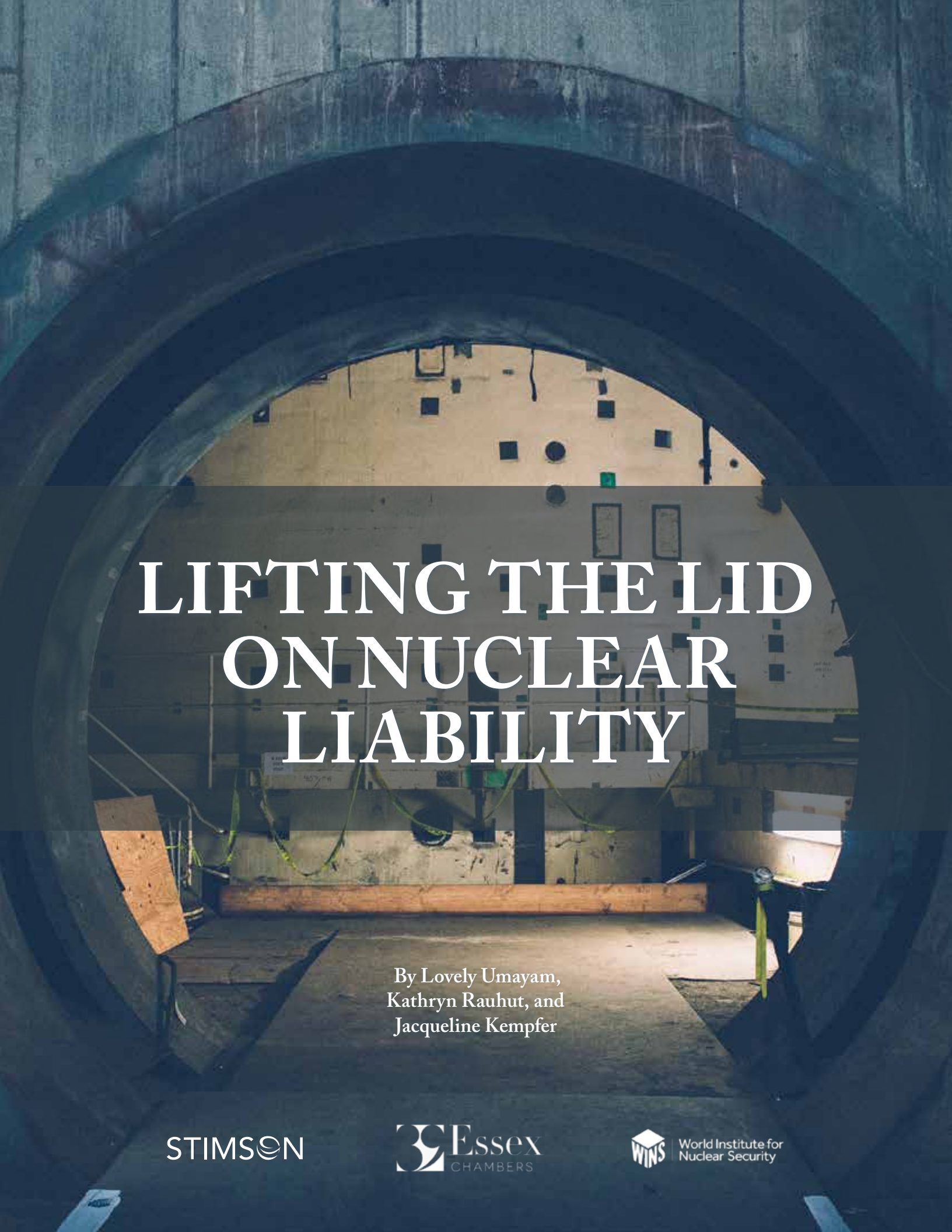


LIFTING THE LID ON NUCLEAR LIABILITY

By Lovely Umayam,
Kathryn Rauhut, and
Jacqueline Kempfer

STIMSON

Essex CHAMBERS

WINS World Institute for Nuclear Security

On the cover:
"Satsop Nuclear Power Plant - Washington State"
by Tony Webster (sharkhats via flickr)

Stimson Center
1211 Connecticut Avenue, NW, 8th Floor
Washington DC 20036
www.stimson.org

Acknowledgements

The Nuclear Security: Demonstrating Strong Governance and Due Care roundtable and this report are sponsored by the U.S. Department of Energy — Partnership for Nuclear Threat Reduction, the MacArthur Foundation, and the Carnegie Corporation.

We are grateful to the World Institute for Nuclear Security, 39 Essex Chambers, the Security Awareness Special Interest Group, and Nuclear Risk Insurers for their continued support and feedback to this project. Finally, the roundtable and this summary report would not have been possible without the lively debates and insights from the roundtable participants: Nawah, Freshfields, Context, Northcourt Limited, Norton Rose Fulbright, Burgess Salmon, Chatham House, and Westminster Energy Forum.

Flickr: Michael Kappel

THE CHALLENGE

Navigating a Dynamic Security Environment

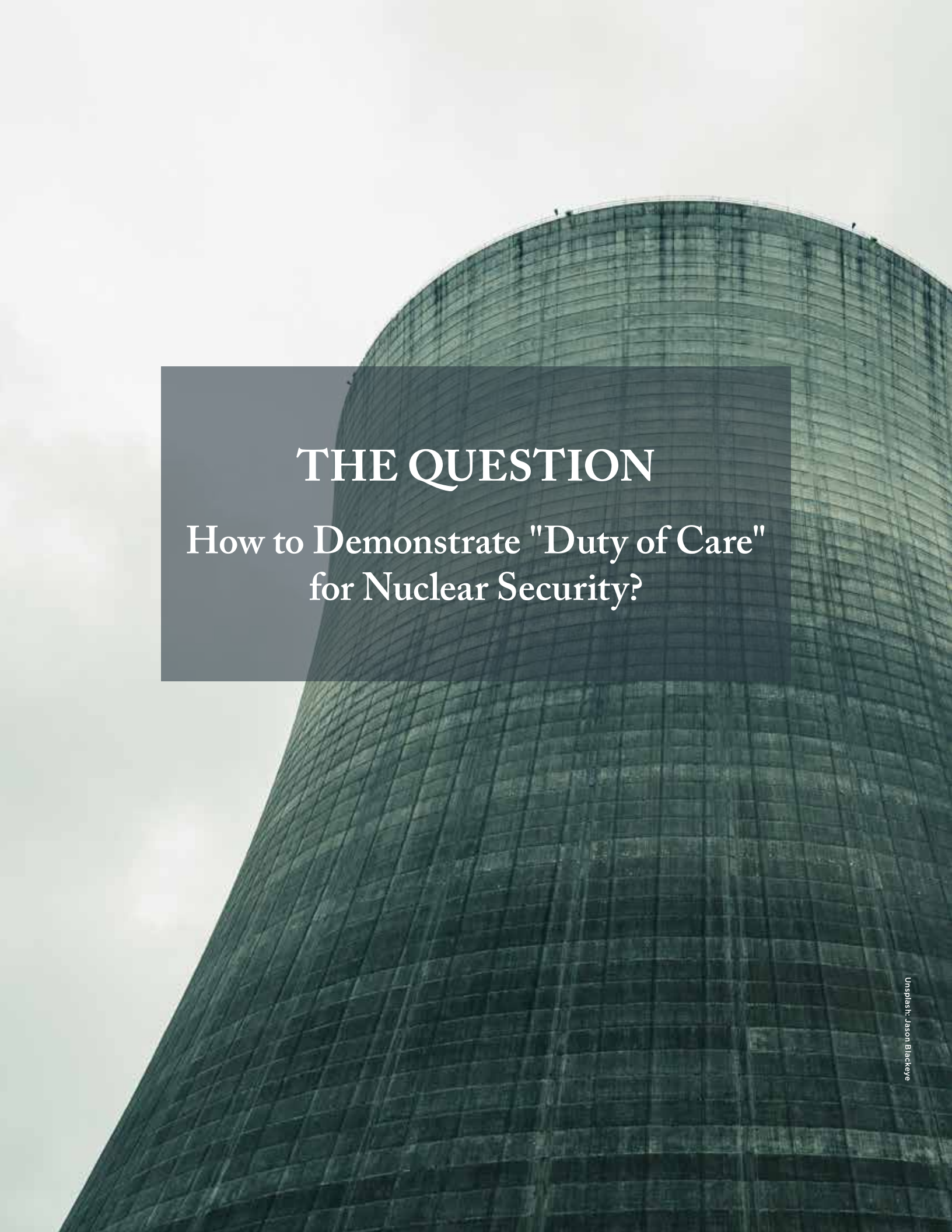
Unsplash: Markus Spiske

Cybersecurity incidents are sadly the new normal — in 2017 alone, cyber hackers compromised millions of items of personal information, with some attacks making news headlines for successfully exploiting the security vulnerabilities of big-name businesses[1]. In addition to data theft, cybersecurity experts have pointed to the increasing complexity and risk of cyber attacks on critical infrastructure, including obtaining operational access to the power grid[2]. **Along with the steady rise of attacks comes a culture shift towards security awareness and accountability — a growing demand from the public that companies do better to institute proactive security practices so that they learn from past incidents and stay ahead of the threat curve.** Being cyber secure is no longer confined within the realm of IT; board and executive level spending decisions significantly impact the security culture of a given organization or company, which in turn affect how cyber security is prioritized, managed, and implemented at the operational level. Indeed, recent extreme examples of corporate leaders hiding data breaches and complying with hacker's demands[3] do not bolster public confidence that individuals at the top of the organizational chain are making the right decisions to manage cyber risks effectively.

In the nuclear sector, the consequences of a cyber attack could go far beyond loss of data — there is a spectrum of undesirable outcomes, from theft of nuclear material to an all-out radiological release. A security incident in a nuclear facility is also likely to involve an insider threat component[4]; whether out of negligence or malicious intent, an assist from someone with authorized access to a facility's computer systems can make it easier to execute an attack. While the nuclear community recognizes the dynamic nature of cyber and insider threats and their potential overlap, there is still more to be done in understanding how nuclear facility operators can reasonably limit or manage the risk from such threats. In a security environment that is growing in complexity, including possible blended cyber-physical attack vectors[5] that make it difficult to anticipate the sequence and pace of attack, risk management and an organizational culture attuned to security vulnerabilities are becoming important considerations for prevention and resilience. The nuclear industry acknowledges that regulatory compliance is a baseline[6]; it is therefore incumbent upon both governments and industry stakeholders continuously to improve security approaches and consider how lack of awareness and organizational accountability could not only affect the organization's business, but also inflict reputational damage to the entire sector. Operators are held captive to each other's performance; a security or safety incident at any facility will have significant repercussions for all. In the aftermath of a serious security incident, owners and operators of nuclear facilities have the potential for significant civil and criminal liability for failure to take reasonable measures to protect the public. **The public will want to know who is responsible and what could have been done to prevent the incident or mitigate its effects; nuclear executives and their boards will be under intense scrutiny for the security decisions they made that might have prevented the incident.**

THE QUESTION

How to Demonstrate "Duty of Care" for Nuclear Security?



Unsplash: Jason Blackeye

As part of a long-standing series examining legal accountability and liability for nuclear security[7] the Stimson Center, in partnership with the World Institute for Nuclear Security (WINS) and UK Barristers' Chambers, 39 Essex Chambers, hosted a closed roundtable on *Nuclear Security: Demonstrating Strong Governance and Due Care*. Participants from civil society, regulatory bodies, and nuclear industry attended the event to discuss the implications of a cyber-physical security incident on a hypothetical nuclear facility, and the ways in which the operator may face legal inquiries about the *reasonableness* of its security decisions and practices in light of the incident. The roundtable featured a mock trial component in which retired and current criminal and civil judges, upon hearing debates on possible civil and criminal claims resulting from the incident, offered rulings on whether the operator of the hypothetical plant in question would be held liable for civil and criminal charges for failure to prevent or mitigate against a terrorist related event.

Ultimately, the purpose of exploring gray areas of existing liability mechanisms is to identify potential economic incentives for industry stakeholders to make more careful and sustainable security decisions. While avoiding lawsuits and fines is a powerful motivator for corporate executives and government operators, the end goal is to shift mindset and behavior, in particular senior management who are faced with difficult spending decisions on low probability, but high risk and high consequence considerations, such as security enhancements. 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.

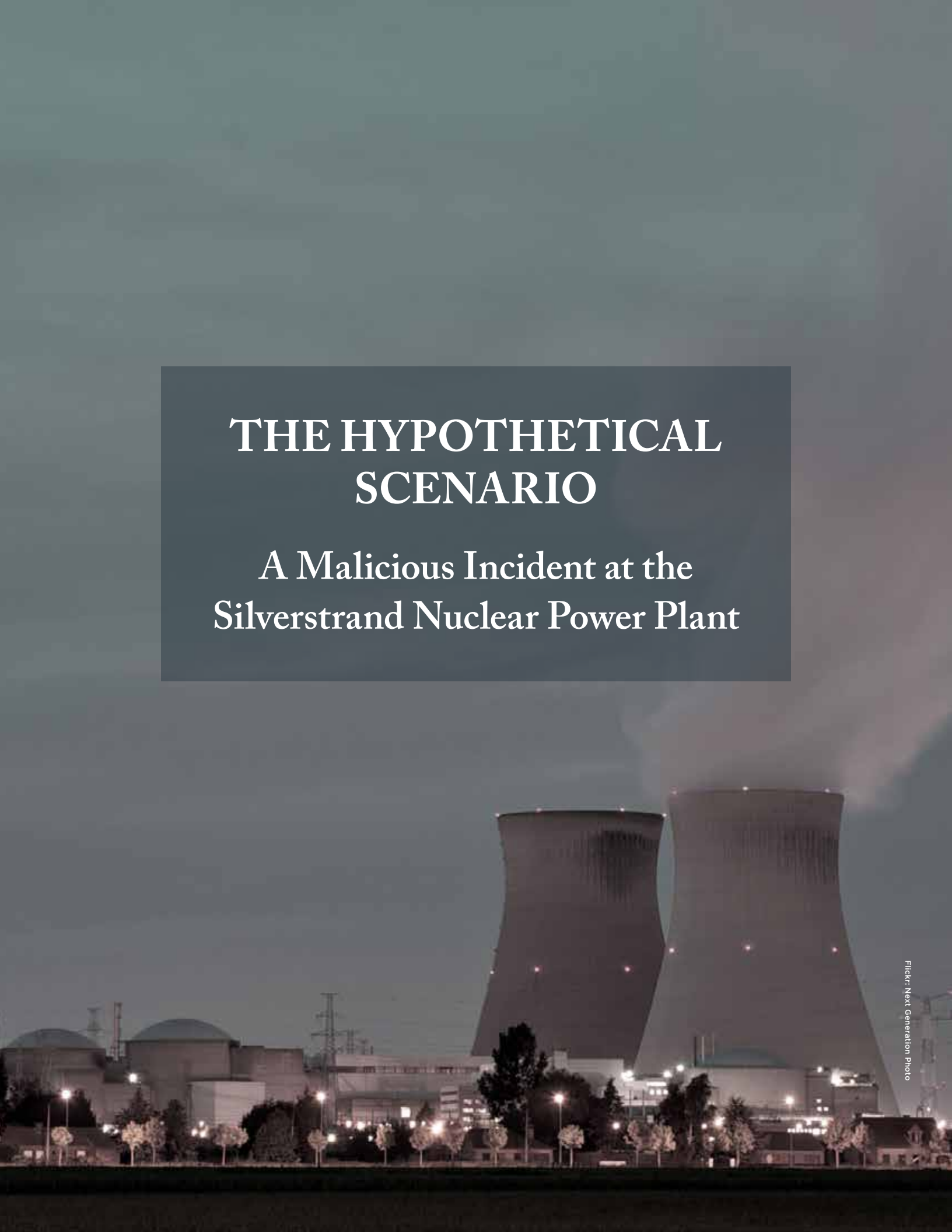
Of special interest are two gray areas: (1) understanding the legal consequences of a security incident that does not result in radiological contamination, thereby potentially circumventing strict operator liability under existing international and domestic liability regimes[8]; and (2) identifying factors aside from regulatory compliance that could help ascertain whether an organization exercised its duty of care to successfully defend against a claim of negligence. Duty of care is the legal obligation of a company to take reasonable care or exercise reasonable skills in its operation of a nuclear facility to protect members of the public from a malicious act. It refers to the care, caution, or action a reasonable person is expected to take under similar circumstances. It is important because it is often the case under national legislation that a defendant must prove that all precautions, reasonable under the circumstances, were taken to prevent or mitigate losses from a terrorist related event. If the defendant fails to do so, she/he can be held liable for civil or criminal negligence under the law. Because there is no international standard or precedent in nuclear or cyber security for what is "reasonable under the circumstances," there is a need to focus on a standard for liability, whether it is civil or criminal. In countries such as the US, where there is long experience of such litigation flowing from terrorism related events, case-law may provide guidance around the relevant concepts for liability. In other jurisdictions, including the UK, the case-law is less developed. Roundtables and scenario exercises can help inform operators when determining "how much is enough' when it comes to reasonable care.

In addition to regulatory compliance, a facility owner or operator also needs to demonstrate that it considered industry best practices, and has made organizational decisions on security that are based on a risk-informed approach. **Thus, Stimson presented a draft Nuclear Security Organizational Governance Template[9] — a voluntary reporting framework that would help industry stakeholders explain their decision-making processes for nuclear security, particularly in cultivating security culture in the workplace — and asked participants whether such a template could help an organization demonstrate its duty of care.**

The following are reflections and main conclusions from the group.

THE HYPOTHETICAL SCENARIO

A Malicious Incident at the Silverstrand Nuclear Power Plant



Flickr: Next Generation Photo

To set the stage for a structured and spirited conversation, Stimson, WINS, and 39 Essex presented a hypothetical scenario involving a cyber-insider incident at the Silverstrand Nuclear Power Plant (SNPP) in the fictitious country of Ruritania.[10] While this incident did not result in a core meltdown or release of radiation, it successfully triggered a reactor shutdown, which consequently strained the power grid, and resulted into a major power outage during one of the worst heatwaves of the year. The outage caused billions of dollars in damage and losses, as well as several deaths due to heat-induced illnesses. Police investigations revealed that a disgruntled employee influenced by a terrorist organization developed malware that granted him full access rights to the physical protection of the facility, which allowed him to sabotage the plant. It was also discovered that SNPP management refrained from implementing several security recommendations, including improved training resources and patch management policies per security audit findings, due to financial considerations and the fact that Ruritania does not have specific regulatory requirements related to cyber security. The incident yielded two legal cases against the owner/operator of SNPP: a class action civil claim filed by those affected by the outage, as well as criminal proceedings against the CEO, Operations Director, and Chief Security Officer.

This hypothetical scenario represents a *black swan* event[11] — an unlikely outlier that yields extreme impact (and in hindsight, is perceived to have been predictable). Although the series of events that unfolded at the fictional SNPP are low probability, discrete security vulnerabilities in the scenario were drawn from actual incidents, among them a weak security culture that breeds an insider threat, and lenient cybersecurity practices that ultimately led to a vulnerability in the plant's physical protection system. Examining black swan events can help illuminate the limitations of current thinking, especially the ways in which the "unknown" shapes the way we manage and respond to risk. For the roundtable discussion, the goal was to encourage participants to examine the implications of a security incident that falls outside of the existing nuclear liability regime: ***without a radioactive release and strict operator liability, what factors should be considered in the court of law to ascertain whether the duty of care was breached by the operator?***

LEGAL DELIBERATIONS

Unsplash: Sebastian Pichler

Outcome of Deliberations

- Executives and boards are responsible for investment and operational decisions concerning nuclear safety, security and emergency preparedness, but such decisions will involve trade-offs between corporate profitability and other operational issues. **Participants agreed that putting emphasis on organizational governance and accountability for nuclear security would incentivize nuclear operators to make business decisions that adapt to and reduce risk.** Although addressing security threats are traditionally under the purview of the State, the private sector — in this case licensee holders managing and operating nuclear facilities — have a prominent role to play as the ultimate implementer of physical protection systems. This duty is articulated[12] in the recently amended Convention on the Physical Protection of Nuclear Materials (Fundamental Principle E), as well as International Atomic Energy Agency (IAEA) nuclear security guidelines.
- To determine whether "duty of care" has been breached, one must pose the question: **did the license holder (in the case of the presented hypothetical scenario, the SNPP management) fail to take *reasonable* care or *reasonable* skill in the operation of the facility, including the security of material, equipment, and personnel?** Thus, the issue at hand is not whether the license holder is obligated to protect against malicious acts by a third-party adversary, but whether the license holder has contributed to risk by failing to uphold practicable security measures, which inevitably made the facility vulnerable to such malicious acts.
- Under the court of law, various factors other than regulatory requirements may be used to determine "reasonableness," including the license holder's actions to address or correct foreseeable threat and vulnerabilities (i.e., the State has notified the facility operators of potential threats, or audits have revealed specific security deficiencies). Common industry practices such as codes of conduct, as well as voluntary best practice guides developed by authoritative sources such as the IAEA, could also be referenced to form a baseline upon which to measure reasonableness. **Thus, it is in the license holder's interest not only simply to comply with regulations, but also exhibit organizational capacity for continuous improvement, by way of considering best practices outside of regulatory requirements.**
- Some participants stressed the importance of **distinguishing between taking *all reasonable precautions* (i.e., a control system has been established by the license holder to manage and address security risks) and *all due diligence* (i.e., measures have been taken to ensure that the established system is working consistently and satisfactorily).** Both elements must be satisfied to demonstrate compliance with the operator's duty of care.
- The magnitude of the potential risk should also be carefully evaluated when attempting to ascertain the duty of care. Risk management always involves a cost benefit analysis in which grave risks demand a higher standard of care. Cybersecurity and risks posed by combined physical cybersecurity threats are steadily escalating. **Hence, license holders must have the organizational capacity to respond swiftly to these developments, and may sometimes be called upon to act beyond regulatory requirements, especially if regulations have not been adjusted to address dynamic threats.**
- Participants debated whether an intervening third-party had broken the chain of causation between the license holder's actions and loss, i.e., whether the SNPP manager should not be held responsible for the power outage since a third-party adversary — the disgruntled employee — carried out the attack. **Referencing *Environment Agency v. Empress Car Company. [1999] 2 AC 22*[13], it was ultimately decided that if the license holder owes a duty to prevent (as is in the case of for upholding nuclear security), when there is a failure to discharge that duty, there is no break in the chain of causation. In short, the license holder will be found accountable.**

THE FINAL VERDICT

Unsplash: Beatriz Pérez Moya

Judges' Ruling

The judges delivered opinions after both civil and criminal deliberations. They ruled that the SNPP management was civilly and criminally liable. **According to the rulings, there were clear indications that organizational leadership within the SNPP failed to reasonably address security deficiencies since management did not perceive value in pursuing additional security measures despite security audit recommendations and other signs that improvements must be made.** An eroding security culture (i.e., ineffective cybersecurity training) also exacerbated existing vulnerabilities that the adversary exploited. It did not matter whether the actions of SNPP management were in violation of regulations; it recognized the risk, but decided against any significant changes to security practices. The Chief Executive and Chief Security Officer of SNPP were found guilty of connivance — they were aware of the criminal acts (a breach in duty of care) as they were being performed.

Value of the Governance Template in Mounting a Defense

Participants were asked if the adoption of the proposed nuclear security governance template would help the SNPP management demonstrate its duty of care, and potentially reduce liability. **Participants acknowledged the template as a useful risk assessment and mitigation tool since it forces license holders to explain a holistic strategy — from risk management communication at the executive-level to cultivating security culture among operational personnel — to achieve and maintain nuclear security without divulging any specific, sensitive information.** Several participants also noted that the format of the template is quite flexible, allowing license holders to tailor their answers to match a changing threat environment.

But while the template can help outline the license holder's duty of care as it relates to security, it cannot stand alone as proof. Thus, the template alone only demonstrates reasonable precaution. The judges determined that the template is useful in building a case, as it demonstrates how and why risk management (cost-benefit) decisions were made. Whether those decisions were reasonable under the circumstances is a decision for the trier of fact. Without a more thorough demonstration of their efforts the defendant was found guilty. However, organizational governance efforts that had been made by SNPP, including the adoption of the template, would be taken into consideration as a sentencing factor. Any framework or voluntary standard can be influential in shaping due diligence as the standards can become "de facto" industry requirements. In the wake of a security event, these industry norms can play a defining role in evaluating liability.

Overall, the template is strongest when it is considered as a complement to existing regulation. While regulatory requirements establish the ceiling for culpability, the template helps contextualize organizational decisions around security, and if filled out consistently, can also illuminate trends in how organizational governance adjusts to evolving threats.

Citations

1. Larson, Selena. "The Hacks that Left Us Exposed in 2017." CNN, December 20, 2017. Accessed February 15, 2018. http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html.

2. Greenberg, Andy. "Hackers Gain Direct Access to US Power Grid Controls." Wired, September 6, 2017. Accessed February 15, 2018. https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/.

3. Pollard, Jeff, and Heidi Shey. "Uber's Uber Breach: A Stunning Failure in Corporate Governance and Structure." Forbes, December 5, 2017. Accessed February 15, 2018. https://www.forbes.com/sites/forrester/2017/12/05/ubers-uber-breach-a-stunning-failure-in-corporate-governance-and-culture/#5188e6cb59fc.

4. Bunn, Matt, and Scott D. Sagan. Insider Threats. Ithaca, NY: Cornell University Press, 2017.

5. St. John-Green, Mike. " 'Differences between defence-in-depth for computer security and physical protection." Presentation at The International Conference on Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, Austria, November 13-17, 2017.

6. "Joint Statement of the 2016 Nuclear Industry Summit." Nuclear Industry Summit 2016, March 30, 2016. Accessed July 11, 2017. http://nis2016.org/agenda/documents/documents-nuclear-industry-summit-2016-joint-statement/.

7. "Demonstrating Due Care: Cyber Liability Considerations in Nuclear Facilities." Stimson Center, April 24, 2017. Accessed February 15, 2018. https://www.stimson.org/content/demonstrating-due-care-cyber-liability-considerations-nuclear-facilities.

8. International nuclear liability regimes (The Vienna Convention on Civil Liability for Nuclear Damage and Paris Convention on Third Party Liability in the Field of Nuclear Energy), as well as domestic law (i.e., U.S. Price-Anderson Act) generally cover damage from a radiological release or a precautionary action, such as an evacuation, related to a potential release.

9. "Nuclear Security Governance Template, Draft." Stimson Center, October 3, 2017. Accessed February 15, 2018. https://www.stimson.org/nucleargovernance.

10. Full hypothetical scenario is available upon request. Please contact nuclearsecurity@stimson.org for more information.

11. Taleb, Nassim Nicholas. "First Chapter: 'The Black Swan: The Impact of the Highly Improbable.'" New York Times, April 22, 2007. Accessed February 15, 2018. http://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html.

12. "An Industry-Led Governance Framework for Demonstrating Strong Security." Stimson Center, November 16, 2017. Accessed February 15, 2018. https://www.stimson.org/content/industry-led-governance-framework-demonstrating-strong-security.

13. A case in which the defendant company (Empress Car Company) kept diesel in a tank with an unsecured tap, in a yard directly drained into a river. An unknown passerby opened the tap and the diesel consequently overflowed into the river. The House of Lords held that Empress Car Company has still "caused" the incident for maintaining noxious substances unprotected. For more information, see https://webstroke.co.uk/law/cases/environment-agency-v-empress-car-co-1999.

LIFTING THE LID ON NUCLEAR LIABILITY

ABOUT STIMSON

The Stimson Center is a nonpartisan policy research center working to solve the world's greatest threats to security and prosperity. Think of a modern global challenge: refugee flows, arms trafficking, terrorism. These threats cannot be resolved by a single government, individual, or business. Stimson's award-winning research serves as a roadmap to address borderless threats through collective action. Our formula is simple: we gather the brightest people to think beyond soundbites, create solutions, and make those solutions reality. We follow the credo of one of history's leading statesman, Henry L. Stimson in taking, "pragmatic steps toward ideal objectives." We are practical in our approach and independent in our analysis. Our innovative ideas change the world.

STIMSON

Essex CHAMBERS

WINS World Institute for Nuclear Security