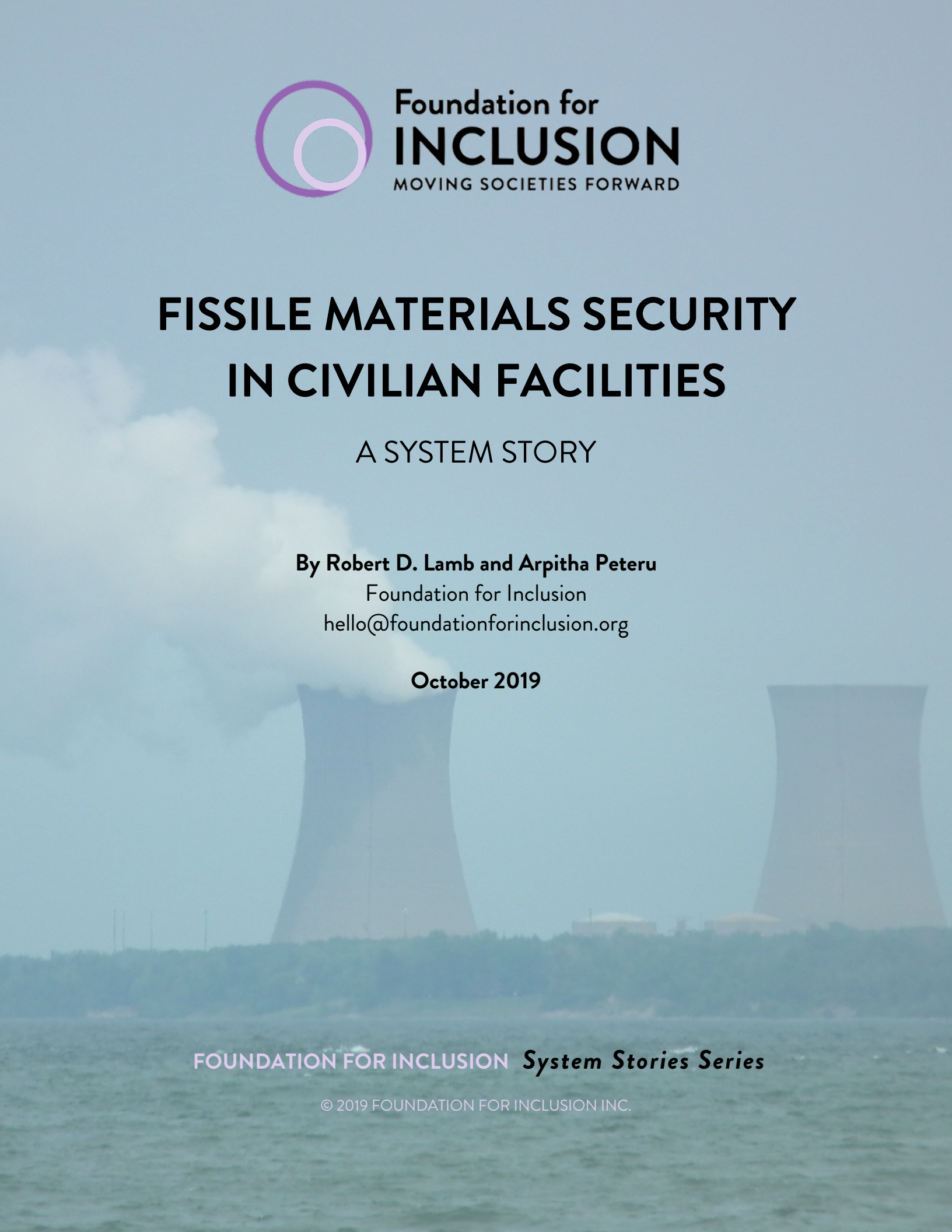


Foundation for INCLUSION
MOVING SOCIETIES FORWARD

FISSILE MATERIALS SECURITY IN CIVILIAN FACILITIES

A SYSTEM STORY

By Robert D. Lamb and Arpitha Peteru
Foundation for Inclusion
hello@foundationforinclusion.org

October 2019

FOUNDATION FOR INCLUSION *System Stories Series*

TABLE OF CONTENTS

COVER IMAGE: Perry Nuclear Power Plant (Erik Drost)
flickr.com/photos/edrost88/7284006342

FOREWORD

Human institutions and the people who manage them make and implement decisions based on a wide variety of considerations, some rational, some habitual, some instinctive.

Civilian institutions that use fissile materials for energy, propulsion, medical devices, and research are no different. Around the world, these facilities are subject to a wide range of regulations regarding safety, security, and accountability, and some have adopted practices that go beyond what is legally required.

But there has long been a concern that too many facilities are not adequately protected against theft or sabotage by terrorists and criminals or against diversion into military nuclear-weapons development programs. And while there are ongoing discussions about how to improve nuclear security, many experts remain concerned that key vulnerabilities are not being adequately addressed quickly enough.

Governmental and nongovernmental organizations that advocate for improved nuclear security have traditionally focused considerable attention on the development and advocacy of global standards and their implementation at the national level, an approach that has been effective in a number of key areas of concern. But in recent years, as globalism is increasingly displaced by a resurgent nationalism, progress toward a more effective global system of nuclear governance has slowed considerably—and collective efforts have largely stalled.

Nuclear security advocates and facilities face a wide range of different challenges to making and implementing decisions that would improve nuclear security beyond the status quo. Those challenges emerge from interactions between so many factors—financial incentives, social pressures, information, norms, etc.—that some believe a new approach might be needed just to make sense of that complexity.

To that end, Nancy Gallagher and Jonas Siegel of the Center for International and Security Studies at Maryland (CISSM) commissioned us to map out the complexities involved in the effort to

achieve nuclear security, suggesting we focus on the barriers to fissile materials security as a way of bounding the problem.

Our organization was founded to help coalitions and organizations overcome the complexities involved in their efforts to solve very challenging global problems, such as human trafficking, climate inaction, and declining economic mobility. We approach this work using multidisciplinary tools designed for understanding and influencing complex systems. Our goal is to help our partners identify and activate effective, self-sustaining strategies.

CISSM was interested in seeing how our approach could be applied to enhancing nuclear security. This report presents the results of our scoping work on this topic. In the future, CISSM hopes to build on this analysis to cover all aspects of nuclear governance and show how different types of nuclear risk reduction efforts could be used in mutually reinforcing ways.

In addition to presenting our initial findings on the complexities of nuclear security advocacy, this report also represents the first official publication of the Foundation for Inclusion's *System Stories Series.* It is common among systems practitioners to present the results of their scoping research in the form of system maps—visual charts showing how all relevant factors affect each other. (Subsequent phases turn system maps into simulations that let stakeholders *interact* with such knowledge.) But system maps can be difficult to read and comprehend. So for our scoping work we prefer to present our results in simplified charts portraying only the most important dynamics, with labels showing "system stories" and "subplots."

- *System stories* are the main research findings that explain, at the system level, why a problem persists—usually because one or more feedback loops make the problem self-perpetuating.

- *Subplots* are factors—often overlooked—that influence some aspect of those feedback loops and that therefore have the potential to help break the cycle and contribute to self-sustaining solutions.

We have found this approach to be an effective early stage in a broader effort to rigorously test different potential solutions across a wide range of scenarios and uncertainties (e.g., through participatory research and complex-system simulation modeling).

We would like to thank Nancy and Jonas of CISSM for their support and guidance and the Yamamoto Fund for its financial support. We had fruitful conversations as well with Laura Holgate, Roger Howsley, Kingston Reif, Sara Kutchesfahani, and Andrew Semmel, and we are grateful to them for their time and feedback. Any errors of fact or interpretation are our own. For more information about the Foundation for Inclusion or the *System Stories Series,* please contact us at hello@foundationforinclusion.org.

—Bob Lamb and Arpitha Peteru
September 2019

1. INTRODUCTION

RADIATION

In 1985, a private radiotherapy clinic in the city of Goiânia in Goiás, Brazil, was relocated, but much of its equipment was left behind, including a therapy unit that used cesium-137 (Cs-137) as its radiological fuel. Two years later, the abandoned unit was stolen for scrap. The thieves who dismantled it, enchanted by the glowing blue substance they found inside, showed it off to family and friends before selling the remaining scrap to another dealer. By the time a family member realized the glowing substance was making people sick and turned it in to local authorities, thousands of people had been exposed to radiological contamination, with dozens suffering effects ranging from nausea to amputation. Four people died of radiation poisoning. It was one of the worst nuclear accidents ever to emerge from a civilian source of radiological materials.[1]

One decade later, the leader of the Chechen rebel movement publicly announced a capability to produce a radiological dispersal device,[2] at one point telling a television network he had buried a container of Cs-137 in a public park in Moscow. Despite repeated threats, Chechen rebels never detonated it. When authorities found the Cs-137 container in Izmailovskiy Park, it was wrapped in explosives—probably the closest the world has ever come to an intentional attack via radiological dispersal, in this case a so-called dirty bomb. But other extremist organizations have expressed interest in or attempted to assemble the materials for a dirty bomb or to sabotage nuclear power plants in the hope of having the same effect.[3]

While the source of radiation in both of these cases was Cs-137 that had previous been used for legitimate civilian purposes, Cs-137 is neither the only nor the most dangerous source of radiation in use by civilian institutions worldwide. Cobalt-60 (Co-60), iridium-192 (Ir-192), radium-226 (Ra-226), and other radioactive isotopes are commonly used for cancer therapy, food irradiation, industrial gauges, industrial radiography, radioisotope thermoelectric generators (heating devices), radiological research, and well logging (analysis of boreholes). All have legitimate civilian purposes, and any of them would put public safety at risk in an incident of theft or accidental dispersal.

Fissile Materials

None of these radiological elements, however, can be used to create nuclear energy. That requires fission of an isotope of either uranium (U-235) or plutonium (Pu-239) or a blend of both in oxide form called mixed oxide (MOX) fuel.[4] These fissile materials, including low-enriched uranium (LEU, a fuel containing only 3–5 percent of U-235), can be used for nuclear energy generation and in research laboratories (e.g., to produce neutrons). But only Pu-239 and highly enriched uranium (HEU, a fuel with 20 percent U-235 or more) can be used to make a nuclear weapon. These fissile materials—Pu-239, LEU, HEU, and MOX—are also much more powerful sources of radiation than the radiological materials mentioned in the opening paragraphs. That makes them efficient sources of radiation for energy (power plants, research and test reactors), propulsion (ice breakers), and the production of medical isotopes (imaging, radiotherapy). But it also makes them more attractive targets for sabotage and theft for terrorist purposes or for diversion into nuclear weapons programs, all of which pose a threat to public safety.

Are civilian facilities and transportation services around the world adequately securing the fissile materials under their control?

Believing they were not, the United States invited other states to participate in the first of a series of four biennial Nuclear Security Summits (NSS) in 2010 with the purpose of helping states lower the risk of nuclear terrorism by reducing and securing civilian fissile materials. The nuclear industry hosted a series of official side events, the Nuclear Industry Summits (NIS), with the same general objectives, but involving industry leaders rather than government officials. Nongovernmental organizations (NGOs) focusing on nuclear-security issues organized similar events.

The main accomplishments of the NSS series centered around actions undertaken by participating states (and some others) that secured HEU by converting HEU reactors to LEU reactors, moved unused HEU stocks or spent fuel into more secure facilities, downblended HEU to LEU (i.e., reduced the percentage of U-235), destroyed plutonium stocks, repatriated unused HEU stocks and spent fuel to countries where it could be stored securely, purchased excess HEU and converted it to LEU for use in civilian energy, and passed national laws and changed certain practices to strengthen nuclear and radiological security and prevent smuggling. Some observers celebrated the summits for introducing the innovation of "gift baskets" (voluntary commitments), a practice that was replicated to some success at the climate action talks in Paris in 2015.[5]

But these accomplishments, while important, were the "low-hanging fruit" of nuclear security.[6] Multidimensional problems usually have a range of "fixes," some easier to implement than others. As the easier fixes are implemented, the average difficulty of the remaining ones increases. Even successful strategies eventually fail, because there are diminishing returns on success. In an international system dominated by a few powerful states, small states can be pressured to downblend or repatriate HEU, for example. Over time, however, HEU stocks will remain mainly in states with just enough power to resist pressure. At the facility level, the low-hanging fruit was for facility managers to hire security teams to help them comply with security regulations. Getting them to convert HEU reactors to LEU reactors is a tougher sell when customers don't demand it and owners don't see a business case for investing in conversion.

The final Nuclear Security Summit in 2016 ended with far more commitments than accomplishments, and the more difficult goals of the NSS series remain far from having been achieved.

It had been expected that, after the four planned summits, the five key international organizations with authority over some aspect of nuclear security—the International Atomic Energy Agency (IAEA), the United Nations (UN), the International Criminal Police Organization (Interpol), the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (GP), and the Global Initiative to Combat Nuclear Terrorism (GICNT)—along with the nuclear industry would gather for lower-level summits after 2016. But that has not happened.[7]

With the rise of anti-globalist leaders and populist movements worldwide, there is little likelihood that a high-level multilateral approach of any sort will be launched in the near future.[8]

Moreover, the NGOs that monitored the summits and advocated for specific issues to be addressed in the agendas have lost some of their collective energy since the summits ended.

For example, the Fissile Materials Working Group (FMWG) is a global coalition that was founded as a coordinating body on nuclear security issues on behalf of about 80 NGOs worldwide. During the summits it took a leading role in monitoring, agenda-setting, and tracking the commitments made by the 53 states participating in the summits. At the final summit, it recommended that, to continue the summit's momentum, participating states should prioritize the elimination of HEU from civilian applications, prioritize the security of

military nuclear materials, improve information sharing on standards and best practices, and encourage the strengthening of security culture at the international and national levels.[9]

The FMWG, its network of NGOs concerned about fissile materials security, and other NGOs concerned primarily with radiological materials or related issues all continue to be interested in improving the security of these materials, but their collective efforts toward that goal have largely stalled. Without the summits to focus their attention, disagreements among members over goals and strategies combined with a restrictive decisionmaking structure have stalled the FMWG, and the collective work of advocacy groups more generally has fragmented.[10]

Given this state of play—stalled multilateral action, fragmented advocacy—the time seems right to ask what it will take at this point to encourage civilian facilities to adopt safer alternatives to fissile materials and, more broadly, to develop a culture of security enabling facilities to be more proactive in mitigating and adapting to risk as it emerges and evolves.

Method and Roadmap

This report presents the results of a preliminary study focused on that question. Its purpose is not to provide a definitive answer but to map the factors affecting nuclear security so the next phase of research can prioritize attention to the dynamics most likely to influence the quality of nuclear security governance in the future. Perhaps more importantly, this report seeks to draw attention to underemphasized opportunities to experiment with different pathways to nuclear security.

For this scoping study, the general problem of nuclear security governance needed to be bounded, so this report's primary focus is on the security of fissile materials. But a number of our observations are likely to be applicable to radiological materials as well.

Given the preliminary nature of this study, these observations should be taken as hypotheses that are worth testing, rather than as robust findings. Our recommendations are therefore geared toward future research rather than policy and governance.

Our primary audience is the nuclear security NGO community and their funders rather than government or industry. Throughout this report we use the terms "advocates" or "experts" as a convenient

shorthand for this audience, even though we recognize that different NGOs have different missions and take different approaches: some as scholars, some as conveners, some as advocates. Most, however, seem to focus their efforts on what it will take to improve nuclear security, however they individually define it. And most seem to recognize that their collective efforts and progress toward their collective goal have both stalled.

The focus of this study, therefore, was on the factors that stand between their efforts and their goals, asking: Why isn't nuclear security improving at the rate or scale advocates believe is necessary? What are the factors and dynamics preventing progress? And where are the most promising opportunities for kickstarting progress?

The approach we took to answer these questions is a *system mapping* exercise. System mapping involves a set of well-developed methods and visualizations for making sense of situations involving many factors, many actors, and perplexing outcomes. By displaying how different factors affect each other, we are able to show the causal structure of the problem[11] in a way that clearly identifies the likely dynamics preventing progress, plus potential paths to self-sustaining solutions. A system map also makes it easier for anyone working on any aspect of nuclear security see how their work fits in to the collective effort. (It can also serve, in future research, as a basis for simulating different strategies to aid in decision making.)

To identify relevant factors, determine their causal relationships, and identify key dynamics, we reviewed relevant published works and interviewed a number of experts who focus on nuclear security at the international, national, and facility levels.

In the section that follows (Section 2, "Goals and Risks"), we offer some background and a system map showing current risks to nuclear security and a brief summary of the state of play on goals and efforts to improve nuclear governance, with an emphasis on efforts focused on industry.

The key finding of this preliminary study is that the most promising alternative to a multilateral pathway to enhanced nuclear security seems to be an industry pathway. It is, after all, the owners or managers of the civilian facilities themselves whose practices will need to change if nuclear security is to be enhanced. This is not to downplay national and international efforts, which have been the primary focus of much of the nuclear security and arms control communities for half a century, with important (if mixed) results. Rather, the fo-

cus on industry is a response to the reality of rising sentiment worldwide against globalism and the concerns of some experts that multilateral pathways are increasingly blocked.

The justification for this focus on an industry pathway is provided in Section 3 ("Four Stories about Fissile Materials"). We offer a concise system map showing how four feedback loops interact to produce today's stagnation in efforts to enhance nuclear security.[12] The complexity of these interactions can only be understood fully through computer simulation, which was beyond the scope of this study (but could be part of future work). But some of that complexity can still be explained by the system's structure.

Because system maps can be challenging to understand on their own—they are designed, after all, to portray a problem's complexity—we convey our findings through simple "system stories." Each system story focuses on a particular set of factors and their causal structure.

Section 3 includes four interrelated stories—addressing issues of awareness, advocacy, pressure, and motivation—that together explain why progress on nuclear security has stalled. The system map in Figure 2 portrays not only the system structure and these stories but also several "subplots." Subplots are factors that are not part of the main feedback loops the stories describe but that do influence factors within those stories. Subplots, as we treat them, point to potential opportunities for overcoming resistance to progress.

Section 4 ("Pathways to Nuclear Security") picks up where these stories leave off, shifting the focus to the owners and operators of facilities who are the ones making the practical decisions that affect security directly. A third system map (Figure 3) shows a set of factors at the international, national, industry, and individual levels that interact in ways that influence facility-level decisionmaking. Three system stories emerge from this chart, focused around the norms, narratives, and actions of facility managers.[13] As in the previous section, these system stories have subplots that are suggestive of potential pathways to stronger nuclear security within facilities.

In the final section (Section 5, "Recommendations for Future Research"), the stories and subplots are summarized and used as a springboard for recommending several specific lines of research to determine which of the potential opportunities to break through the stagnation have the most promise.

Specifically, three lines of future research are recommended: one focused on the public (designed to both elicit information and raise awareness), one focused on advocacy organizations (to identify the elements of a collective strategy), and one focused on facilities (to understand and bridge narratives about nuclear security governance).

2. GOALS AND RISKS

Natural uranium (U) is made of up mostly the isotope U-238, with less than 1 percent of the highly radioactive isotope U-235. Natural uranium can be enriched into a fuel containing 3–5 percent of U-235 to produce LEU, or more than 20 percent U-235 to produce HEU. Pu-239 is a highly radioactive isotope of plutonium that is produced during the decay of U-238. It needs to be isolated from spent fuel to be reprocessed into a usable form. Both Pu-239 and U-235 can be converted to their oxides and combined to create MOX fuel. Once used in nuclear energy generators or research reactors, LEU, HEU, and MOX produce spent fuel, which can either be reprocessed into usable fuel or stored in water for cooling, in some cases later transferred to dry casings for permanent storage. Unused HEU can also be downblended into usable LEU. Pu-239 waste is extremely dangerous and must be stored securely.

In general, the goal of nuclear security is to ensure that the most radioactive and toxic of these substances—namely, HEU, Pu, MOX, spent fuel, and nuclear waste—are produced, transported, used, and stored in a way that minimizes risks during all phases of the nuclear fuel cycle.[14]

Figure 1 is a type of system map, called a *stock-and-flow diagram,* portraying how fissile materials move (or "flow") between different use scenarios. The most dangerous fissile materials (HEU, Pu, and MOX) that are currently in use in civilian applications are aggregated into a single stock shown at the center (labeled "fissile materials currently in use"). This stock increases as more fissile materials are produced (bottom-center green arrow, "production"). Safer alternatives (such as LEU and natural uranium) that some facilities currently use—and that other facilities could use if they were to adopt different technologies—are aggregated into a single stock shown at the top of the figure ("alternative tech in use"). This stock increases as more of these safer fuels are produced (top green arrow, "alt tech production").

There are four things that can happen to the most dangerous fissile materials during normal use (follow the arrows from the center). They can be:

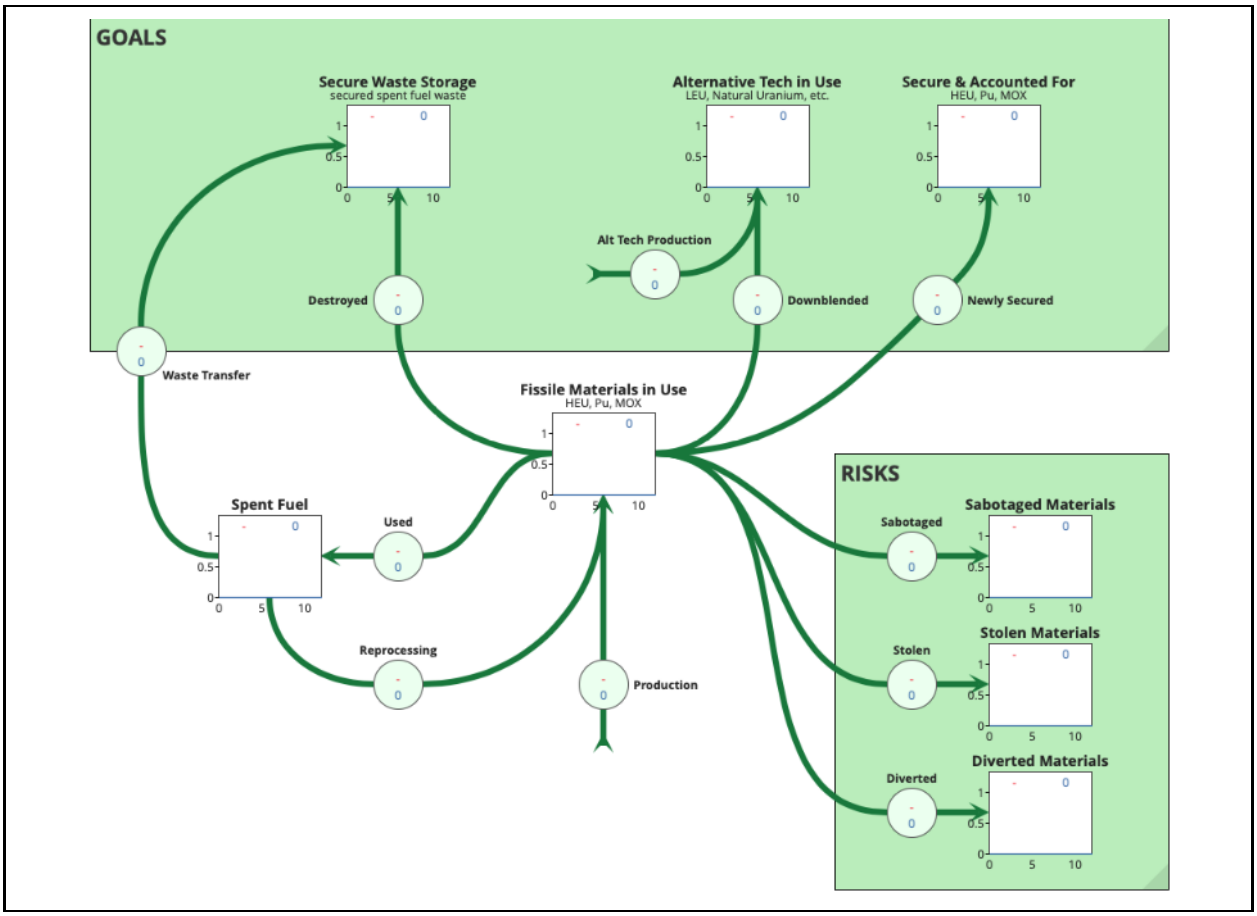


FIGURE 1. PATHWAYS TO RISKS AND GOALS

- *used,* which turns them into spent fuel (Figure 1, left), which itself can be either reprocessed back into usable fuel (bottom-left) or stored as waste (top-left);

- *destroyed* and stored as waste (top-left);

- *downblended* and used in alternative technologies (top-center); or

- *secured* and accounted for and either continue to be used in civilian applications or stored in ways that are considered responsible (top-right).

The goals of nuclear security tend to revolve around these last three pathways (the green arrows flowing from the center stock to the three stocks at the top of Figure 1): *destroying* the most dangerous fissile materials and storing them in a secure-waste facility; *down-*

blending them into LEU or natural uranium for use in civilian applications; or doing a better job of *securing* and accounting for the more dangerous materials that continue to be in use.

The more fissile materials that are moved into these "goal" pathways, the less likely it is that they will move down one of the three main "risk" pathways (the green arrows flowing from the center stock to the stocks in the bottom-right corner of Figure 1). In these risk pathways, fissile materials can be:

- *sabotaged* in a physical or cyber attack resulting in local radiological dispersal;
- *stolen* for potential use in a radiological dispersal attack elsewhere; or
- *diverted* for military use in nuclear weapons.[15]

There is some debate surrounding how serious these risks are in the real world. Risk is usually measured as a combination of probability (the likelihood an event will happen) and value (the severity of the event if it were to happen).

It is generally agreed that there have been very few attempts to sabotage or steal fissile materials and even fewer successful attempts.

The concern tends to be one of transparency and tracking: we simply do not know the scale of the problem because data collection and reporting are not comprehensive or systematic. The CNS Global Incidents and Trafficking Database identified 870 incidents between 2013 and 2017 in which nuclear or radiological materials were discovered not to be under regulatory control somewhere in the world, but very few involved uranium, plutonium, or thorium.[16] For example, in 2017, only two incidents involving fissile materials were serious: missing HEU and an illegal attempt to sell P-239 and P241.[17]

At worst, it seems, there are occasional attempts to steal but rarely any attempts to sabotage fissile materials (or at least no systematic, open-source reporting of such incidents). One industry expert, who explicitly was not downplaying the risks, nevertheless pointed out that, "After 70 years, there have been six fatalities associated with attacks at nuclear facilities worldwide—compared to 9,000 in aviation, for example."[18]

The low number of attempts seems to argue that nuclear security should not be a serious concern: If there are so few attempts because terrorist or criminal entities have determined that the difficulty of getting access to fissile materials or facilities is not worth the effort when there are other, easier ways to achieve their illicit goals, then stronger nuclear security is not needed: it is already deterring attacks.

That is not, however, the view of most nuclear security experts and advocates, who tend to focus on the other side of the risk equation: the severity of an attack were it to happen in terms of deaths, injuries, long-term health consequences, and psychological effects on the population. "No one knows what the real probability of nuclear terrorism is. It may well be quite low," wrote Matthew Bunn and Nickolas Roth in late 2017. "Given the scale of the consequences, the countries of the world have an obligation to do everything in their power to ensure that the dark day after a terrorist nuclear blast never comes."[19] An early 2019 report from Harvard's Managing the Atom Project summarized what is known about nuclear and radiological security risks this way:

> No one really knows what the chances are that adversaries would try to steal nuclear material or cause a major radioactive release from any particular nuclear site or transport. No one really knows what the chances are that such adversaries would use particular tactics or capabilities. No one really knows what the chances are that the security system in place would succeed in stopping such an attempt. No one really knows what the chances are that if adversaries managed to steal nuclear material they would make and detonate a nuclear bomb, or what the chances are of different levels of radioactive release resulting from sabotage or attack.[20]

Protecting citizens from terrorist attacks of any sort is one of the most important responsibilities of a state. As the Irish Republican Army announced after a failed assassination attempt against Margaret Thatcher, "Today we were unlucky, but remember we only have to be lucky once. You will have to be lucky always."[21]

To prevent disastrous consequences, in other words, experts and advocates generally argue that there is an ongoing need to monitor vulnerabilities and fill gaps.

A number of vulnerabilities have been identified: the way fissile materials are transported, the potential for theft or sabotage by facility staff (insider threats), a culture within facilities that views security as the job of the security team rather than all personnel, the potential

for cyber attacks (such as network intrusions and phishing), and ongoing weaknesses in physical protection that fail to limit access by unauthorized personnel or new technologies such as drones.[22] This is a demanding list of risks to monitor and it is not clear how facilities should prioritize limited resources to address them.

Several organizations are looking at ways to address these vulnerabilities, and some are also advocating that alternative technologies be adopted so the most dangerous materials are taken out of circulation.

But the nuclear security advocacy community, like the arms control community more broadly, tends to focus primarily on the need for government action—creating legal and regulatory requirements that facilities will be required to comply with.

Within industry, however, are a number of people who are equally concerned about nuclear security but who believe the focus on government action has had the unintended consequence of minimum regulatory compliance: facilities create a security department and give them the responsibility for security compliance, so staff and management have never needed to consider security to be a broader responsibility, and as a result, a culture of security has very rarely developed to the same extent as safety culture.[23]

Perhaps the most important message of this report is that the advocacy community has played an important role in motivating government action in the past and can therefore take a great deal of credit for the low level of nuclear security risk the world faces today. That work needs to continue: there is an ongoing need for effective and appropriate regulation.

But the political will globally to go above and beyond today's level of nuclear security regulation is practically subterranean, and the path from regulation to security today is foggy, bumpy, and perhaps too serpentine to be efficient.

Other pathways need to be explored, and there seems to be more focus behind the collective action on the industry side today than on the collective action on the advocacy side. There seems, therefore, to be a promising set of pathways that might go through more collaboration between the two sides.

To find those opportunities, we need to begin with the barriers.

3. FOUR STORIES ABOUT FISSILE MATERIALS

As the last section discussed, the main risks surrounding fissile materials are sabotage, theft, and diversion, and the main goals of nuclear security are to destroy, downblend, or secure fissile materials. It was suggested that it might be useful to look for opportunities for progress in the perspectives of the owners and operators of facilities and in collaboration between advocates and industry.

As a matter of logic, facilities are using fissile materials and associated technologies for a reason: there is some legitimate civilian purpose to their operations (e.g., electric power, research, etc.). Facilities operators will not destroy or downblend their stocks, for example, unless they have alternative materials and technologies that enable them to accomplish that same civilian purpose at a reasonable cost. And they will not spend limited resources to further improve the security of their facilities in the absence of a compelling reason to do so.

Figure 2, therefore, portrays some of the factors that facility managers would likely be influenced by when presented with the option of adopting new security practices or new technologies to deliver services to their customers.

Adoption is the main outcome indicator (Figure 2, green box, top-center) because, as the last section discussed, the goal of nuclear security is ultimately to get facilities to adopt some new set of practices (e.g., new machines that use natural uranium, more intensive security training for staff, better cybersecurity, etc.).

Facilities are indeed adopting new security practices and improving existing ones, just not at the rate or scale that had been advocated during the Nuclear Security Summits. This relative inaction exists despite pressure from advocates intended to increase adoption. Resistance to change in the face of efforts to prompt change is usually a symptom of one or more feedback loops counteracting those efforts.[24]

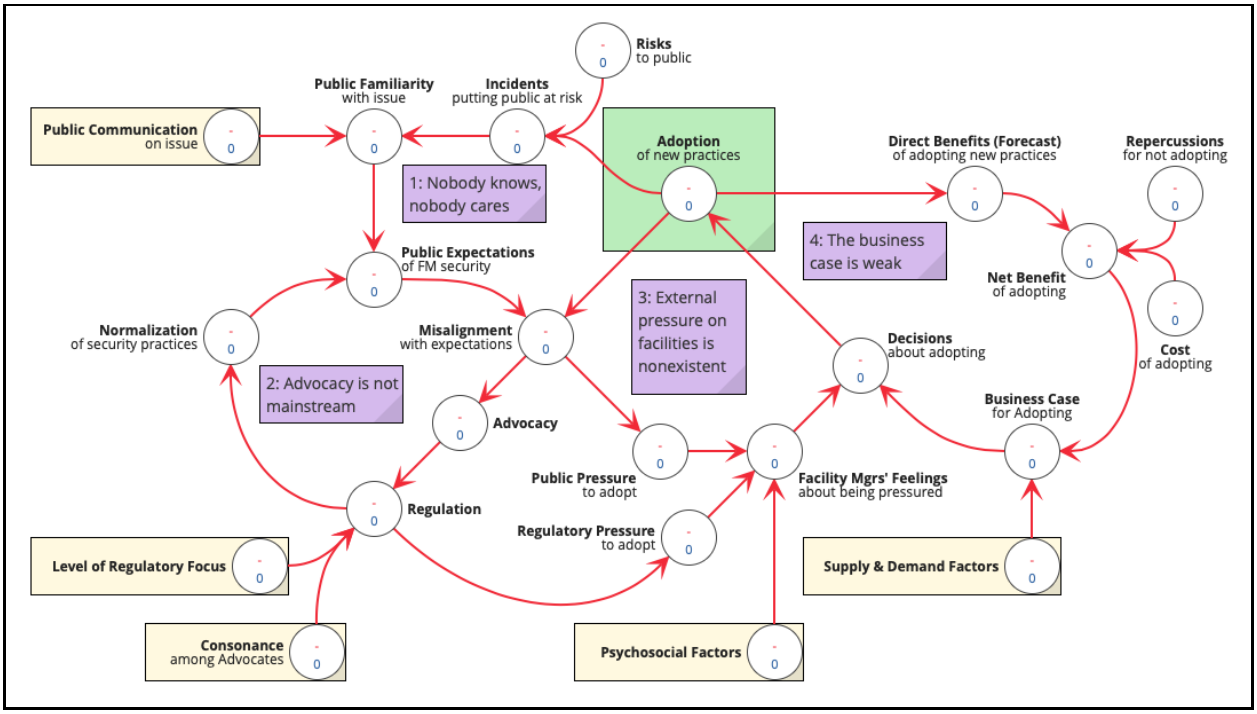
In Figure 2, we have identified four key feedback loops that tell four "system stories" centered around public awareness, policy advo-

cacy, external pressure, and internal motivation.[25] Each story derives from a set of factors that feed off each other in a way that pushes the overall system toward inaction.

It pays to clarify that these stories are not about *existing* security practices but about the adoption of new, stronger security practices, the adoption of new technologies, and the embrace of a stronger culture of security within facilities.

For example, the third story, "external pressure on facilities is nonexistent," is *not* saying that facilities refuse to comply with regulations or don't account for public opinion when making decisions about how best to secure their facilities. Most facilities are actually quite good about compliance with existing regulations—and some go beyond the minimal requirements. Instead, that story is saying simply that public opinion and new regulations are not giving facilities reasons to adopt *new and stronger* security practices, such as adopting technologies that use alternative fuels or integrating security practices into staff training as a matter of course. To put it another way, in facilities that *are* adopting new practices, the third story is saying only that they are doing so for reasons *other than* external pressure.

FIGURE 2. FOUR STORIES EXPLAINING FISSILE MATERIALS SECURITY



Similarly, the fifth story, "normative pressure is weak," is not arguing that international, national, and industry norms are not an important reason facilities comply with security standards—on the contrary, the system maps shows clearly that norms *are* an important source of compliance. It is simply arguing that, in the absence of *new* normative requirements, if advocates want facilities to adopt even stronger practices, they will need to either work harder to get new norms passed or find some other path to the adoption of new security practices.

In general, if we include a variable on a system map, it means we believe that variable *is* a contributing factor to facility-level decisionmaking; the stories are primarily conveying that the *values* of those variables are simply too low to make a difference today but could change in the future.

Story 1. Nobody Knows, Nobody Cares

The first story to emerge from this study is about public awareness (see Figure 2a): the general public seems to know next to nothing about nuclear security in civilian institutions and seems not to care enough about the topic to learn. There is obviously a public understanding that nuclear energy exists and is potentially dangerous, but it doesn't seem to be a pressing concern except when there is an incident—as when a nun and two other protesters broke into a high-security nuclear weapons facility[26]—or when there is a proposal to build a nuclear power plant in one's community.

In the United States, Gallup polling has found Americans' support for nuclear power seems mainly to correlate with the price of oil rather than any direct knowledge of nuclear security. In March 2019, 47 percent of respondents said they consider nuclear energy safe, while—for the first time since Gallup began asking about public safety—a higher number (49 percent) considered it unsafe.[27] But that was a question about public safety—likely interpreted by respondents as being about nuclear accidents—not about security risks related to theft, sabotage, or diversion. As the keynote speaker at an IAEA event on public involvement put it, "It is surprising how often there is a disconnect between the very knowledgeable, passionate nuclear scientist and the general public."[28]

In this first story, public familiarity with accurate details of nuclear security is low, and the adoption of new security practices is low—and there is a stagnating feedback loop between them that keeps them both low.[29]

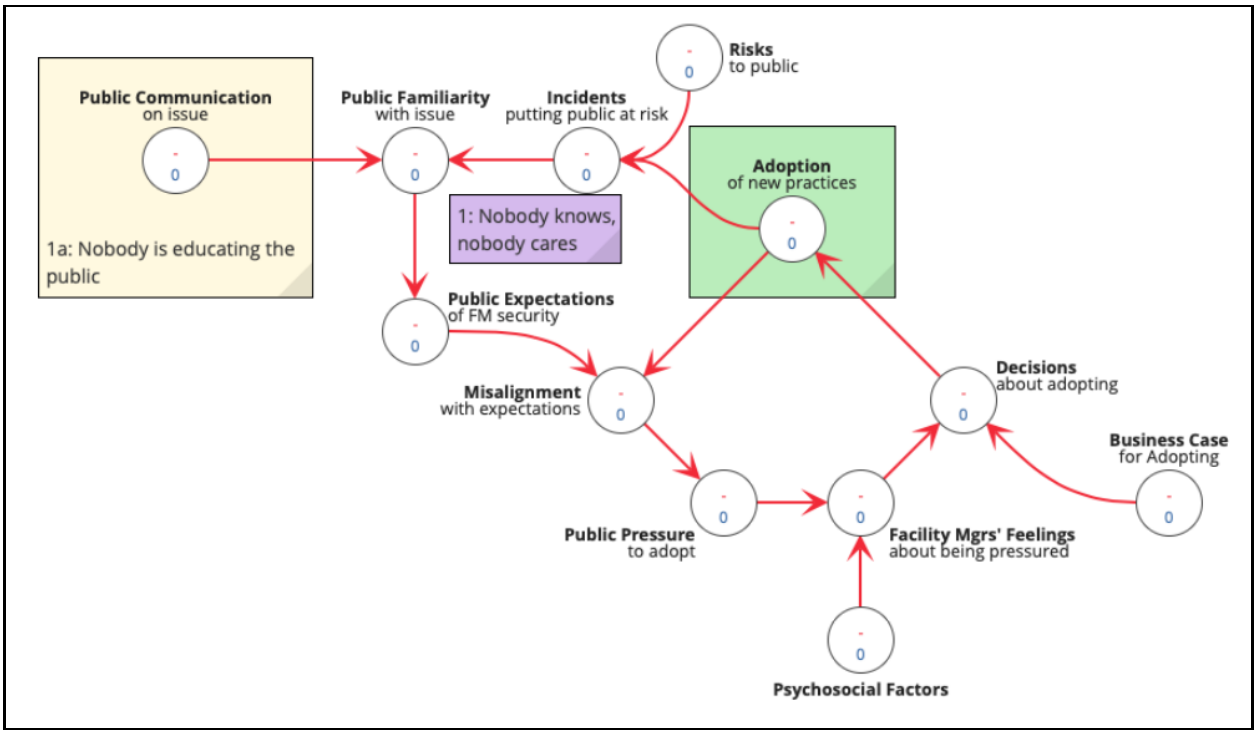


FIGURE 2A. STORY 1 AND THE "AWARENESS" FEEDBACK LOOP

To find the loop, start with *adoption* (Figure 2a, green box, and in **bold** below) and follow the arrows through the following variables:[30]

- ***Adoption*** + *Risks* → *Incidents.* Facilities are not adopting new security practices. With the adoption rate low, the public is exposed to risk. Adopting new security practices would decrease the likelihood of an attempt (to steal, attack, or divert) or would decrease the severity of a successful attempt. But because the number of attempts is so low to begin with, the number of incidents that put the public at actual risk is too low to be newsworthy.

- *Incidents* + *Public Communication* → *Public Familiarity.* As noted earlier, the public does not generally think about fissile material security unless a serious security breach gets reported in the news. Because the number of incidents is low, and because there is very little communication to the public about the risks and benefits of nuclear security, the public's familiarity (with nuclear security, risks, and the benefits of facilities' adopting new security practices) remains low.

- *Public Familiarity → Public Expectations.* Because public familiarity is low, the public has effectively no expectations that facility managers should adopt new practices.

- *Public Expectations + Adoption → Misalignment.* With public expectations so low, the current low adoption rate *already meets* the public's expectations, meaning there is no (perceived) misalignment between the public's expectations and the facilities' *adoption* rate.

- *Misalignment → Public Pressure.* If there were a misalignment (i.e., if the public believed facilities were not adopting new practices enough), there would likely be some public pressure on the facilities to adopt. But with no misalignment, there is no public pressure.

- *Public Pressure + Psychosocial Factors → Facility Managers' Feelings.* People respond to different kinds of pressure in different ways. How they feel about public pressure depends on the form that pressure takes and a whole host of psychological and social factors that influence decisionmaking.[31] In this case, public pressure is nonexistent, so facility managers' feelings about being pressured are irrelevant to their decisions about whether to adopt new practices.

- *Facility Managers' Feelings + Business Case → Decisions.* If feelings about being pressured are not relevant to their decisions, then facility managers will make decisions about whether to adopt new practices based on other considerations, primarily the business case for adopting or not adopting new practices (see Story 4).

- *Decisions →* ***Adoption***. Given all of the above, this "awareness" feedback loop shows that, under current circumstances, public pressure will play no role in facility-level decisions about adoption. In other words, if this were the only dynamic at play, facility managers would never adopt new security practices.

This first story tells us that, unless something changes, decisions at the facility level will not be driven by public pressure but by some combination of the business case, regulatory pressure, or some change in the psychosocial profile of facility managers themselves.

This story does have an important "subplot": At the moment, nobody is really educating the public about risks and benefits at the scale needed to activate this feedback loop.

There have been times when public familiarity has risen as a result either of news reporting on some incident or of an active effort to educate the public—communication that has activated this feedback loop. For example, news reports about nuclear accidents or security breaches have resulted in the public's expectations for safety and security newly exceeding existing practice, leading to demands for improved safety and security, exactly as this feedback loop predicts.[32] In cases where efforts have been made to educate the public about the quality of a facility's safety and security, that has also activated the feedback loop—but in the other direction: the public came to realize existing practice exceeded their own expectations, and there was no need to demand improvements. British Nuclear Fuels Ltd. (BNFL) led the most extensive such effort to engage the public on nuclear issues through its National Stakeholder Dialogue between 1998 and 2004, with precisely that result.[33] The structure of Figure 2 explains both outcomes.

The IAEA has offered guidance on stakeholder engagement throughout the nuclear fuel cycle, and in mid-2019 it held a roundtable and launched a webinar series on ways to involve the public more.[34] A number of organizations, such as the Nuclear Security Working Group in the United States, work to educate public officials and policy makers.

But overall there remains very little effort to reach the general public. Even funding for educating legislators has been declining.[35]

In our system map, the variable *public communication* (Figure 2a, yellow box) acts as a switch that—by analogy to an electric circuit—turns *public familiarity* "on" and "off": no communication, no familiarity; more communication, more familiarity. Communication seems to be the only factor in this feedback loop that could be directly influenced by some group of motivated actors, given the appropriate focus, funding, and scale.

If *public communication* and therefore *public familiarity* were to improve, the public would have better-informed *expectations,* which might or might not be aligned with facilities' current security practices or with the adoption rate of new practices. So the nature of that communication matters: depending on the substance and framing of that communication, public familiarity with current security prac-

tices could either reassure the public that nuclear security is adequate or trigger an increased concern about its inadequacy. To the degree there was a *misalignment* between *public expectations* and *adoption,* that misalignment would tend to create *public pressure* on facilities to change their practices, giving this feedback loop the potential to influence *decisions* at the facility level.

One has to be careful, however, that public pressure doesn't backfire. The form that public pressure takes can interact in unexpected ways with the particular *psychosocial factors* driving facility managers' responses to pressure (see Story 3), due simply to normal human psychology. An increase in public pressure in the absence of concern for the business pressures they face, for example, could potentially make facility managers feel resentful and encourage them to resist the proposed changes even more strongly.

The moral of this story—and all of them, in fact—is that the *interaction of factors* is what will influence decisions more strongly than any individual factor.

Story 2. Advocacy Is Not Mainstream

In the first story, we saw that the public has no expectations that facilities should change their current practices, and therefore there is no misalignment between expectations and reality.

That is where the second story begins. Like the first stagnating feedback loop, which kept public awareness and expectations low, there is a second stagnating feedback loop that keeps advocacy from gaining enough force to enter the mainstream and feed public expectations about nuclear security (Figure 2b).

- ***Misalignment*** → *Advocacy.* Policy advocacy is most effective when the target policy has broad or well-funded support and supporters believe current practice is not in alignment with the desired practices.[36] As noted in the first story, there is no real misalignment today between what facilities practice and what the public expects them to practice, because expectations and the adoption of new practices are both very low. As a result—and in the absence of high levels of advocacy funding (not shown)—the public's perceptions of alignment does not put any real force behind the advocacy movement. There is no mainstream constituency advocating for change.[37]

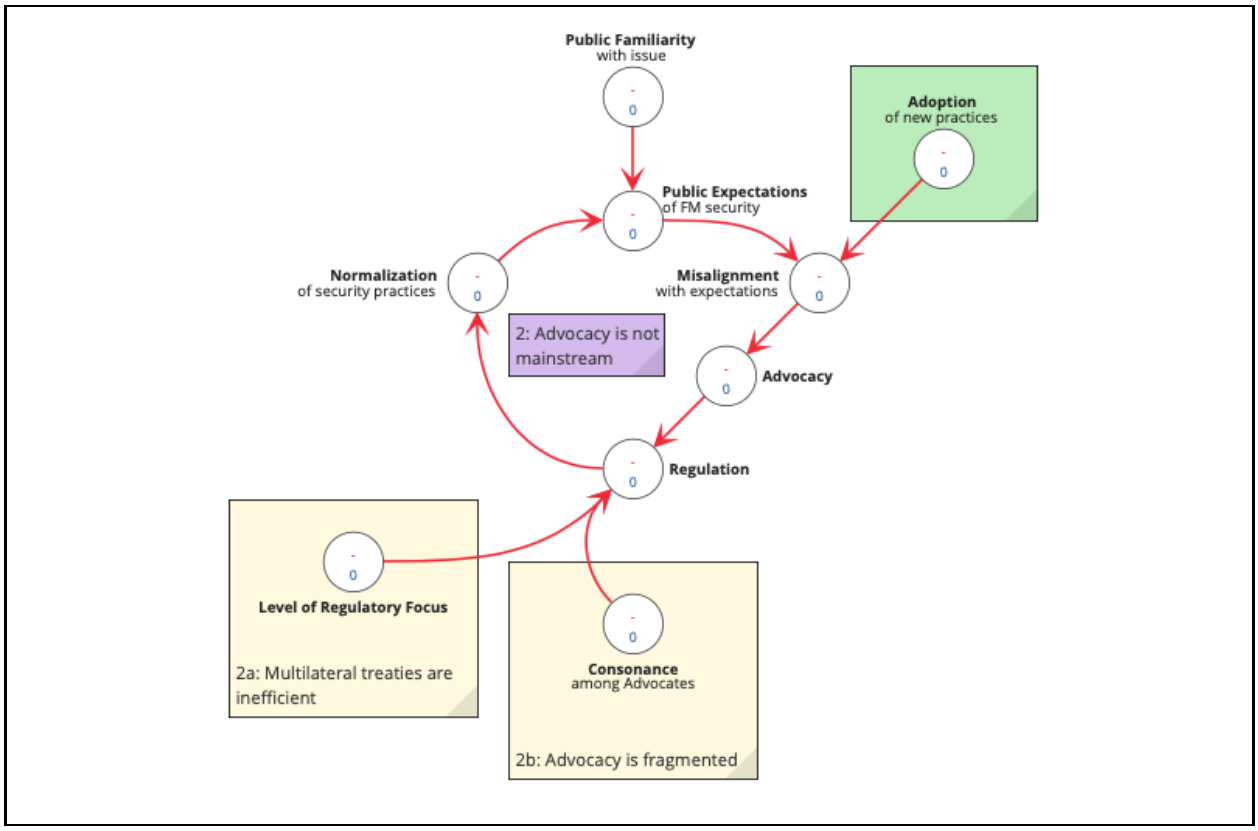


FIGURE 2B. STORY 2 AND THE "ADVOCACY" FEEDBACK LOOP

- *Advocacy → Regulation.* Without adequate public and financial support, advocacy today is having little success at passing new policies at the international, national, or facility levels.

  Conventional nuclear security advocacy has tended to focus on progress at the international level, believing multilateral treaties are a key leverage point in the system. This has been a reasonable position for many years, since a single treaty, once passed, will require state signatories to put national policies in place that would in turn require facilities to engage in better nuclear security practices. In practice, of course, this has never been so straightforward. But in today's global context of growing nationalism and populism, it is even less straightforward, as the international level (Figure 2b, bottom-left) has been dramatically weakened as a leverage point.

  Advocates can no longer expect to make national- and facility-level progress on regulation all at once through multilateral treaties—at least not very efficiently. This is especially

so now that the advocacy movement itself has fragmented in the wake of the NSS. During the NSS, the global NGO coalition had a single series to put their energies behind, the FMWG provided one key means to focus that energy, and disagreements between NGOs were not as salient as their collective opportunity for progress.

Today, the advocacy movement lacks this kind of internal consonance (Figure 2b, bottom): it is divided in a number of ways, not the least of which is between NGOs in non-nuclear weapon states, which place relatively more emphasis on the risks of theft and sabotage, and those in nuclear weapon states, which tend to emphasize diversion risks. With the end of the NSS, NGOs no longer look to the FMWG for leadership or coordination.

In short, progress on regulation is not driven by traditional advocacy as much as advocates would like, due to weaknesses in public support for advocacy, weaknesses within the advocacy movement itself, and global changes that make the traditional focus of advocacy an unlikely avenue for progress.

- *Regulation → Normalization.* A regulation has two important effects. One is to put the power of the state behind the demand for certain behavioral changes (see Story 3). The other is to signal to members of a society, including industry, that those behavioral changes are becoming "normal" in that society.

  In this case, regulations requiring additional nuclear security practices would create a signal that those practices should be seen as normal in facilities using fissile materials; as those regulations are enforced, that signal would become increasingly strong over time. The types of regulations put in place, of course, affect what types of practices become normalized. Stronger nuclear security governance could be normalized via regulation, but that is not really taking place today.

- *Normalization + Public Familiarity → Public Expectations.* If stronger regulations were to be put in place—and assuming the public actually knew about it—then that normalization of nuclear security would have a tendency to raise the public's expectations for the kinds of security practices facilities should adopt: facilities would be expected to comply

with those new regulations. None of this is happening today, and that keeps public expectations low.

- *Public Expectations* → ***Misalignment***. If the public expected facilities to begin complying with new norms of behavior surrounding nuclear security, but the facilities failed to adopt new practices, then that would create a misalignment between public expectations and reality. That misalignment could potentially put some force behind advocacy, because advocates would have more public support to press facilities into compliance. That is not the case today, however, because every other variable in this feedback loop is weak: weak advocacy, weak regulatory change, weak normalization, low expectations, and no misalignment between expectations and reality. As a result, advocates have very little fuel with which to power their efforts toward stronger regulation, and the cycle of stagnation continues.

This story has two subplots, however, that might offer opportunities to shift this feedback loop out of stagnation mode.

First, as has been noted several times, one reason regulations are not getting passed is the *level of regulatory focus* (Figure 2b, bottom-left): multilateral treaties are no longer an efficient means to enforcing behavioral change in facilities worldwide. In fact, of all the ways to put normative pressure on facilities to adopt new technologies, a multilateral approach might now be the least efficient.

In the absence of public interest or unified advocacy, international rules and multilateral treaties would be slow and laborious to achieve under normal circumstances. In a world where more and more national leaders—even in the liberal West—are backed by growing populist movements that want to reverse globalism, it is likely that international rules, multilateral treaties, and voluntary commitments are only going to get more difficult to achieve.[38]

On many issues, multilateral governance centered around states is slowly making way for some form of multistakeholder governance—stubbornly, but likely inevitably.[39]

That is both a problem and an opportunity. The opportunity is that more advocacy organizations could choose to shift the focus of their efforts to the national and facilities levels. Working on a bilateral basis might not be any more efficient than working multilaterally, but there might be enough low-hanging fruit to make progress.

Working through and with industry seems to have a great deal of promise (see Story 4 and Section 4).

The second subplot explaining slow regulatory progress is a lack of *consonance* between and among advocacy organizations (Figure 2b, bottom). When a movement's efforts and messages are unified or at least coordinated, they tend to have more force; a divided movement is a relatively ineffective movement.

The advocates who are active on this issue today are so divided in their motivations, missions, and messaging that their collective influence is diluted.[40]

For example, there is a tendency for advocates in nuclear-weapon states to emphasize the importance of non-diversion to weapons programs at the expense of a focus on public safety and physical security. That focus that has been building up resentment among advocates in non-weapon states for years. There are a wide variety of goals beyond diversion, and there are disagreements over how the various goals should be prioritized.

Even within countries, there are disagreements. Advocacy groups that believe nuclear energy is essential to addressing the climate crisis support progress on security. Those who oppose nuclear energy entirely argue that a nuclear phase-out would be the most effective measure for safety and security.

This lack of consonance among advocates weakens their advocacy and muddies the public's understanding of the issue and its importance, making it harder to get either regulation or public pressure.[41] Effective coordinating structures are needed to give voice to differing viewpoints within the movement and to present a unified set of proposals to the outside world.[42]

Story 3. External Pressure on Facilities Is Nonexistent

The third story incorporates most of factors (and parts of the feedback loops) of the first two stories.

In this story, advocacy, regulation, and public opinion have the potential to generate pressure on facility managers to adopt new security practices. But these external pressures are balanced against facilities' internal motivations. If external pressures are weak or nonexistent, then facilities will make decisions based mainly on

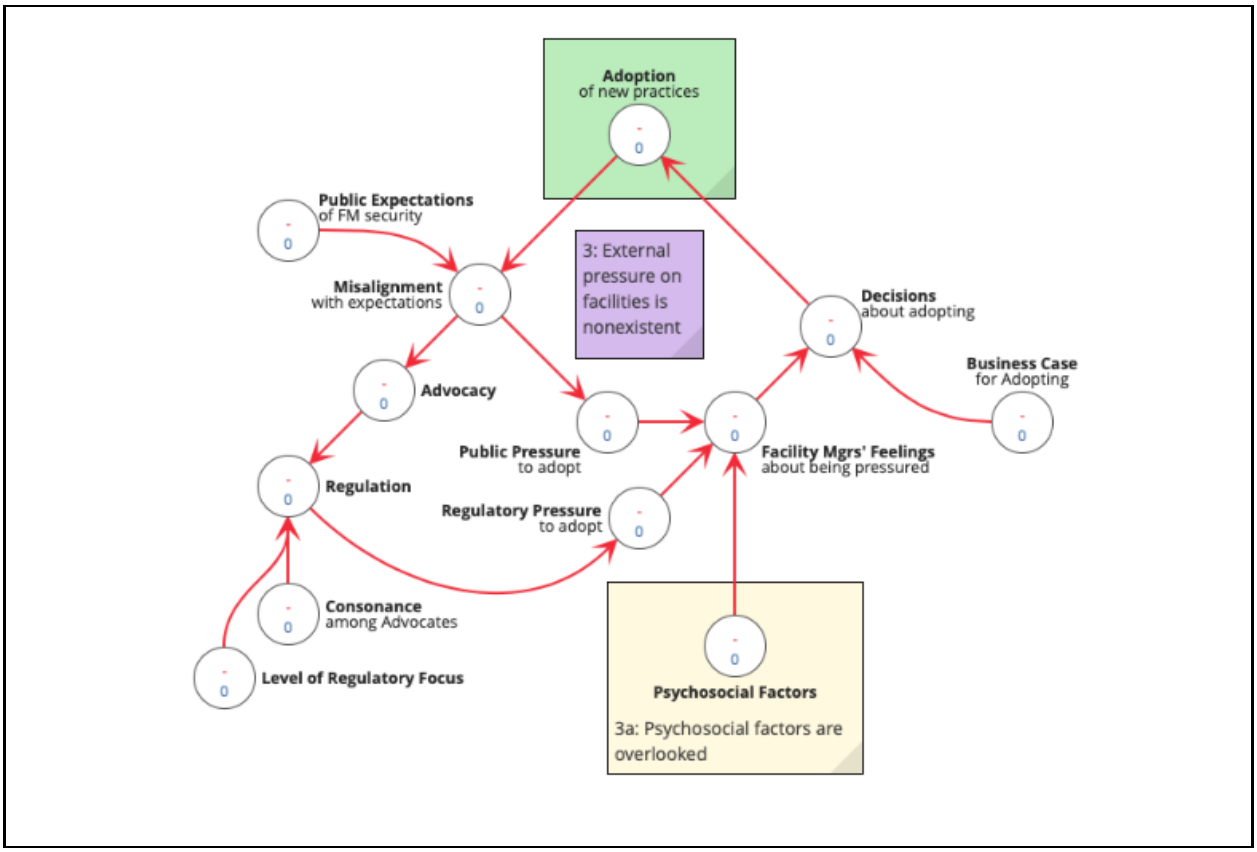


FIGURE 2C. STORY 3 AND THE "PRESSURE" FEEDBACK LOOP

their internal motivations (see Story 4). That seems to be the case today.

This "external pressure" feedback loop begins with the slow progress in the adoption of new security practices (Figure 2c, green box, top).

- ***Adoption*** → *Misalignment* → *Advocacy* → *Regulation.* In Story 1 we saw that misalignment is the difference between expectations and reality with regards to nuclear security.[43] In Story 2 we saw that misalignment has the potential to put force behind advocacy to help pass new regulations. All factors in this causal chain have very low values today. This doesn't mean new regulations are *not* being put into force; regulatory progress is being made, for example, in cybersecurity, a shift toward more outcome-based regulation, and the security of small modular reactors.[44] But many advocates remain concerned that the pace of regulatory progress is too slow relative to the seriousness of the risks.

- *Regulation → Regulatory Pressure.* In Story 2 it was observed that a key purpose of regulation is to put the power of the state behind the demand for facilities to adopt new nuclear security practices and technologies (see Story 2, "Regulation to Normalization"). At the moment, however, most facilities are already complying with national laws related to safety and security, and national laws are generally consistent with multilateral treaties. Being mostly compliant already—and in the absence of new regulations—it is no surprise that facilities today face little to no *regulatory* pressure to adopt new practices.

- *Regulatory Pressure + Psychosocial Factors → Facility Managers' Feelings* (about being pressured). The dynamic in this link is the same as that of "Public Pressure to Facility Managers Feelings" in Story 1: facility managers' feelings about being pressured will depend on how regulatory pressure and public pressure interact, both with each other and with the particular psychosocial profile of the managers themselves.

- *Facility Managers' Feelings → Decisions →* ***Adoption***. As we saw in Story 1, decisions about adopting new security practices are a function of (1) external pressures (the combination of public pressure and regulatory pressure), (2) psychosocial factors, and (3) internal motivations (represented in Figure 2 as the business case for adopting). External pressure does not really play a role in facility managers' decisionmaking today, because there is so little of it, so psychosocial factors (via *feelings* in Figure 2c) and the business case (Figure 2c, right) remain the primary contributors to decisionmaking.

These psychosocial factors are central to the key subplot in this story. The advocacy community has tended to overlook psychosocial factors as contributors to facility-level decisionmaking (Figure 2c, yellow box).

Corporations respond to more than just market and regulatory incentives. There is a whole host of psychosocial factors that influence executives' and managers' decisions about what business practices to adopt, including their risk profile, openness to novelty, organizational culture, social network effects (i.e., what peers are doing), values orientation, the compliance effects of participation, knowledge of options, understanding of risks and benefits, and many other interrelated factors.

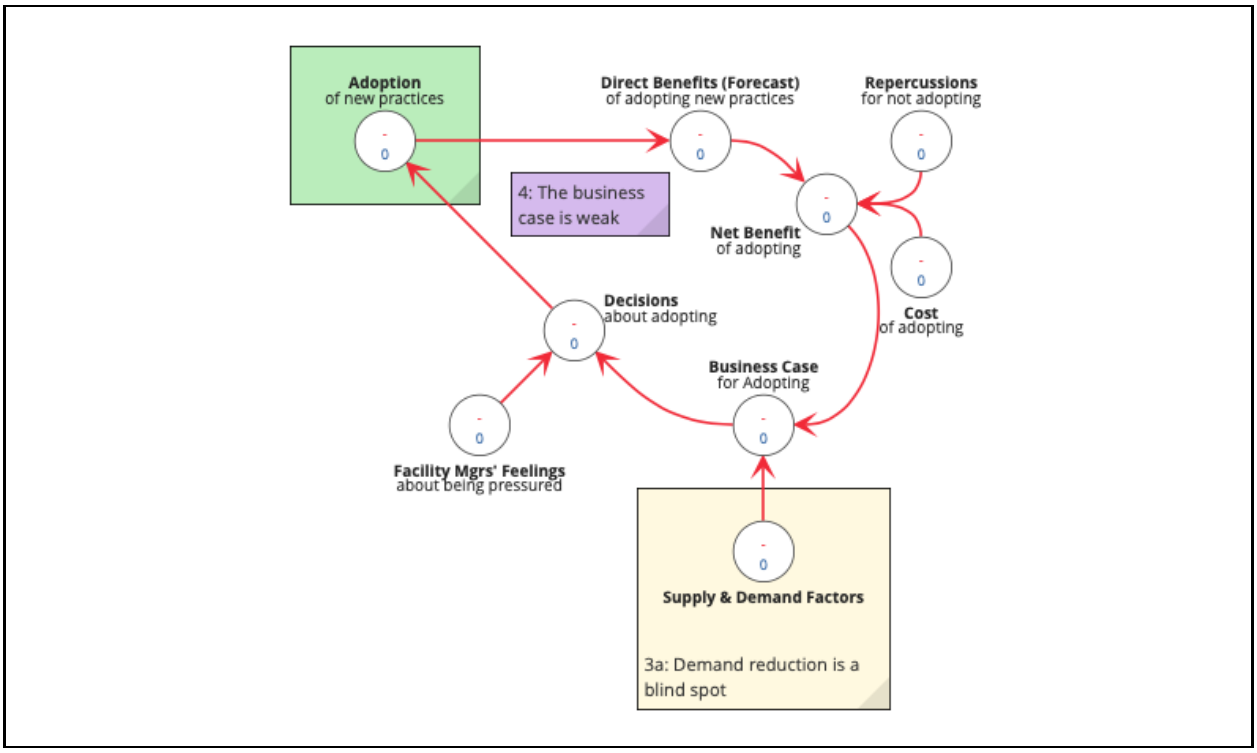


FIGURE 2D. STORY 4 AND THE "MOTIVATION" FEEDBACK LOOP

Research on corporate decisionmaking has found that attention to psychosocial barriers and opportunities can contribute to effective strategies for influencing corporate behavior.[45]

STORY 4. THE BUSINESS CASE IS WEAK

The fourth story is the logical conclusion of the first three. Decisions about what security practices to adopt are made based on a combination of external pressures and internal motivations. The first three stories were about the weakness of external pressure. That leaves internal motivations as the primary motivator for decisions to adopt. The main influence over facility-level decisionmaking, therefore, is inevitably going to be the business case.

Business-case decisionmaking focuses on forecasts about future costs and benefits. The fourth story, therefore, centers around what is called a "feedforward" loop (Figure 2d). A feedforward loop is similar to a feedback loop but instead of the key decision being influenced by knowledge of the past and present, the decision is influenced by a *forecast* of how the decision might affect key outcomes (e.g., profit or the ability to deliver a quality product).

- ***Decisions*** → *Adoption* → *Direct Benefits* (of the new practice). A facility manager's decision about whether to adopt a new security practice is likely to begin with a forecast of the benefits the new practice offers the facility. For example, if the performance of a new material (e.g., LEU) or new technology is thought to be inferior to materials currently in use (e.g., HEU), that will count as points against adoption. Happily, there are indeed safer materials available today that provide similar performance for a number of civilian applications. So this story, at least, has *potential* for a happy ending.

- *Direct Benefits* + *Costs* + *Repercussions* → *Net Benefit.* Net benefit is a function of (1) the direct benefits of adopting the new practice, (2) the *cost* of adopting it, and (3) the *repercussions* for not adopting it. Even where there are potential direct benefits from adopting, there are still costs involved in switching to new security practices or alternative technologies, and today there are few repercussions for *not* doing so (e.g., fines, higher insurance rates, staff turnover, etc.). Where facilities are adopting new security practices, they clearly see a net benefit to doing so. Where they are not, they apparently see the net benefit as being zero or negative. Those advocating for new practices need to account for these net benefit calculations.

- *Net Benefit* → *Business Case* → ***Decisions***. Current practice is current practice for a reason: the materials in use do what the facilities need them to do (subject to the difficult physics involved, especially around separated plutonium), and the system for securing them has worked well enough for a reasonable enough cost that there is little to no *business case* to be made for changing much. When presented with the option of adopting new practices, therefore, facility managers are likely to make decisions based on forecasts of the net benefits of adopting and on *supply and demand factors,* which have to do with the price and availability of new technologies and with the needs of their own customers, staff, or mission. All of those factors today mitigate against adoption.

Like the others, this final story has a subplot: demand reduction seems to be a blind spot (Figure 2d, yellow box). The business case for adopting new practices (especially new technologies that use safer materials) is too weak to motivate change at the scale advocates prefer. But much advocacy work seems focused on a supply-side strategy encouraging the removal of fissile materials from the civilian market. Progress in that regard has been slow.

Instead of trying to restrict supply, there might be opportunities to find ways to reduce demand for fissile materials by making alternatives more attractive. That might involve education and training, subsidizing the costs of switching to safer materials, or supporting research and development to find ways to improve the performance of alternative technologies.

4. PATHWAYS TO NUCLEAR SECURITY

Section 3 walked through the key challenges and opportunities surrounding nuclear security. It told a series of stories that began with a lack of public awareness and ended with the need for a better business case for adopting new practices. Subplots to those stories suggested a set of opportunities advocates might pursue as potential elements of a new approach to nuclear security governance.

This section picks up where those stories left off. All paths to nuclear security pass through the owners and operators of the facilities themselves: they are the ones who decide how to address security concerns. In some cases, those decisions might be overdetermined, as when regulators would shut down their operations if they failed to comply with regulations. So regulations—formal norms—are clearly powerful tools. But we saw in the previous section that regulation is unlikely to progress at a pace nuclear security advocates would prefer. That suggests a need to explore additional ways to influence decisionmaking at the facility level.

Nuclear security advocacy has long focused on formal norms at the global and national levels, so it makes sense to begin by studying the path from those norms to facility-level decisions. It is apparently not a straight path—or if it is, the path is now largely blocked. The mandate, therefore, is to find any branching paths that could serve as alternative routes to facility-level decisionmaking, and any feedback loops that could make the alternative routes self-sustaining.

The system map in Figure 2 showed that there are two basic paths between regulation and facility-level decisionmaking:

- **regulation** → regulatory pressure → facility managers' feelings → **decisions**

- **regulation** → normalization → public expectations → misalignment → public pressure → facility managers' feelings → **decisions**

The first relates to formal norms; the second relates to informal norms and narratives. What factors influence formal norms, informal norms, and narratives? The literatures on social psychology and the behavioral sciences in general identify more factors than can be addressed within the scope of this preliminary study.[46] But some basic observations can be made here.

Figure 3 maps out some of the key factors influencing norms (top), narratives (bottom-left), and actions (bottom-right). Each of these tells its own story about the pathways available to influence facility decisionmaking.

Story 5. Normative Pressure Is Weak

The three "pathway" stories—Stories 5, 6, and 7—together describe the simplest feedback loop that can be distilled from the rich literatures in behavioral science and social psychology: *norms* influence *narratives,* narratives influence *actions,* and actions influence norms (see Figure 3). Story 5 begins and ends with norms but previews the remaining stories by taking a journey through narrative and action.

International norms clearly influence facility-level security (the arrows, after all, trace a path from the top-left to the bottom-right of

Figure 3. Three Stories on the Pathways to the Adoption of New Security Practices

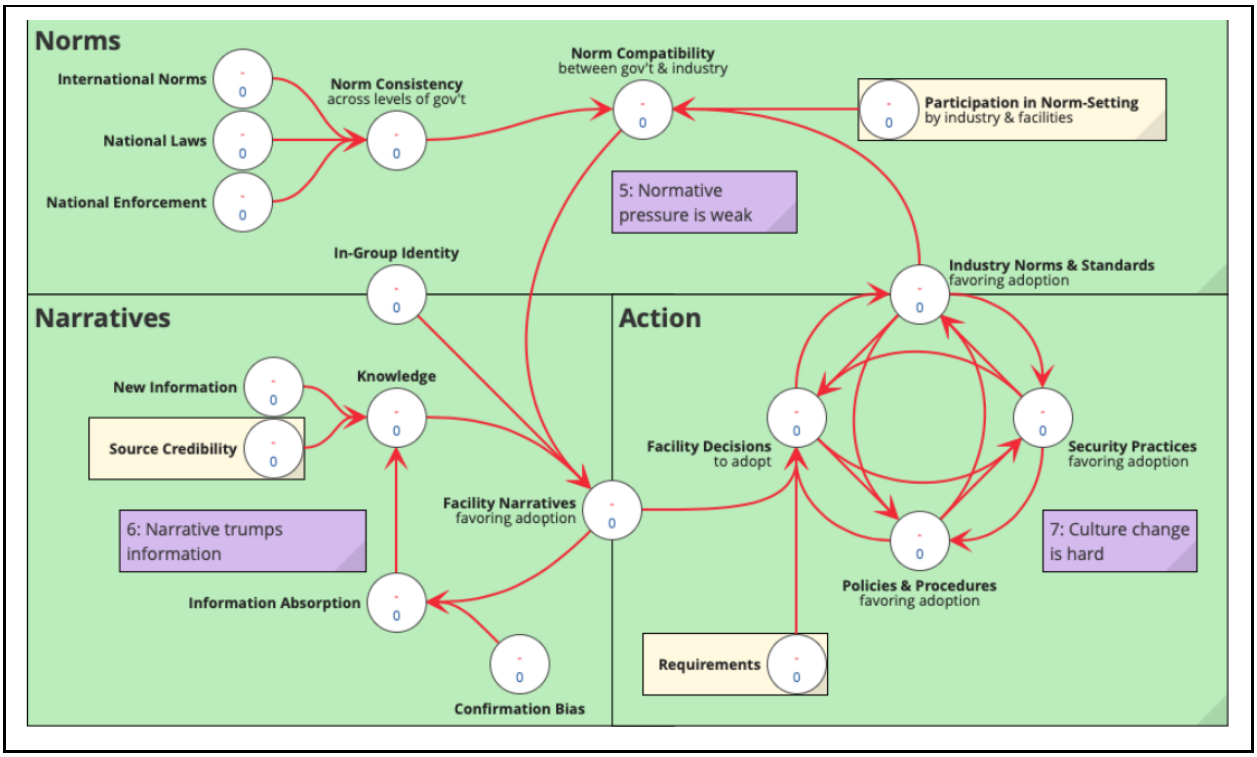


Figure 3). But there are few new formal norms coming on line today, and the likelihood of multilateral action is so low at this point that the most promising pathway from norms to actions is through *industry* norms and standards.

Psychosocial dynamics tend to privilege "in-group" perspectives over "out-group" perspectives,[47] and for facility managers, industry is the in-group, so industry norms and standards will tend to trump the preferences of the nuclear security advocacy community (to the degree the preferences of the two communities differ).

- *Norm Consistency → Norm Compatibility.* Ideally, formal norms such as multilateral treaties and national laws should be mutually reinforcing. Global standards will have less force on facility decisionmaking if they are not consistent with the national laws of the country a facility is in. Even with complete consistency among formal norms, other factors have commensurate influence. Facility managers, staff, regulators, inspectors, vendors, and others all live in a social context and are subject to the same social-network effects and intergroup biases as everyone else.[48] That means their interactions with others in their professional circles will inform their opinions about those formal norms.

  Norm compatibility (Figure 3, top-center) is the degree to which facility managers perceive the broader norms to be consistent with their industry's norms and standards (Figure 3, bottom-right). High norm compatibility is desirable, because having all norms pointing in the same direction will tend to encourage high compliance with those norms, whereas having different norms pointing in different directions will make it difficult for facilities to know whose directions to follow. Norm compatibility will tend to be higher the more industry actors participate in formal norm-setting (Figure 3, yellow box, top-right).

  It is important to note that having high norm compatibility does not mean all the norms are compatible with better security practices—only with each other. In fact, that is the case today: there is, generally, reasonably good compatibility across norms and levels of norms.[49] But those norms do not require the kinds of security practices and technologies that have been identified in this study as the goals of improved nuclear security.

- ***Norm Compatibility*** + *Knowledge* + *In-Group Identity* → *Facility Narratives.* Human beings have an understanding of the world that tends to be more or less consistent with the views of society, with the views of others they closely identify with, and with the knowledge they have absorbed about how the world works (see Figure 3, *in-group identity* and *knowledge,* left). This understanding of the world is sometimes called a mental model, a worldview, or—the term used in this study—a narrative. People's narratives—the stories they tell themselves about the world—shape their behavior.[50]

  Facility managers are no different from anyone else: They have narratives about the world, in this case narratives about nuclear security in general and the security of their facilities in particular. Those narratives are not static. In fact, they are changing today in response to information about market pressures: as nuclear energy becomes less cost-competitive, the cost-effectiveness of different practices is becoming salient in facility-level security narratives.[51] Conversations taking place within industry ("in-group" knowledge-sharing) about security and the cost-effectiveness of improving it are highly influential on the evolution of facility managers' narratives.

- *Facility Narratives* → *Facility Decisions* → *Industry Norms and Standards.* Back in Story 4, facility-level decisionmaking was influenced by a mix of external pressures, psychosocial dynamics, supply and demand factors, and the general business case for adopting new security practices (see Figure 2d). Here in Story 5, these factors are not shown (to keep Figure 3 readable); it is assumed that facility managers have incorporated these influences into their narratives about nuclear security.[52] Those narratives influence decisions within facilities, including decisions about the establishment and implementation of policies and procedures for securing fissile materials (see Figure 3, bottom-right). These security practices, when aggregated across many facilities, have an important influence on the emergence of industry norms and the development of industry standards (see Story 7).

- *Industry Norms and Standards* → ***Norm Compatibility***. Norm compatibility is simply the degree to which industry norms and standards are consistent with international and national norms. As already noted, norm compatibility is high

> today, but the content of the norms is consistent with a narrative of stasis: most facility managers have no reason to believe they need to adopt new practices. In their minds, their decisions and practices are already consistent with industry standards, and because industry standards are already generally compatible with existing norms at all levels, there is little need to change in the ways advocates desire.[53]

This story has a key subplot: Participation is an opportunity (Figure 3, yellow box, top-right). An approach to fissile materials security that focuses primarily on international norms and national laws, at the expense of facility-level perspectives, is not likely to have much influence over security culture at facilities.

It will be better for industry and advocacy to participate in each other's processes for collecting and sharing information.

There are some industry-led efforts to define and implement stronger security. They are making progress for exactly the reasons Figure 3 suggests: facilities are participating in processes that set industry norms that influence facility narratives and decisions.[54]

Advocates are making less progress for the same reason: they are not participating in the processes that facilities consider credible. If NGOs advocating for stronger nuclear security are not participating in such efforts, they will be the ones who will be excluded from the development of (industry-driven and -implemented) norms (see Story 7).

Story 6. Narrative Trumps Information

In Story 6, we are concerned mainly with the *narratives* that facility managers (and others) have of nuclear security—that is, the sum of the things they believe to be true about fissile materials, the way they arbitrate and prioritize different values (the rightness of laws, what counts as appropriate practices, etc.), their understanding of the sources of risk and security, and so on.

Narratives tend to have more influence over human decisionmaking and behavior than facts do.[55] Ideally, the narratives driving the behavior of any particular group will be based on facts (or beliefs) that are true. Where narratives differ between groups that value truth, the difference tends to be one of the interpretation or prioritization of facts.

To the degree there is a difference between advocates and industry with regard to nuclear security, Story 6 says the difference is likely one of perspective driven by normal human psychology and social interaction—and there is enough knowledge about psychosocial dynamics to inform an effort to bridge the differences. This story begins with existing narratives of facility managers (Figure 3, center).

- ***Facility Narratives*** + *Confirmation Bias* → *Information Absorption.* As humans, our existing narratives about the world limit the kind of information we are capable of noticing and absorbing. Due to a well-documented set of cognitive biases, especially confirmation bias, information is unlikely to be absorbed if it is not consistent with our existing understanding of the world—that is, with our narratives.[56]

  If facility managers believe their practices, policies, and procedures are already compliant with relevant standards and commensurate with risks, they are likely—but not certain—to dismiss information that suggests they are misreading the standards or risks.

- *Information Absorption* → *Knowledge.* If facility managers (like all humans) are predisposed to pay attention primarily to confirmatory information, then what they believe about the world—their mental database of factual knowledge about things like security breaches, near-misses, best practices, and theft—will be biased in such a way that their conclusions will be overdetermined: there is little need for change.[57] Sharing *new information* (Figure 3, center-left) about the benefits of alternative technologies and materials, for example, might not be the most effective way to influence facility action—unless that new information is provided to facilities by a source they consider to be credible, such as another industry insider: "Peer review is hugely influential."[58] (Figure 3, *source credibility,* center-left).

- *Knowledge* + *In-Group Identity* → ***Facility Narratives***. Story 6 tells us that our narratives influence the information we absorb, which influences the content of our knowledge base, which influences our narratives, which are also influenced by our in-group peers—a feedback loop, driven by cognitive bias and social identity, that can complicate communication between outside experts and practitioners.

The key subplot of Story 6 shows a promising way to break into that feedback loop: source credibility (bottom-left, 2a). It is possible to

successfully introduce new information into a closed system, but it requires the use of a source of information the audience finds credible—someone who shares their (in-group) identity, values, and narratives or who at least demonstrates familiarity and respect for their existing knowledge and narratives.[59]

In a situation where a facility manager, regulator, or other decisionmaker does not see the need to improve security practices, it makes sense for NGOs advocating for nuclear security to find a different messenger, perhaps by partnering with industry NGOs, standards bodies, or facilities that have already embraced strong security practices. Instead of sharing knowledge, a better approach might be to *co-produce* knowledge with industry and facilities—the knowledge exchange is likely to be a two-way street.

Story 7. Culture Change Is Hard

Story 7 is the finale. Stories 1, 2, 3, and part of 5 showed that public opinion, advocacy, and formal norms are not significant enough factors to influence facility decisionmaking about security practices in the foreseeable future. Stories 4, 5, and 6 showed that business considerations and industry narratives and norms are the dominant factors driving nuclear security decisionmaking today and therefore represent promising pathways to explore.

These previous stories were all about factors that are too weak to overcome the inertia of stagnating feedback loops. Story 7 is more about stagnation driven by complexity—by the thick interdependencies that makes culture change so hard. That is why the "Action" section of Figure 3 (bottom-right) looks so different from the rest: it represents tightly interrelated factors that influence discrete decisions and long-term culture change alike.

- *Facility Decisions → Policies & Procedures ↔ Security Practices ↔ Industry Norms and Standards.* The ultimate goal is to get facilities worldwide to put in place a set of practices, policies, and procedures capable of preventing theft, sabotage, and diversion of fissile materials. While the adoption of alternative technologies and other practices and policies is an important component of the strategy for achieving that goal, it is the underlying culture—the patterns of thought and behavior—with regard to nuclear security that will sustain any gains made in the years ahead.[60]

  The owners and operators of facilities are the ones who make

decisions about policies, procedures, and practices with regard to facility security. They are influenced by the practices of their peers and industry norms more generally, which in turn are influenced by facilities in aggregate.

For example, it is common for security at the facility level to be largely outsourced to security departments, often made up of former military and police personnel who focus mainly on physical security and only secondarily on insider threats, cyber sabotage, and other sources of risk. By contrast, industry norms encourage facilities to train staff to consider *safety* to be "everyone's job"—to avoid accidents and injuries—and as a result there is a strong culture of safety throughout the industry. That is not the case with security, which at the facility level is generally treated as "someone else's job."[61]

A facility that is being encouraged to distribute security responsibilities more broadly to its staff is likely to look to other facilities to see if they have done so—and if not, why not. Unless there is a good business reason or the facility is owned or operated by people whose psychosocial profile predisposes them to be early adopters, that facility is not likely to change.

Some industry insiders are working to press for such changes, both at the level of industry norms and within individual facilities. But culture change is hard when there are so many different actors and factors involved. Efforts by one set of actors, or improvements in one set of factors, are likely to be counterbalanced by the more dominant dynamics stabilizing the system—unless there is broader coordination of efforts across a range of key factors.

The subplot of this story centers around one such set of key factors: the requirements facility managers have to take into consideration when deciding how to structure security (Figure 3, yellow box, bottom). These include requirements of their customers, the requirements of the industry in the form of formal standards and informal best practices, and the requirements of other private-sector entities that facilities depend on (e.g., accounting, insurance, and investors). All of these requirements are core to the business case and they tend to both reflect and contribute to industry norms.

If these requirements for security were to *exceed* the requirements of existing laws and regulations—for example if investors or insurers were to change how they calculate risk—then facilities would be likely to adopt more effective security practices.

Requirements are not necessarily easy to influence by any single actor, but the processes and institutions that are in place to change them are likely to be accessible to advocates of nuclear security who wish to have a voice, as long as those advocates recognize the lessons Stories 5 and 6 teach about source credibility and in-group identity: industry narratives and norms will be much more strongly influenced by industry actors than by others perceived as outsiders. A credibility-building process might well be a prerequisite to effective engagement.

Organizations such as the World Nuclear Association (WNA) and the World Nuclear Transport Institute have processes in place for deliberation and development of requirements related to security. For example, WNA's Working Group on Security, which has been chaired by the founder of the World Institute for Nuclear Security (WINS) since January 2019, is working to "develop a coordinated industry view on how nuclear security objectives are implemented, cooperate with the IAEA with the aim of communicating the industry viewpoint, [and] encourage newcomer countries to apply appropriate effective security arrangements."[62] Issues under discussion include "mitigating insider threats; cybersecurity; the safety-security interface and culture; and security oversight as part of good corporate governance."[63] These topics are very consistent with the goals of nuclear security outlined in Section 2 (see Figure 1).

Within the NGO advocacy community, it has been proposed to engage with industry to develop formal (ISO) standards for nuclear security.[64] These processes and ideas are worth pursuing.

5. RECOMMENDATIONS FOR FUTURE RESEARCH

This report has told a tale of two paths. On one path are public opinion, policy advocacy, and formal norms. On the other are business considerations, facility narratives, and industry norms. The first path was once a bustling throughway to nuclear security, but it has recently become obstructed and no longer seems fully viable. The second path remains largely unexplored. The sequel to this story, therefore, should be one of collaborative exploration.

This overall tale was told through seven interrelated stories that together explain why one path has become a barrier and the other an opportunity:

1. **Awareness.** Public familiarity with accurate details of nuclear security is low and not enough effort is being put into educating the public.

2. **Advocacy.** Nuclear security advocacy is not a mainstream movement. Its focus on political will is no longer viable in a world turning its back on multilateral action. Its collective fragmentation has gotten worse since the end of the Nuclear Security Summits.

3. **External Pressure.** Without public or regulatory pressure, facility managers will naturally make security decisions based on internal motivations. Different managers have different psychosocial profiles, which means some will be more open to engagement on questions of security than others.

4. **Business Case.** The most important internal motivation at the facility level is the business case for adopting or not adopting new security practices, including alternative technologies that apparently have not yet been made attractive enough (from a cost-benefit perspective) to adopt.

5. **Normative Pressure.** There are still some normative pressures that facility managers are likely to respond to: the norms and standards of their industry. But most nuclear security advocates are not engaging industry on voluntary standards.

6. **Narrative.** Industry norms and knowledge shape facility narratives about nuclear security, and those narratives in turn shape facility decisions about what practices to adopt. Advocacy narratives have less influence, due to normal psychosocial dynamics.

7. **Culture.** Patterns of belief and behavior are hard to change because they are influenced by so many different factors and actors. This preliminary study of that complexity suggests there is room for growth in the requirements that are established by facilities' customers, industry bodies, vendors, and investors with regard to their security practices.

The sequel to these stories will begin with the nuclear security advocacy community at an important crossroads with no common roadmap. Three lines of research should be pursued as the first steps of a new journey.

Advocacy

When advocacy has succeeded in influencing international and national norms, it has been for reasons consistent with the system maps shown in Figures 2 and 3: there was consonance among advocates' goals and tactics, they were focusing on a level of regulatory action that was suited for its time, and they had shared narratives that made them effective at communicating their desired outcomes.

As the global landscape has changed and advocacy has fragmented, differences within the advocacy community have become more salient and need to be bridged. Most salient is the tension between NGOs in nuclear weapon states and those in non-nuclear weapon states over the prioritization of diversion risks above theft and sabotage risks. Equally important will be differences over the degree to which industry engagement will be fruitful.

An observation about narrative can be borrowed from the sixth story: differences between advocates are likely to be driven more by narrative than by fact (because that is the case for all human beings).

Research is therefore needed to map the content of the narratives espoused by different advocacy groups, experts, and coalitions worldwide. Such a narrative-mapping exercise can then be used as the basis for a collaborative initiative designed to find bridging narratives and turn them into a collective strategy for nuclear risk reduction.[65]

That would enable everyone to see how their own work fits in to the collective effort—particularly important given the large number of NGOs in this space—and would provide raw material for the development of a new vision of nuclear security governance.[66]

Industry

Industry has made progress on security over the years—just not at the pace or in the way many advocates think is needed. Their progress has come as a result of dynamics that are consistent with the system maps in Figures 2 and 3: there was regulatory pressure, there were market signals, and facilities had shared some narratives about security that influenced facility-level decisions and industrywide norms.

To make further progress, many of those same dynamics need to be accounted for. Within industry, as within advocacy, there are different narratives about nuclear security between different facilities, industry bodies, and other industry insiders, as well as differences between industry and advocacy.

An industry-focused narrative-mapping exercise could be run in parallel with the advocacy-narrative exercise recommended in the previous section. That mapping exercise could be used as the basis for developing engagement strategies targeting different industry actors based on their narrative, psychosocial, and business profiles.

More generally, more opportunities should be organized to encourage industry-advocacy engagement and collaboration. For example, advocates and their funders could make more of an effort to participate in industry-led efforts organized by groups such as WINS and WNA.

Public Engagement

Finally, the public's lack of familiarity with nearly any detail of nuclear security is a missed opportunity.

Some efforts are already being undertaken to encourage and teach better public engagement, including a new webinar series hosted by IAEA, and these are a good start.[67] WINS has done some work on encouraging public disclosure of facilities' governance arrangements to give the public (and investors) a better sense of the risks.[68]

The system map in Figure 2 shows why efforts such as these have been effective, at least at the community level (see Story 1, p. 18).

For public communication to be effective at the scale needed to put force behind effective advocacy, however, research is needed that goes beyond aggregate polling and takes an approach that has proven effective in commercial marketing: segmenting populations based on their values and narratives then testing different combinations of message (what is communicated), messenger (who communicates it), and medium (the channels through which it is communicated, e.g., news, education, fiction, social media, etc.).[69] Such a study then should be used as the basis for funding a scaled-up public awareness campaign that targets each population segment according to the media, the messages, and the messengers most likely to resonate.

Doing that successfully will likely require a new system map—or perhaps a simulated version of a system map that would enable advocates to interact with this kind of knowledge to inform their decision making, population segment by population segment.

To Be Continued . . .

When the Nuclear Security Summits were taking place, countries were making commitments and NGOs had energy driving them toward focused collaboration.

Much of that work has largely stalled. Populist resurgence, cognitive biases, social network effects, public familiarity, divided advocacy—all of these factors and more are pushing in the same direction: the system of nuclear security advocacy is in stasis and nuclear security is at risk of backsliding.

The path of regulation should not be abandoned: states have a responsibility to protect citizens against nuclear threats, and advocates should continue holding them to account for that responsibility as they have done successfully for decades.

But other paths are opening up. There is energy and interest within industry to strengthen nuclear security—and there remains interest and urgency within the advocacy community for the same basic goal. The characters in this story might have different perspectives on what drives the plot forward, but this story can have a happy ending.

NOTES

[1] *The Radiological Accident in Goiânia*, International Atomic Energy Agency, 1988.

[2] National Academy of Engineering and National Research Council of the National Academies, "Radiological Attack: Dirty Bombs and Other Devices," *News & Terrorism: Communicating in a Crisis,* Department of Homeland Security fact sheet, 2004.

[3] Jeffrey Bale, *The Chechen Resistance and Radiological Terrorism,* Nuclear Threat Initiative, April 2004.

[4] U-233 and Pu-241 are also highly fissile materials but they are significantly less commonly used.

[5] Sara Z. Kutchesfahani, Kelsey Davenport, and Erin Connolly, *The Nuclear Security Summits: An Overview of State Actions to Curb Nuclear Terrorism, 2010–2016,* Arms Control Association and Fissile Materials Working Group, July 2018; Michelle Cann, Kelsey Davenport, and Jenna Parker, *The Nuclear Security Summit: Accomplishments of the Process,* Arms Control Association and Partnership for Global Security, March 2016.

[6] Kingston Reif, personal communication, July 2019.

[7] Sara Kutchesfahani, personal communication, February 2019; Jonas Siegel, personal communication, January 2019.

[8] Most experts interviewed for this study expressed some variation of this point.

[9] *The Results We Need in 2016: Policy Recommendations for the Nuclear Security Summit,* Fissile Materials Working Group, 2015; Igor Khripunov, "A Culture of Security: Focus for the Next Nuclear Security Summit?" Bulletin of Atomic Scientists, June 2015

[10] Several experts interviewed for this study expressed this view anonymously.

[11] technically, the structure of the system producing the problem

[12] A feedback loop is a causal structure in which one factor influences a second factor, which then influences a third factor (etc.), which in turn influences the first factor again. In some feedback structures ("positive feedback"), each link in the chain reinforces the previous and you get vicious or virtuous cycles; in others ("negative feedback"), one or more links in the chain balance each other out and you get stability and resistance to change. Interactions between feedback loops can cause unpredictable behavior. In the system maps in Figures 2 and 3, the values of one or more variables are too low to activate positive feedback or counteract negative feedback, so the result is stagnation. For a theoretical review of feedback, see George P. Richardson, *Feedback Thought in Social Science and Systems Theory,* Waltham, Mass.: Pegasus Communications, 1999. For a practical treatment, see *Systems Practice,* Omidyar Group, undated, https://docs.kumu.io/content/Workbook-012617.pdf.

[13] In this report, "facility managers" is used as a term of convenience to refer to the owners, officers, security managers, operators, and others who have decisionmaking authority over some civilian entity that produces, transports, or uses fissile materials for some civilian application.

[14] Jonas Siegel, personal communication, May 2018; Nancy Gallagher, personal communication, May 2018;

[15] While this study focuses on fissile materials in civilian applications, similar concerns exist with regard to radiological materials, as illustrated at the beginning of this paper, with the exception of diversion (because only fissile materials can be used in nuclear weapons).

[16] Thorium is technically a "fertile" rather than a fissile material, but it is used in nuclear fuel to breed U-233.
[17] James Martin Center for Nonproliferation Studies, *CNS Global Incidents and Trafficking Database: 2017 Annual Report,* Washington, DC: Nuclear Threat Initiative, July 2018.
[18] Roger Howsley, personal communication, September 2019.
[19] Matthew Bunn and Nickolas Roth, "The effects of a single terrorist nuclear bomb," *Bulletin of the Atomic Scientists,* September 28, 2017.
[20] Matthew Bunn, Nickolas Roth, and William H. Tobey, "Revitalizing Nuclear Security in an Era of Uncertainty," Project on Managing the Atom (Harvard Kennedy School Belfer Center for Science and International Affairs), January 2019, pp. 46–47.
[21] Peter Taylor, *Brits: The War Against the IRA*, London: Bloomsbury Publishing, 2001, p. 265.
[22] Experts interviewed for this study identified these vulnerabilities. See also Matthew Bunn et al, "Revitalizing Nuclear Security in an Era of Uncertainty," 2019; and *CNS Global Incidents and Trafficking Database,* 2018.
[23] Roger Howsley, personal communication, June 2019.
[24] See Note 12.
[25] Here, "external" and "internal" are from the perspective of the facility.
[26] Eric Schlosser, "Break-in at Y-12," *The New Yorker,* March 1, 2015, https://www.newyorker.com/magazine/2015/03/09/break-in-at-y-12.
[27] RJ Reinhart, "40 Years After Three Mile Island, Americans Split on Nuclear Power," Gallup, March 27, 2019, https://news.gallup.com/poll/248048/years-three-mile-island-americans-split-nuclear-power.aspx
[28] Sandy Wilkes (Bisconti Research), keynote address, IAEA meeting on stakeholder engagement, June 2019; quoted in Elisabeth Dyck and Lisa Berthelot, "Public Opinion Research Can Guide Stakeholder Communication for Nuclear Power," IAEA, June 21, 2019, https://www.iaea.org/newscenter/news/public-opinion-research-can-guide-stakeholder-communication-for-nuclear-power
[29] Technically, the system map in Figure 2a contains two feedback loops, one directly connecting five variables (with *adoption* at the apex), one connecting those same five factors plus the three "public" factors to their left. But the two loops combine in a way that tells a single coherent story.
[30] The arrows should be interpreted as a statement about causation or, better, influence: A→B should be read as "Variable A influences Variable B." The plus signs (+) should be interpreted as an interaction between the variables: A+B→C should be read as "Variable A and Variable B interact in ways that together influence Variable C." Mathematically, A and B could interact in any number of ways (not just addition). A true mathematical model would include additional variables and constants that are not shown here because they do not contribute to the core findings.
[31] Arthur Bandura, *Social Foundations of Thought and Action,* Englewood Cliffs, NJ: Prentice-Hall, 1986.
[32] Eric Schlosser, "Break-in at Y-12," 2015.
[33] Roger Howsley, personal communication, September 2019. See also Anthony Perret, "BNFL National Stakeholder Dialogue: A case study in public affairs," *Journal of Public Affairs* 3, no. 4, November 2003, pp. 383–391.
[34] IAEA, Stakeholder Involvement Throughout the Life Cycle of Nuclear Facilities, IAEA Nuclear Energy Series, 2011; Lisa Berthelot, "IAEA Launches Webinar Series on Stakeholder Involvement in Nuclear Power Programmes,"

IAEA, May 27, 2019, https://www.iaea.org/newscenter/news/iaea-launches-webinar-series-on-stakeholder-involvement-in-nuclear-power-programmes

[35] Andrew Semmel, personal communication, June 2019.

[36] Among other factors; see Katherine Cullerton, Timothy Donnet, Amanda Lee, and Danielle Gallegos, "Effective Advocacy Strategies for Influencing Government Nutrition Policy: A Conceptual Model," *International Journal of Behavioral Nutrition and Physical Activity* 15, no. 83, 2018, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6119246.

[37] Several experts interviewed for this study expressed this view anonymously.

[38] See, for example, Johannes Linn, "Recent Threats to Multilateralism," *Global Journal of Emerging Market Economies* 9, no. 1–3, pp. 86–113, January 2017.

[39] Nancy Gallagher and Jonas Siegel, "Conceptualizing Governance: A Summary Paper," prepared by the Center for International and Security Studies at Maryland (CISSM) for the "Governing Global Challenges" dinner meeting, October 19, 2016.

[40] Several experts interviewed for this study expressed this view anonymously.

[41] Sara Kutchesfahani, personal communication, June 2018.

[42] Jonas Siegel, personal communication, May 2018.

[43] Technically: *public expectations* minus *adoption* equals *misalignment*.

[44] Roger Howsley, personal communication, September 2019.

[45] For useful summaries of research on the links between psychosocial dynamics and behavior, see Pascal J. Gambardella and David W. Lounsbury, "Annotated Bibliography: Modeling Psychological and Sociological Dynamics," version 6, July 13, 2015; Daniel Kahneman, *Thinking, Fast and Slow,* London: Penguin, 2011; and Paul Slovic, Melissa L. Finucane, Ellen Peters, and Donald G. MacGregor, "Rational Actors or Rational Fools? Implications of the Affect Heuristic for Behavioral Economics," paper prepared for the Second Annual Symposium on the Foundation of the Behavioral Sciences, "Behavioral Economics and Neoclassical Economics: Continuity or Discontinuity?" American Institute for Economic Research, Great Barrington, Massachusetts, July 19–21, 2002.

[46] Ibid.

[47] For a good summary of social-identity theory, see John T. Jost, Diana Burgess, and Christina O. Mosso, "Conflicts of Legitimation Among Self, Group, and System: The Integrative Potential of System Justification Theory," in *The Psychology of Legitimacy: Emerging Perspectives on Ideology, Justice, and Intergroup Relations,* ed. John T. Jost and Brenda Major, New York: Cambridge University Press, 2001, p. 3.

[48] For a good discussion of norm dynamics, see, Jonathan Ring, "An Agent-Based Model of International Norm Diffusion," paper presented at New Frontiers in Policy Diffusion, Iowa City, Iowa, March 14-15, 2014.

[49] Laura Holgate, personal communication, June 2019.

[50] For a good synthesis of the literature on narrative, see The World Bank Group, *World Development Report 2015: Mind, Society, and Behavior,* International Bank for Reconstruction and Development, Washington, DC, 2015, https://www.worldbank.org/content/dam/Worldbank/Publications/WDR/WDR%202015/WDR-2015-Full-Report.pdf

[51] Roger Howsley, personal communication, September 2019.

[52] A simulation model (and a type of system map called a causal-loop diagram) would make these relationships explicit.

[53] Roger Howsley, personal communication, June 2019.

[54] Ibid.

[55] World Bank, *Mind, Society, and Behavior,* 2015; Walter R. Fisher, "Narration as a Human Communication Paradigm: The Case of Public Moral Argument," *Communication Monographs* 51, March 1984, pp. 1–22.

[56] Nickerson, Raymond S., "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises," *Review of General Psychology* 2, no. 2, June 1998, pp. 175–220; Charles G. Lord, Lee Ross, Mark R. Lepper, "Biased Assimilation and Attitude Polarization: The Effects of Prior Theories on Subsequently Considered Evidence," *Journal of Personality and Social Psychology* 37, no. 11, 1979, pp. 2098–2109; David Hackett Fischer, *Historians' Fallacies: Toward a Logic of Historical Thought,* New York: Harper & Row, 1970.

[57] See Emily Thorson, "Belief Echoes: The Persistent Effects of Corrected Misinformation," *Political Communication* 33, no. 3, November 2015; and Stephan Lewandowsky, Ullrich K. H. Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook, "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest* 13, no. 3, September 2012, pp. 106–131.

[58] Roger Howsley, personal communication, September 2019.

[59] Carl Hovland and Walter Weiss, "The Influence of Source Credibility on Communication Effectiveness," Public Opinion Quarterly 15, no. 4, 1951, p. 635; Arthur Bandura, "Social Cognitive Theory of Mass Communication," *Media Psychology* 3, no. 3, 2001, pp. 265–299.

[60] Sara Kutchesfahani, personal communication, June 2018; Igor Khripunov, "A Culture of Security," 2015; IAEA, "Nuclear Security Culture: Implementing Guide," *IAEA Nuclear Security Series,* no. 7, 2008.

[61] Roger Howsley, personal communication, June 2019.

[62] "Dr Roger Howsley to Chair the Next Meeting of Security of the International Fuel Cycle, a Working Group of the World Nuclear Association," WINS, December 5, 2018, https://wins.org/dr-roger-howsley-to-chair-the-next-meeting-of-security-of-the-international-fuel-cycle-a-wna-working-group/.

[63] "Working Groups," WNA, https://www.world-nuclear.org/our-association/what-we-do/working-groups.aspx/#security.

[64] Laura Holgate, personal communication, June 2019.

[65] For information about collective strategy development, see Robert D. Lamb, "Collective Strategy: A Framework for Solving Large-Scale Social Problems," *FFI Research Brief* no. 1, January 8, 2018, https://foundationforinclusion.org/research/collective-strategy-framework.

[66] Jonas Siegel, personal communication, May 2018.

[67] Lisa Berthelot, "IAEA Launches Webinar Series on Stakeholder Involvement in Nuclear Power Programmes," IAEA, May 27, 2019.

[68] Roger Howsley, personal communication, September 2019.

[69] For an excellent example on a different topic, see Cara Pike, Bob Doppelt, and Meredith Herr, *Climate Communications and Behavior Change: A Guide for Practitioners,* The Climate Leadership Initiative, 2010, https://climateaccess.org/system/files/Climate%20Communications%20and%20Behavior%20Change.pdf.