)

Cyber intrusions are also becoming increasingly common in non-nuclear thefts. Nuclear security planners must plan for the possibility of combined cyber and physical thefts and assaults. Conceptually, cyber means can be used to undermine all of the principal nuclear security measures—physical protection, material control and accountability, and personnel reliability programs. For example, cyber means could be used to disable key elements of physical protection systems (which are now increasingly digital); to alter nuclear material accounting and control records; to turn off key intrusion detection systems; to create false alarms and with them complacency; to sabotage facilities; to alter personnel records, and more. Increasingly, cybersecurity is being recognized as a fundamental part of effective nuclear security [9]. Fortunately, considerable collecting and sharing of cyber threat information is already taking place, in a number of industries. In the United States, for example, Information Sharing and Analysis Centers (ISACs) have been established for firms in a range of economic sectors, from finance to software.

Some promising work in recent years has helped countries develop design basis threats (DBTs) or threat statements drawing on such incident information, including open-source information [10]. In addition to using such information to support regulatory decisions on the types of adversary capabilities and tactics nuclear materials and facilities should be protected against, states should make information about incidents and lessons learned available to operators, to help them understand the threat environment and strengthen their motivation to provide effective security. In 2003, for example, a Russian court case revealed that a Russian businessman had been offering $750,000 for stolen weapon-grade plutonium for sale to a foreign client, and had made contact with two people from the closed nuclear security of Sarov, who promised to steal the plutonium for him. (Fortunately for the world, the two were scam artists [11].) At the time, $750,000 was approximately a century of the average Russian's salary. If such a sum is being offered for stolen plutonium, that would seem to be something nuclear security managers should know about; yet the authors have rarely encountered Russian nuclear security managers who were aware of this incident.

In addition to information about the tactics and capabilities of adversaries, incident information and lessons learned should include information on particular vulnerabilities that were exploited in past incidents (so operators can avoid leaving similar vulnerabilities in their systems) and the actions taken to prevent a recurrence (so operators can take similar actions). It is important to distribute information to operators on vulnerabilities in widely-used systems, so the operators can find and fix those vulnerabilities in their own operations. For example, after the September, 11 attacks in the United States, the U.S. Department of Energy (DOE) distributed a film, "Systems Under Fire," which detailed potential vulnerabilities to weapons such as armor-penetrating rocket-propelled grenades; high-caliber armor-piercing rounds; and "Bangalore torpedoes" (tubes filled with explosive) slipped under fences. The intent was to ensure that security managers at DOE's sites were aware of these vulnerabilities and took action to address them [12].

Of course, some information about incidents – and particularly about potential vulnerabilities of security systems – is secret or highly sensitive. But it should be possible to find arrangements to share such information between a national government and nuclear operators and others with key roles in nuclear security within that country. Lessons based on analysis of open-source incidents should be possible to share more broadly.

Unfortunately, in dealing with intelligent adversaries who learn, change, and react to their perception of what they need to overcome changing defenses, the past is not always a reliable guide to the future. Information from incidents that have already occurred should be only a starting point for analysis, not the end. For example, the number of attackers adversaries have used in past assaults may simply reflect the number they judged were needed to accomplish their objectives; they might use more in the future, if they judged more were needed, and if they judged that they could organize a larger attack without being detected in advance by intelligence and law

enforcement agencies. States should regularly scan the horizon for emerging threats, and use "red teams" working from an adversary point of view and other techniques to assess the credibility of new tactics and capabilities not yet included in their DBT or threat statement.

4. PROTECTING AGAINST A COMMON BASELINE THREAT

Clearly, plausible adversary threats vary from one part of the world to another, and each state with major nuclear activities needs to make its own assessment of the capabilities and tactics against which nuclear operations in its country should be protected. Nevertheless, in a world in which both terrorists and criminals are increasingly globally networked, no state is so safe that it can afford not to protect weapons-usable nuclear materials and major nuclear facilities against a common baseline level of threat. (The Västberga heist, with criminals from Serbia striking in Sweden, is just one example of a broader phenomenon.) Anywhere in the world, a modest group of well-armed and well-trained outsiders, capable of operating as more than one team; a well-placed insider; and both the outsiders and the insider working together are plausible threats that weapons-usable nuclear materials and major nuclear facilities should be protected against. Cyber threats, including the use of cyber assaults to compromise or confuse security systems to facilitate a physical theft or assault, should also be included in such a common baseline.

Today, there is no international agreement or recommendation that establishes any such common baseline level of threat that all such materials and facilities should at least be protected against, even at the broad level of generality described above. As a result, DBTs vary significantly from country to country – and unfortunately, nuclear security experts in several countries with weapons-useable materials dismiss as implausible adversary capabilities and tactics that have already been demonstrated in thefts from and attacks on non-nuclear facilities [13].

Protection at least against such a common baseline threat might be achieved through individual state decisions – in some cases, decisions that resulted in part from discussions and cooperation with other states. Or, as discussed below, nations could join together and outline a common baseline, pledging that they would ensure that their weapons-usable nuclear materials and major nuclear facilities were effectively protected against it.

Of course, some countries have more capable terrorists or thieves operating on their soil than other countries do. For example, a nuclear security system capable of reducing the risk of nuclear theft to a very low level in Canada might not be remotely adequate in Pakistan, where both outsider and insider threats are far more substantial. Hence, any common baseline should be a floor, not a ceiling; where needed, states should provide protection going well beyond the baseline. The existence of an agreed-upon baseline that security measures should not fall below would not relieve states of the burden of assessing the actual security environment in their own country and region.

In short, all states using weapons-usable nuclear materials or operating nuclear facilities whose sabotage could cause unacceptable consequences should protect these materials and facilities against at least a baseline level of threat – and states whose assessment suggests that they face higher levels of adversary capability should protect against still more substantial levels of adversary capability [14].

5. INTERNATIONAL COOPERATION TO ENSURE PROTECTION AGAINST THE FULL SPECTRUM OF ADVERSARY TACTICS AND CAPABILITIES

Though each state needs to make its own sovereign decisions about nuclear security, international cooperation – bilateral, regional, among groups of like-minded states, and fully international – can help achieve the goal of ensuring that all nuclear weapons, weapons-usable nuclear materials, and high-consequence nuclear facilities are effectively protected against the full spectrum of plausible threats in the location where they exist. Indeed, international initiatives from bilateral cooperation to nuclear security summits to activities of the IAEA Division of Nuclear Security have done a great deal to strengthen nuclear security around the world and build international consensus that the threat of nuclear terrorism is real and that nuclear security is a critical element of reducing the risk.

As noted above, international agreements and recommendations already highlight the need for states to provide appropriate and effective protection against their assessment of the threats that exist in their country – though existing instruments do not outline any common baseline of what such DBTs or threat statements should include. Is there room for a next step in this direction?

What is needed is an agreed set of principles specific enough to be meaningful, but broad and flexible enough to permit each country to implement nuclear security in its own way [15, pp. 100-102]. For better or worse, the experience of the decades required to negotiate the amendment to the physical protection convention and bring it into force makes clear that governments will not negotiate a treaty establishing stringent nuclear security principles in the near term. A political commitment to a set of nuclear security principles by a group of like-minded states might be a more plausible approach. Such a commitment could potentially be worked out in experts' meetings of the permanent five members of the UN Security Council, within the Nuclear Security Contact Group (or a subgroup within it), by a new working group of the Global Initiative to Combat Nuclear Terrorism (GICNT), or in a new grouping established for this purpose. The initial participating states (which should begin with states with substantial stocks of weapons-usable nuclear materials) could invite all other states with plutonium, HEU, or high-consequence nuclear facilities on their soil to join them in the commitment, and offer help to those countries wishing to implement the principles but needing technical or financial help to do so.

The initial participants in such a commitment would have to work out what the specific principles would be. One approach would be to look to the goals in areas such as physical protection, material control, and material accounting that Russian and U.S. experts agreed to work toward in their technical cooperation [16]. The most fundamental element of such a set of principles should be a commitment to require facility operators and transporters to protect nuclear weapons, HEU, separated plutonium, and high-consequence nuclear facilities against the full range of adversary capabilities and tactics their national security agencies judge to be plausible—including, at a minimum, the kind of baseline threat described above. Such an initiative would be a substantial complement to INFCIRC/869, offering significantly stronger nuclear security commitments and clearly extending to both military and civilian stocks.

There are important obstacles to international cooperation to put in place such a common baseline DBT. Secrecy is one of the biggest barriers. States keep the specifics of the threats they are planning to defend against secret, so as not to alert adversaries to what they might be up against. In some cases, states that were closely cooperating on nuclear security have been able to share at least general DBT information. In others, new agreements would probably be required to provide a legal basis for exchanges in this area. In still others, it might be possible for states to join in the common commitment without providing any sensitive information about their specific approach to delineating the DBT, and which aspects of their domestic DBT might go beyond the common baseline.

Some may argue that a widely known common baseline DBT could give adversaries a target to plan against, but two factors mitigate that risk. First, as noted above, any common commitment should be expressed in general terms, and described as a floor – with substantial variation above the floor among the participating states. Second, if the most severe dangers involve the cooperation of an insider, the adversaries would presumably have even more detailed information about the security system they had to defeat

The participants in such an initiative should also explore means by which they could build confidence that they were fulfilling their commitment to the agreed principles without revealing sensitive information. Particular elements of such an approach could include review of their security arrangements by international experts, or sharing of information on particular elements of their approach. If other countries knew that a country required operators to protect nuclear weapons, HEU, separated plutonium, and high-consequence nuclear facilities against a robust range of potential adversary threats; understood the inspection and testing program used to confirm that operators were meeting these requirements; knew that a large fraction of the facilities had been shown in inspections to meet these standards; and understood that thorough and effective corrective actions were taken in response to any weaknesses identified, this could increase confidence in nuclear security substantially [15, pp. 124-127].

Essentially all states participating in international nuclear security discussions would want the IAEA to have a central role in helping to implement such an initiative. Once the initial principles had been worked out, they could be memorialized in an INFCIRC open to all states, as was done with the initiative that became INFCIRC/869. The IAEA could then play a role, at states' request, in helping to implement the agreed principles, conducting reviews, and the like. For defense-purpose materials, it seems very likely that states would not want the IAEA to play such roles; various forms of bilateral and small-group cooperation might contribute to what would primarily be national implementation.

6. ENSURING THAT NUCLEAR SECURITY SYSTEMS WILL PERFORM AS REQUIRED

It is one thing to establish requirements for certain levels of nuclear security performance; ensuring that the nuclear security systems in place are really meeting those standards is another thing entirely. Many systems appear highly secure – with fences, barriers, armed guards, and the like – but in fact can be readily defeated by intelligent adversaries who study the system to find its weaknesses. For example, the theft of tens of millions of dollars of jewels and other valuables from the Antwerp Diamond Center in 2003 occurred despite a security system in place that appeared to many to be impregnable [17]. Hence, states should put in place effective mechanisms for assessment and realistic testing to ensure that their security systems really can defend against people looking for clever ways to defeat them.

Here, too, the issue is already the subject of IAEA recommendations (and hence is part of states' INFCIRC/869 commitment to carry out the intent of IAEA recommendations). INFCIRC/225/Rev. 5 recommends that nuclear operators have quality assurance programs to ensure that security systems can effectively protect against the DBT. Further, it recommends that these programs should include force-on-force exercises conducted at least annually [4]. To be genuinely effective, other key elements of a quality assurance programs should include:

- Making sure that force-on-force exercises are as realistic as possible, within safe parameters, including realistic tests of the system's ability to defend against intelligent adversaries (insiders and outsiders) trying to find ways to defeat it.
- Establishing "red teams" whose job is to find security vulnerabilities and propose solutions. These teams should include individuals with a creative, "hacker" approach. They should have incentives to find vulnerabilities, and protected from potential organizational backlash. (Such "red teams" are already in widespread use in cybersecurity, but are less common in nuclear physical protection or material control and accounting.
- Conducting "tabletop" exercises, computer simulations, and brainstorming workshops to identify and assess tactics adversaries might use.

Of course, operating organizations must take action to address weaknesses identified in such vulnerability assessments and performance testing. The IAEA should develop guidance and advisory services for states on how to conduct such tests, as well as realistic tests of protections against insider threats.

Such realistic assessments and tests are important not only for identifying weaknesses to be corrected but also in building confidence that the security in place really is effective – and in overcoming complacency when more needs to be done. In the U.S. case, for example, embarrassing failures in nuclear security inspections or tests—often followed by Congressional investigations—have repeatedly driven action to strengthen nuclear security, convincing senior policymakers that additional security steps really were needed, and were not just the wish lists of security managers. Nothing is quite so convincing in countering the complacent view that a site's security measures are impregnable as a test in which mock adversaries manage to defeat them.

One particular issue, if the state's rules assign some responsibilities to nuclear operators and others to local response forces or the state, is to ensure that all relevant parties can fulfill their respective responsibilities. Each of the relevant organizations should conduct regular exercises to test its abilities, and where cooperation is needed among different organizations, there should be regular joint exercises to ensure this cooperation works in practice. In the United States, for example, U.S. Nuclear Regulatory Commission rules require operators to provide protection against the regulatory DBT, and give the state the responsibility to handle beyond-DBT threats. The operators' security programs are tested by both inspections and force-on-force exercises. But the state's ability to carry out its supplementary responsibilities is rarely if ever subject to exercises and tests.

For these reasons, the IAEA, the United States, and other interested parties should work to convince as many as possible of the countries with nuclear weapons, HEU, separated plutonium, or high-consequence nuclear facilities to carry out regular, realistic tests of both their protection against insider thieves and their protection against outsiders trying to break in. Such exercises should be included in the commitment to stringent nuclear security principles suggested above, and should be a focus of nuclear security technical cooperation programs (which should include allowing experts from other countries to observe such exercises where appropriate).

7. CONCLUSIONS

Nuclear security is only as strong as its weakest link, both within a facility and among states. Ensuring that all nuclear weapons, weapons-usable nuclear materials, and high-consequence nuclear facilities are effectively and sustainably protected against the full spectrum of plausible adversary tactics and capabilities is fundamental to reducing the risk of nuclear terrorism. Reaching that goal will require action by both national governments and nuclear operators – and can be facilitated by international cooperation. States have an obligation to take effective action to ensure that the world never has to live through the day after a nuclear terrorist attack.

REFERENCES

[1] BUNN, M., MALIN, M.B., ROTH, N., TOBEY, W.H., "Key steps for continuing nuclear security progress," CN-244-574, International Conference on Nuclear Security: Commitments and Actions (Proc. Int. Conf., Vienna, Austria, 2016), International Atomic Energy Agency, Vienna (2016).
[2] U.N. Security Council Resolution 1540 (New York: United Nations, 2004).
[3] Convention on the Physical Protection of Nuclear Materials and Facilities, INFCIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016).
[4] Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities, INFCIRC/225/Rev.5, IAEA, Vienna (2015).
[5] Communication Received from the Netherlands Concerning the Strengthening of Nuclear Security Implementation, INFCIRC/869, IAEA, Vienna, 2014.
[6] LAFLEUR, J; PURVIS, L.; ROESLER, A., The Perfect Heist: Recipes from Around the World, SAND-2014-1790, Sandia National Laboratories, Albuquerque, N.M. (2014).
[7] BUNN, M., SAGAN, S.D., eds., Insider Threats, Cornell, Ithaca N.Y., 2017.
[8] GRAHAM, S., "Robbers 'Dressed as Police' in Multi-Million Pound Heist at Johannesburg Airport, The Telegraph, 8 March 2017.
[9] International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange (Proc. Conf. Vienna, 2015), IAEA, 2016.
[10] EK, D., "Pilot approach to develop a DBT-like threat statement from open source data," International Conference on Nuclear Security: Commitments and Actions (Proc. Int. Conf., Vienna, Austria, 2016), International Atomic Energy Agency, Vienna (2016).
[11] "Plutonium con artists sentenced in closed city of Sarov," NIS Export Control Observer, November 2003.
[12] Systems Under Fire (film), U.S. Department of Energy, Washington, D.C., 2003.
[13] BUNN, M., HARRELL, E., Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey, Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, Mass. (2014), pp. 22-23
[14] BUNN, M., MASLIN, E.P., All stocks of weapons-usable nuclear materials worldwide must be protected against global terrorist threats, *J. Nucl. Mater. Mngmt.,* **39**, 2 (Winter 2011), 21-27.
[15] BUNN, M., MALIN, M., ROTH, N., TOBEY, W., Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline? Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, Mass. (2016).
[16] TOBEY, W.H., Building a Better International Nuclear Security Standard, U.S.-Korea Institute, Johns Hopkins University School of Advanced International Studies, Washington, D.C., 2012.
[17] SELBY, S.A., CAMPBELL, G., Flawless: Inside the Largest Diamond Heist in History, Union Square Press, New York (2010).