BEYOND A REASONABLE DBT

Kathryn Rauhut[1], Donald Dudenhoeffer[2], Jacqueline Kempfer[3], Madison Hissom[4]

Abstract

As nuclear power plants have become increasingly dependent on digital technology for daily operations, so too have they become increasingly vulnerable to malicious cyber-attacks. In the wake of an incident, the public will likely ask: What could have been done to prevent it? Who was responsible? Were all reasonably adequate measures taken?

States address these questions by establishing a Design Basis Threat (DBT), which identifies the maximum reasonable set of threats against which a nuclear operator can be expected to defend. A DBT acknowledges that nuclear operators are unable to defend against the entire spectrum of security threats, including possible state-sponsored actions. For these threats that lie beyond the DBT, the responsibility for prevention and rests primarily with the state. States, along with the operator, must periodically review their DBT to ensure it results in a reasonable assurance of adequate protection. For instance, after 9/11, the US NRC required improved measures for both physical and cyber-based security, adding cyber-based attacks as characteristic of the DBT.

Despite these periodic reviews and expansions, the demarcation between the DBT and what lies beyond it, for which the state (and not the licensee) is responsible, is blurred and depends in part on who is perceived to be best equipped to defend against a particular threat. Legal liability also depends on which actors are perceived as being in the best position to prevent or mitigate damage or harm.

There is a great deal of concern and confusion about how emerging threats, including cyber-attacks, are incorporated into the DBT. This allocation of responsibility is important since the range of cyber threats is practically unbounded and the attacks themselves are challenging to attribute to a particular threat actor. The question of liability becomes even more complicated for cybersecurity events which fall outside of the existing nuclear reliability regime, such as an attack that does not result in a radiological release. Given the complexities around liability for a nuclear incident, it is important for all stakeholders, operators, regulators and policymakers to be clear about the expectations that nuclear facility operators will be held up to if it occurs.

---

[1] Kathryn Rauhut is a Nonresident Fellow at The Stimson Center in Washington, D.C. She is based out of Vienna, Austria.
[2] Donald Dudenhoeffer currently works for the Austrian Institute for Technology (AIT). He is also based out of Vienna, Austria.
[3] Jacqueline Kempfer is a Research Associate at The Stimson Center in Washington, D.C.
[4] Madison Hissom is a Postgraduate Research Intern at the Center for Global Research at Lawrence Livermore National Lab.

This paper will analyze the legislative history behind the DBT, which is grounded in the concept of "reasonableness," and will discuss the interplay between what exists in the DBT and what goes beyond it, paying particular attention to the dilemma that licensees find themselves in when determining their responsibility to secure facilities against emerging risks. Finally, it considers an industry-approved governance template as a tool with which licensees can demonstrate due care.

Introduction

With the world's increasing dependence on digital technology, nuclear licensees are grappling with implications on the way digitized processes can impact the security of their operations and the protection of sensitive data. Unlike physical security, which is clearly defined and easily quantified, the cyber threat is unbounded and less tangible. Concrete barriers, for example, can be tested and retested against known forces, such as bullets, oncoming vehicles, or explosions. There is no easy parallel for this process in the cyber realm.

Cyber security and nuclear security pose complex technical and strategic challenges to the nuclear energy market. The operator who manages these assets for civilian purposes confronts a sophisticated public liability amidst an uncertain threat landscape**.** What happens when energy supply is disrupted at a nuclear power plant because of a lapse in the operator's cyber security which weakens the plant perimeter and who is responsible? While current threat assessment procedures clearly mark the allocation of responsibility between the operator and the State in the case of a physical attack, this line is blurred in cyberspace. Although responsibility is shared, it is the operators who are on the front lines maintaining both the physical and cyber gates to their nuclear assets.

With some exceptions, civilian nuclear power around the world is increasingly deregulated and privatized. Thus, nuclear power plant operators ("private operators" or "licensees") assume considerable risk, both to their own operations and the public. The necessary investment in costly cyber security mitigation measures is predicated on a clear understanding of the shared respective responsibility and accountability of corporate and government leaders. The current ambiguous allocation of responsibility between the private sector and government poses unique liability concerns for both parties. Namely, if security efforts fail, who is responsible?

The standard of due care that will be expected in liability claims is informed by the State's unique threats, or the adversary characteristics against which licensees are required to defend. This so-called design basis threat (DBT) is defined by the State, which is responsible for establishing its own DBT through its regulator. Additionally, the DBT can provide compliance metrics as both: **a)** An ex-ante standard to meet when employing security measures, and **b)** An ex-post evaluation of whether security measures were adequate.

The need for threat awareness and a threat-driven approach for the physical protection of nuclear materials and facilities has been further formalized through international instruments [1] and international guidance [2][3]. The IAEA's Nuclear Security Series No. 20, *Objective and Essential Elements of a State's Nuclear Security Regime*, (NSS20) regards the nuclear security regime as an essential priority, directing States to identify and assess possible threats to nuclear security within their borders [4][5]. The IAEA's INFCIRC 225, *The Physical Protection Nuclear Materials* (as well as NSS13: *Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities*) further elaborates on this priority, directing States to define requirements for the physical protection of nuclear materials

and facilities based on the threat assessment or DBT [6][7]. Additionally, it states that the licensee should develop a security plan based on this assessment or DBT [8].

Thus, the question emerges, how does an operator match the imperative for physical protection to the pressing need for protection from cyber threats? Just as the former is informed by the DBT, the latter must also rely on a *reasonable* assessment of States' cyber threats and their *reasonable* responsibility to respond to such threats. Critically, there is no consensus on the meaning of "reasonable" in the cyber context.

In order to speculate on future additions to the DBT, we first explain its application to nuclear security. This paper begins with a discussion of the U.S. Nuclear Regulatory Commission's (NRC) DBT, where the concept was initially established, and the subsequent internationalization of that concept by the International Atomic Energy Agency (IAEA). Next, we discuss the evolution of the DBT and the "Enemy of the State Rule" as it applies to operator's responsibility compared with the States. We inform this discussion with the complications of creating a DBT to account for threats in cyberspace. Finally, we present recommendations for guidance that may be valuable for operators not only in evaluating compliance, but also in demonstrating and documenting how and why risk management decisions are made.

While nuclear power is privately produced and operated in many countries with unique commercial, legal, and security regimes, this paper principally cites the experience of the United States. Though U.S. governance comprises most of the case data provided, its lessons and principles are instructive to evaluate an international framework in addressing nuclear and cyber security.

What is the DBT?

The DBT enumerates the range of adversary characteristics against which licensees and State organizations must protect. The DBT delineates the requirements placed on the licensee as well as what protection functions are the purview of State organizations as the two entities share responsibility and accountability for protection [9].

In addition to delineating State and licensee responsibilities, the DBT also serves as a comprehensive description of the spectrum of motivations, intentions, and capabilities of potential adversaries within a region. Physical Protection Systems (PPS) and response forces at nuclear facilities are developed to protect against a specific threat level or adversary capacity along this spectrum and are evaluated by their ability to do so [10][11]. In short, the DBT defines the most credible threat against which an operator can be reasonably expected to defend their facility against. This allows the DBT to serve both as a tool for operators when designing protection systems and as a tool for regulators to evaluate the effectiveness of such systems.

The DBT has long been established for design and verification of classical physical protection systems (PPS), i.e. guns, guards, and gates. PPS design and implementation nominally relies on the three principle functions of Detection (detect an attack), Delay (delay the attack), and Response (use response forces to defeat the attack). The prevalent reference for DBT development and use is the IAEA's Nuclear Security Series No. 10 *Development, Use and Maintenance of the Design Basis Threat* (NSS10). As such, the use of the DBT is often called out in national legislation and/or regulation for nuclear security. The use of a DBT is likewise not limited to nuclear facilities. Some States use a DBT for the implementation of security at

other high-value facilities. The application of the DBT for computer security is more recent and is evolving, but with challenges.

The NRC and its licensees use the DBT as a basis for designing security systems to protect against acts of radiological sabotage [12] and to prevent the theft of special nuclear material [13]. The DBT is described in detail in Title 10, Section 73.1(a), of the *Code of Federal Regulations*, which states that nuclear facility licensees are expected to demonstrate they can defend against the DBT [14].

History of the DBT

To understand the nuclear DBT and its now global reach, one has to start with the origin of the U.S. NRC and its predecessor agency, the Atomic Energy Commission (AEC). Originally established in 1946 to develop the use of atomic energy for the U.S. Government, the AEC's scope was increased after World War II to develop and regulate the burgeoning possibility of civilian nuclear energy.

Following controversy and concerns of conflict of interest over one agency both developing and regulating nuclear power, the AEC was dissolved into two agencies in the 1970's: The Nuclear Regulatory Commission (NRC) and Energy Research and Development Administration (ERDA) [15]. While ERDA would soon be combined with the Federal Energy Administration (US-FEA) to form the United States Department of Energy (US-DOE), the NRC remained as an independent federal regulatory agency responsible for licensing and overseeing the safe operation of civilian nuclear installations and the safe use of specified radioactive materials in the U.S. [16].

NRC's adequate protection standard and enemy of the state rule

The U.S. NRC is unique among administrative agencies in its broad ability to decide how to meet its statutory objectives. The Commission reports to Congress and operates only within the authority given to it under the Atomic Energy Act of 1954 (AEA). The AEA requires licensees to operate "in accord with the common defense and security" and to "provide *adequate protection* [emphasis added] to the health and safety of the public" [17]. "Adequate protection" is neither defined by statute nor regulation, but subsequent case law sheds light on this standard. Under what has been referred to as NRC's first tier of regulation, NRC must ensure that its licensees meet this statutory minimum safety standard before licensed activities can begin [18].

In 1967, the Atomic Energy Commission (AEC) instituted the "Enemy of the State Rule," which lifts the burden from nuclear power plants of protecting themselves from enemies of the United States. Under the rule, operators are not required to provide for design features for the specific purpose of protecting against the effects of these attacks and destructive acts, including sabotage. The NRC inherited this rule from the AEC, specifying that privately-owned nuclear facilities were not responsible for defending against attacks typically carried out by foreign military organizations.

The Cuban Missile Crisis at the height of the Cold War provided the backdrop for the first case in which the concept of "adequate protection" was challenged and the "Enemy of the State Rule" was invoked. At the time, Florida Power and Light Company was constructing two nuclear reactors at Turkey Point in southern Florida. At issue was whether the U.S. NRC, in licensing nuclear reactors for civilian use, had to require its licensees to provide protection against the contingency of hostile enemy action.

In *Siegel v. Atomic Energy Commission* the Court upheld the NRC's "Enemy of the State Rule" stating that "[t]he risk of an enemy attack or sabotage against such structures, like the risk of all other hostile attacks which might be directed against this country, is a risk that is shared by the nation as a whole" [19]. *Siegel* also illustrates how a court interpreted the allocation of responsibility between the private sector and the government, firmly drawing a line in the sand against adding design features to a reactor for the specific purpose of protecting against enemy attacks and destructive acts. Although it declined the responsibility of requiring its licensees to shoulder this burden, the NRC assured that in the event of such an attack many of the design features would assist in assuring adequate protection, such as radioactive containment and the procedures and systems for rapid shutdown of the facility [20].

NRC's imposition of additional safety measures beyond adequate protection

The NRC, taking its own initiative, conceptualized the first DBT in 1977 to protect nuclear reactors from industrial sabotage. The regulation was initially limited to protecting against industrial sabotage by groups and individuals with possible insider information and hand-held weapons, but recognized that the Commission may need to change this limitation as time goes on.

While the Commission cannot consider costs in determining adequate protection, it can consider other factors including the extent of the risk involved. *Union of Concerned Scientists v. NRC* made it clear that adequate protection does not mean absolute protection and permits the acceptance of some level of risk [21]. In short, "safe" does not imply "risk-free." An operator can, however, consider costs if it is an additional safety measure beyond that required by adequate protection [22]. The NRC also has authority under the AEA to issue regulations or standards above and beyond this first tier of regulation to protect public health or to minimize danger to life or property [23]. "Thus, while the NRC *must* provide adequate protection of public health and safety, the NRC *may* provide protection above and beyond adequate protection, if certain conditions are met" [24].

In 1994, the NRC revised the DBT in light of several recent incidents, including an intrusion at a nuclear power plant, the 1993 World Trade Center bombing, and intelligence that indicated that Middle Eastern extremists had the capability and intent to continue to execute major vehicle-borne bombings like the World Trade Center attack [25]. Thus, the revised DBT incorporated the possibility of adversaries using vehicles both for transportation and as bomb-delivery systems. While issuing the revised DBT, the Commission denied that these changes were necessary to meet the adequate protection standard but were being issued under their authority to outline additional safety measures.

Following 9/11, the Commission once again recognized the need for a change in the DBT as many studies showed that nuclear power plants were not designed to withstand an attack using commercial aircraft. Following the implementation of numerous security improvements, the NRC conducted a series of site-specific and detailed studies in order to evaluate the vulnerabilities of nuclear power plants to deliberate attacks involving large commercial aircraft. In June 2004, the Commission proposed an amendment to the DBT to encompass threats including attack forces equal to those of 9/11.

1. The final DBT rule released in March 2007 significantly increased the scope of the threats and, for the first time, included cyberattacks. However, the Commission determined that an air-based attack was not an event against which a private security force could reasonably be expected to defend. Therefore, it judged that such an attack was beyond the reasonable expectation standard. The Commission reasoned that the responsibility for actively protecting against the threat lies

with other organizations of the federal government, as it does for any U.S. commercial infrastructure [26]. In the same report, the Commission also emphasized that "the DBT rule does not focus on the identity, sponsorship, or nationality of the adversaries," but rather a "range of attacks and capabilities" against which private facilities can be "reasonably expected to defend regardless of whether it would or would not be deemed an 'enemy of the state'" [27]. In a later 2008 ruling NRC imposed requirements for aircraft crash impact assessments but it was limited to new reactors only. While this accident assessment is now required in new reactors, the NRC has determined that preventing the impact of a large commercial aircraft is a beyond design basis event [28].

Changing risk calculus

Though the complete scope of the expanded 2007 DBT is classified, the NRC's decisions have clearly been animated by considerations of the credibility of the threat at issue and whether private forces can reasonably be expected to actively engage that threat. The reasonableness concept is perhaps even more animated by the expectation of litigation between victims, nuclear watch dog groups, licensees and regulators in the event of an attack. For nuclear to remain a viable and profitable energy source, it is important to come to common agreement among stakeholders on how to approach defining what is reasonable.

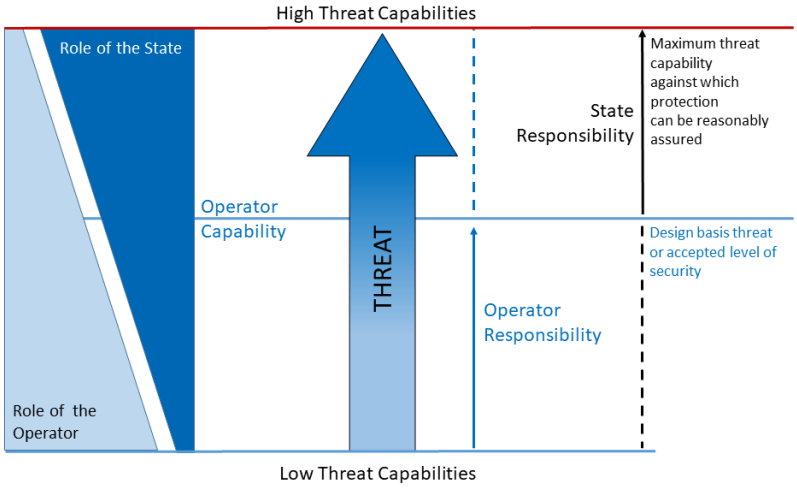
Beyond-DBT scenarios

Before examining the application of the DBT to computer security, it is important to understand the multiple facets of the DBT and its use. Figure 1, adapted from the IAEA, illustrates the concept of the DBT and the allocation of responsibility between the licensee and state.

As we have discussed, the DBT serves as a threshold of responsibility for an operator to defend against and respond to an attack. Imagine a theoretical DBT for a hypothetical facility: an adversarial force of up to five individuals, moderately trained, armed with automatic assault rifles, utilizing motorized transportation, and intent on sabotaging operations at the facility. Given this DBT, the site's PPS should be designed to resist such an attack force with detection, delay, and response measures. The physical nature of such an attack makes it easy to conceive. The PPS could be designed to provide physical intrusion detection, create standoff ranges, withstand expected ballistics, and provide adequate response forces on-site to counter the attack. The operator would be expected to be capable of defending against this event and it is against this capability that a regulating authority would validate protection both in licensing and in assessment activities.

While the operator will always have a responsibility to defend their facility or operation, there are situations in which they cannot be expected to do so alone. Consider the previous hypothetical facility with the same DBT. However, now the facility faces an assault by a paramilitary unit of 100 heavily armed soldiers with artillery and armored vehicles. The operator cannot reasonably be expected to defend against this attack, making it a "beyond DBT" scenario. The operator would depend on the State's assistance to jointly respond to the event. Again, due to the physical nature of this example, the threshold between sole operator responsibility and jointly administered responsibility is easily understood and communicated. Most organizations train for such an event and have implemented well-established protocol to engage State forces.

Figure 1: an illustration of the role of DBT in incident response



International Atomic Energy Agency, "Computer Security for Nuclear Security: Draft Implementing Guide," (2016). NST045, IAEA, Vienna (2018 Member State Approved).

The DBT in cyberspace

Compared to a physical attack, a cyberattack or a hybrid cyber-physical attack is more complicated. NSS13 specifically cites the need to protect computer-based systems used for physical protection, nuclear safety, and material accountancy and control against compromise consistent with the DBT or threat assessment [29]. NSS10, however, provides little discussion of cyberattack considerations. In its discussion of adversarial attributes and characteristics, NSS10 discusses cyber capabilities of adversaries in the context of supporting physical attacks, intelligence gathering, and attacks directly on computer-based systems [30] [31].

Many States use the language of NSS13 as a basis for computer-security regulation and may further define threats, activities, and scenarios against which protection of computer-based systems are required on an ad-hoc basis. Guidance on developing the cyber portion of a DBT is practically non-existent. The IAEA has noted this gap and is nearing completion of an update to NSS10, which will provide greater detail on integrating cyber threat considerations into the DBT. NST045 *Computer Security for Nuclear Security* (in draft form as of 2018) also provides discussion on cyberattack considerations for the DBT [32].

Difficulties of establishing a cyber-DBT

The DBT is a well-established design and regulatory tool, while cyberattacks by adversaries are relatively new. As cyber capabilities increase, the integration of digital technologies into nuclear facilities has grown, creating a target rich environment for potential adversaries. It is a natural progression, therefore, for States to integrate cyberattack considerations into their existing DBT frameworks. Some States create a separate "cyber-DBT" document while other States integrate cyberattack considerations

directly into the existing DBT document. In either scenario, this integration comes with significant challenges.

It is easy to grasp the threat from physical attacks. One can imagine the attackers, their weapons, and their potential impact or damage. Consider the AK-47, a formidable and common assault rifle. The characteristics and ballistics of the weapon are well known, and defenses can be designed to provide detection, delay, and response to its impact. A person armed with an AK-47 represents a narrow threat range based on his or her experience and training. Now consider a laptop computer. We can most certainly define the physical characteristics of its CPU, RAM, battery life, etc., but it is much harder to qualify the exact nature of the impact that an attack using the computer can cause in the same way as one would characterize the AK-47. Whereas ten people armed with assault rifles will almost always be more dangerous than one, one skilled hacker can easily surpass the efforts of a group of ten novices. As such, the metrics and processes used to quantify physical attacks are difficult to apply to the characterization of cyberattacks and cyber threat actors. Unlike conventional off-the-shelf weapons, cyber weapons are reconfigurable, rapidly diversifiable, and continuously evolving. The nature and extent of cyber threats evolves daily and requires immediate and effective countermeasures.

Cyber threats

While cyber threats are more difficult to quantify, they are no less real—and grave—than physical attacks. Consider the following cases:

From December 2011 through June 2012, hackers launched a coordinated and sustained cyberattack targeting 23 U.S. natural gas pipeline operators. The hackers, believed to be linked to the Chinese military, stole valuable information that could potentially be used to sabotage U.S. gas pipelines. The hackers used a campaign of emails sent to key personnel at the companies that tricked them into clicking on malicious links or file attachments allowing the hackers to gain access to the companies' networks. The information stolen included not only sensitive operational and technical details but information that could be used to blow up multiple compressor stations simultaneously [33].

In 2013, Iranian hackers were able to successfully access the Bowman Avenue Dam in Rye Brook, New York, roughly 30 miles north of Manhattan. The Iranians gained access to the dam's control system and were able to gather information on water-level and temperature and would have been able to operate the floodgate remotely. Fortunately, the floodgate was not operating at the time. The hackers were able to access the command and control system through a cellular modem as the control system was being run remotely via the internet [34].

In 2015, Ukraine suffered a massive power outage that left 230,000 people in the west of the country without power for hours. The outage was traced to a cyberattack on the supervisory control and data acquisition (SCADA) system through simple spear phishing emails. In 2016, precisely a year after the first attack, the Pivichna substation near Kiev was targeted, resulting in an hours-long blackout in the surrounding area. While smaller in scale, the second attack showed the increased sophistication of the hackers, who are believed to be Russian. Whereas the 2015 attack involved gaining access to the Ukrainian utilities' networks and manually switching off power to the electrical grid, the 2016 attack was fully automated using malware, alternately named "Industroyer" or "Crash Override." The malware is the second-ever known case of malicious code purpose-built to disrupt physical systems. The malware was programmed to include the ability to "speak" directly to grid equipment, sending commands to switch the

flow of power on and off. Together, these two incidents are the only confirmed cases of blackouts directly caused by hackers [35].

On March 15, 2018, the United States Computer Emergency Readiness Team issued an alert titled 'Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors'. The report details attempts by Russian cyber government actors to target government entities and multiple U.S. critical infrastructure sectors, including energy, nuclear, water, aviation, and various other commercial facilities since at least March 2016. The report details the sophistication of the attack, detailing the two distinct categories of victims (staging and intended targets), the variety of tactics used, and walking the reader through the different stages of the attack [36].

Cyber threats beyond the DBT

As the cases above illustrate, State or State-sponsored actors pose significant cyber threats. One can imagine the line between DBT and "beyond DBT" quickly blurring—indeed it has already blurred—as licensees need to defend against a large spectrum of threats, from individual hackers to military offensive cyber units. How should one define a "beyond DBT" cyber event and the corresponding required response capabilities? While it seems reasonable that any facility should be able to defend against a nominally hostile cyber environment and a certain level of directed attacks, what are the thresholds or indicators that signal a licensee requires State resources to repel an attack?

Possible indicators include:

- the geographic origin of the cyberattack – though this is often incredibly hard to determine, especially as the attack is unfolding;
- the identity of the attacking group – though attribution is very challenging both in real-time and after the fact; and
- the type of cyberattack – however, as demonstrated in the cases above, even sophisticated attackers use trivial methods for compromise.

Perhaps better indicators could focus on the capability, resources, and intention of the attacker.

Such indicators could be:

- Persistence of the attack;
- Multiple methods and breadth of the attack;
- Attack targeting (people or systems); or
- Potential impact of the attack.

If a cyberattack meets some agreed threshold, then external response capabilities may be required. The required expertise, knowledge, and allowable actions of the external responding forces could vary dramatically depending on whether the cyberattack targets IT/business systems, physical protection

systems, or engineering systems. It is paramount that licensees, regulators, and response organizations establish and formalize the protocols for response prior to an event occurring.

Conclusion: Developing Tools to Articulate Reasonableness and Duty of Care

As nuclear operators seek protection from civil litigation in the event of a nuclear security incident, they will have to demonstrate that their actions were reasonable and that have met *the necessary standard of care. Were our actions and policies reasonable in the context of current threats and available precautions?* As noted above, this question is harder to answer than it seems – as technology changes, so too does the concept of reasonableness.

For an example of how technology changes reasonableness over time, one does not need to look at cases of cutting-edge technology, but to a relatively old invention: the radio. In 1928, in the *TJ Hooper* case, a tugboat company lost its cargo after being caught in violent weather at sea [36]. The owners of the cargo sued, arguing that the tugboat company's failure to install a radio (a technology that could have provided weather reports promptly) constituted negligence. The defendant argued that since radios were not previously common on tugboats, it should not be included in calculating its standard of care. The court ruled in favor of the plaintiff, stating that changes in the availability and utility of a technology affect whether it can be deemed necessary to meet a standard of care. The cost of the radio would have been far less than the loss of the cargo. In essence, reasonableness translates into what is "reasonably practicable" in a cost-benefit analysis, and that continuous re-examination of this calculus *over a period of time* is critical to reasonable decision-making.

Within the nuclear context, this means that practices considered safe and secure *today* will inevitably be outdated *tomorrow*, and importantly, practices that reduced liability *yesterday* are not guaranteed to limit liability *today*. Cyber threats can complicate this further; while chain-link fences may deter and delay a wide swath of threats in the physical realm, defense from one cyber threat may require a very specific practice or technology. Thus, it is especially challenging to place cyberspace within the wider context of country-level threat assessments and DBTs, as regulatory bodies cannot foresee each and every possible vector of the cyber threat. The operator's risk-accepting authority faces similar limitations as it works to meet its own standard of care.

As a way to help track reasonableness, the Stimson Center, along with various partners from civil society and nuclear industry, is developing an *Organizational Governance Template for Nuclear Security* – a reporting tool that can help operators illustrate and track they have acted reasonably and could provide a transparent statement of criteria that were evaluated by those making risk management decisions. The governance template pulls from a wide variety of existing security guidelines, including IAEA nuclear security series documents, and the WINS Best Practice Guide on Security Governance. It also incorporates insights from the World Association of Nuclear Operators (WANO) and the U.S.-based Institute of Nuclear Power Operators (INPO) industry guidance for safety as these leadership recommendations can also help develop strong nuclear security practices. To date, Stimson has received positive feedback from industry stakeholders on the structure and individual questions in the template, in an effort to ensure that top-level managers and boards/advisors find it a useful tool in presenting their security governance model. Overall, the template serves as a resource to help nuclear operators illustrate how security considerations are decided, implemented, and internalized by the entire organization. Doing so, enables individuals outside of an organization to understand how the demonstrates its "duty of care," i.e., not only by adhering to minimum regulatory requirements but also

by fostering a work environment that promotes continuous improvement, adapts to evolving risks and embeds nuclear security as a core value.

During the 2016 Nuclear Industry Summit (NIS), Working Group III reviewed the "Nuclear Security Governance Reporting Template," a document originally developed and included in the WINS Corporate Governance Arrangement for Nuclear Security report released earlier that year. The goal is to present the 10 questions in the template as a resource for nuclear operators as they think through their decisions on how to prioritize and implement nuclear security in their respective facilities. Answers to the template could also be incorporated in annual reports, to demonstrate good security governance, without divulging sensitive information.

Since the 2016 NIS, the Stimson Center, along with the WINS, expanded on the original version of the template. Over the past two years questions have been developed based on existing guidance documents from the International Atomic Energy Agency and the WINS Best Practice Guide on Security Governance — one of the earliest analyses linking corporate governance and security culture. It incorporates insights from the World Association of Nuclear Operators (WANO) and the U.S.-based Institute of Nuclear Power Operators (INPO) industry guidance for safety as these leadership recommendations can also help develop strong nuclear security practices. The current template is meant to be a resource to help nuclear operators illustrate how security considerations are decided, implemented, and internalized by the entire organization.

Stimson's Nuclear Security Governance Template has been tested through a series of three roundtables over as many years. These roundtables have gathered nuclear industry stakeholders including nuclear lawyers, insurers, regulators, operators, suppliers, and communications specialists from around the world. The first two meetings examined executive and corporate responsibility in demonstrating 'duty of care', and testing whether a voluntary reporting template can help an organization demonstrate its duty of care if the need arises to defend against a negligence claim. In October of 2017 Stimson, in partnership with 39 Essex Barristers and WINS, held a mock trial, based on a hypothetical scenario involving a cyber/physical incident that did not result in a radiological release. A radiological release is avoided, in order to circumvent strict operator liability under existing international and domestic liability regimes. Stimson has also received feedback from individual industry stakeholders on the structure and individual questions in the template, in an effort to ensure that top-level managers and boards/advisors find it a useful tool in presenting their security governance model.

The overarching goal of this work is to promote transparency by enabling individuals outside of an organization to understand how the organization/company demonstrates its "duty of care," i.e., not only by adhering to minimum regulatory requirements but also by fostering a work environment that promotes continuous improvement, adapts to evolving risks and embeds nuclear security as a core value. Thus, the focus is on organizational decision-making and how this affects the beliefs and attitudes of the individuals tasked as the responsible stewards of nuclear material and technologies.

Acknowledgements

This paper was sponsored by the U.S. Department of Energy – Partnership for Nuclear Threat Reduction, the MacArthur Foundation, and the Carnegie Corporation. We are grateful to WINS for the inspiration provided for this paper. Finally, the roundtable and this summary report would not have been possible without the lively debates and insights from numerous nuclear professionals throughout the world and the outstanding editorial support from our Stimson intern Jared Zimmerman.

References

[1] International Atomic Energy Agency, *Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1*. Vienna, 1980.; International Atomic Energy Agency, *Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10–GC(49)INF/6*. Vienna, 2005.
[2] International Atomic Energy Agency, *Objective and Essential Elements of a State's Nuclear Security Regime, Nuclear Security Fundamentals.* No. 20. IAEA Nuclear Security Series. Vienna, 2013.
[3] International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).* No. 13. IAEA Nuclear Security Series. Vienna, 2011.
[4] International Atomic Energy Agency, *Objective and Essential Elements of a State's Nuclear Security Regime, Nuclear Security Fundamentals.* No. 20. IAEA Nuclear Security Series. Vienna, 2013.
[5] International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).* No. 13. IAEA Nuclear Security Series. Vienna, 2011.
[6] International Atomic Energy Agency. *Development, Use and Maintenance of the Design Basis Threat, Implementing Guide*. No. 10. IAEA Nuclear Security Series. Vienna, 2009
[7] International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).* No. 13. IAEA Nuclear Security Series. Vienna, 2011.
[8] International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).* No. 13. IAEA Nuclear Security Series. Vienna, 2011.
[9] "Design Basis Threat (DBC)," U.S. NRC, Last modified December 9, 2014, accessed September 7, 2018, http://www-ns.iaea.org/security/dbt.asp?s=4.
[10] International Atomic Energy Agency. *Development, Use and Maintenance of the Design Basis Threat, Implementing Guide*. No. 10. IAEA Nuclear Security Series. Vienna, 2009
[11] International Atomic Energy Agency, *Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1*. Vienna, 1980.; International Atomic Energy Agency, *Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10–GC(49)INF/6*. Vienna, 2005.
[12] "Radiological sabotage," U.S. NRC, Last modified July 6, 2018, accessed September 4, 2018, https://www.nrc.gov/reading-rm/basic-ref/glossary/radiological-sabotage.html.
[13] "Special nuclear material," U.S. NRC, Last modified July 6, 2018, accessed September 4, 2018, https://www.nrc.gov/reading-rm/basic-ref/glossary/special-nuclear-material.html.
[14] United States of America. Nuclear Regulatory Commission. *Rules and Regulations: Design Basis Threat.* Vol. 72. Series 52. Government Publishing Office, 2007. 12705-2727. Accessed August 31, 2018. https://www.gpo.gov/fdsys/pkg/FR-2007-03-19/pdf/07-1317.pdf.
[15] "The Nuclear Regulatory Commission," Union of Concerned Scientists, accessed September 7, 2018, https://www.ucsusa.org/nuclear-power/whos-responsible-nuclear-power-safety/the-nuclear-regulatory-commission#.W5KEWs5KgdU.
[16] "About NRC," U.S. NRC, Last modified February 12, 2018, accessed September 7, 2018, https://www.nrc.gov/about-nrc.html.
[17] United States of America. Nuclear Regulatory Commission. *United States Code: Title 42 - The Public Health and Welfare § 2232 License Applications.* Government Publishing Office, 2017. 4854-855. Accessed August 31, 2018. https://www.gpo.gov/fdsys/pkg/USCODE-2017-title42/pdf/USCODE-2017-title42-chap23-divsnA-subchapXV-sec2232.pdf.

[18] Ostendorff, William C., and Kimberly A. Sexton. “Adequate Protection after the Fukushima Daiichi Accident: A Constant in a World of Change.” *Nuclear Law Bulletin*, 2013/1, no. 91 (2013): 23-41. Accessed August 31, 2018. https://www.oecd-nea.org/law/nlb/nlb91.pdf.
[19] Siegel v. Atomic Energy Commission (D.C. Circuit 1968).
[20] Siegel v. Atomic Energy Commission (D.C. Circuit 1968).
[21] Union of Concerned Scientists v. NRC (D.C. Circuit 1987).
[22] Ostendorff, William C., and Kimberly A. Sexton. “Adequate Protection after the Fukushima Daiichi Accident: A Constant in a World of Change.” *Nuclear Law Bulletin*, 2013/1, no. 91 (2013): 23-41. Accessed August 31, 2018. https://www.oecd-nea.org/law/nlb/nlb91.pdf.
[23] U.S. NRC, “Atomic Energy Act of 1954,” (Washington, D.C. USA: 83rd United States Congress, 1954), Section 161.
[24] Ostendorff, William C., and Kimberly A. Sexton. “Adequate Protection after the Fukushima Daiichi Accident: A Constant in a World of Change.” *Nuclear Law Bulletin*, 2013/1, no. 91 (2013): 23-41. Accessed August 31, 2018. https://www.oecd-nea.org/law/nlb/nlb91.pdf.
[25] Public Citizen v. Nuclear Regulatory Commission. (9th Circuit 2009).
[26] United States of America. Nuclear Regulatory Commission. *Rules and Regulations: Design Basis Threat.* Vol. 72. Series 52. Government Publishing Office, 2007. 12705-2727. Accessed August 31, 2018. https://www.gpo.gov/fdsys/pkg/FR-2007-03-19/pdf/07-1317.pdf.
[27] United States of America. Nuclear Regulatory Commission. *Rules and Regulations: Design Basis Threat.* Vol. 72. Series 52. Government Publishing Office, 2007. 12705-2727. Accessed August 31, 2018. https://www.gpo.gov/fdsys/pkg/FR-2007-03-19/pdf/07-1317.pdf.
[28] United States of America. Nuclear Regulatory Commission. *Consideration of Aircraft Impacts for New Nuclear Power Reactors*, Final Rule, 74 Federal Register 28111, June 12, 2009.
[29] International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).* No. 13. IAEA Nuclear Security Series. Vienna, 2011.
[30] International Atomic Energy Agency. *Development, Use and Maintenance of the Design Basis Threat, Implementing Guide*. No. 10. IAEA Nuclear Security Series. Vienna, 2009.
[31] International Atomic Energy Agency, *Computer Security for Nuclear Security: Draft Implementing Guide*. NST045. Vienna, 2016. (2018 Member State Approved).
[32] International Atomic Energy Agency, *Computer Security for Nuclear Security: Draft Implementing Guide*. NST045. Vienna, 2016. (2018 Member State Approved).
[33] Clayton, Mark. “Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage.” *The Christian Science Monitor*, February 27, 2013. Accessed on August 21, 2018. https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage
[34] Thompson, Mark. “Iranian Cyber Attack on New York Dam Shows Future of War.” *Time*, March 24, 2016. Accessed on August 21, 2018. http://time.com/4270728/iran-cyber-attack-dam-fbi/
[35] Greenberg, Andy. “‘Crash Override’: The Malware That Took Down a Power Grid.” *Wired*, June 12, 2017. Accessed on August 21, 2018. https://www.wired.com/story/crash-override-malware/
[36] Department of Homeland Security. *Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.* United States Computer Emergency Readiness Team. Last modified March 16, 2018. Accessed August 21, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A
[37] The T. J. Hooper. The Northern No. 30 and No. 17. The Montrose. In re Eastern Transp. Co. New England Coal & Coke Co. v. Northern Barge Corporation. H. N. Hartwell & Son, Inc., v. Same. (2nd Circuit 1932).