DETERRING NUCLEAR AND RADIOLOGICAL MATERIAL THEFT, SABOTAGE, OR ILLICIT TRAFFICKING

Authors: Olympia Hunt and Stephen V. Mladineo, Pacific Northwest National Laboratory

Vienna, Austria and Washington, D.C.

May 23, 2023

Abstract
Although deterrence is a foundational aspect of defense strategies, recent threats of the use of nuclear or radiological weapons have cast a new light on its meaning. Distinctly different from compellence, deterrence places the autonomy of decision on the potential aggressor. In the case of deterrence, potential aggressors are not directly forced to restrain themselves from attacking, instead, they decide that it is in their best interest to self-restrain based on the nature of the environment that they find themselves in. However, the recognized vulnerability of deterrence is that it relies heavily on understanding an adversary's value and risk metrics.

Advances in decision science and human behavior analytics have enriched our understanding of motivations and reasons for decisions beyond rational choice theory. In addition, changes in environment can also alter motivations for action. For example, 'rational' cost benefit analysis is significantly different for decision-makers during wartime versus peacetime. Specifically analyzing nuclear and radiological security during wartime, this paper will incorporate recent developments in decision science and deterrence theory, in addition to real-world case studies, to identify predicted vulnerabilities in reliance on deterrence in these situations.

Introduction
President Biden recently released National Security Memorandum (NSM-19) to Counter Weapons of Mass Destruction Terrorism and Advance Nuclear and Radioactive Material Security worldwide. One of the important policy tenets of this document is that the U.S. Government should: "Deter and prevent actors from supporting WMD terrorism."[1] While deterrence has been a key part of U.S. National Security Strategy for a long time, the concept has principally been applied to nuclear weapons policy. Officials outside of the Defense Department have objected to explicitly incorporating deterrence into their programmatic strategies because it is perceived to be too hard to measure accurately. This paper explores the history and applicability of deterrence theory and attempts to answer the question of how to think about deterring nuclear and radiological material theft, sabotage, and illicit trafficking. In addition, the paper touches on nuclear and radiological security during wartime.

History
Deterrence theory is an ancient concept described by Cesare Beccaria (1738–1794), considered the father of deterrence theory related to criminology. He argued that the swift, sure, and strong punishment of criminals would prevent others from choosing criminal activity.[2] After World War II scholars picked up the concept as a way of considering the impact of nuclear weapons on warfare.

Thomas Schelling approached the topic of deterrence from an Economist's perspective. In his books Strategy of Conflict and Arms and Influence, using a game theoretical approach, he noted

[1] White House Briefing Room, "Fact Sheet: President Biden Signs National Security Memorandum to Counter Weapons of Mass Destruction Terrorism and Advance Nuclear and Radioactive Material Security," last modified March 2, 2023, accessed March 3, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-president-biden-signs-national-security-memorandum-to-counter-weapons-of-mass-destruction-terrorism-and-advance-nuclear-and-radioactive-material-security/.

[2] On Crimes and Punishments, Marchese Beccaria Cesare Bonesana, 1764, Original in Italian

two types of deterrence: deterrence by denial and deterrence by punishment. Deterrence by punishment is commonly understood to be what prevents criminal acts, as the potential criminal fears the consequences such as imprisonment. Deterrence by denial is a strategy that seeks to prevent the adversary from attempting an attack by making the act appear so difficult that it is not worth attempting. Political Science and International Relations scholars including Albert Wohlstetter, Herman Kahn, and others at the RAND corporation expanded on the concepts. Kahn posited an escalation ladder as a guide to nuclear strategy.[3] These early scholars focused primarily on deterrence of war by threats of the use of nuclear weapons, but there are aspects of their discussions that continue to apply at the level of criminal behavior and of the calculus of terrorists contemplating the theft, trafficking, or sabotage of nuclear and radioactive material.

A RAND study by Michael J. Mazarr summarizes three main factors that scholars have identified that determine the success or failure of deterrence. These are level of aggressor motivation, clarity about the object of deterrence and actions the defender will take, and that the aggressor must be confident that the deterring state has the capability and will to carry out threats.[4] Differences in perception of these factors by the aggressor and the defender are the main causes of deterrence failure.

Specifically analyzing nuclear and radioactive material management security, this paper will explore decision science and deterrence theory, applying them to real-world case studies, to highlight credibility and vulnerabilities of deterrence in these situations. As noted, most deterrence literature focuses on deterrence of nuclear weapons use. Recent scholarly studies have continued that emphasis. Our aim is to apply the theoretical basis discussed by the deterrence scholars to the deterrence of theft, diversion, or illicit trafficking of nuclear or radioactive materials.

The purpose of physical security systems is risk reduction against intentional criminal or malicious acts. Their employment contributes to deterrence as a direct result of the attempt to reduce risk. Regarding nuclear and radioactive materials, the aim of deterrence is to dissuade potential aggressors from attacks that could result in health effects in addition to the substantial potential for negative economic or psychological outcomes. Activities designed to prevent theft and diversion of nuclear and radioactive materials can also serve as a deterrent.

This paper focuses on deterrence in the context of nuclear and radiological material security, but the underlying themes apply to higher levels of security and other disciplines. At its core, security is a basic human need, encompassing both tangible and intangible aspects. People desire physical safety as well as emotional and intellectual security. These complement each other in people's perception of threats and responses to them. However, people's perception of a situation depends on their personal experience. They see what they have been conditioned to see. In other words, people would rather misperceive a situation rather than deal with unknown or conflicting

[3] Michael J. Mazarr, "Understanding Deterrence" (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/perspectives/PE295.html.

[4] Mazarr, "Understanding Deterrence"

information.[5] This tendency towards misperception regarding security is central to deterrence discussions - both as a strength and weakness.

A challenge with deterrence, specifically deterrence by punishment, is that it assumes that the aggressor has something to lose. For this reason, it is unclear whether it would be possible to deter a terrorist organization. In most examples of deterrence, you are using an adversary's fear of punishment against them; that they will not attack because they do not want to deal with the anticipated consequences. However, certain terrorist organizations and countries with dictatorial leadership may not care about threats of punishment. In those groups, the lives of the members may not be valued by decision-makers. So, decision-makers could be less concerned with avoiding 'punishment' and might consider some loss of civilians or fighters as a reasonable sacrifice for the survival of the controlling elite. It is in response to this concern that deterrence by denial, rather than deterrence by punishment, is likely to be more effective in these cases. Nevertheless, a strategy that includes both types of deterrence will also protect against adversaries who do fear punishment.[6]

An additional problem with deterrence is the likelihood that the deterrence message delivered by one party is not perceived in the same way by the recipient. In the context of security, misperception can be described as an inaccurate perception of intent or resources invested in a security effort or campaign. In other words, it is when the perceived strength of a defender by an adversary does not match the actual strength. This is not an inherently negative property – it can amplify the efficacy of bluffing, for example. Depending on the situation, and perspective of the antagonists, misperception can have either an advantageous or disadvantageous effect on deterrence. Advantageous misperception, or bluffing, can result in a preferred outcome at a lower cost, disadvantageous misperception can require a high cost of resources for little gain.

Robert Jervis, a foundational scholar of International Relations who pioneered many of the discussions regarding the involvement of psychology in nuclear deterrence discussions, pointed out that theorists often like to compare security strategy to games such as chess, or where chess falls short as an analogy, the use of poker due to its use of bluffing and uncertainty of information, but Jervis points out that neither of these are truly accurate analogies. Because in both situations, each player is playing the same game.[7] Whereas, when it applies to real-world situations regarding deterrence, one player might be playing chess and the other could be playing poker. To further complicate things, the chess player might assume that their adversary is playing chess with them, even though the adversary is under the impression that both are playing poker.

Despite these complications, interest in deterrence persists, because, as with other situations of investment regarding uncertainty, the potential for advantageous outcomes at a discounted cost is

---

[5] Robert Jervis, "Hypotheses on Misperception," *World Politics* 20, no. 3 (1968): 454–79, https://doi.org/10.2307/2009777.

[6] Robert F. Trager and Dessislava P. Zagorcheva, "Deterring Terrorism: It Can Be Done," International Security 30, no. 3 (Winter 2005/06): 106, http://www.jstor.org/stable/4137488.

[7] Brown Political Review, "Perception in Politics: BPR Interviews Robert Jervis," last modified September 14, 2020, accessed March 14, 2023, https://brownpoliticalreview.org/2020/09/perception-in-politics-bpr-interviews-robert-jervis/.

appealing. This is the reason that the lottery has a market. But as with the lottery, success is not guaranteed. However, with the lottery, there is a limit to the potential loss. The cost of the ticket. Whereas regarding nuclear deterrence, misperception acts as a multiplier, and although the positive outcomes are straightforward and limited in nature (no nuclear war), the potential negative outcomes are exponentially grim.

Russia/Ukraine

The Russian Federation's unprovoked, unlawful invasion of Ukraine has highlighted both the successes and the failures of deterrence strategies. Deterrence through the threat of unprecedented U.S. and NATO sanctions (punishment) failed to deter Russia from its course of invading. So far, the threat of massive retaliation has deterred Russia from the use of nuclear weapons despite calls for their use by Russian elites. From the Russian perspective the threat of Russian nuclear retaliation has deterred direct NATO and U.S. participation in the defense of Ukraine. While it is unclear whether deterrence has prevented some Russian attacks against nuclear and radiological facilities in Ukraine, the U.S., IAEA, and NATO's spotlighting of false Russian claims of Ukrainian plans for detonation of dirty bombs may be responsible for having deterred Russia from spreading radioactive substances and blaming Ukraine.

In the case of the Russian invasion of Ukraine there are numerous examples of failures of deterrence, and conditional examples of success; conditional because the war is not over, and deterrence may yet fail. The most striking failure was the final decision by Russia to attack Ukraine despite clearly communicated threats of sanctions. This includes Russian attacks against the Kharkiv nuclear research facility, the Chornobyl site, and the Russian takeover of the Zaporizhzhia Nuclear Power Plant. An arguable success was the standdown of an implied threat by Russia to fabricate a dirty bomb incident and blame it on Ukraine. We suspect that this may have been more of an intelligence success story than a deterrence success, but the diplomatic messaging by the U.S. and NATO surrounding this threat seemed to defuse it. Similarly, the U.S. made clear to the Russian Federation that the use of a nuclear weapon by Russia would result in the most profound consequences. And Russia has not attacked a NATO target because of the certainty that NATO would respond. President Biden publicly made this point in his speech in Warsaw on February 21, "An attack against one is an attack against all. It's a sacred oath."[8]

In his classic book The Causes of War, Geoffrey Blainey explores possible causes of war. He gives examples of theories such as accidental war, wars of succession, rivals for colonies, and popular revolutions as reasons that nations go to war. In each example he finds counterexamples of similar situations where war did not occur. Underlying causes seem to have led to war in some cases and not in others.[9] To oversimplify his argument, a decision to go to war seems to stem from the belief by one side that its power is greater than the other to such an extent that it will defeat the other by going to war. Thus, a decision to go to war can be a failure when the

[8] White House Briefing Room, "Remarks by President Biden Ahead of the One-Year Anniversary of Russia's Brutal and Unprovoked Invasion of Ukraine," last modified February 21, 2023, accessed March 1, 2023, https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/02/21/remarks-by-president-biden-ahead-of-the-one-year-anniversary-of-russias-brutal-and-unprovoked-invasion-of-ukraine/.

[9] Geoffrey Blainey, *The Causes of War*, 3rd ed. (The Free Press, 1988).

perception of the decider is wrong. This was the situation with Russia's invasion of Ukraine. Russia misperceived the relative strengths of the two nations. In this case the deterrence to Russia's attack failed because Russia discounted the strength of the deterrent. Russia's experience with the 2014 invasion of Ukraine, and its successful war against Georgia may have colored Russian judgment of relative strengths.

To expand on the relevance of Blainey's theories in this situation, not only did Russia initially misperceive the relative strength of Russia in comparison to Ukraine, but despite the early introduction of information that contradicted this claim, Russia (or at least President Putin) continued to maintain this perspective. Deception is not always intentional, nor does it always originate from external sources. People act upon biases and cognitive shortcuts without realizing it. Thus, we can be both the recipients of intentional misperception efforts from adversaries and prone to deception because of our own failures.

Jervis, as introduced earlier, authored a paper in 1968 that introduced 14 hypotheses on misperception.[10] His first hypothesis touches on this issue of commitment to inaccurate perceptions and the vulnerability of decision-makers to integrate contradicting information into their existing perspectives.

> Hypothesis 1) that decision-makers tend to fit incoming information into their existing theories and images.

Here, Jervis claims that decision makers are heavily influenced by initial impressions. As a result, decision makers are often reticent to change course once a direction or perspective is decided. This was evident in the early stage of Putin's invasion of Ukraine. Jervis points out that once decision-makers have decided on a narrative that describes the situation, they tend to use that as a framework to hang all the evidence that is subsequently gathered. He notes that decision-makers are reticent to deviate from their original narrative even in the face of new information. In other words, if conflicting information trickles in, leaders are much more likely to attempt to make that information fit into the existing theory rather than overhaul the framework to incorporate the new facts.

Nobel Prize winner Daniel Kahneman warns against the human predisposition towards 'cognitive ease'. Sifting through conflicting information takes time and energy – during which the uncertainty is unsettling. So instead, decision-makers tend to subconsciously (and instantaneously) substitute the problem with an easier question and answer the secondary question. More concerning than this is the fact that they often make this substitution without even realizing it. In other words, people wholeheartedly think they made their resulting decision based on the answer provided for the original, more complex problem, rather than the simpler (and different) question that they answered.[11]

---

[10] Robert Jervis, "Hypotheses on Misperception," *World Politics* 20, no. 3 (1968): 454–79, https://doi.org/10.2307/2009777.

[11] Daniel Kahneman, "Chapter 5: Cognitive Ease," in *Thinking, Fast and Slow* (Farrar, Straus and Giroux, 2011), 59-74.

Material Security

Fortunately, discussions regarding Radiological Dispersal Devices have been theoretical so far. To our knowledge, a Radiological Dispersal Device (RDD) has never been used. However, there have been some threats of RDD use and examples of the use of a Radiological Exposure Device (RED). A Sandia National Laboratories report detailed five examples. In 1974 a United States petroleum engineer irradiated his son. In 1983 a Russian official at a packing company died from radioactive material planted in his chair. In 1995-1997 a Russian man died because of radiation from a source in his truck door. In 2003 a Chinese nuclear researcher irradiated a colleague and other hospital staff by placing a source in the ceiling. In 2006 former Russian KGB agent Alexander Litvinenko was killed after he ingested the radionuclide Po-210.[12]

Strategies employed by the U.S. National Nuclear Security Administration's Office of Global Material Security (GMS) are effectively supporting deterrence both by denial and punishment. The mission of GMS is to enhance U.S. national security by working with partners worldwide to build sustainable capacity to secure radioactive and nuclear materials, and to interdict and investigate the trafficking of those materials. Component Offices employ strategies to fulfill this mission. The Office of International Nuclear Security works to prevent theft and sabotage of nuclear materials and facilities worldwide. The Office of Radiological Security prevents high-activity radioactive materials from being used in acts of terrorism. And the Office of Nuclear Smuggling Detection and Deterrence builds global capability to detect, disrupt, and investigate the smuggling of nuclear and radioactive material before it can be used in an act of terrorism.[13]

While these Offices focus on their security missions, their activities also have a deterrent effect. For example, For example, the enhancement of patrol and radiation detection capabilities along borders deters transnational smuggling of radiological and nuclear materials. The installation of razor wire on the perimeters of nuclear facilities deters adversaries from planning to attack the facilities, instead leading them to choose facilities with less obvious protection. High radioactivity signs in hospitals act as a deterrent to theft of radioactive material.

The physical protection strategy of detection, assessment, delay, and response is intended to keep the adversary from completing his task time to steal or sabotage nuclear or radioactive materials before the response force can interdict and defeat the attempt. Knowledge by the adversary that the defenders have instituted measures to protect the nuclear and radioactive materials is an effective deterrent. Examples of denial by punishment include security cameras that are used for either surveillance or alarm assessment. Adversaries may be deterred by their perception of the risk of interdiction. Armed or even unarmed security guards also act as a deterrent. Deterrence by denial examples include hardened doors, window grates, and visible motion detection systems such as microwave and infrared detectors. Biometric access devices and enforced systems of two person rule can be effective in deterring a potential insider threat. In the case of border detection equipment searching for material out of regulatory control, visible detectors provide a deterrence

[12] Jesse John Bland, Charles A. Potter, and Steven Homann, "Radiological Exposure Devices (RED) Technical Basis for Threat Profile," (United States: 2018), https://doi.org/10.2172/1452666, https://www.osti.gov/servlets/purl/1452666.

[13] GMS Command Brief, March 2023

function by channeling smugglers away from normal border crossing points. Uncertainty in the case of the adversary about other discreet detection equipment is also a deterrent.

Issues of Metrics

How should we think about deterrence at the level of nuclear and radiological security? And why is it important to investigate? The U.S. government has always had a focus on accountability and reporting through congressional briefings and organizations such as the Government Accountability Office (GAO). However, in the age of data analysis, the value of quantifiable success defined by clear metrics has grown in importance. This poses a problem for operational offices that wish to include deterrence in their strategic mandate. For example, the U.S. Office of Global Material Security (GMS), is an office that receives congressional funding, and has an obligation to report on outcomes from that funding. How can they define deterrence success? For GMS, metrics of success include facilities protected, devices removed and replaced with non-radio isotopic sources, individuals trained, or detection equipment procured and fielded. Annually, these achievements are counted, consolidated, and presented to congress.

For offices seeking to include deterrence in their programs, how should this be approached and reported? Regarding deterrence, what could be considered a metric of success? Eric F. Taquechel, and Ted G. Lewis attempted to answer these questions in their article in *Homeland Security Affairs:* "How to Quantify Deterrence and Reduce Critical Infrastructure Risk." Their approach uses a version of the Risk equation to quantify changes in risk. Using the formula Risk=T*V*C, where T is threat, V is vulnerability, and C consequences they attempt to demonstrate a reduction in risk using a game theoretical approach and quantifying outcomes using such inputs as adversary cost and upgrade cost in some case studies.[14] The study is appealing and does demonstrate that measuring deterrence is possible. There are questions about the conditionality of the risk formula because the decision to attack is part of the threat term. Also, other subjective factors remain, and there is no claim that the methodology is a definitive answer.

Conclusions

The concept of deterrence depends upon a shared perception of the consequences of an action by the defender and the adversary. In the case of nuclear deterrence between two countries that possess nuclear weapons the mutual perception of the consequences of the use of nuclear weapons has prevented the breakout of a nuclear war for the past 70+ years. Where conventional wars have occurred, the perceptions of the potential consequences of war have been different between the actors, and whatever deterrence existed was inadequate, or we can say that deterrence failed to prevent the war. Misperception of relative strength is likely to be the trigger that caused deterrence to fail.

In the case of nuclear and radiological security, deterrence by punishment may not be successful in preventing a terrorist adversary from attempting to steal, sabotage, or traffic nuclear or radiological material. However, deterrence by denial can be effective. Physical security measures

[14] Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8, Article 12 (August 2012), https://www.hsaj.org/articles/226.

that offer detection, assessment, delay, and response will have a deterrent effect, causing the adversary to choose softer targets rather than to risk failure of his attack. While the physical security elements are intended to prevent successful attack, they also provide a deterrent.

To the argument that deterrence is not measurable we would say that deterrence can be found to be successful or to fail. When deterrence fails, the adversary either achieves his goal, or is thwarted by physical security measures. When deterrence is successful no attack takes place. Although there may be many other reasons that an attack did not take place, including that no adversary ever considered attacking, this does not discount the validity of the deterrent. It is hard to prove a negative, that no attack took place because of our deterrent. But the deterrent exists, and programmatic officials should take credit for it.

Bibliography

Blainey, Geoffrey. *The Causes of War*. 3rd ed. The Free Press, 1988.

Bland, Jesse John, Potter, Charles A., and Homann, Steven. 2018. "Radiological Exposure Devices (RED) Technical Basis for Threat Profile". United States. https://doi.org/10.2172/1452666. https://www.osti.gov/servlets/purl/1452666.

Brown Political Review. "Perception in Politics: BPR Interviews Robert Jervis." Last modified September 14, 2020. Accessed March 14, 2023. https://brownpoliticalreview.org/2020/09/perception-in-politics-bpr-interviews-robert-jervis/.

GMS Command Brief, March 2023

Jervis, Robert. "Hypotheses on Misperception." *World Politics* 20, no. 3 (1968): 454–79. https://doi.org/10.2307/2009777.

Kahneman, Daniel. "Chapter 5: Cognitive Ease." In *Thinking, Fast and Slow*, 59-74. Farrar, Straus and Giroux, 2011.

Mazarr, Michael J., Understanding Deterrence. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/perspectives/PE295.html.

On Crimes and Punishments, Marchese Beccaria Cesare Bonesana, 1764, Original in Italian

Taquechel, Eric F., and Ted G. Lewis. "How to Quantify Deterrence and Reduce Critical Infrastructure Risk." *Homeland Security Affairs* 8, Article 12 (August 2012). https://www.hsaj.org/articles/226

Trager, Robert F., and Dessislava P. Zagorcheva. "Deterring Terrorism: It Can Be Done." International Security 30, no. 3 (Winter 2005/06): 89-118. Accessed March 21, 2023. http://www.jstor.org/stable/4137488.

White House Briefing Room. "Fact Sheet: President Biden Signs National Security Memorandum to Counter Weapons of Mass Destruction Terrorism and Advance Nuclear and Radioactive Material Security." Last modified March 2, 2023. Accessed March 3, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-president-biden-signs-national-security-memorandum-to-counter-weapons-of-mass-destruction-terrorism-and-advance-nuclear-and-radioactive-material-security/.

White House Briefing Room. "Remarks by President Biden Ahead of the One-Year Anniversary of Russia's Brutal and Unprovoked Invasion of Ukraine." Last modified February 21, 2023. Accessed March 1, 2023. https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/02/21/remarks-by-president-biden-ahead-of-the-one-year-anniversary-of-russias-brutal-and-unprovoked-invasion-of-ukraine/.