2017

The Frontiers of Technology in Warhead Verification

Henrietta Toivanen

The Frontiers of Technology in Warhead Verification

A Thesis Presented
by
Henrietta Toivanen

To the Keck Science Department
Of Claremont McKenna, Pitzer, and Scripps Colleges
In partial fulfillment of
The degree of Bachelor of Arts

Senior Thesis in Biophysics and International Relations
April 24, 2017

Table of Contents

Abstract

How might new technical verification capabilities enhance the prospects of success in future nuclear arms control negotiations? Both theory and evidence suggest that verification technologies can influence the dynamics of arms control negotiations by shaping and constraining the arguments and strategies that are available to the involved stakeholders. In the future, new technologies may help transcend the specific verification challenge of high-security warhead authentication, which is a verification capability needed in future disarmament scenarios that address fewer warheads, limit new categories of warheads, and involve nuclear weapons states other than the United States and Russia. Under these circumstances, the core challenge is maintaining the confidentiality of the classified information related to the warheads under inspection, while providing transparency in the verification process. This analysis focuses on a set of emerging warhead authentication approaches that rely on the cryptographic concept of zero-knowledge proofs and intend to solve the paradox between secrecy and transparency, making deeper reductions in warhead arsenals possible and thus facilitating future nuclear arms control negotiations.

Acknowledgements

First, I am grateful for all the people who I was able to talk with throughout my thesis research process. My early inspiration emerged from the work of the Nuclear Futures Laboratory at Princeton University, which introduced me to the theme of my thesis. I would like to thank everyone in the program for sharing their time and thoughts with me. I am grateful for the other exceptional experts in the field of nuclear policy with whom I was able to speak, including Rajamurti Rajaraman, Steve Fetter, Thomas Shea, Andrew Newman, R. Scott Kemp, and many others. Particularly, I am thankful for the Project on Nuclear Issues at the Center for Strategic and International Studies, who provided me with opportunities to participate in and present at conferences at the Sandia National Laboratories in Albuquerque, New Mexico; at the CSIS headquarters in Washington D.C.; and at the United States Strategic Command in Omaha, Nebraska. The people I was able to connect with through the conference series – Rebecca Hersman, Michael Elliott, Amy Woolf, Ronald Lehman, and others – allowed me to engage with the segments of the nuclear policy community that I otherwise would not have been able to reach.

I would like to thank the faculty and staff at Claremont McKenna College for supporting my research. Particularly, I am deeply grateful for Professor Jennifer Taw, my first thesis reader, who has been an extraordinary source of support both as a professor and as a friend throughout my time at CMC. Especially in this past year, her advice and support has kept me on track with my thesis research and with many other aspects of my senior year. I am also very grateful for Professor Scot Gould, my second reader, who has been my academic advisor since freshman year and has helped me in the many important decisions I have had to make about my future. His help in integrating the technical dimensions to the political ones in my thesis was very important from early on in the research process. Many other important people and resources at CMC, including the International Relations Program and the Keck Center for International and Strategic Studies, have been critical for making my research possible.

Lastly, I am grateful for my friends and family for of their support. My exceptional friends in Claremont helped me in many ways throughout this past year. In Finland, my mother, Danuta, and my brother, Henri, have been a true lifeline for me throughout the year. I cannot emphasize enough how critical their support has been. Rakastan teitä valtavasti, kiitos kaikesta tuesta ja ymmärryksestä!

Introduction

Over the past decades, the United States and Russia, formerly the Soviet Union, have engaged in negotiating warhead reductions that have brought the global stockpile of nuclear weapons to only a fraction of what it was at the height of the Cold War. These disarmament agreements focused on limiting warheads that were affiliated with operationally deployed strategic delivery systems, allowing their reductions to be verified through monitoring the delivery platforms.[1] Disarmament in the U.S.-Russia context, however, is unique in many respects and this past strategy of warhead reductions will cease to be feasible in the future stages of arms control. The past definition of treaty-accountable nuclear weapons will become insufficient in future disarmament scenarios, which include addressing lower numbers of warheads, where the diversion of even one warhead becomes increasingly significant; considering new categories of weapons under limitations, including tactical and non-deployed; and engaging other nuclear weapons states than the United States and Russia.[2] All of these factors contribute to the need to shift from a verification approach based on delivery systems, to a verification approach focused on the warheads themselves.

---

[1] *Operationally deployed strategic warheads* refer to strategic nuclear weapons that are mounted on their ballistic missile launchers or that are located at aircraft bases, although the definition is somewhat dependent on the context. (Source: Hans Kristensen and Robert Norris, "Status of World Nuclear Forces," *Federation of American Scientists*, accessed March 2, 2017, available at https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/.)

The process of *verification* is comprised of collecting the information relevant to the treaty, which is referred to as monitoring, and assessing what it signals about compliance, which is verification. In this thesis, I focus on this process as a whole and use the term verification.

[2] State Department definition of warhead categories: "The *nuclear stockpile* includes both active and inactive warheads. *Active warheads* include strategic and non-strategic weapons maintained in an operational, ready-for-use configuration, warheads that must be ready for possible deployment within a short timeframe, and logistics spares. They have tritium bottles and other Limited Life Components installed. *Inactive warheads* are maintained at a depot in a non-operational status, and have their tritium bottles removed. A retired warhead is removed from its delivery platform, is not functional, and is not considered part of the nuclear stockpile. *Warheads awaiting dismantlement* constitute a significant fraction of the total warhead population and will continue to grow as the New START Treaty is implemented and as unneeded warheads are retired. A *dismantled warhead* is a warhead reduced to its component parts." (Source: U.S. Department of State. "Fact Sheet: Transparency in the U.S. Nuclear Weapons Stockpile," https://2009-2017.state.gov/documents/organization/241377.pdf.)

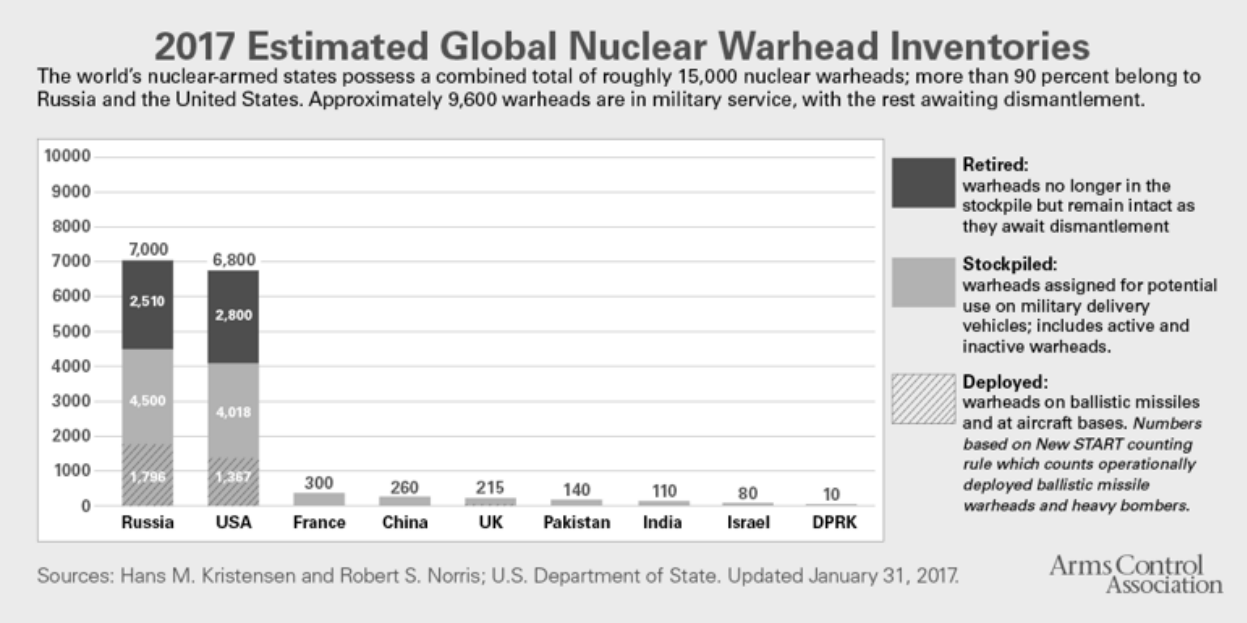

Figure 1. Source: Arms Control Association, "Nuclear Weapons: Who Has What at a Glance," updated January 2017, available online from https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat.

The problems associated with the verification of individual warheads are multifold. The core technical verification challenges in this disarmament scenario will relate to the high-security authentication of warheads, their unique identification, maintaining the continuity of knowledge throughout their life cycle, and several other issues.[3] These technical verification challenges will emerge at different stages of a warheads' life cycle, from the initial tagging of the warheads when they leave the production facility, to authentication when they enter the dismantlement facility, but all of these different elements play a role in creating confidence and trust in an arms control agreement focused on warheads.[4] In this thesis, I will be focusing on the specific verification challenge of authenticating warheads, or proving that the warhead under consideration is genuine and that the host state is not

[3] Nuclear Threat Initiative, "Verifying Baseline Declarations of Nuclear Warheads and Materials," *Innovating Verification Series*, July 2014, http://www.nti.org/media/pdfs/WG1_Verifying_Baseline_Declarations_FINAL.pdf?_=1405443895.

[4] Frank von Hippel, "Verification of Nuclear Warheads and Their Dismantlement: A Joint American-Soviet Study," INMM 31st Annual Meeting (1990): 1.

trying to deceive by offering blank warheads or employ other spoofing mechanisms. This verification challenge is only one of the pieces of the puzzle in future disarmament verification, each of which requires unique technical capabilities. This thesis will focus on exploring the applicability of novel technical approaches to this specific future verification challenge.

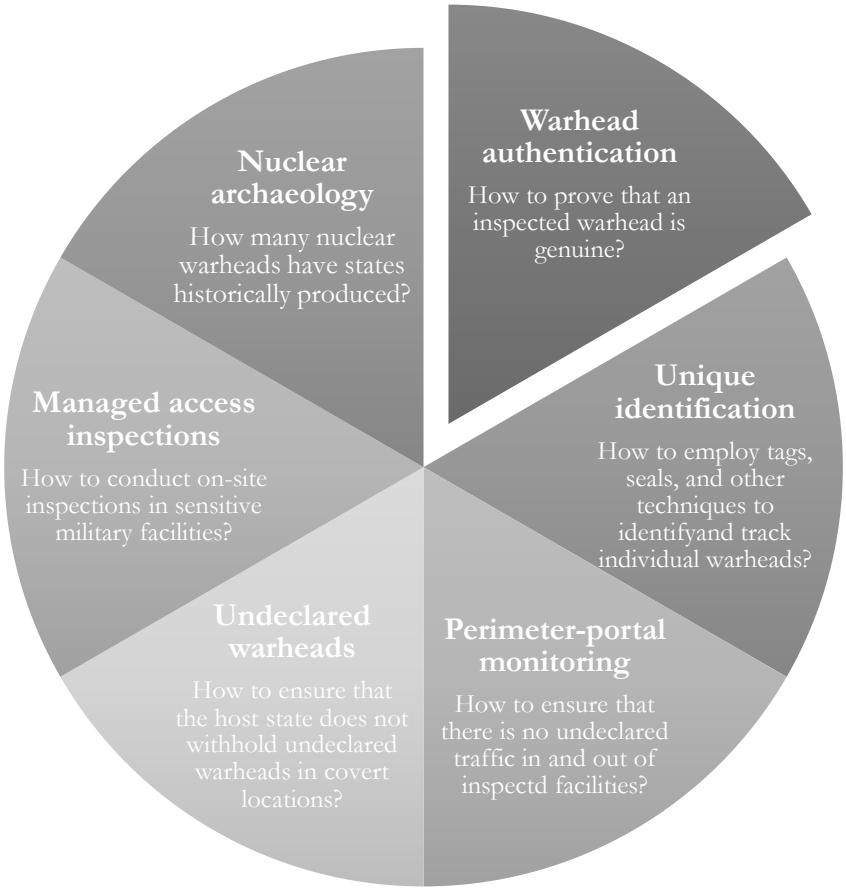

Figure 2. Verification challenges associated with disarmament agreements that focus on warheads, rather than their delivery systems. The figure intends to illustrate the challenges involved, but is not fully comprehensive. I thank Rebecca Hersman for helping me visualize these challenges, as represented in this figure.

These verification challenges may be in the longer-term horizon, but overcoming them will be essential for making future steps in disarmament possible. It is critical to think about these challenges

now, even if further bilateral reductions in warheads between the United States and Russia are highly uncertain, not to mention the prospects of negotiations with countries such as North Korea or Pakistan. While these are the geopolitical realities at the moment, it does not mean that the circumstances can change relatively rapidly. Furthermore, there is an argument to be made that these interval periods are exactly the time new verification approaches can be conceptualized and developed.

These efforts are also driven by the increasing pressure from the international community towards the nuclear weapons states, particularly in the context of the humanitarian movement to bring attention to the catastrophic consequences of nuclear weapons. As reflected in the Resolution A/C.1/71/L.41 that was passed in the United Nations General Assembly in October 2016 to begin negotiations of a nuclear weapons ban treaty, the international community is increasingly willing to call for the nuclear weapons states to move towards disarmament, as outlined in their obligations under Article VI of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT).[5] The key question now is how the P5 states, or the five nuclear weapons defined under the NPT, are going to respond to this pressure and engage with the rest of the international community. Beyond the P5, the nuclear weapons states outside the NPT framework are creating increasing anxieties within the international community. The nuclear balance in South Asia remains to be a key security concern for many, as does North Korea.

The core of my thesis focuses on the particular verification challenge of authenticating nuclear warheads. More specifically, the focus is on a presumed tradeoff of secrecy and transparency in the authentication process, as it requires highly intrusive radiological measurements.[6] The central challenge

[5] United Nations General Assembly, 71st Session. *General and complete disarmament: taking forward multilateral nuclear disarmament negotiations*, 2016 (A/C.1/71/L.41), available from http://www.un.org/ga/search/view_doc.asp?symbol=A/C.1/71/L.41.

[6] Jie Yan and Alexander Glaser, "Nuclear Warhead Verification: A Review of Attribute and Template Systems," *Science & Global Security* 23 (2015), http://scienceandglobalsecurity.org/archive/sgs23jieyan.pdf.

is maintaining the confidentiality of classified and sensitive information related to the inspected warheads, while providing transparency and a high level of confidence in the verification process. As will be discussed, states have technical, political, and legal concerns related to revealing details about their warheads, whereas from the inspectors' perspective, this information is essential for the validity of the authentication process. The specific warhead authentication mechanisms that I focus on in the last chapter of the thesis, which use physical cryptography and zero-knowledge proofs, intend to challenge this assumed tradeoff between secrecy and transparency.

Before the focused examination of this challenge, however, I establish a theoretical understanding of the role of verification technologies in the politics of verification. This allows me to create a more nuanced understanding of why verification matters, and move beyond the two extremes that are continually argued in the arms control community – that either verification does not matter at all, or that trust can only be achieved with stringent verification provisions. In the first chapter, I make the case that the story is more complicated than what these two arguments assert. Methodologically, this research applies the comparative method, as I operationalize verification technologies as the variable under consideration and explain the causal mechanisms that explain how they can contribute to negotiating nuclear weapons reductions, under conditions of high levels of secrecy and distrust. My description of these processes involves two frameworks, one of which rests on two-level game theory and the other analysis of sociotechnical systems.

I will make evident in the first chapter that the conceptualization of verification technologies cannot be reduced to a purely technical, or a purely political, perspective – these technologies are inherently involved in both dimensions. This is because verification arguments can be operationalized as tools to further the political agendas and interests of the involved stakeholders, who have highly divergent views about the value of arms control. The core argument is that verification technologies

must be understood as both an independent and dependent variable. They can importantly shape the politics of verification by constraining the arguments and strategies that are available to the involved stakeholders, but this influence is dependent on the political conditions at that time. Thus, developing new verification approaches is not going to be a panacea for making next steps in disarmament possible, as these novel mechanisms can either further or impede the prospects for arms control, depending on the political conditions of the time. Nevertheless, they play a meaningful role in the process, which allows them to expand the possibilities and likelihood of new disarmament efforts under the right conditions.

My thesis proceeds in the following way. The first chapter provides a framework for understanding how verification technologies influence the politics of verification and starts to outline the issue between secrecy and transparency. This establishes the basis for the following chapters, by illuminating how the development of new verification approaches has an independent effect in shaping the politics of verification, thus contributing to the dynamics of future arms control processes. Then, the thesis dives into the verification challenge of warhead authentication. The second chapter takes a historical perspective and shows how past warhead reduction measures have addressed the seemingly intractable tradeoff between secrecy and transparency, with a focus on the SALT era, the INF treaty, and the START era. Next, the third chapter explores the efforts have been made in the past to counter the assumption that high-accuracy verification of warheads would not be possible without compromising classified information, but how the issue of the authentication and certification of the technical equipment used in these approaches has prevailed.

The fifth chapter shifts the perspective into the technical dimension of my thesis, providing an overview of the physics, design, and detection of nuclear weapons, which is essential for understanding the sixth chapter, which contains is the core of my technical examination. This chapter

focuses on a set of novel approaches developed over the past years, based on zero-knowledge proofs, where the core idea is that the classified design information is not measured by the verification system in the first place due to the physics of the measurement system itself. Lastly, in my conclusion, I discuss the implications of developing these verification approaches and how it might contribute to the future directions of global nuclear arms control efforts. I argue that while novel verification approaches, such as zero-knowledge verification, may never be fully implemented as such in an arms control treaty, their development is important regardless – both for opening the dialogue on new treaty architecture options, as well as shaping the political dynamics of the treaty negotiations themselves.

1. Why Verification Technologies Matter

I. Introduction

One of the critical questions when thinking about the verification of arms control agreements is the role that verification technologies have in this process. Verification technologies provide the physical capabilities that allow the monitoring of treaty provisions, and subsequently the determination of treaty compliance. The analysis of the role of verification technologies, however, cannot be reduced to only the technical and physical dimension, as they also interlink to the political dimension of verification. The purpose of this chapter is to provide an answer to the question of how verification technologies influence the verification process of an arms control agreement, and why it matters what verification technologies and capabilities are available when negotiating new treaties. This discussion is essential for the overarching argument in this thesis, which is that the emergence of new verification approaches for warheads is an essential step for making further nuclear arms reductions possible.

The commanding theme in answering this question is that verification technologies influence the process of verification through several bidirectional relationships that relate both to technical and political dynamics. This bidirectionality becomes evident in the way verification capabilities are developed, as well as in the way that these capabilities influence verification negotiations. In both of these situations, verification technologies are not only used to answer objective, technical questions, but are also operationalized as political arguments and tools. This bidirectionality is also present in the verification negotiations between states, which can be modeled as two-level games where the domestic and international levels of political dynamics interact.

These mutually influential relationships, giving verification technologies both a technical and political purpose, make the question meaningful to answer. Verification technologies are a fundamental part of the verification process, but changes in the level of verification capabilities do not

lead to simple, predictable effects. Instead, these effects vary as a function of the political conditions in which they take place, most importantly the current political actors and their interests. Ultimately, understanding the role of verification technologies in the verification process condenses to understanding these dynamic interactions between political negotiations and technology.

I argue that while the emergence of new verification approaches will not be a panacea for settling disagreements about verification, they will importantly shape the politics of verification by constraining the arguments and strategies that are available to the involved stakeholders. New verification approaches can strengthen the positions of those promoting nuclear arms limitations by expanding the verification choices that they can propose in the negotiations. Simultaneously, new verification capabilities can weaken the arguments of arms control opponents who exaggerate verification concerns and potential cheating opportunities. Thus, novel verification technologies contribute to the facilitation of verification debates by altering their dynamics and shaping the arguments that can be made by both opponents and proponents of arms control.

This analysis of the importance of verification technologies provides the justification for the rest of my thesis. By showing that verification technologies can improve the prospects of future arms control agreement, I can explain why developing novel verification capabilities can contribute to future multilateral disarmament processes that involve unique requirements for verification systems and protocols. I will specifically focus on the issue of transparency and secrecy in the ongoing debate about warhead verification, and how the emerging idea of physical cryptographic verification approaches can increase the likelihood of achieving new agreements that limit warheads. While these approaches may never be fully implemented in the verification provisions of future arms control agreements, their existence will have an impact on the argumentation dynamics of both arms control proponents and opponents during the negotiations. These methods will make arms control opponents' arguments

about the 'unverifiability' of warhead limitations appear less legitimate, and allow the proponents of arms control to propose valid mechanisms for verifying the terms of the agreement. Ultimately, the success of these negotiations will depend on the balance of political interests and geopolitical developments, but under the correct conditions, the successful development of these novel warhead verification approaches can make a concrete contribution towards the future prospects of deeper cuts in nuclear weapons.

This chapter will first explain the core technical and political challenges related to verification technologies. Then, the chapter will analyze the existing political science literature on these topics and provides a more formalized framework for understanding these challenges. This literature review allows the discussion to be expanded and leads to my core argument: Changes in the available verification capabilities cannot single-handedly make an arms control agreement possible, in the absence of political will – but they can change the likelihood of an agreement by shifting the dynamics of the negotiations. Thus, the impact of new verification technologies is channeled through both the political and technical levels – they physically influence the choices and arguments that are available to the different stakeholders, and thus shape the arguments that can be made about verification.

II. Technical and Political Challenges

The fundamental purpose of verification is to determine whether parties to an arms control agreement are complying with their commitments. In addition to providing the technical means to monitor and detect potential violations, it also serves a political purpose in assuring the other parties to the agreement that arms control measures promote, rather than compromise, their national security. This assurance is intended for state leaders and political establishments, as well as domestic audiences

who are concerned about compliance issues relating to arms control measures.[7] Furthermore, verification is argued to influence the behavior of the participating states by creating a deterrent against noncompliance. These functions provide the underlying justification for why verification is pursued with arms control agreements, with either unilateral or mutual verification provisions.

A two-fold challenge relates to the technologies used in the verification process – the first dimension is technical, and the second is political. The technical problem is having the right verification capabilities available to satisfy the requirements that arise from both practical and political needs. The second problem is political, meaning that the verification technologies are operationalized as political tools by the different stakeholders in verification debates. The technologies' attributes are used as arguments to promote distinct political ends, which vary depending on the stakeholder in question.

Thus, the attributes of the verification technologies are not only important for the physical verification capabilities that they create, but also the way in which they can either accumulate or alleviate distrust. This political dimension depends deeply on how easy it is to 'verify' the verification capabilities themselves – or confirming that they operate as intended. In the context of warhead verification, this means that the verification capabilities can confidently authenticate warheads without revealing sensitive information; with test ban monitoring, this means that the verification capabilities can detect nuclear explosions with high degree of accuracy within the intended thresholds. This is essential for being able to educate and convince the negotiators that using these verification capabilities will build trust and confidence in compliance. Thus, trust and confidence are critical aspects of verification technologies – they are not only operated by inspectors and technical personnel,

[7] U.S. National Security Council. *National Security Decision Directive Number 65: Establishment of National Security Council Arms Control Verification Committee*. 1982.
https://reaganlibrary.archives.gov/archives/reference/Scanned%20NSDDs/NSDD65.pdf

but are also an important component of political actors' decision-making process. This is why trust becomes a critical variable in verification technologies.

Both the technical and political dimensions operate according to the dynamics of a feedback loop. First, the technical challenge of having adequate technical verification capabilities relates how policymakers define the verification needs in a particular arms control agreement. Negotiators understand what is needed from technical verification capabilities to satisfy the political needs both internationally and domestically. It is important to understand, however, that the process of defining verification needs is highly subjective, and also liable to being used as a mechanism to promote specific political agendas. Stricter requirements entail higher barriers for achieving agreement about arms control, and, as will be discussed later, have been operationalized as a hindrance to arms control.

The requirements for verification technologies are relayed to the technological community, informing technical personnel of the needs from the political side. This process takes place domestically, such as with the U.S. national laboratories. It can also take place internationally, as joint development programs for new technologies. The requirements from the political level inform the technological community, which then adjusts its research programs to align with the conveyed needs. The resulting new verification capabilities contribute to the prevailing systemic environment in which policymakers operate. This links back to the first stage of the feedback loop, with the new systemic environment influencing how policymakers determine the verification needs for a particular treaty. This illustrates how the development of verification technologies and the definition of verification requirements are mutually influential. These dynamics also show why it is too simplified to ask whether policymakers determine the development of verification technologies, or whether available verification technologies determine the verification provisions that are applied. The answer is both, with bidirectional interactions between the political and technological spheres.

It is also important to note that each of the stages of the feedback loop can be independently influenced by external factors. Policymakers' guidance is not the only factor that shapes the development of verification technologies – it is also controlled by the internal dynamics of the technological community and the emergence of new fundamental scientific knowledge. Thus, influence from these factors can have an impact that is outside the control of policymakers, changing the systemic environment in which verification debates take place.

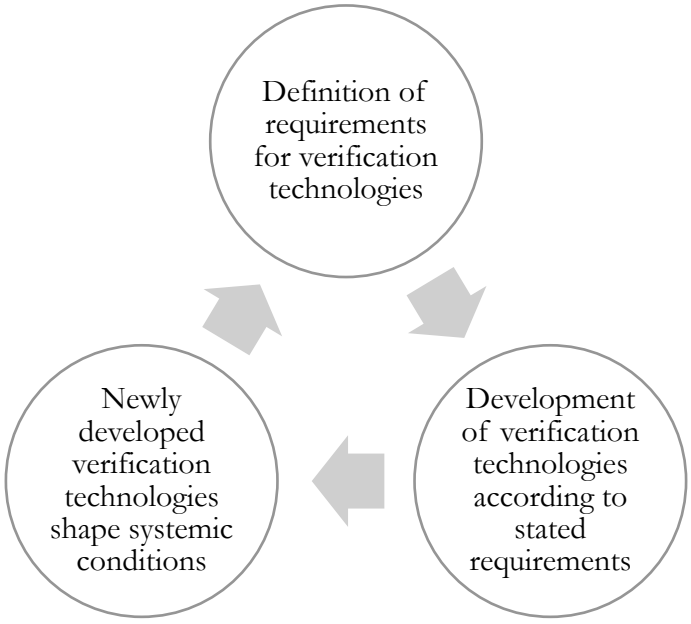

Figure 1.1. The feedback loop describing the dynamic relationship between the political stakeholders defining verification requirements and the technical community developing the verification technologies.

The political dimension operates according to its own feedback loop. These dynamics can be understood as a two-level game theoretical model, as will be discussed later, but also more generally as a mutually influential relationship. This reflects the fact that the politics of verification relate both to the domestic level, as well as the international level. The first level of two-level games takes place in national politics, which are often factional and discordant. Different domestic interest groups interact with governmental actors such that each side is trying to influence the other, or to create

alliances with groups that share their interests. The second level reflects international politics, where state governments represented by selected negotiators interact with each other, and similarly exert pressure or suggest alliances with actors that share their objectives.[8] These two levels can be understood as mutually influential. At the domestic level, international negotiations create external pressure that can be deployed by domestic political actors to argue against their opponents and drive their interests forward. At the same time, the dynamics of international negotiations depend on the domestic political conditions in each participating state. Each national leader is constrained by their domestic constituencies and factions, who must ultimately ratify or endorse the agreement reached with other governments – otherwise the leader of the state may face difficult domestic challenges, or even be voted out of power.[9]

[8] Robert Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," *International Organization* 42 (1988): 434.

[9] Ibid., 437.

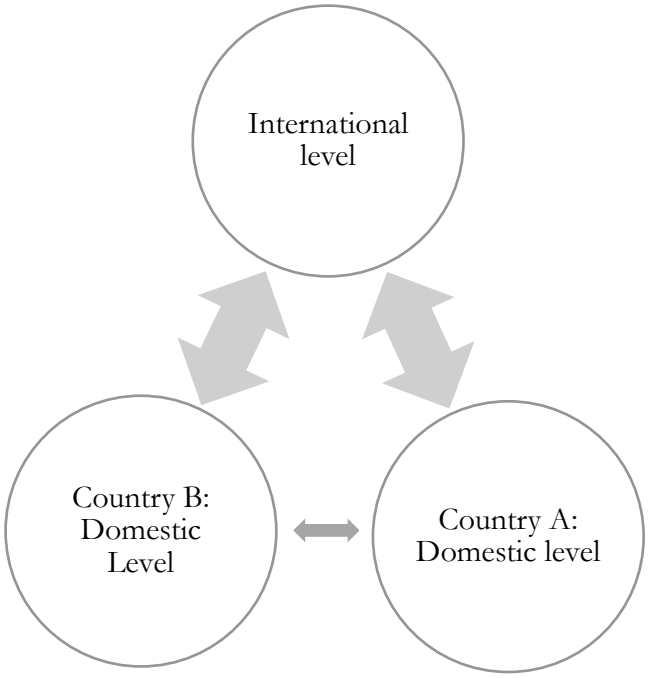

Figure 1.2. The political dynamics of verification negotiations on the international and domestic level. As discussed later, the domestic level can be modeled after Robert Putnam's framing in "Diplomacy and domestic politics: the logic of two-level games." This is also reflected in Table 1.1.

	Country A – United States	**Country B – Russia**
Head of state	Barack Obama (President)	Dimitri Medvedev (President)
Cabinet members	Hillary Clinton (Secretary of State); Robert Gates (Secretary of Defense)	Sergey Lavrov (Foreign Minister of Russia)
Other members in executive branch	Gen. James L. Jones (National Security Adviser)	
Members of parliament	United States Senate	State Duma (lower house of the Federal Assembly of Russia)
Agency representatives	Rose Gottemoeller* (Assistant Secretary of State for Verification, Compliance, and Implementation); Ellen Tauscher (Under Secretary of State for Arms Control); Adm. Mike Mullen (Chairman of the Joint Chiefs of Staff)	Anatoly Antonov* (Director of security and disarmament at the Russian Ministry of Foreign Affairs)
Experts	National laboratories (e.g. Los Alamos National Laboratory)	National laboratories (e.g. VNIIEF in Sarov)
Interest groups	Arms Control Association, Federation of American Scientists, Physicians for Social Responsibility, Heritage Foundation	Political and Military Analysis Institute, Carnegie Moscow Center

Table 1.1. The domestic level as conceptualized by Robert Putnam in "Diplomacy and Domestic Politics: The Logic of Two-Level Games," applied to the real conditions during the New START negotiations between 2009 and 2011. The star refers to the lead negotiators.

III. The Political Stakeholders

As has been alluded to previously, the stakeholders engaged in verification debates may hold differing views about the verification needs for a specific arms control agreement. These divisions surface due to divisions between countries about the purpose and logic of verification, as well as due to divisions within countries. With respect to states, it is evident that there are general differences between state perceptions about the role of verification in arms control. This has been most visible between the United States and Russia, who have had the most experience in negotiating verification protocols. The U.S. position throughout the Cold War was to emphasize the objective, neutral, and technical nature of verification, since depicting "verification demands as scientifically correct and thus nonnegotiable makes for a stronger bargaining position."[10] Cultural factors also contributed to this perception, as it is compatible with the ideals of scientific rationalism, Western empiricism, and the "liberal faith in the unproblematic nature of knowledge."[11] The U.S. perspective can be contrasted with Soviet views about verification, which saw the process as inherently subjective and strategic, as "a double-edged sword that can be used for good or ill, depending on political relations."[12]

These national views, however, can also fluctuate over time. In the 1980s, for example, the United States reduced its verification demands, while the Soviet Union was willing to pursue "triple verification" that included extensive data exchanges and comprehensive on-site inspections.[13] These shifts often reflect more general changes in the state's position on arms control, which illuminates how perspectives about verification are inherently linked to more general attitudes towards arms control. The within-country spectrum of viewpoints about verification, which are discussed next,

[10] Nancy Gallagher, *The Politics of Verification* (Baltimore: Johns Hopkins University Press, 2003), 30.

[11] Ibid.

[12] Ibid.

[13] Murray Feshbach, edit., *National Security Issues of the USSR* (New York: Springer, 1987), 86.

change as the strategic calculations about arms control change. Since the end of the Cold War, the United States has seen warhead reductions as a stabilizer in U.S.-Russian relations and, during the Obama administration, also as an important step in the path towards global disarmament.[14] Russia, on the other hand, is more dependent on its nuclear forces and "fears that continuing cuts to strategic force levels could eventually threaten strategic stability and that the United States might pursue additional cuts with that very goal in mind."[15] These broader views about the strategic logic of arms control will shape both sides' positions on verification, given the way that it can be used as a foundation for political arguments.

In addition to these state-level divisions about arms control and verification, there are also divergences within countries and their political factions that are reflected in the views of stakeholders. Each participant in the arms control negotiations is coming to the table with pre-existing perceptions and preferences about arms control, shaped by their political allegiances and personal views. These notions will shape their approach to verification and the emphasis they place on technical verification needs. They also are constrained by the structural environment in which they interact, with one of the variables defining that environment being the status of verification technologies. As will be discussed later in this chapter, these dynamics have been analyzed from a theoretical perspective in existing international relations literature, but these divisions can also be understood in more general terms.

Stakeholders can be placed on a continuum with respect to their attitudes about nuclear arms control, spanning from stern opponents to ardent proponents. Actors at the two ends, representing the extreme positions, operationalize verification arguments to convince those in the middle to

[14] Aaron Miles, "Adaptive Warhead Limits for Further Progress on Strategic Arms Control," *Real Clear Defense*, February 7, 2017, http://www.realcleardefense.com/articles/2017/02/07/progress_on_strategic_arms_control_110760.html.

[15] Ibid.

support their position on arms control. These dynamics exist both at the national level and on the international stage. Outcomes in verification debates emerge partially as a result of these interactions, as well as due to genuine technical questions and concerns, which shows how the political and technical dimensions of verification dimensions intersect.

IV. Literature Review

The previous discussion establishes how verification technologies operate both as a technical asset and a political tool, which illuminates the complexity of their role in verification debates and in the verification process itself. These observations can be placed in the context of existing political science literature, where these dynamics have been studied from a more theoretical perspective. The focus in the following discussion will be on two theoretical frameworks, developed by Nancy Gallagher and Geoffrey Herrera. Gallagher's framework offers a way of understanding the dynamics of verification debates using a two-level game that has been adapted to involve the influence that the worldviews and identities of the involved stakeholders have on the debates. The framework's conventional understanding of technology as an exogenous variable that aligns with most system-level theories, however, leaves little space for examining the independent effect that emerging verification technologies could have in influencing verification debates. Thus, Gallagher's framework can be complemented and expanded by bringing in insights from Geoffrey Herrera's analytical approach to understanding the relationship between technology and international politics. Herrera's framework conceptualizes technology as an endogenous structural variable in the international system that is interdependent of the dynamics of international politics. Integrating Gallagher and Herrera's approaches will provide an insightful lens for understanding how and why verification technologies influence the politics of verification, and how the development of new verification technologies can contribute to future arms control prospects.

i. Modeling Verification Debates as Two-Level Games

Gallagher's *The Politics of Verification* is one of the seminal works on the political dimensions of verification debates. The framework she develops can be used to conceptualize how the different stakeholders involved in verification debates enter the negotiations with pre-existing interests and ideas, and how these perceptions influence their behavior and decision-making processes. Gallagher's framework conceptualizes the politics of verification as a two-level game that is played both at the international and domestic levels, by stakeholders that can be defined as one of three ideal types: arms control opponents, arms control proponents, and cautious cooperators. Importantly, the framework illuminates that debates about verification are not only an epiphenomenon linked to nuclear arms control negotiations. Instead, the politics of verification is a process that independently influences the verification decisions that are made and can ultimately make or break agreement on arms control efforts.

The first principles of each ideal type qualify the importance that players in that category place on verification technologies. Arms control opponents, for example, see verification technologies from a competitive perspective where the development of verification capabilities can be important for seeking "a verification regime that maximizes their own monitoring capabilities, denies the other side access to sensitive information, and preserves their autonomy to act and judge others in ways that suit their competitive goals."[16] For cautious cooperators, verification technology can become a critical variable in shifting the costs and benefits of cooperation enough to make agreement possible.[17] Their views align with the arguments that verification helps in assuring states that violations will be detected, provides deterrence against cheating, assures that the benefits of cooperation will be reaped, and can

[16] Gallagher, *The Politics of Verification*, 6.

[17] Ibid., 8.

promote domestic support for arms control by allowing leaders to use these arguments in political debates.[18] For arms control advocates, the significance of verification technologies again declines, as they see states' security objectives as fundamentally compatible and compliance as a logical outcome. A minimum level of verification is needed to facilitate cooperation, and anything above it can serve to "promote international openness, strengthen international organizations, and democratize security policy in countries whose civilian oversight of military decisions is weak."[19]

Gallagher argues that debates about verification are a meaningful dimension of nuclear arms control negotiations, and cannot be simplified into the frameworks contained in most literature on verification. More optimistic traditional frameworks argue that verification can be used a tool to incentivize compliance and deter cheating, thus decreasing the costs and risks of arms control agreements and changing state calculus in international negotiations. More pessimistic perspectives do not grant verification an independent effect in making cooperation possible, but instead see it as a mechanism of sabotaging negotiations, gaining political ground, or otherwise being an "epiphenomenon" of arms control negotiations.[20] Neither of these views conceptualize the complexity of verification debates in their true form. Gallagher proposes a framework that accommodates the divergent stakeholders involved in verification debates and who employ varying strategies to pursue their preferred policy path. The solution is not to depoliticize verification debates, but rather to embrace the interconnected technical and political nature of verification arguments.

Gallagher lays out a modified two-level game theoretic model that incorporates both the domestic and systemic levels of analysis to analyze the dynamics of verification debates. Two-level games were originally conceptualized by Robert Putnam in "Diplomacy and Domestic Politics: the

[18] Ibid.

[19] Ibid., 11.

[20] Ibid., 2.

Logic of Two-Level Games," which provides a framework for analyzing the causal relationship between domestic and international factors in determining the outcomes of international negotiations.[21] This framework is highly applicable to verification negotiations, which are influenced by the perspectives of domestic constituencies as well as the positions of the other states at the negotiating table. A fuller description of two-level games is available in Putnam's paper and in subsequent work on the topic, as the focus here is on how Gallagher modifies the game to fit the context of verification debates.

Gallagher modifies the traditional two-level game framework to the context of examining and explaining the verification arguments made during arms control negotiations. The traditional formulation of the two-level game focuses on players' interests as a basis for their preferred outcomes and most often considers these interests to be constant over time.[22] Gallagher argues that in debates about verification, it is also essential to consider the role that ideas, worldviews, and myths have in shaping choices about verification arguments.[23] These factors, together with interests and technical realities, shape verification arguments and positions that are composed of both substantive and strategic components. These modifications, which are rooted in assumptions from the English School of international relations, help explain why certain verification arguments are operationalized by certain actors during negotiations. The debate among the three groups that Gallagher defines is parallel to the central dialogue in international relations theory on the possibilities of international cooperation.[24] The central question is whether verification could reconstruct state behavior such that

[21] Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," 427-460.

[22] Gallagher, *The Politics of Verification*, 41.

[23] Ibid.

[24] Ibid., 4.

durable cooperation would become possible in the absence of transnational enforcement mechanisms. These interactions are at the core of Gallagher's view of the politics of verification:

> Conceptualizing the structure of verification arguments as a two-level game suggests that the causal arrows flow in both directions. Instead of using domestic politics solely to account for national interests or using system-level factors just to explain the outcome of internal policy debates, this approach assumes that national leaders have their own preferences but are simultaneously constrained by what other states will negotiate and what constituents will ratify. Here, the structure of the game is determined by the mix of common and conflicting interests and the allocation of power among national representatives at the negotiating table; it is also determined by the configuration of preferences and the decision-making rules of each participating state.[25]

Gallagher's framework provides an important foundation for understanding how the dynamics of verification negotiations operate through the interactions of the different types of stakeholders. The focus of her analysis is confined within these interactive dynamics, with the structural negotiations environment providing the backdrop for these interactions. This framing, however, leaves out the consideration of the independent effects that changes in the structural negotiations environment can have on the negotiation interactions. One of these structural variables is technology, which is incorporated into Gallagher's framework only as an objective variable that shapes the preferences of each of the three ideal types.

ii. The Role of Technology in Verification Debates

Gallagher's understanding of verification technologies as an objective, constant variable is aligned with the view embedded in many system-level theories. While Gallagher follows the English School, similar views are associated with neorealist, neoliberal, and constructivist views of international relations. Technology is not seen as a component of the international system that can foster change from within, but rather seen as an exogenous variable.[26] My intention is to reverse this view and examine the role that verification technologies play as an endogenous and independent

[25] Ibid., 40.

[26] Geoffrey Herrera, *Technology and International Transformation* (New York: SUNY Press, 2006), 4.

variable in the two-level framework that Gallagher has formulated. I argue that verification technologies can be understood as a structural variable both at the domestic and international levels, with the power to shape the interactions and the dynamics of negotiations at both levels. Verification technologies do not only create a passive technical environment for the negotiations – rather, state leaders and institutions can make conscious and active decision to develop certain verification capabilities. The successful development of these capabilities will result in structural shifts in the negotiations environment, such that the players are forced to reformulate their arguments and positions.

Turning this framing around and making structural variables the focus of analysis can provide critical insights to the dynamics that Gallagher describes in her framework. This shift in perspectives can be approached with the framework that Geoffrey Herrera provides in *Technology and International Transformation*. He conceptualizes technology as an endogenous structural variable that can have independent effects on interaction dynamics in the international system, which challenges traditional representations of technology as an exogenous, passive variable. Making this conceptual shift will allow a more nuanced understanding of how technology and international politics intertwine.

Geoffrey Herrera' *Technology and International Transformation* provides a theoretical foundation for developing the argument above.[27] He challenges the traditional view of technology as an external force and conceptualizes technology as an endogenous structural variable to the system.[28] His analytical framework draws from the classic essay "Do Artifacts Have Politics?" by Langdon Winner, which was a part of an emerging dialogue on what can be called the theory of technological politics.[29] Winner examines how technologies have political effects through two mechanisms, resolving

[27] Ibid.

[28] Ibid., 4, 15.

[29] Langdon Winner, "Do Artifacts Have Politics?" *Daedalus* 109 (1980): 123.

arguments and organizing power and authority, which supports an understanding of technology as a political force: "Rather than insist that we immediately reduce everything to the interplay of social forces, it suggests that we pay attention to the characteristics of technical objects and the meaning of those characteristics. [This] perspective identifies certain technologies as political phenomena in their own right."[30]

Herrera places this argument in the context of structural theories in international relations, which share a general understanding of the definition of structure. Kenneth Waltz, for example, "defined system as being composed of units and their interactions – the interactions forming the structure of the system."[31] Thus, his conceptualization of the international system includes states as the primary units, anarchy as the ordering principle of their interactions, and the distribution of power between them as the structure of the system.[32] A more general definition of structure, however, can be drawn from Waltz's ideas, independent of realist assumptions and balance of power: "A political structure is akin to a field of forces in physics: Interactions within a field have properties different from those they would have if they occurred outside of it, and as the field affects the objects, so the objects affect the field."[33]

Herrera argues that bringing the sources of change in the international system to *within* the system itself, as one of its structural components, can be accommodated by system-level theories. This allows him to conceptualize technology as one of the international system's structural components and understand the relationship between technology and international politics as "fundamental and mutually constitutive."[34] This departs from conceptualizing technology in simply physical terms,

---

[30] Ibid.

[31] Herrera, *Technology and International Transformation*, 13.

[32] Ibid, 15.

[33] Kenneth Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley Pub. Co., 1979), 73.

[34] Herrera, *Technology and International Transformation*, 4.

explaining how this variable interacts with international politics: "Technology is part of the structure of international politics; international politics is one of the factors governing technological change. Together they mutually constitute complex sociotechnical systems that are political at their core."[35]

Herrera's discussion focuses on the unit of analysis of sociotechnical systems, which are comprised of "a complex of machines, operators, procedures and rules, and social institutions for governing them," with the definition referring specifically to technologies that are large in their scale and scope.[36] Herrera's understanding of the relationship between sociotechnical systems and international politics can be scaled to understanding the relationship between verification technologies and the politics of verification. His understanding of technology's role in international politics aligns with how verification technologies relate to the politics of verification – as a structural variable that plays an active, rather than passive, role in influencing the two-level game of verification politics. At the same time, the evolution of verification technologies is shaped by the politics of verification, as decisions over which technologies to develop are inherently political. With respect to scale, while verification technologies are not as expansive in scope as the technologies that are usually understood as sociotechnical systems, their conceptualization as such is valid in the context of verification politics. Verification technologies encompass not only physical equipment and systems, but also the understandings that states develop regarding specific verification technologies and approaches; the protocols that define their use in on-site inspections or other circumstances; and their institutionalization in arms control agreements and treaties. Thus, verification technologies can be

---

[35] Ibid., 2.

Herrera also provides a helpful example of how technology influences the interaction capacity of the system: "Imagine two international systems identical in every important feature – both anarchical and both with an identical distribution of capabilities – but, in the first, horses and sailing vessels are the transport/communications technology matrix, and global computer networks in the second. That difference cannot be attributed to the characteristics of any given state or even groups of states, but is instead a feature of the international system itself. Thus, technology – conceptualized as interaction capacity – is an important feature of the international political system and an appropriate object of study for theory of international politics." (Herrera, *Technology and International Transformation*, 40.)

[36] Ibid., 35.

associated with both material and social dimensions, aligned with the definition of sociotechnical systems.

The critical component of Herrera's analysis with respect to verification technologies is his discussion of the ability of technology to shape the interaction capacity of the international system. In concrete terms, technology influences interaction capacity by being able to "lock in certain political possibilities and lock others out."[37] First, technology can create new options for action by helping "social actors obtain preexisting goals that the prior material environment had made impossible or near impossible."[38] In addition, "they can inspire social actors to imagine new goals that had not occurred to them before the change in the material environment."[39] Second, they can shape the material environment such that certain behaviors, actions, or arguments become limited or impossible. Technology can create "facts on the ground" or reform social or political organization in states, which then influences the options available for state actors.[40]

These mechanics of changing interaction capacity apply to verification technologies at both the technical and political levels. Once a certain technological verification capability has been introduced into the international community at large, the interaction capacity of the system shifts. First, new verification capabilities can expand the options for action both politically and technically. As new verification technologies are created, the options for arms control treaty architecture are expanded, since something that used to be out of reach for monitoring capabilities becomes now possible to detect. This alters the calculations of all stakeholders on the negotiating table about their capacity to detect cheating. This effect is reverberated at the rhetorical level, as the novel verification

[37] Ibid., 4.

[38] Ibid., 33.

[39] Ibid.

[40] Ibid.

capacities also make new arguments available to the negotiators, particularly for arms control proponents. The legitimacy of their arguments about the verifiability of the treaty provisions are increased, enhancing their ability to sway the cautious cooperators towards supporting the arms control agreement.

Second, in addition to increasing options for action, new verification technologies can also create limitations for behavior. Again, this relates both to technical and rhetorical dimensions. The new verification capability may render a certain form of cheating impossible or very easily detectable, which makes previous arguments about the unverifiability of the agreement lose their strength. While those opposing the arms control agreement might still choose to imagine obscure cheating scenarios within the new limits of verification capabilities – and are quite likely to, since these have proven successful strategies in the past – the modified claims lose legitimacy in the eyes of the other stakeholders in the negotiations. Arms control proponents can call their bluff, or show that the potential cheating scenario would have no military significance, which would help them convince the undecided segment to support their positions. Again, it is critical to recognize that this verification debate is taking place within a greater political context, but the point is that in tiebreaker situations, the strength and legitimacy of verification arguments matter. If the new verification capabilities shift these two variables, then the dynamics of the negotiations are different than if those novel verification technologies had not been developed.

Another important dimension of Herrera's conceptualization of technology is his critique of both deterministic and social constructivist understandings of technology in the existing literature on the history and philosophy of technology.[41] Deterministic viewpoints understand technology to be

[41] In the determinist approach, promoted by neorealism and often liberalism, technology is seen as an exogenous variable that can influence politics, but its development is shaped by apolitical factors. In neorealism, for example, military technologies are seen as factors that define a state's military capabilities, and the acquisition of a new technology

above politics with respect to its development, to create political effects that are predictable and definable, and to require no political analysis for understanding its effects on society.[42] In terms of international relations, "the underlying technological environment determines the nature of political authority or, more precisely, the institutions of security provision."[43] Social constructionism challenges this deterministic view of technology's impact and emphasizes the role that human agency, politics, and economics have in facilitating its role in society. The implication of understanding technology as a social construct is to say that social and political processes shape the way that humans interpret any given technology, which then gives rise to its significance and impact.[44] Herrera argues that both determinism and social constructionism are too extreme in their interpretations of technology, with the truth being something in between. Technology is "both a social product and an important independent force because it confronts actors as a real resource or impediment."[45]

In the context of verification technologies, this argument adds substance to Gallagher's framework of the politics of verification and adds to how the framework accounts for the influence of verification technologies. Changes in the available verification capabilities cannot single-handedly make an arms control agreement possible, in the absence of political will – but they can change the likelihood of an agreement by shifting the dynamics of the negotiations. Their impact is not only channeled through the rhetorical level, in the arguments that are made about verification – they also actively and physically influence the choices and arguments that are available to the different stakeholders. This simultaneous influence of verification technologies in defining the physical

by one state can have effects on other actors in the anarchical system. (Herrera, *Technology and International Transformation*, 28.)

[42] Herrera, *Technology and International Transformation*, 28.

[43] Ibid., 29.

[44] Ibid., 31.

[45] Ibid., 7.

capabilities and concrete mechanisms by which actors can monitor and verify arms control agreements, and in shaping the argumentation dynamics of the involved actors, characterizes their role as an independent structural variable. The impact of verification technologies is neither purely deterministic or socially constructed, but a combination of the two.

V. Emerging Verification Capabilities

Linking Gallagher and Herrera's theoretical frameworks together provides a gateway for expanding the analysis of the role that verification technology plays in the politics of verification. It is possible to proceed beyond simple visions of verification technologies as the panacea for resolving verification debates, or the reverse, of understanding verification decisions as purely political, completely isolated from technological development. Gallagher and Herrera's frameworks create a foundation for conceptualizing verification technologies both as an independent and dependent variable and provide a more theoretical footing for the two feedback loop models. This examination now allows for a sharper analysis of how innovations in verification technologies and mechanisms can shift the politics of verification and impact the future prospects for arms control.

One of the important implications of the dynamic interactions between verification technologies and politics is that new verification capabilities can either promote cooperation or intensify competition, depending on what their attributes are and how those attributes are operationalized in the politics of verification. Even if a verification technology is developed with the intention that it will expand the opportunities for verification and enhance the prospects for arms control agreements, there is a risk that the attributes of the technology can be used against this purpose, for example if it has the possibility of providing asymmetric backdoor advantages for the verifier or another party. Thus, in order for the verification technology to serve its intended purpose and be able to foster trust, there has to be verification of the verification technology itself – controlling

the properties of the new capabilities such that no counterproductive side effects will emerge. Ultimately, new tools in the verification toolbox can serve as generic multipliers, either enhancing the likelihood of collaboration, or increasing the chances of competition. Going back to Gallagher's framework, the balance of these dynamics depends on what strategies and arguments are used by arms control opponents and proponents, and how they can use verification capabilities in advancing their political position.

One particular debate, about the tradeoffs between secrecy and transparency in verification, has stirred verification negotiations continuously and connects strongly to the question of how novel verification technologies shape interaction capacity in the politics of verification. In all forms of arms control agreements, states must determine what their interests are in maintaining secrecy about their capabilities, and collaborating transparently with other nations involved in the treaty. Balancing these two interests determines the ways in which the states decide to interact and provide information about their adherence to the treaty provisions.

This verification issue is particularly critical to limitations about warheads, where the host state would need to prove to the verifier that they are truly decreasing their arsenals according to the treaty provisions, for example by demonstrating that they are dismantling authentic nuclear warheads, but doing so without revealing sensitive or classified information about the warheads or their design. The severity of this tradeoff is tied into states' interaction capacity – how much they are able to communicate in the verification process before hitting their hard limits on secrecy – which depends on the nature of the verification technologies available. If it is possible to develop technologies that ameliorate this tradeoff, such that an increase in transparency does not lead to a proportional sacrifice in secrecy, then these technologies would result in an increase in the interaction capacity of the international system.

The effort to develop verification approaches that do this has been ongoing since the early days of U.S.-Soviet arms control negotiations, but only in the past decades have there been concrete successes. The next chapters will outline the history of these development efforts, as well as focus on a specific category of technologies conceived in the past few years that represent the newest generation of these efforts. Before going in depth in describing these verification approaches, it is critical to understand how they fit into the greater context of the politics of arms control, and why is it important to invest in developing these verification capabilities. This can be done by framing this verification issue within the discussion of this chapter.

As Gallagher's framework illustrates, each participant in the arms control negotiations is coming to the table with pre-existing perceptions and preferences about arms control. These notions will shape their views about verification and the emphasis they place on technical verification needs. On the other hand, they are constrained by the structural environment in which they interact, with one of the variables defining that environment being the status of verification technologies. Aligned with Herrera's conceptualization of technology as an endogenous structural variable to the international system, it is possible to imagine verification technologies as something that can be actively and deliberately shaped by the political actors involved in negotiations. The changes in the nature and quality of verification technologies will consequently shape the dynamics of the verification debates.

In the specific context of warhead limitations and the verification of these limitations, technical verification capabilities are currently the limiting factor that constrain treaty architecture and the factor that gives a comparative advantage to those who oppose agreements that pose numerical restrictions. Current verification mechanisms focus on monitoring delivery vehicles, as they are sufficiently large for detection by national technical means and are also compatible with the on-site inspection

procedures in use.[46] These verification approaches, however, pose severe limitations for future disarmament prospects and agreements that expand beyond the status quo – those that address much lower numbers of warheads, involve new categories of nuclear weapons, and engage states that have very little experience in arms control.

An illustrative example of the restricted nature of the existing warhead limitation strategies can be drawn from the New START counting rules, applied to China's nuclear arsenal. Under New START counting rules, China has virtually no treaty-accountable nuclear weapons, because the treaty only considers warheads that are affiliated with operationally deployed strategic delivery systems.[47] Since China only mounts its warheads with delivery systems for testing purposes, and at other times keeps them separate, the approach used in New START has little practical use as a foundation for agreements that limit China's nuclear weapons. This insight applies to every other nuclear weapons state other than the United States and Russia, who are the only states who keep their warheads deployed and operational.[48]

The verification needs in agreements that intend to involve one of the three parameters above – lower arsenals, other warhead categories, and new states – are impossible using current technical verification capabilities, since they require authenticating individual warheads. The premise here is that states would want to ensure that their opponents' reductions are genuine, with the fear that the other

[46] National technical means refer to state-controlled intelligence capabilities aimed at detecting noncompliance, including imaging reconnaissance satellites, aircraft radars and optical systems, sea- and ground-based radar and antenna systems, radio-technical reconnaissance, and many other classified mechanisms. (Source: Congress of the United States, "Verification Technologies: Measures for Monitoring Compliance with the START Treaty," Office of Technology Assessment, available at http://govinfo.library.unt.edu/ota/Ota_2/DATA/1990/9029.PDF; also William Burr, "The Secret History of The ABM Treaty, 1969-1972," *National Security Archive Electronic Briefing Book No. 60*, November 8, 2001, http://nsarchive.gwu.edu/NSAEBB/NSAEBB60/index2.html.)

[47] Steven Pifer, "U.S. Military Advantages and the Future of Nuclear Arms Control." *Heinrich Boell Stiftung*, October 10, 2013, https://www.boell.de/en/2013/12/20/us-military-advantages-and-future-nuclear-arms-control

[48] Arms Control Association, "Nuclear Weapons: Who Has What at a Glance," updated January 2017, available online from https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat.

side would be dismantling 'blanks' and hiding the authentic warheads to a covert storage facility. While it is possible to agree on further warhead reductions without these authentication protocols, either using START-type counting rules or even without any verification provisions, as with SORT, it is unlikely that this would be politically acceptable. Especially in the 'hardest' cases, such as in disarmament agreements between India and Pakistan, the level of mistrust is likely to be so high that the countries will pursue the strictest possible verification provisions.[49] Under these conditions, the authentication of warheads becomes a political necessity, but the current verification capabilities do not make this technically possible without revealing information about the characteristics of the warheads themselves – which in turn would hit another barrier of political unacceptability.

The emergence of novel verification capabilities, however, can transform the situation both politically and technically. The verification approaches discussed in a following chapter, which employ physical cryptographic proofs in a high-security authentication protocol, or 'zero-knowledge verification', would provide a technical capacity that meets the most rigorous demands that policymakers could make. These verification approaches would be a significant technical asset for arms control treaty architecture, because they would allow addressing new categories of warheads that were previously unattainable, by creating the ability to authenticate and track individual warheads, and re-authenticate them during their movement in the dismantlement process. On the political side, the development of these new verification approaches would change the arguments made both by arms control opponents and proponents. They eliminate the technical argument that warhead limitations cannot be verified with a high level of accuracy, or that the verification process reveals sensitive information which would be a national security threat. Thus, the existence of these technologies would

[49] Of course, the question here is how the states could have come to an agreement under these conditions, but that is outside the scope of analysis here. One possibility would be an internationally enforced disarmament treaty, for example, but also voluntary agreements after the relations between the states have improved, but not sufficiently to overcome the long-standing mistrust between the countries.

be an essential asset for disarmament negotiators, as it constrains the arguments and strategies that are available to the involved stakeholders, builds trust in the verification process, and helps gain support for the arms control efforts within domestic constituencies.

As has been addressed in this chapter previously, however, the dynamic interactions between the technical and political dimensions make the impact of novel verification capabilities unpredictable. Verification is never perfect, as the capabilities of verification technologies are always constrained in one way or another.[50] The specific issues and limitations relating to zero-knowledge verification approaches will be discussed in a later chapter, but several challenges are inherently connected to these mechanisms. The critical question is, then, how policymakers and negotiations – especially in an international context – will assess the fundamental uncertainties relating to these and other verification technologies. The traditional way to assess verification provisions is to focus on their ability to detect militarily significant violations, but this standard is very subjective and liable to political maneuvering.[51]

The answer to the question of how to deal with the imperfection of verification technologies has two components – one relating to the dissemination of information about the technologies themselves, and another focusing on the context in which verification negotiations take place. The first dimension has been mentioned previously in this chapter, which is that there is a need to verify the verification technologies themselves. More specifically, certification is the process by which the host state verifies the technical equipment, whereas authentication is the parallel process from the inspector side.[52] The easier that these two functions are to do, the easier it is to inform the

[50] Amy Woolf, *Monitoring and Verification in Arms Control* (Washington D.C.: Congressional Research Service), https://www.fas.org/sgp/crs/nuke/R41201.pdf, 6.

[51] Ibid.

[52] Sébastien Philippe, Boaz Barak, and Alexander Glaser, "Designing Protocols for Nuclear Warhead Verification," *INMM 56th Annual Meeting* (2015): 2.

policymakers about the technical verification capabilities and build trust around the new verification capabilities.

The second component is that the process of negotiating verification provisions, as well as the actual implementation of verification protocols, involves iterated relationships that persist over time. This is true between policymakers and the technical verification community, as well as at the international level in the negotiations between states. These iterated interactions are visible in the feedback loops described earlier. Robert Axelrod has discussed the significance of iterated relationships in game theoretic terms, arguing that the strategy of tit for tat – "starting with cooperation, and thereafter doing what the other player did on the previous move" – is the best option for sustaining cooperative behavior between actors.[53] One of his observations is that reciprocity becomes more effective when interactions are decomposed, or take place in smaller increments.[54] In the context of arms control, this is a critical factor that can help overcome imperfect verification, which is essentially an issue of not knowing whether the partner adhered to their commitments in past moves or not:

> Of course, a major question in arms control is whether each side can, in fact, know what the other side actually did on the previous move – whether they cooperated by fulfilling their obligations or defected by cheating. But for any given degree of confidence in each side's ability to detect cheating, having many small steps will help promote cooperation as compared to having just a few big steps. Decomposing the interaction promotes the stability of cooperation by making the gains from cheating on the current move that much less important relative to the gains from potential mutual cooperation on later moves.[55]

Yet, when Axelrod's game is run under conditions of uncertainty due to "moderate error in perception," which can result from random noise, systematic misperception, or other factors, the

[53] Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1981), viii.

[54] Ibid., 132.

[55] Ibid., 132.

strategy of reciprocity still remains the best option for the players.[56] What Axelrod has observed in game theoretic terms – that under iterated interaction dynamics, "cooperation can get started and prove stable in situations which otherwise appear extraordinarily unpromising" – is also generalizable to human affairs and international relations at large, including nuclear disarmament efforts.[57]

Ultimately, the combination of the gradual development in verification capabilities and the facilitation by iterative relationships both within and between states could bring states to the required threshold of trust that is needed for disarmament, despite the inherent imperfectness of verification. The situation has analogy to Zeno's Paradox, as formulated by Aristotle:

> In a race, the quickest runner can never overtake the slowest, since the pursuer must first reach the point whence the pursued started, so that the slower must always hold a lead.[58]

Verification negotiations can be understood as a race of sorts, where the 'slower' party is trying to develop verification technologies that allow them to catch up to the 'faster' party, or those who always ask for stricter barriers against cheating and create new possibilities for deception. In a sense, this is a competition between trust and mistrust, with technological capabilities trying to bridge the gap to the required level of confidence and trust in verification. Axelrod's observations, however, provide the missing piece here – iterated relationships, jointly with progressive technological development, will allow enough trust to be accrued. At that critical point, the political incentive to create the agreement will outweigh the risk of being deceived by the other side. This idea aligns with the mathematical solution to Zeno's paradox of motion, which is that the sum of an infinite series (the steps of the quicker runner to catch up to the slower one) can be finite, if the series is convergent

---

[56] Ibid., 222, Chapter 8, Note 5.

[57] Ibid., 21.

[58] Aristotle, Physics VI:9, 239b15; cited in Donald Byrd, "Zeno's "Achilles and the Tortoise": Paradox and the Infinite Geometric Series," February 2010, revised December 2012. http://homes.soic.indiana.edu/donbyrd/Teach/Math/Zeno+Footraces+InfiniteSeries.pdf.

– meaning that the terms get progressively smaller.[59] Similarly, Axelrod argues that decomposing a relationship into smaller pieces of interaction makes the difference between cooperation and competition.

To put this in the specific context of warhead verification, the objective of the verification technologies under development is not to become a panacea that solves perfectly the tradeoff between secrecy and transparency, but to elevate it to a level that is acceptable to states and that provides sufficient level of trust with respect to both concerns. At some point, determined by the balance of political interests, these verification capabilities will reach a critical threshold that allows states to be content with the verification capabilities that have been developed. Importantly, however, this threshold level is transient and may even be unknown to the negotiators themselves. The implication is that the ongoing research must set the standards they are pursuing at the highest possible level, to be sufficient for even the hardest cases and conditions.

While I will provide a historical context for this verification challenge in the following chapter, I want to emphasize that the purpose of this thesis is not to be a historical, *de post facto* examination of the issue. The debate about the future of arms control persists, even if we may be in a moment of slowdown, with the technological development process being pursued in national laboratories, academic institutions, and multilateral endeavors. My purpose is to contribute to these ongoing dynamics and bring attention to the fact that by taking active agency in developing novel verification capabilities, we have the power to shape the prospects of future agreements to limit nuclear weapons. The verification approaches I describe in this thesis may never be fully implemented in an arms control treaty, but I argue that they are important regardless – both for opening the dialogue on new treaty

[59] Byrd, "Zeno's "Achilles and the Tortoise": Paradox and the Infinite Geometric Series."

architecture options, as well as shaping the political dynamics of the treaty negotiations themselves, as this chapter has shown.

2. Past Verification Approaches

I. Introduction

Past disarmament regimes have taken different approaches to controlling nuclear arms, from limiting the testing of these weapons to reducing their numbers.[60] All of these measures have contained some provisions for verification, through different mechanists and at varying levels of intensity.[61] Overall, the evolution of the agreed verification provisions reflects a trend towards more complexity, in terms of the requirements for effective verification and the monitoring technologies employed to meet these requirements.[62] As was discussed in the previous chapter, however, the political dynamics of the verification negotiations is a more complicated story than simply defining the requirements for verification and then creating technologies to fulfill them. While these political dynamics are an essential part in understanding how verification decisions are made, the following discussion on the history of disarmament treaty verification also emphasizes how the availability of verification technologies determine the limits of possibility for decision-makers when making judgments about the requirements of the verification process.

Past nuclear arms reductions have been pursued mainly in the context of the United States and Russia, and, earlier, the Soviet Union. These bilateral disarmament efforts started with the Strategic Arms Limitation Talks (SALT) I and II in 1972 and 1979, respectively, at the peak of the

[60] Nuclear Threat Initiative, "Nuclear Disarmament Timeline," http://www.nti.org/analysis/articles/nuclear-disarmament-timeline/.

[61] United Nations Institute for Disarmament Research and the Verification Research, Training and Information Centre (VERTIC), *Coming to Terms with Security: A Handbook on Verification and Compliance* (London: VERTIC, 2003), p. 1.

[62] Rudolf Avenhaus, Nicholas Kyriakopoulos, Michel Richard, and Gotthard Stein, *Verifying Treaty Compliance: Limiting Weapons of Mass Destruction and Monitoring Kyoto Protocol Provisions* (Berlin: Springer, 2006), 13.

Cold War.[63] These were followed by the Anti-Ballistic Missile (ABM) Treaty, which was signed in 1972, and the Intermediate-range Nuclear Forces (INF) Treaty, signed in 1987.[64] After the dissolution of the Soviet Union, the United States and Russia continued these arms reduction efforts through the Strategic Arms Reduction Talks (START), with the first agreement being made in 1991 and the second in 1993.[65] Following this, the Strategic Offensive Reductions Treaty (SORT) was signed in 2002 and the New START in 2011.[66] Several unique factors relating to the nature of U.S.-Russia bilateral relations and the states' nuclear capabilities have made this cooperation possible and enabled the states to come to an agreement on how these disarmament efforts can be verified.

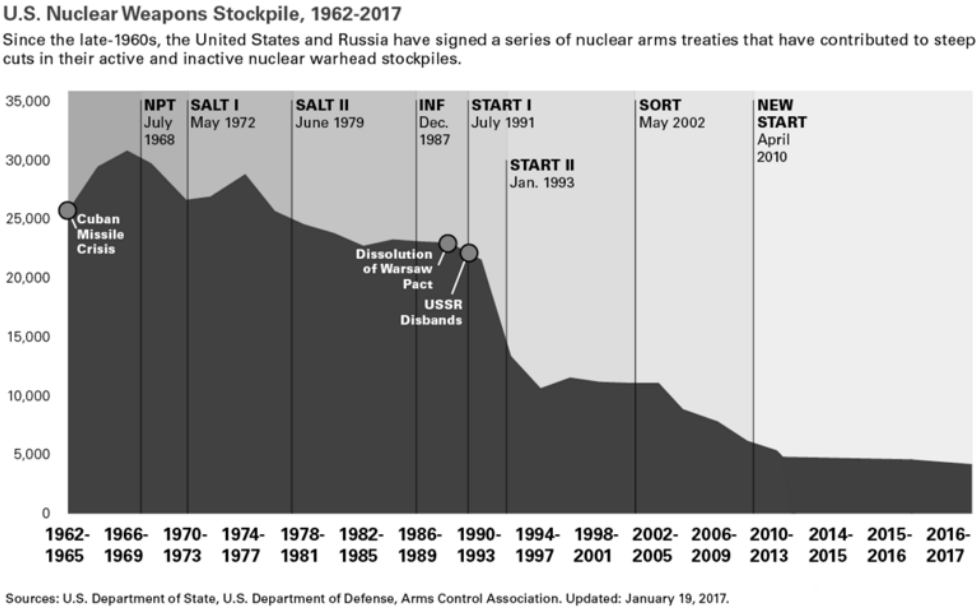

Figure 2.1. Source: Arms Control Association, "Nuclear Weapons: Who Has What at a Glance," updated January 2017, available online from https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat.

[63] Steve Tulliu and Thomas Schmalberber, *Coming to Terms with Security: A Lexicon for Arms Control, Disarmament and Confidence-Building* (Geneva: United Nations Institute for Disarmament Research, 2003), 78, https://www.files.ethz.ch/isn/92883/Full-text.pdf.

[64] Ibid.

[65] Ibid., 79.

[66] Arms Control Association, "U.S.-Russian Nuclear Arms Control Agreements at a Glance," April 2014, available at https://www.armscontrol.org/factsheets/USRussiaNuclearAgreementsMarch2010.

In these agreements, the tension between intrusiveness and confidentiality has been circumvented by not defining warheads themselves as the treaty-accountable item, but rather focusing on their delivery vehicles and launchers.[67] Authenticating reductions in these larger systems requires less intrusive verification protocols, as they only require negative verification of the absence of warheads beyond the maximum number agreed in the treaty.[68] The accounting system is designed such that each delivery vehicle has a specified number of attributed warheads and the verification protocol aims to establish that there are no deployed warheads beyond this. This can be contrasted with positive verification, which would entail verifying that a nuclear warhead is truly what it is stated to be, possibly even ensuring that it is of the correct type. In addition, these past treaties were very conservative in terms of allowing access to territory or collecting information about other military activities.[69]

The chapter outlines the past trajectory of nuclear verification provisions, by first analyzing disarmament agreements made in the U.S.-Soviet and U.S.-Russia context, then explaining the unique characteristics of disarmament between the two countries and identifying challenges that are likely to arise in a multilateral context, and then exploring past verification efforts carried out internationally. The chapter starts by exploring the SALT era, where verification was focused on national technical means. Next, the chapter focuses on the INF Treaty, which contained several innovations in verification, including radiological measurements and on-site inspections. After this, the focus is on the START era – including START I, which employed many of the verification mechanisms used in the INF Treaty; START II, which was not ratified; SORT, which did not contain verification

[67] Congress of the United States, "Verification Technologies: Measures for Monitoring Compliance with the START Treaty."

[68] Ibid.

Chantell Murphy and James Doyle Johnson, "Recovering START Institutional Knowledge," *INMM 52nd Annual Meeting* (2011): 2.

[69] Woolf, *Monitoring and Verification in Arms Control*, 9.

provisions; and finally, New START, which intended to simplify the original START treaty's verification provisions without losing their robustness.

After explaining this historical trajectory, the chapter illustrates why the verification choices made in these past treaties were possible in the specific U.S.-Soviet or U.S.-Russia context. After this, the focus is on the factors that will make future disarmament efforts fundamentally different. Next, the chapter explores the few concrete experiences that the international community has had in verification, which are limited to verifying the dismantlement of nuclear programs in Iraq, South Africa, and Libya. In each of the three cases, it is highlighted how concerns about proliferation-sensitive information shaped the structure of the verification programs and how concerns about legitimacy emerged.

II. The SALT Era

The first SALT negotiations resulted in the Interim Agreement on Offensive Arms and the ABM Treaty, which were aimed at limiting both offensive and defensive strategic systems and stabilizing the accelerating arms race between the two states.[70] Under SALT I, both sides refrained from producing new intercontinental ballistic missile (ICBM) silos and submarine-launched ballistic missile (SLBM) silos.[71] It also enforced limits on the number of SLBM launch tubes and SLBM-capable submarines.[72] The treaty was limited in its ability to contain nuclear arms buildup, however, as it did not limit the actual number of deployed warheads. Both states could increase their nuclear capabilities through acquiring more strategic bombers, which the treaty did not control, or deploying

[70] Ibid.

U.S. Department of State, Office of the Historian, "Strategic Arms Limitations Talks/Treaty (SALT) I and II," available online at https://history.state.gov/milestones/1969-1976/salt.

[71] Arms Control Association, "U.S.-Russian Nuclear Arms Control Agreements at a Glance."

[72] Ibid.

ballistic missiles carrying several warheads instead of one (multiple independently targetable reentry vehicles, MIRVs) in the allowed number of ICBMs and SLBMs.[73] The ABM treaty limited the strategic missile defenses of both states to 200, and later 100, interceptors.[74]

Concerns about verification were a key factor in both the SALT I and ABM Treaty negotiations, significantly influencing the ultimate contents of the agreed treaties.[75] For the ABM Treaty, the political preference for both sides would have been to allow nationwide ABM deployments, but the treaty negotiations concluded with permitting only one local ABM system.[76] If a nationwide radar system would have been permissible, it would have been exceedingly difficult for both sides to verify the true extent of the system.[77] Similarly, the political incentives would have been in place to expand the SALT I limitations to missiles and missile characteristics, but required measures for verification would have been unacceptable due to their intrusiveness.[78] In the end, national technical means of verification (NTM) were agreed to as the key verification mechanism in the treaties, which refer to state-controlled intelligence capabilities aimed at detecting noncompliance.[79] This also included non-interference with the other state's intelligence collection and verification efforts.[80]

The SALT II agreement intended to address some of the systems that SALT I had left untouched, particularly MIRVs, as well as further limit the number of delivery vehicles and limit

---

[73] Ibid.

[74] Ibid.

[75] U.S. Department of State, "Action Memorandum, January 13, 1972," available at http://nsarchive.gwu.edu/NSAEBB/NSAEBB60/abm29.pdf.

[76] Jan Lodal, "Verifying Salt," *Foreign Policy*, No. 24 (1976): 41.

[77] Ibid., 40.

[78] Ibid., 41.

[79] Congress of the United States, "Verification Technologies: Measures for Monitoring Compliance with the START Treaty."

William Burr, "The Secret History of The ABM Treaty, 1969-1972," *National Security Archive Electronic Briefing Book No. 60,* http://nsarchive.gwu.edu/NSAEBB/NSAEBB60/index2.html.

[80] Woolf, *Monitoring and Verification in Arms Control*, 9.

nuclear weapons development.[81] Again, verification became a key issue, as concerns about Soviet cheating in SALT I made America extremely sensitive about verification and intent on ensuring airtight protocols.[82] For example, limiting MIRVs would require both sides to be able to distinguish between MIRVed and un-MIRVed missile launchers.[83] Ultimately, SALT II verification was also based on NTM. The treaty contained further provisions for not obstructing the other state's NTM, including the collection of electronic signals (telemetry) and use of photo-reconnaissance satellites.[84] The ability to collect telemetry information, which is generated during missile flight tests and contains details about weapon function, was a key concern for the states, as the treaty included limitations on weapons characteristics.[85] The issue of encryption of telemetry information, however, remained tense throughout and beyond the negotiations, as the two sides had divided opinions of the importance of this verification mechanism.[86] SALT II also included provisions for ensuring the distinguishability of different weapons types through "externally observable differences" or "functionally-related observable differences" that could be detected by NTM.[87] Questions about verification confidence were a partial reason, alongside greater geopolitical concerns such as the Soviet invasion of

[81] U.S. Department of State, Office of the Historian, "Strategic Arms Limitations Talks/Treaty (SALT) I and II."

[82] Office of the Secretary of State, "Memorandum for the President: SALT Verification," August 7, 1978, http://nsarchive.gwu.edu/NSAEBB/NSAEBB231/doc14c.pdf.

U.S. National Security Council. "Memorandum for the Members of the Verification Panel: Preparations for Next Round of SALT," December 30, 1969, http://nsarchive.gwu.edu/nukevault/ebb281/6A.PDF.

Lodal, "Verifying Salt," 41.

[83] Lodal, "Verifying Salt," 41.

[84] U.S. Department of State, Office of the Historian, "Strategic Arms Limitations Talks/Treaty (SALT) I and II."

[85] Woolf, *Monitoring and Verification in Arms Control*, 9.

[86] "SALT II and the Growth of Mistrust," *Transcript of the Proceedings of the Musgrove Conference of the Carter-Brezhnev Project*. May 7-9, 1994, 83, http://nsarchive.gwu.edu/carterbrezhnev/C-B%20-%20SALT%20II%20-%20Musgrove%20master%20transcript.pdf.

[87] Woolf, *Monitoring and Verification in Arms Control*, 9.

Afghanistan, that led the Carter administration to turn its back on the agreement and ask the Senate not to ratify the treaty.[88]

III. The INF Treaty

As disarmament negotiations between the United States and the Soviet Union continued later in the 1980s, increasing interest emerged in novel forms of verification. The instrumentation for these approaches, which included on-site inspections and other more intrusive verification mechanisms, would need to be developed to make the verification provisions possible. The key motivation to acquire these verification capabilities was further limitations on ballistic missiles that carried multiple warheads, which had only been verified through NTM in the SALT treaties. These missiles may not carry the maximum number of warheads that their structure would allow, but instead the loadout could include penetration aids, telemetry systems, or other non-nuclear objects.[89] The national laboratories in the United States engaged several research projects to understand how this authentication task could be executed, considering the key limiting factors that the verification process would encounter. One of the key concerns was protecting sensitive and classified design information, which would be at risk during the measurement process.

These new verification measures were implemented in the INF Treaty, which was unprecedented in its verification scope insofar as it included on-site inspections and data exchanges for the first time.[90] The INF Treaty contained a provision for being able to distinguish the treaty-accountable SS-20 intermediate-range ballistic missiles from the non-limited SS-25 intercontinental

[88] U.S. Department of State, Office of the Historian, "Strategic Arms Limitations Talks/Treaty (SALT) I and II."

[89] Murphy and Johnson, "Recovering START Institutional Knowledge," 2.

[90] Nuclear Threat Initiative, "Nuclear Disarmament Timeline," http://www.nti.org/analysis/articles/nuclear-disarmament-timeline/.

ballistic missiles.[91] The challenge was that the missile types used the same first stages, including engines and fuel tanks, and were indistinguishable based on external characteristics.[92] As the verification provisions didn't allow inspection access to the missiles themselves, radiological measurements were agreed on as a proxy measure of the missiles' internal structure. Two approaches were approved – distinguishing between the radiological "fingerprints" of the missiles in their normal loadouts, and measuring radiographically the external structural features of the missiles, including length.[93] In determining the fingerprint of a particular missile, a simple neutron detector would be used to measure neutron count rates at pre-selected points surrounding the warhead, which had been found to enable their accurate differentiation.[94]

The experiences in developing and negotiating the INF verification provisions motivated further research into warhead-focused verification. The INF system was focused on differentiating two specific types of missiles, but future arms reductions would involve a wide range of weapons systems, possibly even individual warheads. In 1990, the national laboratories in the United States engaged in a demonstration that highlighted how any feasible measurement approach would need to be able to accommodate a range of weapons systems designs, which would create distinct radiation fields indicative of their configurations.[95] The verification system demonstrations at the Francis E. Warren Air Force Base in Wyoming used the Peacekeeper missile (MX, LGM-118) as its model system, as it doesn't conform to the standard configuration of an axially symmetric design.[96] The measurement systems tested in the demonstrations, based on circumferential gamma or neutron

[91] Murphy and Johnson, "Recovering START Institutional Knowledge," 2.

[92] Ibid.

[93] Ibid.

[94] Ibid., 5.

[95] Ibid., 2.

[96] Ibid.

radiation scanning, revealed important challenges relating to environmental conditions and measurement system optimization and engineering, but most importantly, to security. The information generated in the tests would have been classified as Secret/Restricted Data (S/RD) and required the inspectors to have very intrusive access to the missiles.[97] These research efforts were made particularly with the START negotiations in mind, but the U.S. national laboratories (and those in other states) have continuously engaged in this type of research. One of the first such American experiments was the Project Cloud Gap, which included Field Test 34 in 1967 that investigated the use of radiation detection equipment in the context of dismantling nuclear weapons, and the extent to which classified information would be at risk in this scenario.[98]

IV. The START Era

Ultimately, the following START negotiations could not find a mutually agreeable way to overcome the issue of classified information and succumbed to a warhead accounting system that did not require specific individual counting of warheads. Instead, the treaty contained a complex accounting system for the limit on deployed ICBMs, SLBMs, and heavy bombers, and for the total number of warheads attributed to each of the delivery vehicles, including sub-limits.[99] The warheads were counted based on a warhead attribution number specific to each delivery vehicle, which are determined based on telemetry data obtained through missile flight tests.[100] Each delivery vehicle was assumed to carry the maximum loadout of nuclear warheads, which then defined the upper limit for

[97] Ibid., 3.

[98] David Cliff, Hassan Elbahtimy and Andreas Persbo, "Verifying Warhead Dismantlement: Past, Present, Future," *VERTIC Research Reports,* Number 9, September 2010, 22 http://www.vertic.org/media/assets/Publications/VM9.pdf.

[99] U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Strategic Arms Reduction Treaty (START I): Executive Summary," http://www.acq.osd.mil/tc/treaties/start1/execsum.htm.

[100] Union of Concerned Scientists, "Verification of New START," July 2010. http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/inspection-fact-sheet-1.pdf.

treaty-accountable warheads.[101] This accounting, however, was only done on a theoretical basis and did not necessarily reflect the true loadouts in each system. For example, the treaty attributed one warhead to each non-LRNA heavy bomber, even though they have the capacity to carry multiple.[102] Thus, START I verification protocols are only intended to ensure that these theoretical warhead limits were not exceeded in any missile type, rather than establishing the exact number of warheads held by each country.[103]

The furthest that START I went in terms of verification sophistication was the provision it contained for the use of radiation detection equipment in a situation where a treaty partner would want to confirm the non-nuclear nature of an object, container, or space.[104] This was very similar to the INF Treaty provision on the use of radiological measurements and relied on the same detector technology.[105] Under START I, a state had the right to authenticate the radiological signature of a long-range-non-nuclear air-launched cruise missile, ensuring that it was not nuclear.[106] The procedures for using this equipment specified how the measurement system would be certified, controlled, and used such that no sensitive information would be at risk.[107] The treaty's very limited on-site inspections

---

[101] Murphy and Johnson, "Recovering START Institutional Knowledge," 2.

[102] L.L. Gaines, *Start II: Thinking One Move Ahead* (Washington D.C.: United States Department of Energy, Argonne National Laboratory, 1991).

[103] Union of Concerned Scientists, "Verification of New START."

[104] Murphy and Johnson, "Recovering START Institutional Knowledge," 1.

[105] Ibid., 7.

[106] Annex 4 to the Protocol on Inspections and Continuous Monitoring Activities: "Inspectors shall have the right to view a long-range-non-nuclear ALCM, to use radiation detection equipment to confirm that the ALCM is non-nuclear, and to make linear measurements ... If, by viewing such an ALCM, inspectors are unable to confirm that the ALCM is not a long-range nuclear ALCM, a member of the in-country escort may allow the inspectors to carry out additional actions, which may include ... using radiation detection equipment to confirm the presence of features that make the ALCM distinguishable from long-range nuclear ALCMS .... If, by viewing the contents of the container designated for inspection to confirm that a long-range nuclear ALCM is not contained therein inspectors are unable to confirm that the contents are not a long-range nuclear ALCM, the in-country escort shall remove the contents from the container. Inspectors shall have the right to use radiation detection equipment to confirm that the contents are non-nuclear ... The radiation detection equipment and a radiation source may also be used to confirm that the container does not conceal the presence of radiation." (Source: Murphy and Johnson, "Recovering START Institutional Knowledge," 1.)

[107] U.S. Department of State, "Annex 15: Procedures for the Use of Radiation Detection Equipment," START Treaty. http://www.state.gov/documents/organization/27380.pdf

did not allow the verification of the specific number of warheads in delivery vehicles, only that the warhead limits and sub-limits were not exceeded.[108]

START II was a continuation and an addition to START I, maintaining the earlier treaty's provisions and building on its verification model, in addition to expanding it in certain dimensions.[109] In START II, warheads were attributed to their delivery vehicle based on their true carrying capacity, which addressed the inaccuracy in START I warhead counting.[110] START II also contained new verification provisions for observing SS-18 missile silo conversion, missile elimination, exhibitions, as well as visual inspections of heavy bombers.[111] START II never entered into force, however, due to disagreements on U.S. ratification of the treaty and withdrawal from the ABM Treaty.[112]

The New START Treaty was signed in 2010, after the expiration of START I in 2009 and the negotiation of the SORT agreement, which contained no verification provisions.[113] New START continued the legacy of the verification systems implemented under START I, combining on-site

---

[108] Union of Concerned Scientists, "Verification of New START."

[109] Nuclear Threat Initiative, "Treaty Between the United States of America and the Union of Soviet Socialist Republics on Strategic Offensive Reductions (START II)," updated October 26, 2011. http://www.nti.org/learn/treaties-and-regimes/treaty-between-united-states-america-and-union-soviet-socialist-republics-strategic-offensive-reductions-start-ii/.

[110] Gaines, *Start II: Thinking One Move Ahead.*

The White House, "Background Information: START II Ratification," January 26, 1996, http://fas.org/nuke/control/start2/docs/strtrat.htm.

[111] The White House, "Background Information: START II Ratification," January 26, 1996, http://fas.org/nuke/control/start2/docs/strtrat.htm.

U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Strategic Arms Reduction Treaty (START II): Heavy Bomber Protocol," http://www.acq.osd.mil/tc/treaties/start2/start2_prot_bomber.htm.

[112] Nuclear Threat Initiative, "Treaty Between the United States of America and the Union of Soviet Socialist Republics on Strategic Offensive Reductions (START II)," updated October 26, 2011, http://www.nti.org/learn/treaties-and-regimes/treaties-between-united-states-america-and-union-soviet-socialist-republics-strategic-offensive-reductions-start-i-start-ii/.

[113] Union of Concerned Scientists, "Verification of New START."

inspections, exhibitions, data exchanges, unique identifiers, and national technical means.[114] It modified some of the complex provisions in the past system, but also introduced new measures to ensure accurate accounting.[115] These included unique identifier tags on missiles, their launchers, and bombers, as well as notification protocols related to the movement of delivery vehicles.[116] Most importantly, the new accounting procedure involved counting individual warheads, as opposed to following the strategy in START I of maximum loadouts specified for delivery vehicles.[117] Under New START, each state must define how many individual warheads each missile contains, and during inspections, any of the missiles in the stockpile could be asked to be verified.[118] As in START I, the agreement allows for the use of radiation detection to confirm an object to be non-nuclear.

The verification mechanisms in the INF, START I and II, and New START started to approach the issue of individual warhead verification. Importantly, however, the verification provisions thus far have been a binary true/false measurement of the absence of a nuclear warhead.[119] These agreements do not allow the use of radiation detection equipment to confirm an object to be nuclear, let alone more specific information about warhead characteristics or configuration.[120] As disarmament continues, this may become a key capability requirement for verification provisions,

---

[114] U.S. Department of State, Acting Under Secretary of State Rose Gottemoeller. "The New START Treaty: An Overview of the Verification Regime," P5 Conference, Geneva, Switzerland, http://www.state.gov/documents/organization/208183.pdf.

[115] Union of Concerned Scientists, "Verification of New START."

[116] Ibid.

[117] Ibid.

[118] Ibid.

[119] Murphy and Johnson, "Recovering START Institutional Knowledge," 6.

[120] C. R. Wuest, "The Challenge for Arms Control Verification in the Post-New START World," Lawrence Livermore National Laboratory, July 16, 2012, 8, https://www.nti.org/media/pdfs/Wuest_2012_The_Challenge_for_Arms_Control_Verification_in_the_Post_New_START_World.pdf.

driven by the need to distinguish warheads or their components based on their type or characteristics, not only their nuclear or non-nuclear nature.[121]

V. Challenges of Multilateralization

i. Uniqueness of U.S.-Russia Context

The U.S.-Russia context, and before that the U.S.-Soviet, has been unique in many respects, which has facilitated disarmament despite the inability to count individual warheads and thus construct treaties based on warhead limitations. The critical factor that has made this approach to treaty architecture and verification possible is the vast size of the nuclear arsenals of both states. During the Cold War, both manufactured tens of thousands of warheads, and even after several rounds of arms reduction, still maintain over 1,550 deployed warheads.[122] At this level of nuclear arsenals, both states have a relatively high tolerance for the level of uncertainty contained in treaty verification provisions – a significant diversion scenario threatening strategic stability would be much more than one individual warhead.[123] Thus, both the United States and Russia have been able to negotiate nuclear arms reductions without the ability to fully verify each other's warhead numbers.

Another important factor is that both states have extensive capabilities in national technical means (NTM), including imaging reconnaissance satellites, aircraft radars and optical systems, sea- and ground-based radar and antenna systems, radio-technical reconnaissance, and many other classified mechanisms.[124] This served as a critical confidence-building mechanism in the agreements between the states. These capabilities are highly compatible with the reduction focus on delivery vehicles and

[121] Murphy and Johnson, "Recovering START Institutional Knowledge," 6.

[122] Arms Control Association, "Nuclear Weapons: Who Has What at a Glance."

[123] Wuest, "The Challenge for Arms Control Verification in the Post-New START World," 3.

[124] Congress of the United States, "Verification Technologies: Measures for Monitoring Compliance with the START Treaty," 8.

launchers, as these large systems can be monitored through NTM.[125] These capabilities are held highly confidential, which ensures ambiguity about the specific detection abilities that each state has.[126] This is an important factor that underlies their effectiveness as verification mechanisms. When neither state is fully certain of partner capabilities in independent verification through NTM, they cannot design around this form of verification, which is a concern in cooperative verification mechanisms that are fully known to all sides of the agreement.[127] States can also develop NTM capabilities such that they form synergies with the cooperative monitoring measures and can thus enhance their confidence in their ability to detect deception.[128] Overall, the advanced NTM capabilities in both the United States and Russia act as a backdrop for all disarmament treaties between the states.

The future of disarmament verification will look very different, whether in the context of continued U.S.-Russia bilateral agreements or multilateral disarmament treaties, as none of the unique characteristics of past verification efforts will hold true. First, when discussion concerns hundreds of warheads and levels even below this, the tolerable margin of error diminishes. At these levels, verifying and tracking each individual warhead will become critical. This also involves obtaining knowledge about the type and status of a specific warhead and being able to re-authenticate these attributes in later stages of the dismantlement process. Agreements at these levels will also involve new categories of warheads and items, including non-deployed and non-strategic warheads and warhead components.[129]

---

[125] U.S. Department of State, Acting Under Secretary of State Rose Gottemoeller. "The New START Treaty: An Overview of the Verification Regime."

[126] Jeffrey Riechelson, "Declassifying the "Fact of" Satellite Reconnaissance," *National Security Archive Electronic Briefing Book No. 231*, http://nsarchive.gwu.edu/NSAEBB/NSAEBB231/.

[127] Nancy Gallagher, "The Design of Verification Regimes," in *Nuclear Proliferation in South Asia: The Prospect for Arms Control*, ed. Stephen Cohen (Boulder: Westview Press, 1991), 80.

[128] Congress of the United States, "Verification Technologies: Measures for Monitoring Compliance with the START Treaty," 7.

[129] James Fuller, "Verification on the Road to Zero: Issues for Nuclear Warhead Dismantlement," *Arms Control Association*, December 5, 2010, https://www.armscontrol.org/act/2010_12/%20Fuller.

At these levels, states will also want to have more certainty about the irreversibility of reductions, which requires close monitoring of warheads in their elimination process. During the START II negotiations, one of the concerns was that warheads removed from missiles and bombers could simply be replaced with those remaining in storage, if relations between the states became hostile.[130] Future treaties, especially those also addressing warheads in storage, will need to be able to ensure the irreversibility of warhead elimination with a high degree of confidence.[131] One further complexity is that states may want to reuse delivery vehicles for conventional weapons, which highlights the significance of the irreversibility of the elimination of nuclear warheads, rather than delivery systems'.[132]

Second, NTM verification will be unable to provide a sufficient level of confidence in compliance under future disarmament agreements. The verification provisions in the New START agreement already reduced reliance on NTM, particularly telemetry information.[133] Telemetry was no longer used as a basis for warhead calculations, as the treaty provisions involved actual accounting for warheads and verifying them through on-site inspections.[134] New START still contained provisions for exchanging telemetry information on the basis of promoting openness and transparency.[135] In future disarmament efforts, the role of NTM will shift further and continue losing its informational significance. First, states other than the United States and Russia have very divergent capabilities and

---

[130] Steve Fetter, "A Comprehensive Transparency Regime for Warheads and Fissile Materials," *Arms Control Association*, January 1, 1999, https://www.armscontrol.org/act/1999_01-02/sfjf99.

[131] Ibid.

[132] "Security Dialogue Discussions, Moscow, Russia, December 15, 2008," January 14, 2009. https://search.wikileaks.org/plusd/cables/09MOSCOW68_a.html.

[133] Union of Concerned Scientists, "Verification of New START."

[134] Ibid.

[135] U.S. Department of State, Bureau of Verification, Compliance, and Implementation. "Fact Sheet: Telemetry," April 8, 2010, http://www.state.gov/t/avc/rls/139904.htm.

U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "New START: Article-by-Article Analysis Telemetry Annex," http://www.acq.osd.mil/tc/treaties/NST/Art%20By%20Art/art_telemetry_annex.htm.

resources in NTM, from availability of collection capabilities, to ability to analyze the data effectively. States with inferior capabilities would be highly opposed to agreeing on a verification approach that would rely significantly on NTM, as they would not be sufficiently confident in their abilities to do this. They would also be reluctant to leave the monitoring responsibilities to other states, without independent means of assessing compliance. On the other hand, states with superior NTM capabilities would be reluctant to share the collected information, if it compromised sensitive knowledge about their collection capabilities and analysis methods.[136] In future multilateral treaties, cooperative verification measures must be able to provide sufficient confidence for all treaty partners independent of states' ability to confirm these compliance assessments with NTM.

ii. Multilateral Verification

The bilateral U.S.-Soviet, or U.S.-Russia, disarmament agreements and their verification provisions established the traditional paradigm for verification in nuclear arms control. Outside of this context, there are only a handful of examples of stringent verification protocols being applied to arms control and disarmament. The international community's experiences are mainly limited to verifying the dismantlement of nuclear programs in Iraq, South Africa, and Libya. Thus, the multilateralization of disarmament beyond the U.S.-Russia context will also involve an important debate about what international authority will carry out the verification mission. The following discussion on the three cases highlights some of the challenges that multilateral verification has encountered in the past, demonstrating challenges that can be expected to be encountered in some shape or form in future cases of disarmament. Importantly, they reflect cases in which states have completely disarmed or

[136] Jeffrey Riechelson, "Iraq and Weapons of Mass Destruction," *National Security Archive Electronic Briefing Book No. 80*, http://nsarchive.gwu.edu/NSAEBB/NSAEBB80/.

dismantled their nascent nuclear weapons programs, but as was discussed at the beginning of this chapter, the dynamics will be different in important ways if states disarm progressively.

The International Atomic Energy Agency (IAEA) is the key international institution involved in nuclear verification, mainly through its civilian safeguards implementation under the NPT, but also through other efforts relating to nuclear safety and security. Information management under IAEA safeguards provisions is very strict, as a majority of the information about a specific state's civilian nuclear materials and facilities is confidential between the state and the IAEA.[137] The few selected instances where the IAEA has been involved in military-related verification missions, however, illustrate how the agency's current capabilities are not set up for sensitive military environments.[138] In addition to significant concerns that states have about allowing access to some of their most critical national security capabilities and facilities, verification in the military context has additional confidentiality requirements mandated by Article I in the NTP. Under the article's provisions, nuclear weapons states are obligated "not to transfer nuclear weapons or other nuclear explosive devices to any recipient or in any way assist, encourage or induce any non-nuclear-weapon state in the manufacture or acquisition of a nuclear weapon."[139] Allowing inspectors from non-nuclear weapons states to analyze weapons design information during the verification mission, for example, could be interpreted as a breach to this obligation, as it also extends to sharing proliferation-sensitive information with multilateral entities.[140]

---

[137] VERTIC, "Confidentiality and Verification: the IAEA and OPCW," *Trust & Verify*, No. 114, May-June 2004, http://www.vertic.org/media/assets/TV114.pdf.

[138] Thomas Shea, "The Trilateral Initiative: A Model for The Future?" *Arms Control Association*, June 11, 2008, https://www.armscontrol.org/act/2008_05/PersboShea.asp%23Sidebar1.

Thomas Shea and Laura Rockwood, "IAEA Verification of Fissile Material in Support of Nuclear Disarmament," *Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School,* May 2015.

[139] U.S. Department of State, U.S. Delegation to the 2010 Nuclear Nonproliferation Treaty Review Conference, "Treaty on the Non-Proliferation of Nuclear Weapons," 4, http://www.state.gov/documents/organization/141503.pdf.

[140] Shea, "The Trilateral Initiative: A Model for The Future?"

iii. The Case of Iraq

The first important case of international disarmament verification took place in Iraq, in the aftermath of the First Gulf War, when Iraq accepted an international inspection and monitoring regime to verify the dismantlement of its WMD program.[141] The United Nations Special Commission on Iraq (UNSCOM) was established in 1991 to implement the verification mission, which continued until 1998, when Iraq ended its cooperation with the program.[142] In 2002, inspections resumed under the auspices of the U.N. Monitoring, Verification, and Inspection Commission (UNMOVIC), which contained even more stringent verification protocols.[143] In both cases, the International Atomic Energy Agency (IAEA) partnered with the mission in the verification of Iraq's nuclear activities.[144] In the first mission, the IAEA Nuclear Monitoring Group (NMG) executed extensive monitoring inspections to Iraqi weapons facilities, resulting in the handover and removal of different equipment related to nuclear weapons development.[145] Joint IAEA/UNSCOM teams also conducted inspections at "capable" sites, including analysis of documents and procurement information.[146] In addition to on-site inspections, the group also used interviews, environmental sampling, and aerial radiometric surveys as a means of collecting information about the country's nuclear activities and adopted new instruments as the mission continued. [147]

---

[141] Riechelson, "Iraq and Weapons of Mass Destruction."

[142] Ibid.

[143] Ibid.

[144] Ibid.

[145] United Nations Security Council. "Note by the Secretary-General," 4, October 8, 1997. http://nsarchive.gwu.edu/NSAEBB/NSAEBB80/wmd07.pdf.

[146] Ibid.

[147] Ibid.

One of NMG's responsibilities was confirming the declarations related to the destruction of Iraq's clandestine nuclear weapons program.[148] In the first phase, the NMG inspected three sites with sub-surface sensing technologies, "provided and implemented by a supporting member State," which confirmed the identity and location of buried metallic items.[149] In the second phase, the inspection mission was expanded to nine other sites. The information obtained in these inspections was compared against Iraq's "Full, Final and Complete Declaration" and its revisions, which the state had made to the IAEA.[150] These declarations included detailed information about equipment, production practices, and other dimensions of Iraq's clandestine nuclear activities.[151] The IAEA, however, found the information insufficient and repeatedly negotiated with Iraq regarding more conclusive documentation about the ultimate capability achievements and foreign assistance involved in the nuclear weapons program.[152] The IAEA gained documentation about Iraq's research and development of weaponization capabilities for implosion-type nuclear weapons, but as a result of Iraq's attempts to conceal and understate different aspects of the program, as well as interfere with the agreed IAEA access, it remained unclear on how far the weapons designs proceeded.[153] The documentation collected included highly proliferation-sensitive information about the structure of the weapons, the high explosives experiments, and many other aspects of the program's technical aspects.[154] The discovered weapons development and production facilities and equipment were destroyed, removed, or converted in the mission.[155] Ultimately, the IAEA/UNSCOM mission ended with no significant

[148] Ibid.

[149] Ibid., 5.

[150] Ibid.

[151] Ibid., 6.

[152] Ibid.

[153] Ibid., 19.

[154] William Broad, "Web Archive Is Said to Reveal a Nuclear Primer," *New York Times*, November 3, 2006. http://www.nytimes.com/2006/11/03/world/middleeast/03cnd-documents.html.

[155] United Nations Security Council. "Note by the Secretary-General," 19.

discrepancies between the IAEA's technical assessment and Iraq's updated declarations, but also with no certainty about the absence of undeclared activities: "Some uncertainty is inevitable in any country-wide technical verification process which aims to prove the absence of readily concealable objects or activities. The extent to which such uncertainty is acceptable is a policy judgment."[156]

Both the inspections and declaration analysis allowed access to information that was highly classified and proliferation-sensitive, which was a significant concern for all sides involved. One critical question was the specific knowledge and background that inspectors would need to have to understand weapons production processes, particularly in dual-use facilities.[157] In addition, the IAEA was very concerned about unauthorized access to proliferation-sensitive information, which would be a violation of Article I under the NTP.[158] The details of the inspection procedures are not public, but it seems that the IAEA only allowed inspectors from nuclear weapons states to be involved in the most sensitive parts of the verification mission. The nationality of the inspectors, however, became a barrier for other reasons as well. At the initial stages of the UNSCOM mission in 1992, Iraq maintained that no British, French, or U.S. weapons inspectors would be permitted to conduct segments of the verification mission, related to its ballistic missile program.[159] This led to serious confrontations between Iraq and the different UN Security Council members and concerns about setting a precedent related to manipulating the composition of international inspection teams.[160] Debate about weapons inspectors and their access continued until the end of the UNSCOM mission. In 1997, Iraq refused to cooperate with U.S. inspectors and asked them to leave the country, fully blocking inspections that

---

[156] Ibid., 20.

[157] Sharon Squassoni, "Iraq: U.N. Inspections for Weapons of Mass Destruction," *Report for Congress*, March 28, 2003, 8, http://fpc.state.gov/documents/organization/19436.pdf.

[158] U.S. Department of State, U.S. Delegation to the 2010 Nuclear Nonproliferation Treaty Review Conference. "Treaty on the Non-Proliferation of Nuclear Weapons." http://www.state.gov/documents/organization/141503.pdf.

[159] Arms Control Association, "Iraq: A Chronology of UN Inspections," October 1, 2002, https://www.armscontrol.org/act/2002_10/iraqspecialoct02.

[160] Ibid.

involve U.S. inspectors.[161] As a response, the IAEA withdrew most of the inspections teams, which were only allowed to return after UN Security Council action and Russian-facilitated negotiations re-established inspections.[162] Iraq's dissatisfaction with the presence of U.S. and British inspectors continued, along with claims that weapons inspectors were collecting intelligence for individual national objectives, such as airstrike targeting information.[163] Overall, both the sensitive information collected through the mission and the intelligence distributed between the participant states and the IAEA/UNSCOM mission remained a difficult challenge.[164] These questions related to handling classified and proliferation-sensitive information re-emerged in 2006, when certain conservative groups in the United States Congress pressured the release of the documents collected by the IAEA weapons inspectors.[165]

iv. The Case of South Africa

South Africa, which maintained an active nuclear program in the 1970s and 80s, is another important case study in past multilateral verification approaches.[166] The program was made public in March 1993, after South Africa had already dismantled the program, signed on to the NPT, and concluded a comprehensive safeguards agreement (CSA) with the IAEA in 1991.[167] The existence of

---

[161] Ibid.

[162] Ibid.

[163] Ibid.

Squassoni, "Iraq: U.N. Inspections for Weapons of Mass Destruction," 9.

[164] Squassoni, "Iraq: U.N. Inspections for Weapons of Mass Destruction," 9.

[165] Broad, "Web Archive Is Said to Reveal a Nuclear Primer."

[166] The program was centered at three facilities in the country - in Pelindaba, the Kentron Circle Facility, and Somchem - and also included testing areas and other locations that were necessary for the nuclear program. (Source: Olli Heinonen, "Verifying the Dismantlement of South Africa's Nuclear Weapons Program," Appendix, 8, http://belfercenter.ksg.harvard.edu/files/Verifying%20the%20Dismantlement%20-%20Heinonen%20Chapter%208.pdf.

[167] Institute for Science and International Security, "Chapter 10: International Verification," 4, available at http://isis-online.org/uploads/isis-reports/documents/Chapter_10_International_Verification_Mechanisms_april_1_2016.pdf.

Heinonen, "Verifying the Dismantlement of South Africa's Nuclear Weapons Program," 1.

the nuclear weapons program, however, had been known among other states for some time.[168] This case constitutes *ex post facto* verification, as the international verification mission was established after the country has already dismantled the facilities and equipment associated with the nuclear weapons program. In Iraq, the IAEA team was involved in this destruction and dismantlement program as well, in addition to carrying out similar "after the fact" analysis activities as in South Africa. The Iraq verification mission influenced the South African case in important ways, as it had revealed significant insufficiencies in IAEA's detection capabilities of covert activities.[169] Thus, verification in South Africa was highly intrusive, intended not only to assess the correctness of the state's declarations, but also their completeness.[170] The verification mission also relied more on member states' intelligence capabilities, alongside IAEA's own verification capabilities.[171]

Verifying South Africa's compliance with its new NPT and CSA obligations, including the completeness of its initial declarations, was requested through resolutions at the IAEA General Conference and at the United Nations General Assembly.[172] A team of senior members at the Department of Safeguards at the IAEA carried out this request. In consultation with the Atomic Energy Corporation of South Africa (AEC), they agreed to receive the historical operating and accounting records of South African nuclear facilities and were allowed to choose a specified number to be audited through on-site inspections.[173] South African officials co-operated with the IAEA

---

[168] Institute for Science and International Security, "Chapter 10: International Verification," 4, available at http://isis-online.org/uploads/isis-reports/documents/Chapter_10_International_Verification_Mechanisms_april_1_2016.pdf.

Heinonen, "Verifying the Dismantlement of South Africa's Nuclear Weapons Program," 1.

[169] Ibid., 3.

[170] Ibid.

[171] Ibid.

[172] IAEA General Conference, 36th Regular Session, "South Africa's Nuclear Capabilities," (GC(XXXV)/RES/567), https://www.iaea.org/About/Policy/GC/GC36/GC36Documents/English/gc36-1015_en.pdf.

United Nations General Assembly, 65th Plenary Meeting, "Implementation of the Declaration on the Denuclearization of Africa: Nuclear capability of South Africa," (A/RES/46/34A), http://www.un.org/documents/ga/res/46/a46r034.htm.

[173] IAEA General Conference, 36th Regular Session, "South Africa's Nuclear Capabilities."

requirements extensively and allowed a high level of access to nuclear facilities based on IAEA requests, building confidence in the state's commitment to abandon its nuclear ambitions.

In the initial declarations and the first IAEA verification reports after the CSA agreements, the only reference to potential non-peaceful uses were the detection of discrepancies in ^{235}U isotope balances in the country's enrichment plants.[174] This conclusion emerged from the calculations that IAEA officials made on the basis of data provided by the AEC.[175] In subsequent reports, these discrepancies in HEU production were examined through further analyzing operating records and supporting technical data provided by AEC.[176]

The IAEA officials were also assigned with assessing the status of South Africa's former nuclear weapons program after its existence was declared in 1993.[177] The objective was to ensure that all materials used in weapons were permanently transferred to peaceful uses, non-nuclear weapons components were destroyed, all facilities had been fully decommissioned or converted to peaceful uses, and weapons-related equipment had been destroyed or converted.[178] Furthermore, the objective was to understand how the dismantling program had been carried out, how the information relating to design and manufacturing of nuclear weapons had been destroyed, and how the dismantling process was carried out.[179] Other assignments included obtaining information about the timing and scope of the nuclear weapons program, decommissioning the Kalahari Desert testing site, visiting the

[174] IAEA General Conference, 37th Regular Session, "The Denuclearization of Africa," (GC(XXXVII)/1075), https://www.iaea.org/About/Policy/GC/GC37/GC37Documents/English/gc37-1075_en.pdf.

[175] Ibid.

[176] Ibid.

[177] Ibid.

[178] Ibid.

[179] Ibid.

decommissioned or abandoned nuclear weapons facilities, and consulting with the South African government to ensure that the nuclear weapons program could not be regenerated.[180]

Similar concerns about sensitive information emerged in South Africa as in the Iraq verification mission. The inspection team involved IAEA Department of Safeguards experts, who were also accompanied by external nuclear weapons experts.[181] This augmentation of the traditional IAEA team, consisting of safeguards experts, was required because the verification mission would involve assessing documents regarding the design and manufacturing of the country's seven gun-assembled nuclear devices.[182] Similar to the Iraq case, these nuclear weapons experts were mostly only from nuclear weapons states, ensuring that no sensitive or unauthorized information would be distributed to non-nuclear weapons states.[183] Their status and expertise allowed them to engage with South African nuclear scientists and officials in a different way that safeguards experts could, increasing access to information about the nation's nuclear weapons program.[184] They also had the necessary expertise to be able to recognize activities specific to nuclear arms research and development efforts during facility inspections.[185]

---

[180] Ibid.

[181] United States Congress, Office of Technology Assessment, *Nuclear Safeguards and the International Atomic Energy Agency* (Washington, DC: U.S. Government Printing Office, 1995), 95, available at https://www.princeton.edu/~ota/disk1/1995/9530/9530.PDF.

[182] Adolf von Baeckmann, Garry Dillon, and Demetrius Perricos, "Nuclear Verification in South Africa," *IAEA Bulletin 1/1995: National Reports*, 42, available at https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull37-1/37105394248.pdf.

[183] VERTIC, "Confidentiality and Verification: the IAEA and OPCW."

Institute for Science and International Security, "Chapter 10: International Verification," 11.

[184] Institute for Science and International Security, "Chapter 10: International Verification," 11.

[185] Ibid.

v. The Case of Libya

A third important case of international verification of nuclear weapons programs took place in Libya, after the state announced the elimination of its weapons-purpose materials, equipment, and facilities in 2003 and singed the Additional Protocol to the NPT the following year.[186] The international verification mission, negotiated between Libyan, American, and British officials, intended to establish the details of the program and its history, as well as understand the origins of the materials and design information.[187] British and American weapons experts continued to play a key role in the verification mission, assisting Libya in destroying nuclear weapons design documents, materials, and equipment and interviewing relevant officials and experts in the country.[188] Again, as in the case of Iraq and South Africa, the nationality of the inspectors was important. The Libyans had initially turned to the British, and the negotiations over dismantling the nuclear weapons program took place between Libya, the United Kingdom, and the United States.[189] At first, in October 2003, trusted access was only provided to inspectors from these two foreign countries.[190] Starting in December 2003, IAEA inspectors were also invited to participate in the verification mission.[191]

Management of proliferation-sensitive information was an important aspect of the verification mission. Libya had reportedly acquired drawings of a weapon design through the A.Q. Khan network,

---

[186] International Atomic Energy Agency, "IAEA Verification of Libya's Nuclear Programme," March 10, 2004, https://www.iaea.org/newscenter/news/iaea-verification-libyas-nuclear-programme.

VERTIC, "Verifying Libya's Nuclear Disarmament," *Trust & Verify* No. 112, January-February 2004, http://www.vertic.org/media/assets/TV112.pdf.

[187] International Atomic Energy Agency, "IAEA Verification of Libya's Nuclear Programme."

[188] Paula DeSutter, "Completion of Verification Work in Libya," *United States Department of State*, September 22, 2004, https://2001-2009.state.gov/t/vci/rls/rm/2004/37220.htm.

[189] Sharon Squassoni, *Disarming Libya: Weapons of Mass Destruction* (Washington D.C.: Library of Congress, Congressional Research Service, 2006), 3.

[190] Ibid.

[191] Ibid., 4.

and in December 2004, these materials were sealed on-site by the IAEA.[192] In the following January, the documents, ccomponents, and equipment that the inspectors discovered were transported to the United States under strict rules, including the IAEA seals.[193] Other measures, such as the conversion of Libya's research reactor, also took place under the multilateral verification mission.

As these experiences in Iraq, South Africa, and Libya demonstrate, the integrity and confidentiality of information about the nuclear weapons programs was a critical concern in the international verification missions. These three cases are unique, however, in that the international verification missions went well beyond the IAEA safeguards principle of collecting the minimum amount of information needed for the agency to fulfill its mandated verification obligations.[194] The discovery of covert, highly developed nuclear weapons programs had shocked the IAEA and the international community, which motivated the extreme intrusiveness that would ensure that all prohibited activities would be identified and assessed. This was enabled by the fact that the states had decided, or were pressured, to fully eliminate their nuclear programs, which made the host countries significantly more open regarding their nuclear weapons programs. Furthermore, none of the cases involved handling or dismantling fully operational warheads – South Africa had already eliminated the state's nuclear weapons stockpile prior to the verification mission, and neither Iraq or Libya had produced fully operational warheads. These factors made the intrusive access both legitimate for the IAEA to implement and possible for the host states to accept.

[192] Ibid., 3.

[193] VERTIC, "Confidentiality and Verification: the IAEA and OPCW."

[194] Ibid.

3. Past Multilateral Verification Systems Protecting Classified Information

I. Introduction

In the future, multilateral verification is likely to take place in a context where nuclear-armed states engage in gradual weapons reductions, which places different pressures to the accompanying verification mission than verifying the full dismantlement of a nuclear weapons program. The intent would be to maintain strategic stability throughout the multilateral reduction effort, ensuring that each state can sustain their deterrent capability while reducing the number of warheads. So long as states maintain some components of their nuclear weapons programs active, they will need to maintain a much higher level of confidentiality and secrecy about warhead designs, materials, and facilities. This would allow much less direct access for inspectors and mandates the use of verification technologies that do not reveal sensitive information. With multilateral, progressive warhead reductions, states will be able to insist upon limited intrusiveness, managed access, and the highest standards of information integrity, which was not the case with Iraq, South Africa, and Libya, which were under intense international pressure to allow full access to the verification mission.

This chapter explores the efforts that have been made in the past decades to counter the assumption that high-accuracy verification of warheads would not be possible without compromising classified information. The focus is on different verification systems that would be able to handle classified forms of fissile materials, with the intention to develop a system that would allow the accurate authentication of warheads without revealing sensitive information. It explores the Trilateral Initiative, which created an attribute verification system (AVNG) in a collaborative effort between the United States, Russia, and the IAEA; unilateral efforts in the United Kingdom and bilateral efforts through the U.K.-Norway Initiative to develop an attribute system on very similar principles; and

unilateral efforts in national laboratories. The chapter also discusses a more recent multilateral initiative, the International Partnership for Nuclear Disarmament Verification, that also has a technical working group focused on the technical challenges related to multilateral disarmament. In all of these efforts, the chapter illustrates how the authentication and certification of the technical equipment remains as the prevailing issue and how challenges in multilateral verification are concentrated on information integrity and transparency.

II. The Trilateral Initiative

One of the pioneering efforts to create mechanisms for this context was the Trilateral Initiative, a collaboration between the United States, Russia, and the IAEA between 1996 and 2002 to solve the challenge of sensitive information and conceptualize mechanisms that would allow classified forms of fissile material contained in their pits and secondaries within a warhead to be handled by the IAEA.[195] The considerations were limited to weapons-usable fissile material, although the parties also considered addressing warheads their components, or entire weapons systems.[196] These levels were seen too complicated, however, due to security issues. Even addressing weapons-origin materials was unprecedented, so this was defined as the initiative's goal.

In essence, the verification of a warhead would only be a more complex case of verifying fissile material, as it is what makes a weapon nuclear and most approaches of identifying a warhead focus on

[195] Shea and Rockwood, "IAEA Verification of Fissile Material in Support of Nuclear Disarmament," 5.

Shea, "The Trilateral Initiative: A Model for The Future?"

Thomas Shea, "The Trilateral Initiative: IAEA Verification of Weapon-Origin Plutonium in the Russian Federation and the United States," *International Atomic Energy Agency Safeguards Symposium*, October 2014, https://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000334.pdf.

[196] Shea, "The Trilateral Initiative: A Model for The Future?"

the attributes of the material contained in the warhead.[197] This had been explored some years prior to the establishment of the Trilateral Initiative, through a joint U.S.-Russia study called the Black Sea Experiments in 1989, which was a one-of-a-kind instance where foreign nuclear scientists have made radiological measurements of an operational warhead without any attempts to cover the classified information.[198] The experiment was done in the context of the START negotiations and intended to understand if and how submarine-launched cruise missiles could be verified and what information would be revealed in the process.[199] The study concluded that while the gamma measurement system used by the U.S. scientists revealed detailed information about the nuclear material contained in the warhead, it did not allow them to identify sensitive design information or warhead yield.[200] Parallel longer-distance measurements conducted by Russian scientists revealed that their remote detection methods could identify the warhead as a neutron source, but not provide more detailed information about its type.[201] This highlighted the importance of on-site inspections and close access to warheads in the verification process to obtain a high level of confidence.

[197] Committee on International Security and Arms Control, National Research Council, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities* (Washington D.C.: National Academies Press, 2005), 45.

[198] Cliff, Elbahtimy and Persbo, "Verifying Warhead Dismantlement: Past, Present, Future," 36.

[199] Ibid., 38.

[200] Ibid.

[201] Ibid.

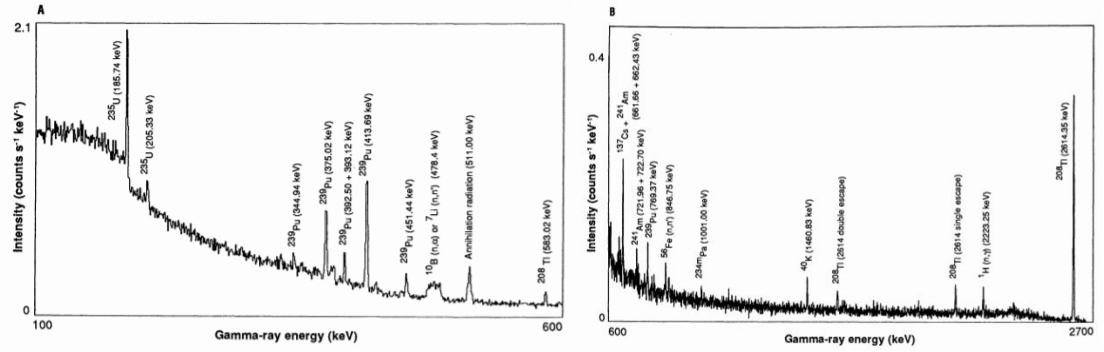

Fig. 2. (**A**) Gamma-ray spectrum from 100 to 600 keV; (**B**) gamma-ray spectrum from 600 to 2700 keV. [Adapted from (*29*)]

Figure 3.1. The radiographic signature obtained in the Black Sea experiment. Source: Steve Fetter et al., "Gamma-Ray Measurements of a Soviet Cruise-Missile Warhead," *Science* 248 (1990), 248.

The objective of the Trilateral Initiative was to develop an on-site verification framework that would protect classified and sensitive information while still providing the highest level of confidence in the disarmament process for the treaty partner and the inspecting agency.[202] These two considerations are referred as certification, or the process carried out by the host state of ensuring that no classified information is released, and authentication, where the inspecting agency assures the validity of the measurements.[203] This would ensure political acceptability for all the involved parties, but also enable the technical intrusiveness required by the treaty verification objectives.[204] The analysis of potential measurement technologies made it evident that unrestricted measurements would be unacceptable, as they would reveal highly sensitive information about the items or materials.[205] This could risk undermining U.S. and Russian obligations under Article I of the NPT, as the IAEA

[202] Shea, "The Trilateral Initiative: A Model for The Future?"

[203] Eckhard Haas, Alexander Sukhanov, and John Murphy, "Trilateral Initiative: IAEA Authentication and National Certification of Verification Equipment for Facilities with Classified Forms of Fissile Material," *Symposium on International Safeguards: Verification and Nuclear Material Security, 2001, Proceedings*, http://www-pub.iaea.org/MTCD/publications/PDF/ss-2001/PDF%20files/Session%2017/Paper%2017-04.pdf.

[204] Shea, "The Trilateral Initiative: A Model for The Future?"

[205] Ibid.

inspectors could gain access to sensitive design or production information relating to the states' nuclear programs.[206]

Balancing the protection of information and allowing the IAEA access led to the exploration attribute verification protocols combined with information barriers. Attribute verification refers to the use of certain characteristics, "attributes," against which the object or material under consideration is compared to.[207] The measurement system, AVNG, consisted of high-resolution gamma ray spectroscopy and neutron multiplicity counting, which would establish the presence of plutonium, the ratio of ^{239}Pu and ^{240}Pu, and the mass of ^{240}Pu.[208] The measurements data to determine these three attributes, however, would not be accessible to the inspector, as it would be considered classified by the host state. Instead, the system utilizes information barriers, which are hardware or software components and methods that divide the measurement information into a classified data layer and an unclassified display layer.[209] The inspector only interacts with the user interface, which only displays the unclassified result.[210] Prior to the system's implementation, however, it is fully open for inspection for all the involved parties, enabling them to verify the system's operability.[211] While the data collected by the system is classified, all the algorithms utilized by the system are fully known by all parties involved.[212]

---

[206] Shea, "The Trilateral Initiative: IAEA Verification of Weapon-Origin Plutonium in the Russian Federation and the United States."

[207] Shea, "The Trilateral Initiative: A Model for The Future?"

[208] Shea and Rockwood, "IAEA Verification of Fissile Material in Support of Nuclear Disarmament," 7.

[209] D.W. MacArthur and R. Whiteson, "Information Barriers in the Trilateral Initiative: Conceptual Description," *Los Alamos National Laboratory*, 1998, https://www.nti.org/media/pdfs/Whiteson_MacArthur_1998_IBs_in_the_Trilateral_Initiative_-_Conceptual_Design.pdf?_=1439480184.

[210] MacArthur and Whiteson, "Information Barriers in the Trilateral Initiative: Conceptual Description."

[211] Ibid.

[212] J.L. Fuller and J.K. Wolford, "Information Barriers," *Symposium on International Safeguards: Verification and Nuclear Material Security, 2001, Proceedings*, http://www-pub.iaea.org/MTCD/publications/PDF/ss-2001/PDF%20files/Session%2017/Paper%2017-01.pdf.

The challenge with information barriers is that the classified side of the system requires multiple layers of protection, from tamper indicators to hardware to complex administrative controls.[213] The complexity of this becomes apparent particularly when the system is under maintenance.[214] The system developed in the Trilateral Initiative was irreversible – once some parts of the system have become classified and measure sensitive information, these segments will remain classified even if the system is cleared of any sensitive material.[215] Later system development led to a model of the AVNG that could shift between open mode, meant for measurements of unclassified material, and a secure mode, which would be used for classified materials.[216]

A proof-of-principle system of the AVNG was demonstrated under the Trilateral Initiative.[217] In addition to the system itself, the initiative also created associated systems relating to containment and surveillance, which would be critical for future warhead verification processes.[218] These would enable the continuity of knowledge of the materials under verification, which were intended to minimize the complexities involved in reverifying the warhead at a later point of the process.[219] The AVNG system development continued after the end of the Trilateral Initiative in collaboration with the United States and Russia, resulting in a fully operational system.[220] In 2009, the system was demonstrated at Russia's Institute of Nuclear & Radiation Research, All-Russian Scientific Research

[213] MacArthur and Whiteson, "Information Barriers in the Trilateral Initiative: Conceptual Description."

[214] Ibid.

[215] Ibid.

[216] Sergey Kondratov et al., "AVNG System Demonstration," *Proceedings of the 51st Annual Meeting of the Institute of Nuclear Material Management,* http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-10-02620.

[217] Shea, "The Trilateral Initiative: IAEA Verification of Weapon-Origin Plutonium in the Russian Federation and the United States."

[218] Ibid.

[219] Ibid.

[220] Kondratov et al., "AVNG System Demonstration."

Institute of Experimental Physics (RFNC-VNIIEF) in the presence of American scientists and officials.[221]

The Trilateral Initiative also involved external partners in limited capacities, allowing their expertise in safeguards and other verification activities to be integrated to the initiative. The United Kingdom hosted a technical workshop related to the state's PuO_2 verification system and plutonium storage system under Euratom safeguards.[222] Japan held a workshop related to the state's modern verification protocols applied to plutonium storage and mixed oxide fuel production.[223] Italy also participated by hosting technical workshop at the Joint Research Centre of the European Commission related to ensuring system certification and authentication.[224] This international collaboration indicated expectations about the shape of things to come – future disarmament would eventually expand to states outside the U.S.-Russia context.

Ultimately, the greatest challenge encountered under the Trilateral Initiative collaboration was the authentication of the verification system.[225] The critical questions related to the manufacturing of the system and its components and the subsequent authentication that would be required.[226] The first logical option would be that the IAEA, or other international verification body, would produce the measurement equipment and allow the host state to authenticate its legitimate operability.[227] In the Trilateral Initiative, it became evident that this would pose challenges. Russian security officials indicated their requirement to use intrusive and unidentified methods to inspect the equipment for up

[221] Ibid.

[222] Shea, "The Trilateral Initiative: IAEA Verification of Weapon-Origin Plutonium in the Russian Federation and the United States."

[223] Ibid.

[224] Ibid.

[225] Ibid.

[226] Ibid.

[227] Ibid.

to 18 months, with the authority to deny the equipment without providing their rationale.[228] If the system was accepted, on the other hand, the IAEA would need to repeat this authentication procedure for ensuring that the system was intact.[229] This would lead to a long cycle of authentication and re-authentication, without certainty for either side of system integrity and validity.[230]

The second option, which the Trilateral Initiative ultimately adopted, would be for the host state to manufacture the equipment.[231] This is referred to as the host-supply principle, according to which the party whose classified information is at risk has the right to supply the equipment and also the right to be the last party with access to the equipment in the authentication process.[232] The three parties would jointly develop the detailed design of the system, the computer processors used, as well as test it together.[233] The actual equipment would be produced within the state where it would be used, with monitoring from the other two partners.[234]

While doing critical technical work for multilateral disarmament relating to classified forms of nuclear material, the Trilateral Initiative left several important issues unaddressed. The AVNG system focused on verifying plutonium, but developing a parallel system for highly enriched uranium could pose unique challenges. Furthermore, in future disarmament steps this material could still be contained within warheads when the IAEA begins the verification mission. The verification mission would expand the whole dismantlement cycle, from demounting deployed warheads from their delivery vehicles and uniquely identifying them, to monitoring their transportation and storage and ultimately

[228] Shea and Rockwood, "IAEA Verification of Fissile Material in Support of Nuclear Disarmament," 10.

[229] Ibid.

[230] Ibid.

[231] Ibid.

[232] Fuller and Wolford, "Information Barriers."

[233] Shea and Rockwood, "IAEA Verification of Fissile Material in Support of Nuclear Disarmament," 10.

[234] Ibid.

their dismantlement process.[235] In addition to IAEA involvement in this process, non-nuclear weapons states may also become important agents in multilateral verification. The Trilateral Initiative's engagement demonstrated that expertise relating to safeguards and other dimensions of the civilian nuclear sector can also be applied to verification in the military sphere. Furthermore, non-nuclear weapons states would also want to gain confidence in the irreversibility and validity of the disarmament process and would likely be interested in gaining understanding of the process. In preparation for future nuclear disarmament, extensive multilateral engagement especially in the technical research and development process would be highly beneficial. This would contribute to multilateral disarmament prospects by pushing the technical solutions forward, but also by creating a common language between the states involved and building the foundations of trust and confidence in the international community.

III. U.K. Efforts and the U.K-Norway Initiative

The Trilateral Initiative was an important stepping stone for multilateral engagement in verifying classified nuclear materials and items and highlighted the importance of future work in this field. The idea of involving non-nuclear states in the disarmament process has been explored in multiple dimensions since the end of the initiative. The legitimacy of the global disarmament effort requires that all sides are knowledgeable of the process – not only nuclear weapons states engaged in it. The 2005 NPT Review Conference introduced several working papers from non-nuclear weapons states related to the disarmament process, including enhancing disarmament and non-proliferation education and developing multilateral verification mechanisms, independent of national technical

[235] Ibid., 12.

means.[236] Particularly important was the final report on a set of studies undertaken by the United Kingdom since 1998, focused on the verification of nuclear warheads and their components.[237] This research was initiated after the 1998 U.K. Strategic Defence Review, which stated that the U.K. is willing to engage in future multilateral nuclear disarmament efforts, on the condition that the process is multilaterally verified.[238] The goals of the project were to explore multilateral verification mechanisms of authenticating warheads and their components, dismantling these items securely, disposing the resulting fissile material irreversibly, and monitoring the overall nuclear weapons complex.[239]

The United Kingdom provided the first interim report of the initiative in 2003 to the Preparatory Committee for the 2005 Review Conference, focused on the first objective of warhead authentication. The focus on the initiative had been on radiometric non-destructive assay (NDA)

---

[236] 2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Working paper on disarmament and non-proliferation education Submitted by Egypt, Hungary, Japan, Mexico, New Zealand, Peru, Poland and Sweden," (NPT/CONF.2005/WP.30), http://www.mofa.go.jp/policy/un/fmv0504/npt4.pdf.

2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Nuclear Disarmament: Working paper submitted by Canada," (NPT/CONF.2005/WP.38).

2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Nuclear disarmament and reduction of the danger of nuclear war: Working paper submitted by China," (NPT/CONF.2005/WP.2).

2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Transparency, verification and irreversibility: essential principles in the process of nuclear disarmament: Working paper by the Republic of Cuba," (NPT/CONF.2005/WP.24).

2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Working paper on nuclear disarmament for Main Committee I: Recommendations submitted by New Zealand on behalf of Brazil, Egypt, Ireland, Mexico, South Africa and Sweden as members of the New Agenda Coalition," (NPT/CONF.2005/WP.27).

[237] Christine Comley *et al.,* "Confidence, Security and Verification: The challenge of global nuclear weapons arms control," *Atomic Weapons Establishment* (2000), http://fissilematerials.org/library/awe00.pdf.

2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Verification of nuclear disarmament: final report on studies into the verification of nuclear warheads and their components: Working paper submitted by the United Kingdom of Great Britain and Northern Ireland," (NPT/CONF.2005/WP.1), http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2005/wp/wp1.pdf, 1.

[238] National Nuclear Security Administration, "Joint U.S.-U.K. Report on Technical Cooperation for Arms Control," Defense Nuclear Nonproliferation, Office of Nonproliferation and Arms Control (2015), https://nnsa.energy.gov/sites/default/files/Joint_USUK_Report_FINAL.PDF, 4.

[239] 2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Verification of nuclear disarmament," 2.

measurement technologies, including passive gamma ray spectrometry, passive and active neutron coincidence counting, and neutron multiplicity, as well as demonstrated their implementation on real warheads and their nuclear components.[240] This work on passive radiation signatures was based on identifying the spontaneous neutron or gamma radiation emitted by the warhead's plutonium and uranium content, which would reveal the presence, distribution, quantity, and isotopic type and composition of the fissile material.[241] The active radiation signatures, on the other hand, relied on active gamma or X-ray irradiation of the low atomic number elements contained in the warheads, such as deuterium, tritium and beryllium.[242] In addition, the technical work also involved computer modelling.[243] These active and passive measurement systems and models were tested on decommissioned warheads (WE177 and Chevaline) and still deployed warheads (Trident), including their primary and secondary sub-assemblies and re-entry bodies, inside and outside different containers.[244]

The first interim report concluded that extensive knowledge about a warhead held in a container can be assessed through these radiation measurements, including type, components, geometrical shape, and internal characteristics.[245] Access to the raw measurement data would make it possible to reverse engineer the design and configuration of the warhead.[246] Thus, one of the key conclusions is that this proliferation-sensitive and classified information ought to be fully protected in

---

[240] Second Preparatory Committee for the 2005 NPT Review Conference, "Verification of nuclear disarmament: First interim report on studies into the verification of nuclear warheads and their components: Working paper submitted by the United Kingdom of Great Britain and Northern Ireland," (NPT/CONF.2005/PC II/WP.1). http://www.acronym.org.uk/old/archive/npt/03wp1.htm.

2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Verification of nuclear disarmament."

[241] Second Preparatory Committee for the 2005 NPT Review Conference, "Verification of nuclear disarmament."

[242] Ibid.

[243] Ibid.

[244] Ibid.

[245] Ibid.

[246] Ibid.

any verification scenario.[247] In addition, the interim report highlighted the importance of developing chain of custody, provenance, and managed access mechanisms in support of the authentication.[248]

The second interim report focused on the dismantlement of warheads, emphasizing that protecting design and security information is one of the most critical aspects of the process.[249] Furthermore, it will be important to develop continuity of knowledge mechanisms to prove that the end products of the dismantlement process came from the intended authenticated warhead.[250] To this end, a template verification system could be implemented with non-destructive analysis images of warheads, enabling the identification of the warhead and its type through time-correlated template comparison.[251] These radiation signature comparisons have been researched in the past, for example in the context of a technical study by the U.S. Department of Energy in 1996.[252] The second U.K. interim report also discussed a mock inspection that the project implemented, including the future importance of these activities and the challenges that remain unresolved.[253]

The final report focused on the management of the nuclear weapons complex, but also brought together the other dimensions of the project.[254] One key conclusion is that advancements in technical fields, such as neutron detection accuracy, can increase the information that is possible to collect in the verification process, but also that this must be balanced with proliferation and national

---

[247] Ibid.

[248] Ibid.

[249] Third Preparatory Committee for the 2005 NPT Review Conference, "Verification of nuclear disarmament: second interim report on studies into the verification of nuclear warheads and their components: Working paper submitted by the United Kingdom of Great Britain and Northern Ireland," (NPT/CONF.2005/PC.III/WP.3), http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/prepcom04/papers/wp3.pdf, 2.

[250] Ibid., 2.

[251] Ibid.

[252] Cliff, Elbahtimy and Persbo, "Verifying Warhead Dismantlement: Past, Present, Future," 47.

[253] Third Preparatory Committee for the 2000 NPT Review Conference, "Verification of nuclear disarmament."

[254] 2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Verification of nuclear disarmament."

security concerns.[255] The combination of different non-destructive assay methods, such as passive auto radiography, gold foil activation, and photo-neutron interrogation, was discussed as a potential mechanism to detect spoofing, but more work needs to be done on identifying the benefits and risks of the different measurement techniques.[256] In addition, information barriers were also researched as a way to protect classified and sensitive information.[257] Overall, the final report concluded authentication to be the most difficult task in disarmament verification, as the techniques would need to simultaneously protect sensitive and classified information, have a high confidence of detecting spoofing, and be otherwise fully secure.[258]

This work contributed to the United Kingdom's continued engagement in developing verification mechanisms for the future. The state began a joint effort with Norway in 2007, which was a first case of close collaboration between a nuclear and non-nuclear weapons state on warhead dismantlement.[259] The initiative also involved VERTIC, a UK-based non-governmental organization focused on verification, monitoring and confidence-building in international agreements.[260] The overarching theme of the U.K.-Norway Initiative was on understanding how non-nuclear weapons states could facilitate trust and confidence in multilateral nuclear disarmament and become involved in the process while not gaining access to proliferation-sensitive information.[261] In practice, it focused on continuing the efforts of the Trilateral Initiative on information barrier technology, as well as conceptualizing managed access methodologies through simulated exercises.[262] First, the initiative

[255] Ibid., 6.

[256] Ibid., 7.

[257] Ibid., 8.

[258] Ibid., 7.

[259] Cliff, Elbahtimy and Persbo, "Verifying Warhead Dismantlement: Past, Present, Future," 9.

[260] VERTIC, "About VERTIC," http://www.vertic.org/pages/homepage/about/about-vertic.php.

[261] Cliff, Elbahtimy and Persbo, "Verifying Warhead Dismantlement: Past, Present, Future," 67.

[262] Ibid., 15.

established that the limited information available about past experiments on information barriers could undermine the trust that non-nuclear weapons states could have on verification systems.[263] In order to facilitate the legitimacy of these instruments, non-nuclear weapons states should be involved in their development and demonstration efforts.[264] The Trilateral Initiative had concluded that the host country should be allowed to manufacture the verification equipment, such as the AVNG system, but the U.K.-Norway Initiative explored how non-nuclear weapons states could be involved, as a means of increasing transparency and trust in the process.[265]At the beginning, the initiative also surveyed the lessons learned from the previous studies carried out by the United Kingdom. One key insight was that the human side of verification has been largely neglected, both from the perspective of undermining the successful use of a verification technologies, but also from the viewpoint of promoting trust through non-technological means.[266] In addition, it was also concluded that a particular technical solution to verification increases in legitimacy based on several characteristics, including the ability to protect sensitive information, its simplicity, familiarity, and lower level of intrusiveness.[267]

The two technical aspects that the initiative focused on, information barriers and managed access, were considered complimentary and interconnected.[268] Managed access would allow inspectors to access sensitive warhead environments and conduct their verification measurements behind an information barrier, allowing proliferation-sensitive information to remain intact.[269]

---

[263] Ibid., 65.

[264] Ibid.

[265] Ibid.

[266] Ibid., 66.

[267] Ibid.

[268] Ibid., 68.

[269] Ibid.

The initiative addressed the initialization problem, which refers to the challenge of authenticating a warhead to be real at the beginning of its dismantlement process.[270] Particularly, the focus was on the involvement of inspectors from non-nuclear weapons states in the process, which would make information integrity even more important, as any breach would violate Article I of the NPT.[271] Two proof-of-concept information barriers were built, one in the United Kingdom and one in Norway, such that strict non-proliferation concerns were addressed and that the involved non-nuclear weapon state would gain confidence through its direct involvement in the design and manufacturing process of the system.[272] As the focus was on illuminating this interactive process, rather than developing a fully demonstrable system, the system detected cobalt-60 inside a mock warhead, instead of weapons-grade fissile material contained in a real warhead.[273] The system was similar to that developed under the Trilateral Initiative, but instead of having three attributes measured, it only determined the presence or absence on cobalt-60.[274] Overall, the system design emphasized simplicity, affordability, and easy maintenance, which are considerations that will be important in the future but have received less attention in past research and development efforts.[275]

On the managed access side, the research started from the assumption that foreign inspectors would need to access highly sensitive facilities and environments, which could risk proliferation-sensitive and security information at risk.[276] Thus, traditional on-site inspection practices must be modified such that the specific conditions are considered.[277]

---

[270] Ibid.

[271] Ibid.

[272] Ibid.

[273] Ibid., 69.

[274] Ibid.

[275] Ibid.

[276] Ibid.

[277] Ibid., 6.

The disarmament research in the United Kingdom also led to ongoing bilateral collaboration with the United States since 2000, focused on monitoring and verifying future nuclear disarmament.[278] The collaboration is facilitated by the fact that the states are able to exchange classified nuclear weapons information between each other, based on the 1958 Mutual Defense Agreement (MDA), which diminishes concerns about breakdowns in information integrity in the testing phases of new measurement technologies or other cases.[279] Thus, the collaboration has tested measurement technologies and methods with actual warheads and components and has been able to discuss and compare differences between the states at a highly detailed level.[280] The focus in the initiative is also on authentication and certification of the measurement technologies, parallel with protecting sensitive information related to warheads and their environments.[281]

Activities under the collaboration have focused on warhead measurement and data analysis, managed access, and other technical fields.[282] In 2011, the states engaged in the Warhead Monitored Dismantlement (WMD) Exercise, which was a fictious scenario of two states negotiating an arms reduction treaty and the affiliated verification provisions, which involved monitored dismantlement.[283] Through joint planning at a Joint Chain of Custody Working Group and Joint Nondestructive Assay Methods Working Group, the states agreed on a monitoring protocol that was tested in an exercise at an operational British nuclear facility that utilized a mock warhead with actual fissile material and simulated explosives.[284] Similar to the findings ender the Trilateral Initiative, one of the important

[278] National Nuclear Security Administration, "Joint U.S.-U.K. Report," 1.

[279] Ibid.

[280] Ibid.

[281] Ibid., 2.

[282] Ibid., 4.

[283] Ibid.

[284] Ibid.

conclusions was that the simultaneous and mutually agreed equipment certification by the host and authentication by the inspector is difficult to achieve.[285]

Another important example of the collaboration's work was the Active Measurement Campaign, which explored the use of active interrogation technologies in verification.[286] The experiment focused on assessing the value of active interrogation systems in warhead verification, as well as solving the concerns relating to shielding and radiation environment dangers for personnel.[287] The researchers concluded that these systems can be highly valuable for verification purposes, especially when the specific technique is chosen based on the target radiation source.[288] The collaboration has also involved two Authentication Workshops, in 2009 and 2014, with one of the key conclusions being that states have differing priorities and concerns in the authentication and certification of measurement equipment in warhead verification.[289] These past joint exercises have contributed to the collaboration's current work on the development of a radiation portal monitoring system under the U.S.-U.K. Portal Monitor for Arms Control (PMAC) project that aims to develop a system enabling simultaneous host certification and inspector authentication.[290] Since 2012, the collaboration has also engaged in collecting a radiation signature data set of nuclear warheads and components, which could significantly contribute to future research on warhead verification.[291]

The U.K.-Norway and U.S.-U.K. collaboration are important examples of engagement in joint development of future verification systems, each initiative contributing unique insights into this field.

---

[285] Ibid.

[286] Ibid., 14.

[287] Ibid.

[288] Ibid.

[289] Ibid., 21.

[290] Ibid., 3.

[291] Ibid., 24.

Going forward, collaboration must become increasingly inclusive and engage states that have not been involved in these efforts, whether nuclear or non-nuclear weapons states. In 2009, the U.S.-U.K. collaboration took an important step towards this direction, expanding the collaboration to the other five nuclear weapons states recognized under the NTP through briefing the states of the findings of the U.S.-U.K. collaboration.[292] This was taken further in the form of a joint presentation in 2014 at the Preparatory Committee for the 2015 NPT Review Conference.[293]

The Trilateral Initiative and the U.K.-Norway Initiative are only two examples of research efforts to develop systems that can handle classified forms of fissile materials, and thus could be used for warhead verification. Several systems have been developed in U.S. national laboratories that have also been demonstrated to Russian officials. Similar to the systems developed in the Trilateral Initiative and the U.K.-Norway Initiative, these systems include TRADS (Trusted Radiation Attribute Demonstration System), AMS/IB (Attribute Measurement System using Information Barriers), NG-AMS (Next Generation Attribute Measurement System), and 3GAMS (Third Generation Attribute Measurement System), which have been created in collaborative efforts between different U.S. national laboratories.[294] Independent efforts have also been done in other countries, including China, where the Institute of Nuclear Physics and Chemistry (INPC) in China Academy of Engineering Physics (CAEP) has developed an attribute verification system for plutonium subassemblies using an information barrier.[295]

---

[292] Ibid., 3.

[293] Ibid.

[294] Dean Mitchell and Keith Tolk, "Trusted Radiation Attribute Demonstration System," *INMM 41st Annual Meeting* (2000), http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/32/016/32016771.pdf.

Yan and Glaser, "Nuclear Warhead Verification: A Review of Attribute and Template Systems," 162

[295] Yan and Glaser, "Nuclear Warhead Verification: A Review of Attribute and Template Systems," 163.

IV. Future Dimensions

The development of verification systems in a multilateral context is critical, as in a potential future disarmament scenario these systems would be used to verify nuclear weapons under international agreements. Pursuing multilateral development efforts, however, also requires a diplomatic framework for facilitating communications between states. An example of a group that has formed in recent years is the International Partnership for Nuclear Disarmament Verification, which is a joint initiative led by the U.S. State Department and the Nuclear Threat Initiative involving 28 nuclear and non-nuclear weapons states focused on nuclear disarmament verification.[296] The fundamental objective of the partnership is to foster common understanding and trust among all involved parties, as well as explore the technical challenges related to multilateral verification.[297] The partnership engages in practical collaboration on new technologies in different phases of disarmament through its three working groups, but the underlying understanding is that a collective sense of confidence is required to establish legitimacy in the all novel verification technologies.[298]

The focus of IPNDV on engaging states with little to no experience in verification outside the civilian IAEA safeguards, which includes most states apart from the United States, Russia, the United Kingdom, and Norway. The partnership enables these states to think about challenging verification issues for the first time, enabling them to understand the professional skills needed in the process and the complexity of the issues involved. One of the key outcomes of the partnership so far is that non-nuclear weapons states could be involved in most activities in disarmament verification without compromising proliferation-sensitive information. This goes against the prevailing assumption among

[296] United States Department of State, "International Partnership for Nuclear Disarmament Verification (IPNDV)," http://www.state.gov/t/avc/ipndv/.

[297] Frank Rose, "Closing Remarks to the 4th Plenary Meeting of the International Partnership for Nuclear Disarmament Verification (IPNDV)," November 3, 2016, https://2009-2017.state.gov/t/avc/rls/264081.htm.

[298] Ibid.

certain actors in the non-proliferation and disarmament communities, according to which the involvement of non-nuclear weapons states could be highly risky. In addition to this key insight, the partnership has also engaged in dialogue on the relationship between political and technical needs and capabilities in verification.

These past multilateral efforts to develop technical verification capabilities demonstrate that states are aware of the criticality of having new verification options available for future stages of arms control. As the previous discussion has shown, the critical challenge will be maintaining the confidentiality of classified and sensitive information related to the inspected warheads, while providing transparency and a high level of confidence in the verification process. Both for nuclear weapons states and non-nuclear weapons states alike, these values would be critical in a future multilateral disarmament agreement. As has been discussed here, past technical solutions have employed information barriers to allow these two objectives to be reached simultaneously. With information barriers, the prevailing challenge continues to be the authentication and certification of the technical equipment, and developing trusted processors that can be used in these processes.[299]

[299] Keith Tolk et al., "Trusted Processor: A Result of the Evolution of Information Barrier Technologies," INMM 48th Annual Meeting (2007).

4. Physics of Nuclear Weapons

I. Introduction

The political and historical perspectives provided in previous chapters pave the way for a discussion on a set of emerging warhead authentication methods, which rely on zero-knowledge proofs to solve the challenge between maintaining the confidentiality of design information and providing transparency in the verification process. Before explaining these emerging approaches in the following chapter, however, it is necessary to explore more in depth the physics and design of nuclear warheads, as well as the methods that can be used to detect them. This will allow for a more detailed discussion of the techniques under consideration in the following chapter.

This chapter explains the fundamental physics of how nuclear weapons operate and illustrates what the key drivers of behind nuclear weapons design are. These general details about the physics of nuclear weapons are available to the public, but as will be discussed later in this chapter, the specifics of modern design features are highly guarded by nuclear weapons states.[300] The discussion in this chapter is limited to the principles that are important to understand from a policymaker's perspective, particularly for the purposes of the following chapter, which leaves out considerations about the quantum mechanical and many other effects associated with the physics. The motivation is to illuminate what the realities of detecting nuclear warheads are, as well as discuss why such a high level of secrecy is associated with specific design features of nuclear warheads. This leads to the discussion in the next chapter, which focuses on verification mechanisms that allow the design details to be kept concealed, while also providing a high-accuracy mechanism for authenticating the warheads. The

[300] Even if states knew the details of each other's warheads, political barriers also come into play: "Aside from commonality in application of basic physical principles and practices, neither side in a treaty is likely to have much detailed knowledge of each other's nuclear warhead design, and if they did they're not likely to admit it." (Alexander DeVolpi, "Tagging and Fissile Material Verification Concepts for Nuclear Warhead Dismantlement," *INMM 31st Annual Meeting* (1990), 1.)

discussion in the chapter shows that the concerns about revealing classified design information can be genuine, although these concerns are also inherently political, which illuminates why these high-security verification mechanisms will remain relevant in the future.

II. Fissile Material

Nuclear weapons can be based on two different physical mechanisms – fission and fusion. The discussion here will be limited to fission weapons, which were the first type of nuclear weapons that was developed, with the *Little Boy* and *Fat Man* used during the Second World War representing this category of weapons. In modern nuclear weapons, fission and fusion are used jointly in the same warhead, which explains why they are significantly more powerful than weapons using either mechanism alone. In these weapons, the fission mechanism is first initiated by explosives, which compress the nuclear material to a critical state. This fission reaction results in the release of high-energy, short-wavelength radiation (X-rays) that increases the temperature and pressure in the material, which then facilitates the fusion mechanism.[301] In this description, the focus is on the first stage – the fission reaction.

Fission reactions, which were discovered in the late 1930s, occur when a heavy nucleus splits into two lighter nuclei, which are called fission fragments.[302] This process releases a large amount of energy – although comparatively much less than fusion reactions do – which can be inferred from the difference in nuclear binding energy between the original and the new nuclei. Binding energy is defined as the energy gain of forming the nucleus, compared to the condition where the constituent protons

[301] Union of Concerned Scientists, "How Do Nuclear Weapons Work?" last modified September 30, 2016, accessed March 27, 2017, http://www.ucsusa.org/nuclear-weapons/how-do-nuclear-weapons-work#.WNXvrjvytPY.

[302] Noboru Takigava and Kouhei Washiyama, *Fundamentals of Nuclear Physics* (Tokyo: Springer, 2017), 46.

and neutrons are separated, and is the result of the residual strong interaction between protons and neutrons.[303] For a mass M(A,Z) the binding energy B(A,Z) is formally defined as:

$$B(A,Z) = Z\,M_p c^2 + (A-Z)M_n c^2 - M(A,Z)c^2$$

The two relevant isotopes for fission reactions utilized in nuclear weapons are ^{235}U and ^{239}Pu. The first one can be accumulated through enriching natural uranium, which is mostly ^{238}U. The plutonium isotope can be produced by irradiating ^{238}U with neutrons in a reprocessing facility. These isotopes are important because they are fissile, meaning that their fission can be initiated when they interact with thermal neutrons.[304] These fissile isotopes are distinct from isotopes that are merely fissionable, where the fission reaction can be induced with high-energy neutrons.[305] This difference stems from the composition of the nuclei, where the odd-even (odd number of neutrons, even number of protons) nucleus of ^{235}U has a higher ground state, or lower binding energy, than the even-even nucleus of ^{238}U (even number of both protons and neutrons).[306] This is because the even-even type of nucleus are generally more stable than even-odd or odd-even one, due to the Pauli exclusion principle.[307] The principle states that no two particles with a half-integer spin (fermions) can be in the same quantum state within the same quantum system. In this context, the principle precludes protons and neutrons (which have half-integer spins as baryons, so they are also fermions) from occupying the same quantum state and they thus would be expected to have opposite spins. Thus, nucleus configurations where there are equal numbers of protons and neutrons are favored, and when this is

[303] Ibid., 32.

[304] Thermal neutrons are defined based on their kinetic energy, which is approximately 0.025 eV. They are formed as a result of elastic collisions with other particles (Source: Ashik Das and Thomas Ferbel, *Introduction to Nuclear and Particle Physics (2nd Edition)* (Singapore: World Scientific Publishing, 2003), 106.)

[305] Das and Ferbel, *Introduction to Nuclear and Particle Physics,* 106.

[306] Ibid., 112.

[307] Sylvie Braibant, Giorgio Giacomelli, and Maurizio Spurio, *Particles and Fundamental Interactions: An Introduction to Particle Physics* (Verlag: Springer, 2009), 427.

not true, there is a correction term that increases in significance as the atomic number increases.[308]

This asymmetry term thus contributes to the binding energy:

	A	Z	$N = A - Z$	$\pm a_4$ (MeV)
(More stable)	Even	Even	Even	+12.6
(Intermediate)	Odd			0
(Less stable)	Even	Odd	Odd	−12.6

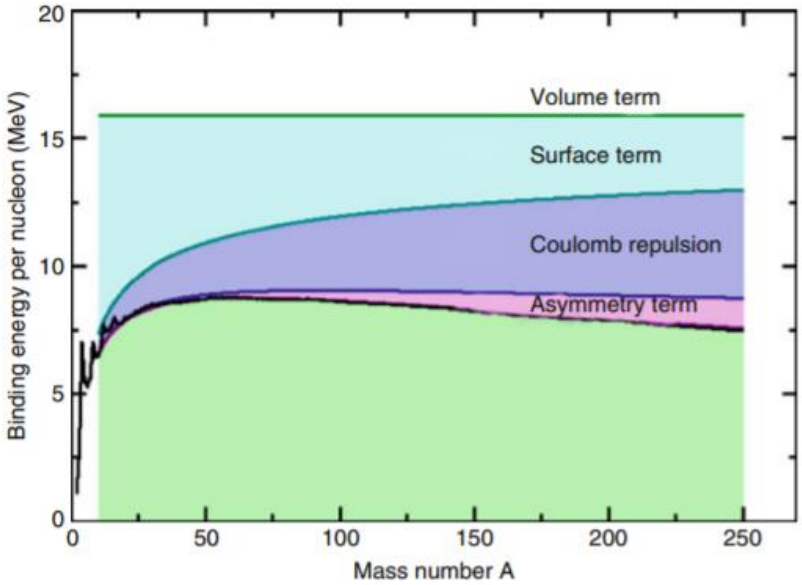

Fig. 14.6 Contribution of various terms of the Weizsacker formula for the binding energy per nucleon as a function of A. The surface, Coulomb and symmetry terms are subtracted to the volume term. The figure does not consider the configuration term

Figure 4.1. Binding energy per nucleon as a function of the atomic mass number, divided between its different components. Source: Sylvie Braibant, Giorgio Giacomelli, and Maurizio Spurio, *Particles and Fundamental Interactions: An Introduction to Particle Physics* (Verlag: Springer, 2009), 428.

[308] Ibid.

The binding energy associated with each isotope can be inferred from the graph representing nuclear binding energy:

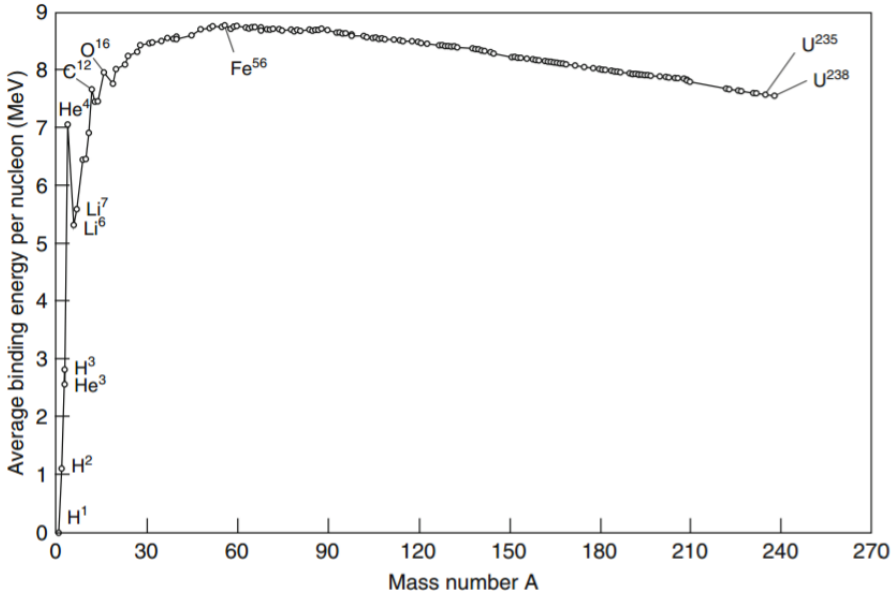

Fig. 14.3 The measured binding energy (BE) per nucleon of stable nuclei measured as a function of A. The peaks correspond to particularly stable nuclei. The curve has a maximum at $A \sim 60$

Figure 4.2. Average binding energy per nucleon as a function of mass number. Note ^{235}U and ^{238}U on the right. Source: Sylvie Braibant, Giorgio Giacomelli, and Maurizio Spurio, *Particles and Fundamental Interactions: An Introduction to Particle Physics* (Verlag: Springer, 2009), 421.

Importantly, both uranium and plutonium are on the right, where the binding energy per nucleon is decreasing as the atomic mass number is increasing. This means that the protons and neutrons in the nucleus are relatively lightly bound together, and the relative contribution of electromagnetic force increases.[309] The resulting fission fragments are medium-sized nuclei that have a higher binding energy per nucleon.

[309] Das and Ferbel, *Introduction to Nuclear and Particle Physics,* 106.

For ^{235}U, there are almost 400 potential fission pathways, with some being more probable than others and involve the transition isotope ^{236}U due to the neutron absorption.[310] One example of a fission reaction is the nuclei's breakdown into ^{148}La and ^{87}Br:

$$^{235}_{92}U + n \rightarrow {}^{148}_{57}La + {}^{87}_{35}Br + n$$

The distribution of these fission fragments of ^{235}U are concentrated such that one of them is highly likely to have a mass number of approximately 90, and the other of 140.[311]

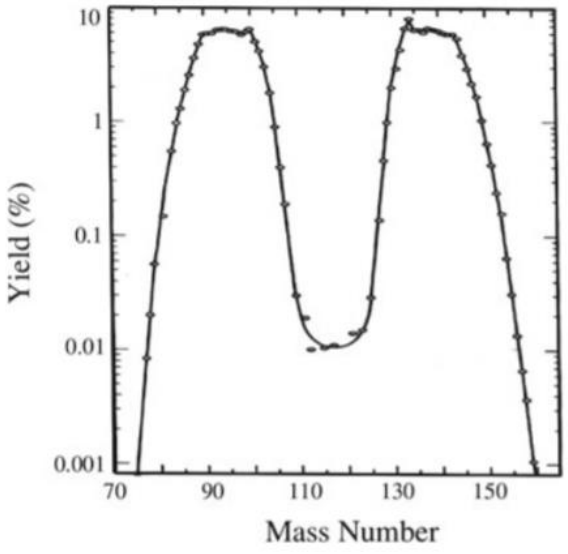

Fig. 2.17 The mass distribution of the fission fragments in the thermal-neutron-induced fission of $^{235}_{92}$U. Taken from [26]

Figure 4.3. The probabilistic distribution of fission fragments that result from the fission of ^{235}U induced by thermal neutrons. Source: Noboru Takigava and Kouhei Washiyama, *Fundamentals of Nuclear Physics* (Tokyo: Springer, 2017), 46.

[310] Mark Tuckerman, "CHEM-UA 127: Advanced General Chemistry I," New York University, http://www.nyu.edu/classes/tuckerman/adv.chem/lectures/lecture_22/lecture_22.pdf, 11.

[311] Takigava and Washiyama, *Fundamentals of Nuclear Physics*, 46.

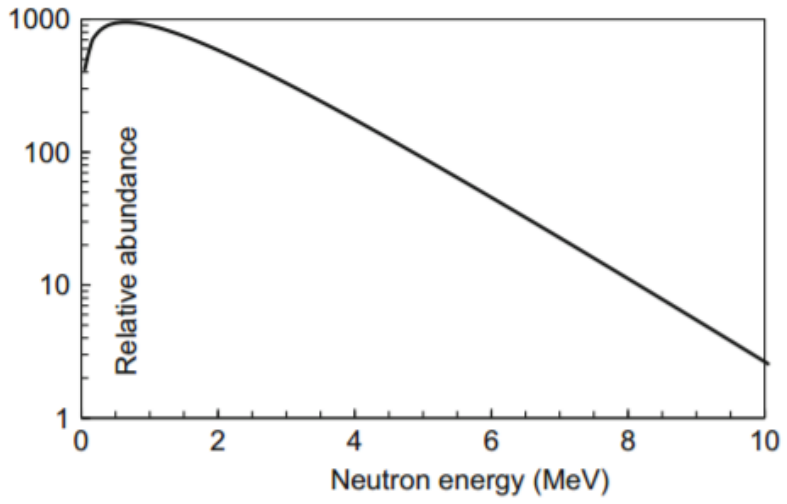

Fig. 1.6 Energy spectrum of neutrons released in fission of ^{235}U

Figure 4.4. The distribution of the neutrons, with varying energy levels, that are released in the fission of ^{236}U. Source: Bruce Cameron Reed, *The Physics of the Manhattan Project* (New York: Springer, 2015), 27.

Energy equivalent to the difference in binding energy between the original and the resulting nuclei is released in nuclear fission, in the form of the kinetic energy of the fission fragments, kinetic energy associated with the released neutrons, and photons.[312] For ^{235}U, the binding energy per nucleon is -7.5 MeV, and for the lanthanum and barium isotopes together it is -8.4 MeV.[313] Thus, the energy release is 0.9 MeV per nucleon in a fission reaction, so in total for the 235 nucleons approximately:

$$235 * 0.9\ MeV = 210\ MeV$$

The average number of immediate neutrons released in the reaction is 2.5, each of which can initiate a new fission reaction.[314] For ^{239}Pu, the average number of neutrons is 2.9. Since the number

[312] Braibant, Giacomelli, and Spurio, *Particles and Fundamental Interactions,* 446.

[313] Das and Ferbel, *Introduction to Nuclear and Particle Physics,* 106.

[314] Braibant, Giacomelli, and Spurio, *Particles and Fundamental Interactions,* 446.

of neutrons produced in the reactions is greater than the number consumed by it, the fission of one nucleus can create more than just one new fission reaction. This feature makes it possible for the fission reaction to proceed as a chain reaction, which is self-sustaining. This process is defined to be critical when self-sustainability is achieved, which can be calculated based on the effective neutron multiplication factor k:

$$k = \frac{Number\ of\ neutrons\ produced\ in\ the\ (n+1)\ stage\ of\ fission}{Number\ of\ neutrons\ produced\ in\ the\ n\ stage\ of\ fission}$$

The factor k describes the number of fission reactions that are initiated, on average, by neutrons that leave the reaction. When k reaches the value of 1, the mass is said to be critical and thus self-sustaining.[315] Below this value, the process is sub-critical. When k is above one, the mass reaches a supercritical stage, where the rate of neutrons produced and thus energy-releasing fission reactions increases exponentially. Reaching this stage is the core idea in nuclear weapons, where the energy release increases exponentially due to the supercritical conditions.

An important concept to understand in this context is critical mass, which determines how much fissile material is required to start the self-sustaining chain reaction. The challenge in sustaining the chain reaction relates to the spatial scale of the events associated with fission reactions, where the nuclei fills only one-thousandth of the space contained in an atom.[316] In order for the fission chain to continue, a released neutron must encounter the nucleus of another atom.[317] The likelihood of this encounter, however, is exceedingly small due to the tiny size of the nucleus as well as the neutron, and the neutron can reach the material's surface before encountering a nucleus.[318] This is the case even in

[315] Das and Ferbel, *Introduction to Nuclear and Particle Physics,* 113.

[316] Jonothan Logan, "The Critical Mass," *American Scientist* 84 (1996): 269.

[317] Bruce Cameron Reed, *The Physics of the Manhattan Project* (New York: Springer, 2015), 55.

[318] Logan, "The Critical Mass," 269.

extremely dense materials, such as solid uranium or plutonium. Quantitatively, the neutron's behavior is described by the variable mean free path, which is the average distance between the collisions.[319] As the size of this mass increases, so does the likelihood that neutrons encounter nuclei on their path and thus spark new fission reactions. Critical mass is the threshold at which the continuation of the fissile chain reactions is ensured and the density of neutrons within the mass is increasing as a function of time.[320]

Critical mass does not only depend on the neutrons' behavior, but also varies as a function of the density of the fissile material, the cross-section of the material, the number of neutrons released, and the kinetic energy of these neutrons.[321] Making calculations about critical mass requires the use of time-dependent diffusion theory, which allows the calculation of a critical radius at which the chain reaction becomes self-sustaining. This radius can then be converted to a critical mass based on which fissile material is used and what its attributes are.[322]

III. Warhead Design

This fission chain-reaction takes place inside nuclear warheads, which can be either implosion- or gun-type. *Little Boy*, the nuclear weapon used in Hiroshima, was a gun-assembly warhead, whereas *Fat Man*, the weapon used in Nagasaki, was implosion-type. The benefit of a gun-assembly weapon is its simple design, but it is less efficient (only 1.38% of the uranium in *Little Boy* was fissioned), only compatible with using ^{235}U, and heavier and larger than implosion-type warheads.[323] Thus, modern nuclear arsenals contain warheads that employ the implosion design, which have the advantage of

[319] Reed, *The Physics of the Manhattan Project*, 55.

[320] Ibid.

[321] Ibid.

[322] Ibid.

[323] James Corson, "Overview of Nuclear Weaponry," *University of Virginia, Metals in Medicine and the Environment*, accessed March 26, 2017, http://faculty.virginia.edu/metals/cases/corson3.html.

compatibility with plutonium, which has a higher fission rate than uranium; better efficiency while using lower amounts of fissile material; and thus overall lower-weigh weapons.[324] The following section briefly describes the mechanisms used in these two warhead types, based on the *Little Boy* and *Fat Man* designs.

In a gun-assembly nuclear weapon, "a conventional explosion forces together two subcritical masses of uranium creating critical mass and starting a nuclear chain reaction."[325] The first subcritical mass is a hollow spherical pit, and the second one is a cylindrical core.[326] Bringing together these two subcritical masses at high speed produces the a supercritical mass, in an assembly where the core is fired through a gun barrel, similar to a bullet, into the pit.[327] This is due to the fact that the density of the system is defined as mass divided by volume, where volume varies as a cube of radius (for a spherical mass). When the original spherical pit (containing one or more critical masses) is made hollow, and a certain amount of fissile material is removed from the core, two subcritical masses are formed.[328] This is because the critical mass has an inverse-square relationship with the density of the fissile material.[329] The core idea is to reunite these two subcritical masses at a later point, under high pressure conditions, to create a mass that is supercritical.

---

[324] Carey Sublette, "Implosion Assembly," *Nuclear Weapons Archive*, accessed March 25, 2017, http://nuclearweaponarchive.org/Library/Implsion.html.

[325] Digital National Security Archive, "Gun-assembly nuclear weapon," *Nuclear History I, 1955-1968*, accessed March 25, 2017, retrieved from http://ccl.idm.oclc.org/login?url=http://search.proquest.com/docview/1679150818?accountid=10141.

[326] Carey Sublette, "Gun Assembly," *Nuclear Weapons Archive*, accessed March 25, 2017, http://nuclearweaponarchive.org/Library/Gun.html.

[327] Sublette, "Gun Assembly."

[328] Ibid.

[329] John Coster-Mullen, *Atom Bombs: The Top Secret Story of Little Boy and Fat Man* (Coster-Mullen, 2009), 17.

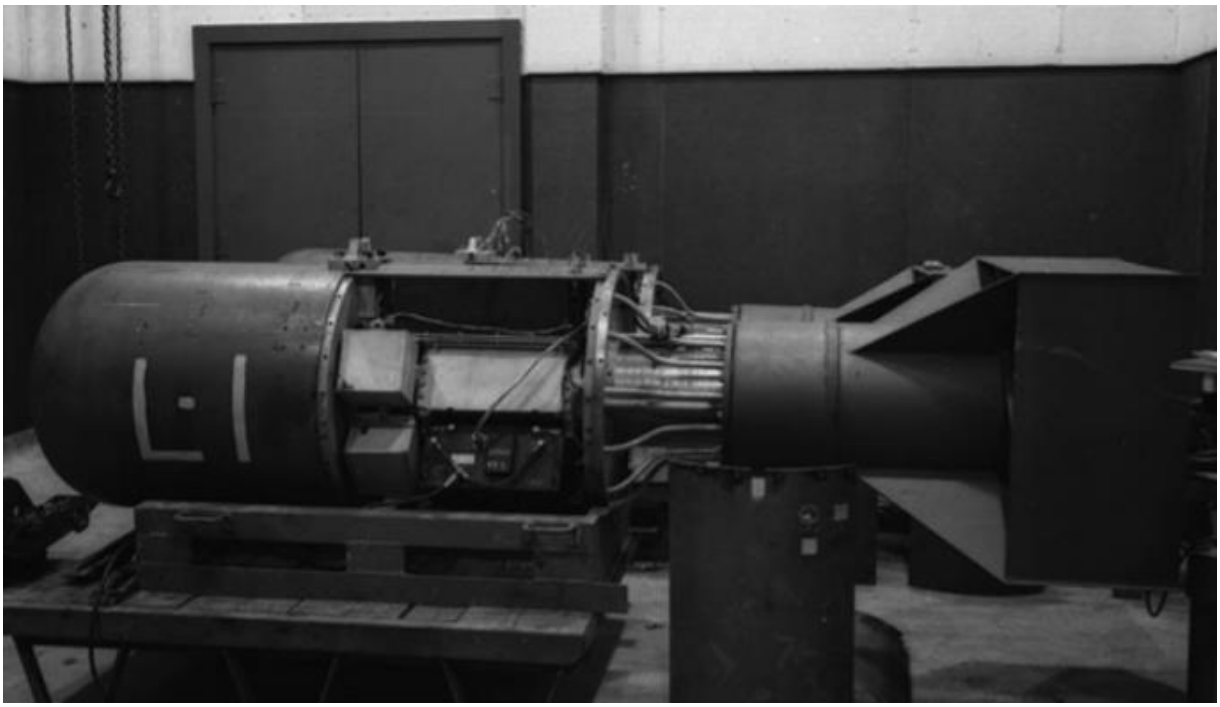

Figure 4.5. Little Boy. Source: Bruce Cameron Reed, *The Physics of the Manhattan Project* (New York: Springer, 2015), 71, originally Alan Carr, Los Alamos National Laboratory.

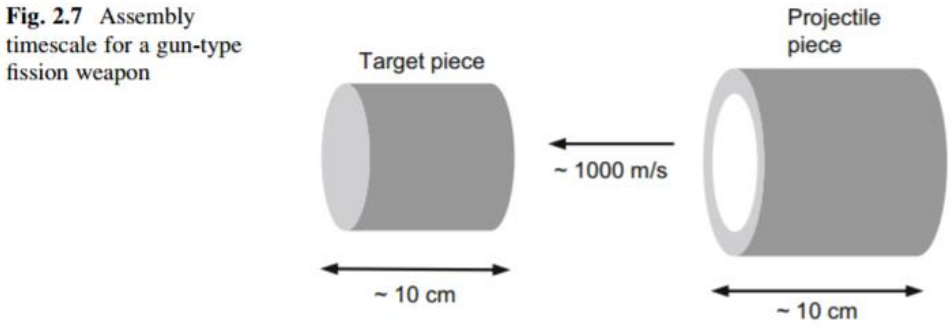

Figure 4.6. Mechanism of an implosion assembly. Source: Bruce Cameron Reed, *The Physics of the Manhattan Project* (New York: Springer, 2015), 70.

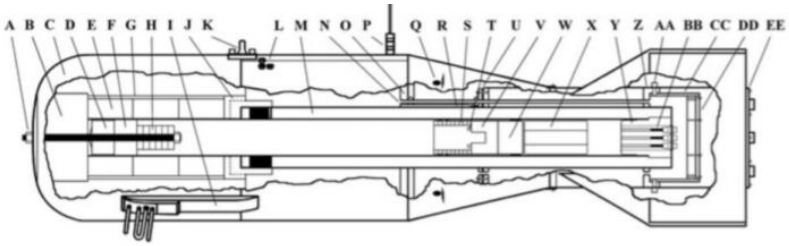

Fig. 2.9 Cross-section drawing of Y-1852 *Little Boy* showing major components. Not shown are radar units, clock box with pullout wires, barometric switches and tubing, batteries, and electrical wiring. Numbers in parentheses indicate quantity of identical components. Drawing is to scale. Copyright by and used with kind permission of John Coster-Mullen

(A) Front nose elastic locknut attached to 1-in. diameter Cd-plated draw bolt
(B) 15.125-in. diameter forged steel nose nut
(C) 28-in. diameter forged steel target case
(D) Impact-absorbing anvil with shim
(E) 13-in. diameter 3-piece WC tamper liner assembly with 6.5-in. bore
(F) 6.5-in. diameter WC tamper insert base
(G) 14-in. diameter K-46 steel WC tamper liner sleeve
(H) 4-in. diameter U-235 target insert discs (6)
(I) Yagi antenna assemblies (4)
(J) Target-case to gun-tube adapter with 4 vent slots and 6.5-in. hole
(K) Lift lug
(L) Safing/arming plugs (3)
(M) 6.5-in. bore gun
(N) 0.75-in. diameter armored tubes containing priming wiring (3)
(O) 27.25-in. diameter bulkhead plate
(P) Electrical plugs (3)
(Q) Barometric ports (8)
(R) 1-in. diameter rear alignment rods (3)
(S) 6.25-in. diameter U-235 projectile rings (9)
(T) Polonium-beryllium initiators (4)
(U) Tail tube forward plate
(V) Projectile WC filler plug
(W) Projectile steel back
(X) 2-lb Cordite powder bags (4)
(Y) Gun breech with removable inner breech plug and stationary outer bushing
(Z) Tail tube aft plate
(AA) 2.25-in. long 5/8–18 socket-head tail tube bolts (4)
(BB) Mark-15 Mod 1 electric gun primers with AN-3102-20AN receptacles (3)
(CC) 15-in. diameter armored inner tail tube
(DD) Inner armor plate bolted to 15-in. diameter armored tube
(EE) Rear plate with smoke puff tubes bolted to 17-in. diameter tail tube

Figure 4.7. The structure of Little Boy**.** Bruce Cameron Reed, *The Physics of the Manhattan Project* (New York: Springer, 2015), 71. Original source: John Coster-Mullen, *Atom Bombs: The Top Secret Story of Little Boy and Fat Man*.

The fissile material is at the core of the weapon, with the gun design forming its spine.[330] In *Little Boy*, the core was in the shape of a projectile, which was fired into uranium target discs to form the supercritical mass. This fissile material is surrounded by tamper or reflector material.[331] The purpose of the tamper material, made out of tungsten carbide mixed with cobalt, is to contain the

[330] Coster-Mullen, *Atom Bombs*, 24.

[331] Ibid., 17.

fissile material in its shape as the chain reaction starts to exert pressure on it and reflect neutrons back into the material.[332] Depleted uranium is another option for the tamper material. Outside this reflector, a heavy steel case supports the material and holds the weapon together.

The mechanism that activates the chain reaction is formed out of four polonium-beryllium initiators, which serves as a neutron generator.[333] Alpha decay takes place in polonium, and the resulting alpha particles (^4_2He) are captured by the beryllium, which then releases neutrons in the reaction. The two materials are initially separated by a thin gold foil, but when the uranium projectile hits its uranium target discs, this foil is also torn in the process and the two materials mix.[334] This results in the immediate release of a large number of neutrons, feeding the chain reaction. The bomb also contains an arming and fusing system that consist of "clock switches, safing and arming plugs, six barometric (baro) switches, and the Radar Network" that together made it possible to send the firing signal when the bomb reached the desired burst height.[335]

An implosion assembly weapon brings its enclosed fissile material to subcriticality through compression.[336] It contains a spherical or cylindrical fissile material mass, originally in a subcritical state, and uses high explosives at the outer surface of the mass to create an implosion shock wave that compresses the mass, increasing its density, and thus allowing it to become supercritical.[337] The mass can also be hollow, with the shock wave collapsing it in the process.[338] The density of the material can become two-fold or more, as the pressure brings the atoms closer together.[339] As was discussed earlier,

[332] Ibid., 18.

[333] Ibid., 28.

[334] Ibid.

[335] Ibid., 19.

[336] Sublette, "Implosion Assembly."

[337] Ibid.

[338] Ibid.

[339] Ibid.

the critical mass varies inversely as a square of density, so by increasing the density by a factor of two, the critical mass becomes four times as large.[340] This means that a mass that starts subcritical becomes supercritical in the compression process. Another effect of the compression is a reduction in the mean free path, or the average distance that a neutron travels between collisions. Mean free path is inversely proportional to density, so an increase in density shortens the mean free path and thus increases the number of neutron collisions in the matter, leading to more rapid and efficient chain reactions.[341] Similar to the gun-type assembly, implosion devices have initiators in the design, but they are located at the center of the core and are mixed when the shock wave from the explosion hits the initiator.[342] In the case of *Fat Man*, the fissile material contained was plutonium, but implosion weapons can use either highly enriched uranium or plutonium.

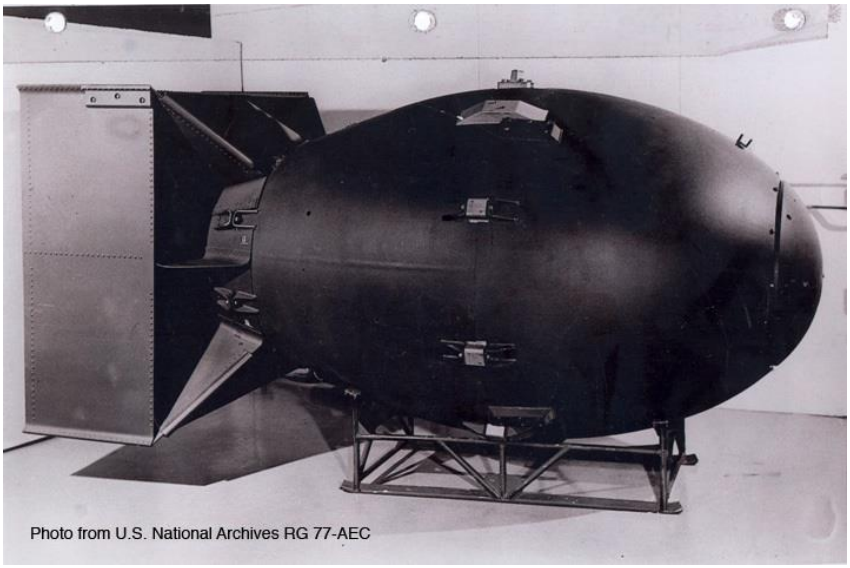

Figure 4.8. Fat Man. Source: James Corson, "Overview of Nuclear Weaponry," *University of Virginia, Metals in Medicine and the Environment*, accessed March 26, 2017, http://faculty.virginia.edu/metals/cases/corson3.html.

[340] Ibid.

[341] Ibid.

[342] Chris Camp, "Why No One Will Ever Build Another Nagasaki Type Bomb," *Arms Control Wonk*, July 15, 2014, http://www.armscontrolwonk.com/archive/604623/why-no-one-will-ever-build-another-nagasaki-type-bomb/

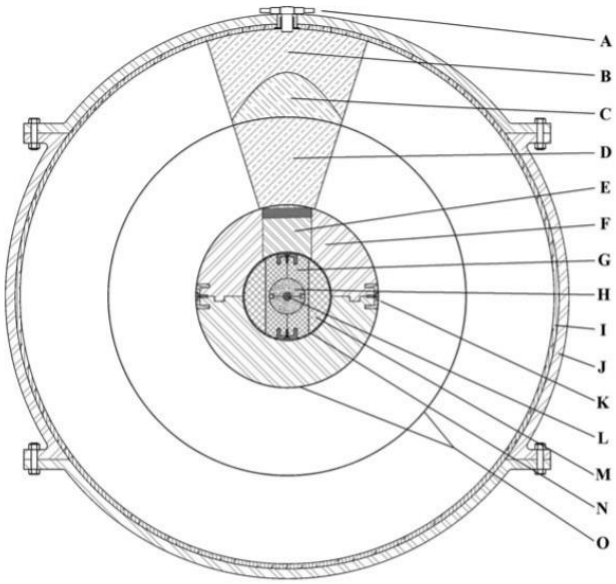

Fig. 4.5 Cross-section drawing of the Y-1561 *Fat Man* implosion sphere showing major components. Only one set of 32 lenses, inner charges, and detonators is depicted. Numbers in parentheses indicate quantity of identical components. Drawing is to scale. Copyright by and used with kind permission of John Coster-Mullen

(A) 1773 EBW detonator inserted into brass chimney sleeve (32)
(B) Comp B component of outer polygonal lens (32)
(C) Cone-shaped Baratol component of outer polygonal lens (32)
(D) Comp B inner polygonal charge (32)
(E) Removable aluminum pusher trap-door plug screwed into upper pusher hemisphere
(F) 18.5-inch diameter aluminum pusher hemispheres (2)
(G) 5-inch diameter Tuballoy (U-238) two-piece tamper plug
(H) 3.62-inch diameter Pu-239 hemisphere with 2.75-inch diameter jet ring
(I) 0.5-inch thick cork lining
(J) 7-piece Y-1561 Duralumin sphere
(K) Aluminum cup holding pusher hemispheres together (4)
(L) 0.8-inch diameter Polonium-beryllium initiator
(M) 8.75-inch diameter Tuballoy tamper sphere
(N) 9-inch diameter boron plastic shell
(O) Felt padding layer under lenses and inner charges

Figure 4.9. The structure of Fat Man. Source: Bruce Cameron Reed, *The Physics of the Manhattan Project* (New York: Springer, 2015), 133. Original Source: John Coster-Mullen, *Atom Bombs: The Top Secret Story of Little Boy and Fat Man*.

IV. Modern Nuclear Weapons

These two simplified descriptions of the dynamics of the two initial designs of nuclear weapons only provide a hint of the complexity associated with the design of modern nuclear weapons. *Little Boy* and *Fat Man* were developed under intense pressure during the Second World War and the design decisions "were products of the circumstances in which they were created, and those

circumstances would not apply to any nation building a bomb since then."[343] The sophistication of modern nuclear weapons designs is exponentially greater and include several important design breakthroughs that have made the weapons significantly more powerful. With respect to implosion-type fission weapons, these advancements include levitated pits, more efficient high explosives, multipoint detonation, and solid state neutron generators as higher-efficiency initiators.[344] In addition, the delivery systems and mechanisms for nuclear warheads have been transformed since the Second World War, which has directed the design of weapons in important ways.[345] The greatest transformation came about with the development of thermonuclear weapons (hydrogen weapons), which employ nuclear fusion. As was discussed earlier, most modern weapons utilize both fission and fusion in their design, for example as fusion-boosted fission weapons, fission-fusion weapons, or fission-fusion-fission weapons.[346] Another modern design feature is variable yield, or 'dial-a-yield' weapons, where the yield of the weapon can be adapted.[347]

The advancements made in weapon miniaturization and other technical features can be tracked through the yield-to-weight ratio, as shown in Figure 4.10, which is one measure of bomb efficiency. It also provides a way to compare *Little Boy* (Mk-1) and *Fat Man* (Mk-3) to modern U.S. nuclear weapons.[348] Thermonuclear weapons, which are much higher yield, but also significantly heavier – note that both the x and y axis are logarithmic – are towards the upper-right hand corner. Tactical nuclear weapons are on the lower left, showing that the demands of lighter weight and smaller

---

[343] Ibid.

[344] Ibid.

[345] Ibid.

[346] Carey Sublette, "Thermonuclear Weapons Design," *Nuclear Weapons Archive*, accessed March 26, 2017, http://nuclearweaponarchive.org/Nwfaq/Nfaq4-5.html.

[347] United States Department of Energy, "Restricted Data Declassification Decisions: 1946 to the Present (RDD-8)," *Office of Health, Safety and Security, Office of Classification*, January 1, 2002, https://fas.org/sgp/othergov/doe/rdd-8.pdf, 68.

[348] Alex Wellerstein, "Kilotons per Kilogram," *Restricted Data: The Nuclear Secrecy Blog*, December 23, 2013, http://blog.nuclearsecrecy.com/2013/12/23/kilotons-per-kilogram/

yield also result in a worse yield-to-weight ratio.[349] Most currently deployed U.S. nuclear weapons are in the middle, as indicated by the redder shade, that are high-accuracy, moderate-yield, and relatively lighter, and have a comparatively good yield-to-weight ratio. One example is the W-88, whose design is shown in Figure 4.11, which is a two-stage implosion weapon with a yield of 475 Kt and weight of approximately 360 kg.[350] The ratio of these modern weapons is still less than half of the optimum that has been possible to reach.[351] The yield-to-weight ratio is also useful for comparing the nuclear capabilities across nations. For example, with respect to the increasing yields of weapons during the peak of the U.S.-Soviet arms race, it was evident that the higher-yield Soviet weapons relied more on direct scaling up rather than technical developments, as the yield-to-weight ratios of the weapons remained stable.[352]

[349] Ibid.

[350] Carey Sublette, "The W88 Warhead," *Nuclear Weapons Archive*, accessed March 25, 2017, http://nuclearweaponarchive.org/Usa/Weapons/W88.html.

[351] Wellerstein, "Kilotons per Kilogram."

Original source: Theodore B. Taylor, "Third Generation Nuclear Weapons," *Scientific American* 256, No. 4 (April 1987), 34.

[352] Wellerstein, "Kilotons per Kilogram."

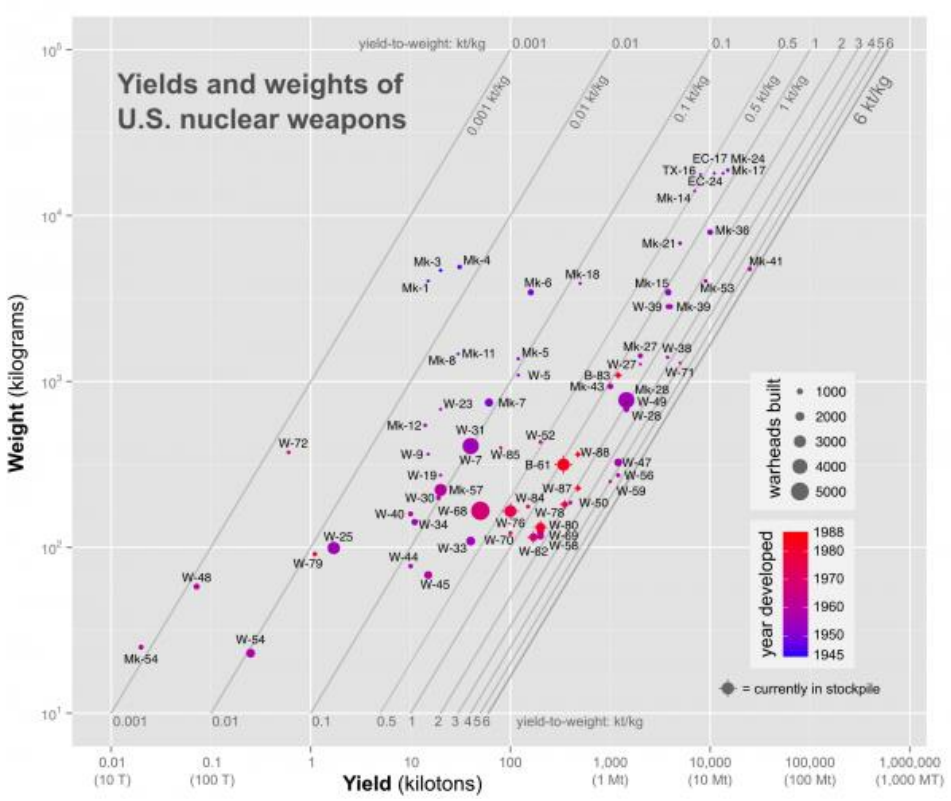

Figure 4.10. The weight of warheads in the U.S. nuclear arsenal as a function of their yield. Source: Alex Wellerstein, "Kilotons per Kilogram," *Restricted Data: The Nuclear Secrecy Blog*, December 23, 2013, http://blog.nuclearsecrecy.com/2013/12/23/kilotons-per-kilogram/

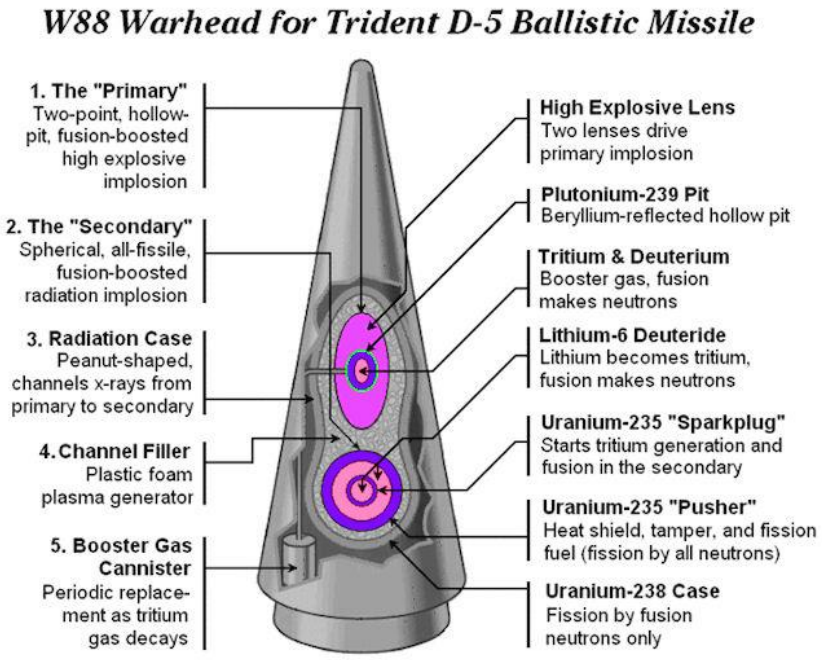

Figure 4.11. The design of W88, one of the modern U.S. warheads. Source: Carey Sublette, "The W88 Warhead," *Nuclear Weapons Archive*, accessed March 25, 2017, http://nuclearweaponarchive.org/Usa/Weapons/W88.html

V. Physics of Radiation Signatures and Warhead Detection

The previous sections discuss the general physics and design of warheads, which can be employed in different ways to create mechanisms to detect these objects. These techniques mainly rely on identifying the radiation outputs from the warheads. As has been explicated, the most important fissile materials used in warheads are $^{235}_{92}U$ and $^{239}_{94}Pu$. These two isotopes are radioactive, meaning that they are unstable and spontaneously undergo fission reactions that emit particles and radiation. This process can also be induced externally by using a radiation source. In general, radioisotopes can produce neutrons, alpha particles (emission of $^{4}_{2}He$), or beta particles (emission of an electron) in the reactions.[353] In the case of $^{235}_{92}U$ and $^{239}_{94}Pu$, the emitted particles are neutrons, but other isotopes also

[353] W. N. Cottingham and D.A. Greenwood, *An Introduction to Nuclear Physics* (Cambridge: Cambridge University Press, 2004), 15, 74.

undergo alpha decay, which results in more complex reactions in the materials contained in warheads.[354] The reactions also release electromagnetic radiation of various wavelengths, most importantly gamma radiation.[355] The spectrum of gamma rays emitted by a specific isotope is unique to that isotope, which can be used as a mechanism to identify it.

As has been discussed, the design of nuclear weapons includes different conformations of the fissile material, as well as other features such as tamper materials, a casing, and non-nuclear components. All of these characteristics affect the way that particles and electromagnetic radiation travel through the materials, including being scattered and absorbed in the process, and thus also affect the radiation signature that is obtained.[356] The interactions can also result in new releases of radiation, such as when the neutrons escape from the fissile material and interact with other materials in the warheads.[357] The geometry of the design and the composition of the materials in the warhead thus result in a distinguishable radiation signature that is unique to each type of warhead. Figure 4.11 shows an example of the radiographic profile of a Soviet warhead, measured in the Black Sea experiment in July 1989, using gamma rays.[358] The warhead design and the radioactive materials determine the techniques that can be used for detection, as they define the range of radiation outputs that reach the warhead environment without being tampered.[359]

---

[354] Steve Fetter et al., "Detecting Nuclear Warheads" in *Reversing the Arms Race: How to Achieve and Verify Deep Reductions in the Nuclear Arsenals*, eds. Frank von Hippel and R. Z. Sagdeev (New York: Gordon and Breach Science Publishers, 1990), 268.

[355] Cottingham and Greenwood, *An Introduction to Nuclear Physics*, 15, 74.

[356] Committee on International Security and Arms Control, National Research Council, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities,* 99.

[357] Ibid.

[358] Steve Fetter, Thomas Cochran, Lee Grodzins, Harvey Lynch, and Martin Zucker, "Gamma-Ray Measurements of a Soviet Cruise-Missile Warhead," *Science* 248 (1990), 248.

[359] Steve Fetter et al., "Detecting Nuclear Warheads," 267.

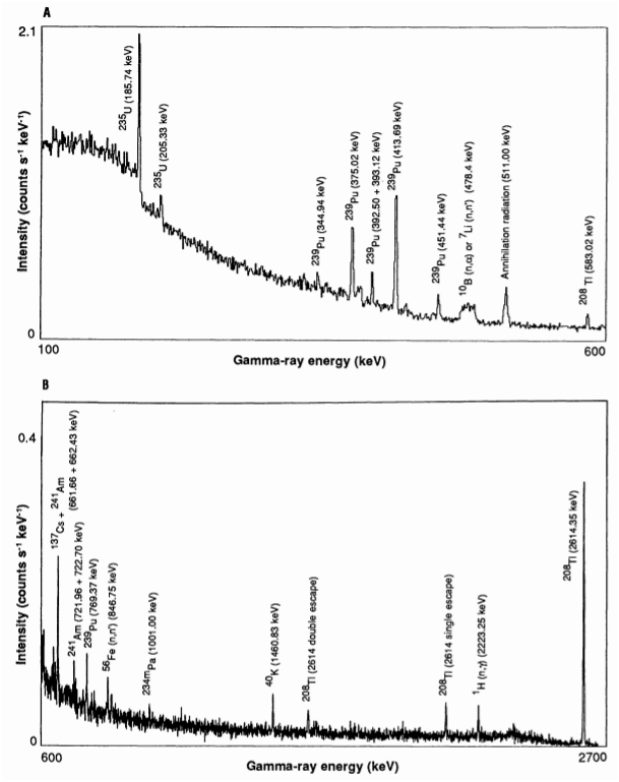

Fig. 2. (**A**) Gamma-ray spectrum from 100 to 600 keV; (**B**) gamma-ray spectrum from 600 to 2700 keV. [Adapted from (*29*)]

Figure 4.11. The radiographic signature obtained in the Black Sea experiment. Source: Steve Fetter et al., "Gamma-Ray Measurements of a Soviet Cruise-Missile Warhead," *Science* 248 (1990), 248.

Spectroscopy refers to passive techniques that detect the electromagnetic radiation absorbed, emitted, or scattered from materials.[360] When spectroscopy is used in the context of warhead detection, the systems mostly focus on detecting neutrons or gamma rays (energy above the 0.1 MeV range), as they are detectable at least at two meters' distance from the warhead.[361] This is because the radiation flux (of either particles or electromagnetic radiation) decreases inversely as a function of the square of the distance from the warhead.[362] Detecting the gamma-ray spectra of a warhead can be done with a

[360] 'Passive' refers to the fact that the method does not involve active measures to excite the nuclei to induce the emission of radiation.

[361] Steve Fetter et al., "Detecting Nuclear Warheads," 268.

[362] Ibid., 271.

high level of accuracy, and the measurement data also conveys the specific material composition of the fissile and other materials in the warhead.[363] Neutron detectors, on the other hand, are less accurate with respect to the energy of the emitted neutrons, and cannot identify the origin. These passive methods, overall, have some disadvantages with respect to specific weapons designs, such as those that use neither plutonium as the fissile material nor depleted uranium as the tamper material.[364] Warheads without these design features, combined with heavy casings, might be very difficult to detect using passive methods.[365]

Active methods can also be used in detecting warheads. Radiography refers to an imaging method that uses of electromagnetic radiation, below the wavelength of visible light, to determine the composition and structure of objects. Radiography can also be used with particles; neutron radiography, for example, is the process of using thermal neutrons to construct high-definition images. The idea is that the transmission of actively produced electromagnetic radiation or particles is measured, with the detection apparatus being on the other side of the object. In the context of warheads, this allows for the identification of the fissile material inside the warhead, because the ${}^{235}_{92}U$ and ${}^{239}_{94}Pu$ isotopes react differently to the radiation than other materials.[366]

The benefit of neutron radiography, compared to electromagnetic radiation, is that the attenuation patterns are more dissimilar between different elements and materials. The X-ray radiographs of the objects, for example, can be too similar to differentiate.[367] This is shown in Figure 4.12, which compares the attenuation patterns of materials for 120 keV X-ray radiography and neutron

[363] Ibid., 270.

[364] Ibid., 278.

[365] Ibid.

[366] Ibid., 280.

[367] Attenuation refers to the reduction in intensity, as the radiation traverses through matter. (Source: Harold Berger, *Neutron Radiography* (Amsterdam: Elsevier Pub. Co., 1965), 335.)

radiography. The greater variation in neutron attenuation patterns, which are distinct even between isotopes, indicates the greater distinguishing ability of this method, compared to X-ray radiography. When comparing the use of neutron and gamma rays for radiography, the latter is not as effective for distinguishing heavy elements from fissile materials. On the other hand, gamma rays produce a higher-resolution radiographs, because developing a well-collimated and monoenergetic neutron source and measuring the energy of transmitted neutrons is more difficult than that of gamma rays.[368] Overall, the choice of radiography method is dependent on what the other potential materials in the warheads are. Thermal neutrons, for example, may not be sufficient to distinguish between the weapons-grade plutonium and uranium from materials that absorb thermal neutrons as efficiently, such as lithium and boron.[369]

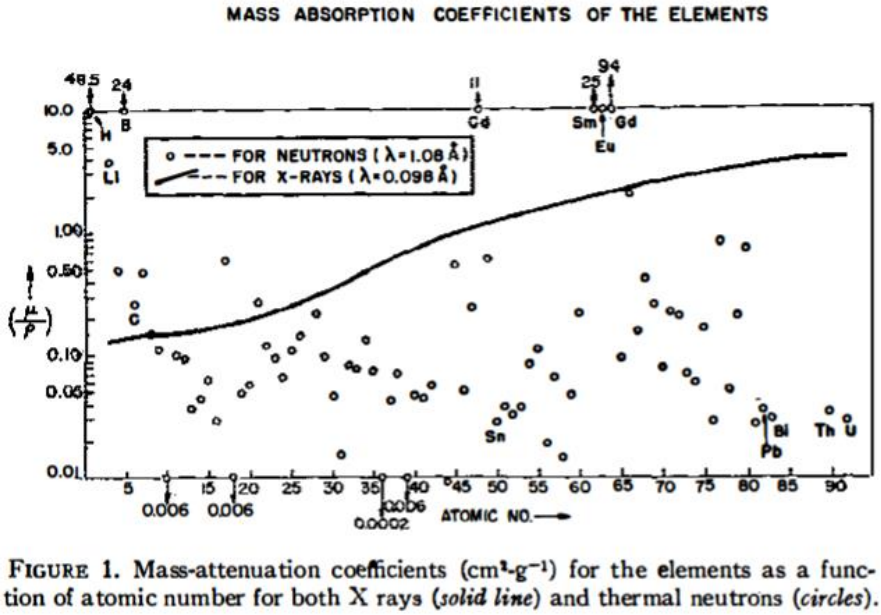

FIGURE 1. Mass-attenuation coefficients ($cm^2 \cdot g^{-1}$) for the elements as a function of atomic number for both X rays (*solid line*) and thermal neutrons (*circles*).

Figure 4.12. The mass attenuation coefficient as a function of the mass number, both for X-rays and thermal neutrons. Source: Harold Berger, *Neutron Radiography* (Amsterdam: Elsevier Pub. Co., 1965), 335.

[368] Collimation refers to the alignment of the transmitted neutrons from the source. (Source: Steve Fetter et al., "Detecting Nuclear Warheads," 280.)

[369] Steve Fetter et al., "Detecting Nuclear Warheads," 280.

The methods discussed in this section are used in the verification approaches described in the next chapter. As has been shown here, both radiography and spectroscopy are useful in different ways for verification purposes, and the choice of the measurement system depends on the specific conditions in question. Radiography would describe more precisely the shape of the object, whereas spectroscopy would determine what materials were used in it. These could also be combined with other techniques, such as neutron multiplicity counting and other assay methods.[370] As will be discussed next, the central issue in these measurements is that the raw data of the spectra could be used to understand the design details of the warheads, which would be hard for states to accept for both technical and political reasons.[371] This is the core challenge that the next chapter will discuss.

VI. Significance of Weapon Design for Verification

The previous analysis of the physics and design of nuclear weapons illustrates how the details of the warheads matter to the efficiency and yield of the weapons. From a state perspective, the value and utility of nuclear weapons is highly dependent on these two parameters, which is one dimension of why they prioritize secrecy with respect to the design of their nuclear weapons. A range of political and psychological variables are also at play, of course, but the following discussion focuses on the technical rationale for maintaining secrecy about weapons design. This is the fundamental reason why it will be important to develop verification mechanisms for warheads that maintain these design secrets concealed, to not force states to choose between disarmament and compromising this classified knowledge.

[370] Shea, "The Trilateral Initiative: A Model for The Future?"

[371] Cliff, Elbahtimy and Persbo, "Verifying Warhead Dismantlement: Past, Present, Future," 59.

Several arguments can be made in support of this culture of secrecy regarding nuclear arsenals. First, if the assumption is that the United States and Russia, or previously Soviet Union, have not been able to discover the details of each other's nuclear arsenals through the means of intelligence, then maintaining these details would be a strategic advantage.[372] From a technical perspective, the details of the bomb design determine the weapon's efficiency, yield, and reliability. The parameters that are relevant to the efficiency of nuclear weapons involve the core size, expansion rate, pressure, neutron density, and energy dynamics.[373] All of these variables change as a function of time, so the specific mechanics of the bomb design are critical for understanding its efficiency and yield.[374] Information that would reveal these parameters can include details about warhead design and configuration, the capabilities of specific components, the quantity and isotopic composition of the weapons material, and other aspects relating to how the warheads operate. Sensitive information can also relate to the warhead environment, including the launch vehicles, storage operations, and many other aspects. Thus, a strategic argument can be made for maintaining a strict level of secrecy regarding design details.

Another strategic argument for secrecy is that knowing the design details would allow other states develop countermeasures against the specific design characteristics of the state's nuclear warheads.[375] For example, "neutrons, in the right quantity, can "kill" a warhead, causing its plutonium to heat and expand, and causing its chemical high-explosives to degrade; if you knew exactly what level of neutrons would kill a nuke, it would play into strategies of trying to defend against a nuclear attack."[376] The revelation of design secrets would undermine nuclear deterrence, if other states would

[372] Alex Wellerstein, "Secrecy, Verification, and Purposeful Ignorance," *Restricted Data: The Nuclear Secrecy Blog*, September 23, 2016, http://blog.nuclearsecrecy.com/2016/09/23/secrecy-verification-purposeful-ignorance/.

[373] Reed, *The Physics of the Manhattan Project*, 70.

[374] Ibid.

[375] Wellerstein, "Secrecy, Verification, and Purposeful Ignorance."

[376] Ibid.

be able to neutralize the nuclear warheads. As will be discussed in the next chapter, the measurement of radiographic profiles of warheads, or other intrusive verification methods, could make 'reverse-engineering' the warhead's exact design possible.[377]

Concerns about classified or sensitive information are specific to each state, due to the differences in their government-regulated classification systems but also based on the distinct status of their nuclear weapons program. States can be concerned that the information could be exploited by competing states and enable them to utilize the information to enhance their capabilities, if they perceive their capabilities superior to adversaries. On the other hand, the information can also reveal vulnerabilities about their capabilities and provide knowledge about the performance and reliability of the warheads, which are amplified if states regard their capabilities to be comparatively inferior or less developed. Especially if states are still in the warhead or material build-up phase, as the states are concerned with relative advantages to others. This could be interpreted from U.S.-Soviet relations during the Cold War, as well as in the current conditions in India and Pakistan. In the U.S.-Russia context, concerns about intrusiveness have decreased as the states have engaged in collaborative disarmament measures. The absence of this history of engagement, however, is likely to make other nuclear weapons states much more cautious regarding the revelation of design secrets.

These differences between state perceptions of confidentiality and their sensitivity to different levels of intrusiveness in inspections should be acknowledged in the process of devising future verification approaches for disarmament treaties. Insights about specific state concerns can inform officials and experts of the best mechanisms in verification approaches that promote legitimacy and confidence in the eyes of different states, advancing their willingness to cooperate in the processes of negotiation, signature, and ratification. On the other hand, these perceptions are also malleable, which

[377] Cliff, Elbahtimy and Persbo, "Verifying Warhead Dismantlement: Past, Present, Future," 59.

is visible in the U.S.-Russia disarmament history. The entire idea of accessing classified and sensitive nuclear facilities, containing some of the most important national security capabilities that states can possibly have, was unimaginable before the United States and the Soviet Union established precedence in this during the Cold War. Progressively, they started opening up their facilities bilaterally for on-site inspections, overflight and satellite monitoring, and many forms of national technical means that enabled the buildup of trust between the two states.

This chapter illustrates how technical, political, and historical factors relate to the design of nuclear weapons, and how a strong culture of secrecy continues to surround states' nuclear weapons programs. One of the key challenges for future steps in nuclear arms control is to find ways around this veil of secrecy, acknowledging state sensitivities but also devising ways to overcome these barriers. This challenge is particularly important for creating new verification mechanisms for individual warheads, which is the focus of the next chapter.

5. Zero-Knowledge Verification

I. Introduction

As has been detailed in previous chapters, the core challenge in nuclear arms control verification is balancing the concerns of the host state in maintaining a strict level of confidentiality, and the interests of other involved parties in establishing confidence in the verification process. This balance between secrecy and transparency has been discussed in relevant arms control literature and evidenced in the negotiating dynamics of past disarmament efforts. The current verification approaches place more significance to host state concerns, as has been evidenced in the context of disarmament between the United States and Russia. Multilateral disarmament is likely to introduce even deeper and complex anxieties about the confidentiality and transparency dimensions of nuclear arms control verification processes.

The conceptualization of this balancing act as a zero-sum game, however, may be misguided. As will be discussed in this chapter, new verification technologies and approaches can contribute to adjusting the scale between confidentiality and transparency, enabling future disarmament verification provisions to equalize these critical interests. Specifically, this chapter focuses on the process of warhead verification, where state concerns about protecting classified information about warheads and their design are contrasted with the interests of the inspecting party in ensuring the authenticity of the measurement process. Emerging approaches that employ physical cryptographic protocols aim to create a mechanism of high-security warhead verification where neither confidentiality or transparency would need to be sacrificed.

This chapter will first provide a brief overview of the issues that drive the need for verification mechanisms that focus on individual warheads, with previous chapters providing a more detailed analysis of the historical background and past technical efforts. Next, the technical basis for physical

cryptographic warhead verification is introduced by discussing the general cryptographic concept of zero-knowledge proofs, and then focusing on their application in the physical domain, specifically in the authentication of nuclear warheads. After detailing the three most advanced implementations of these systems, the chapter will address the core unsolved challenge relating to authenticating the reference warhead. Finally, potential solutions to this question are explored through an analysis of relevant tools in modern cryptography and their application to analogous high-security authentication systems.

II. Contextualizing the Challenge

Disarmament verification is a complex interactive process that is connected to a wide range of technical and political mechanisms, depending on the content and context of the treaty being verified. The technical and political sides are in many ways decoupled from one another, but also inherently interconnected. When considering what forms of verification will be needed for any given disarmament treaty, a critical question is the informational value that the selected verification mechanisms provide for monitoring the treaty provisions, either independently or in conjunction with other mechanisms.[378]

In future agreements focused on individual warheads, the most critical questions relate to the high-security authentication of warheads, their unique identification, and maintaining the continuity of knowledge until they have been dismantled.[379] Perhaps the most challenging one of the three is the ability to conclusively and accurately authenticate a warhead and distinguish its type, while still maintaining the highest level of confidentiality in the process.[380] The use of verification approaches

[378] Private communication with Dr. Thomas Shea, current affiliation with the Federation of American Scientists. Cited with permission.

[379] Nuclear Threat Initiative, "Verifying Baseline Declarations of Nuclear Warheads and Materials."

[380] Comley et al*.,* "Confidence, Security and Verification: The challenge of global nuclear weapons arms control," 11.

that would allow this are inherently intrusive and can reveal extremely detailed, classified information about warhead design. This is a non-negotiable for nuclear weapons states, as the information could be exploited by other states, could reveal vulnerabilities in warhead function, and would also place the states in noncompliance with Article I in the NPT, which prohibits nuclear weapons states from disclosing proliferation-sensitive information.[381]

The future of nuclear disarmament will look very different from previously applied arms reduction mechanisms, which have not defined warheads themselves as the treaty-accountable item, but have rather focused on delivery vehicles and launchers.[382] As discussed in an earlier chapter, unique characteristics of the U.S.-Russia context have facilitated this form of disarmament, enabling the states to circumvent the challenge of accurately counting and verifying individual warheads. Both sides have had a high tolerance for uncertainty in treaty limits and verification effectiveness, driven by the vast size of their nuclear arsenals, and have been able to independently monitor compliance through advanced capabilities in national technical means (NTM).[383] Importantly, analysis of the different negotiation circumstances illustrate that in many cases there would have been political will for deeper reductions and wider capability coverage, if verification mechanisms had been available.

As has been detailed in an earlier chapter, few of the facilitating factors in past disarmament processes will hold true for future disarmament, whether in the context of continued U.S.-Russia bilateral agreements or multilateral disarmament treaties, which will make it essential to shift to a disarmament paradigm that focuses on addressing individual warheads as the treaty-accountable item. When discussion concerns hundreds of warheads or fewer, the tolerable margin of error diminishes.

---

[381] Hugh Chalmers, "The IAEA and Nuclear Disarmament Verification: A Primer," *VERTIC Research Reports*, No. 11 (2015), http://www.vertic.org/media/assets/Publications/VM11%20WEB.pdf.

[382] Congress of the United States, "Verification Technologies: Measures for Monitoring Compliance with the START Treaty."

[383] Also applies to the U.S.-Soviet context.

At these levels, verifying and tracking each individual warhead will become critical. This also involves obtaining knowledge about the type and status of a specific warhead and being able to re-authenticate these attributes in later stages of the dismantlement process. Agreements at these levels will also involve new categories of warheads and items, including non-deployed and non-strategic warheads and warhead components.[384] Non-strategic warheads would be impossible to verify through previously employed accounting methods, as these capabilities are deployed on dual-capable launchers and other delivery systems.[385] Unless the arms reduction agreements would also eliminate these dual-capable systems, such as fighter aircraft, the only option would be to individually verify and eliminate warheads.[386] In either case, defining individual warheads as the treaty-accountable item becomes essential when arms control negotiations start addressing nuclear warheads in storage, whether strategic or non-strategic.[387]

III. Past Verification Approaches

The verification mechanisms in the INF, START I and II, and New START have started to approach the issue of individual warhead verification. Importantly, however, the verification provisions thus far have been a binary true/false measurement of the absence of a nuclear warhead.[388] These agreements do not allow the use of radiation detection equipment to confirm an object to be

---

[384] Benjamin Loehrke, "A nuke by any other name," *Bulletin of the Atomic Scientists*, May 12, 2012, http://thebulletin.org/nuke-any-other-name.

Miles Pomper, Nikolai Sokov, and William Potter, "Breaking the U.S.-Russian deadlock on nonstrategic nuclear weapons," *Bulletin of the Atomic Scientists*, December 4, 2009, http://thebulletin.org/breaking-us-russian-deadlock-nonstrategic-nuclear-weapons.

[385] Non-strategic nuclear weapons are defined as shorter-range and lower-yield capabilities, such as ballistic or cruise missiles. (Source: Amy Woolf, *Nonstrategic Nuclear Weapons* (Washington D.C.: Library of Congress, Congressional Research Service, 2016), available at https://www.fas.org/sgp/crs/nuke/RL32572.pdf.)

[386] Steve Fetter *et al.,* "Detecting Nuclear Warheads," *Science & Global Security* 1 (1990): 244;

Benjamin Loehrke, "A nuke by any other name," *Bulletin of the Atomic Scientists*, May 12, 2012, http://thebulletin.org/nuke-any-other-name.

[387] Pomper, Sokov, and Potter, "Breaking the U.S.-Russian deadlock on nonstrategic nuclear weapons."

[388] Murphy and Johnson, "Recovering START Institutional Knowledge," 6.

nuclear, let alone more specific information about warhead characteristics or configuration.[389] As disarmament continues, this may become a key capability requirement for verification provisions, driven by the need to distinguish warheads or their components based on their type or characteristics, not only their nuclear or non-nuclear nature.[390]

Prior efforts to overcome this challenge have explored the use of an attribute verification approach, combined with information barriers that employ complex algorithmic mechanisms embedded to the equipment software or hardware.[391] Attribution verification intends to authenticate a warhead by confirming that the claimed item conforms to a pre-defined set of characteristics, such as the presence of nuclear material, its isotopic composition, and mass above a certain threshold.[392] One of the challenges with this approach is whether it can use sufficiently targeted attributes to authenticate and distinguish warheads.[393] The selected attributes must be unclassified, as they are known to all involved parties, which limits the options that could be considered.[394] States may be concerned that by defining the specific attributes of a certain treaty-limited warhead, they would be disclosing too detailed information about their design and functional characteristics. In the case of the INF Treaty, for example, the United States needed to provide detailed information that would allow the differentiation between the treaty-accountable SS-20 intermediate-range ballistic missiles from the non-limited SS-25 intercontinental ballistic missiles.[395] The challenge was that the missile types used

---

[389] Wuest, "The Challenge for Arms Control Verification in the Post-New START World," 8.

[390] Murphy and Johnson, "Recovering START Institutional Knowledge," 6.

[391] Nuclear Threat Initiative, "Verifying Baseline Declarations of Nuclear Warheads and Materials."

[392] Yan and Glaser, "Nuclear Warhead Verification: A Review of Attribute and Template Systems."

[393] Richard Garwin, "Technologies and Procedures to Verify Warhead Status and Dismantlement," *SIPRI Workshop* (2001), https://fas.org/rlg/010208-sipri.htm.

R. Scott Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads," *Proceedings of the National Academy of Sciences* 113 (2016): 8618–8623.

[394] D.W. MacArthur et al., "The Effects of Information Barrier Requirements on the Trilateral Initiative Attribute Measurement System (AVNG)," *INMM 42nd Annual Meeting* (2001): 2.

[395] Murphy and Johnson, "Recovering START Institutional Knowledge," 2.

the same first stages, including engines and fuel tanks, and were indistinguishable based on external characteristics.[396] In this case, determining the crude fingerprint with a simple neutron detector was sufficient to distinguish the missiles accurately and was acceptable to both the United States and the Soviet Union.[397] Identifying and distinguishing other types of treaty-accountable items, however, may require much more detailed information. The use of non-nuclear attributes has also been proposed in differentiating between weapons types, but these may also be classified and thus unavailable for use as attributes.[398]

The attribute verification approach makes it essential to use information barriers to protect the measurement information. This, however, also makes the measurement system inaccessible to the verifier and thus makes it difficult to establish trust in the obtained data.[399] These requirements result in highly complex systems, making it difficult to simultaneously achieve equipment certification by the host and authentication by the inspector.[400] For information protection purposes, the information barrier used in the Trilateral Initiative contained a threshold comparison analyzer, an output data barrier, a security status monitor, cabinets and cable shielding, and other structures that intended to protect the measurement information.[401] For data collection, the system employed a multiplicity shift register and a multichannel analyzer, as well as an input data barrier, that aimed to ensure legitimate data collection capability.[402] The host concern with the analysis equipment and software, however, is

---

396 Ibid.

397 Ibid., 5.

398 Fuller, "Verification on the Road to Zero: Issues for Nuclear Warhead Dismantlement."

399 MacArthur et al., "The Effects of Information Barrier Requirements on the Trilateral Initiative Attribute Measurement System (AVNG)," 1.

400 National Nuclear Security Administration, "Joint U.S.-U.K. Report," 4.

MacArthur et al., "The Effects of Information Barrier Requirements on the Trilateral Initiative Attribute Measurement System (AVNG)," 2.

401 MacArthur et al., "The Effects of Information Barrier Requirements on the Trilateral Initiative Attribute Measurement System (AVNG)," 5.

402 Ibid., 6.

that extraneous code could be integrated to the system.[403] In addition, these systems must be used with trusted processors, which must adhere to equally strict requirements for non-intrusiveness, transparency, and authenticity, and validity.[404] Mistrust in the use of information barriers also emerges at the processor level, as reflected in Russia's engagement in developing their own trusted processor design based on a specific set of priorities.[405]

Information barriers are necessary for the system's ability to protect information, but on the other hand, also make certifying and authenticating the equipment very difficult. This may be technically feasible, especially as their development goes further. From a political perspective, however, this complexity and lack of transparency could be used against them. It would be easy to argue – as the Russians did towards the end of the Trilateral Initiative – that they will require a significant amount of time to certify the equipment, and even then, they may not be able to gain sufficient confidence that it would not conduct proscribed measurements or collect the data clandestinely. This time burden and trust deficiency could eventually be used as a reason to disqualify these systems from actual use, which would facilitate a justification for not proceeding with disarmament. This highlights the dual-use nature of verification as a political tool – it can be used as a confidence-building asset, but also as a means of fostering suspicions.

The template approach employs a different strategy in warhead verification, relying on differential measurements between an inspected item and one that is known to be authentic.[406] The basic axiom is that if an item is sufficiently similar, in ideal conditions identical, to a warhead that has

---

[403] Ibid.

[404] Vyacheslav Kryukov et al., "Trusted Processor: A Result of the Evolution of Information Barrier Technologies," *INMM 48th Annual Meeting* (2007): 2.

[405] Ibid., 1.

[406] Differential measurement refers to the fact that only the difference between two physical quantities is being measured, rather than the absolute amounts. (Source: Yan and Glaser, "Nuclear Warhead Verification: A Review of Attribute and Template Systems.")

previously been proven as authentic, it can legitimately be declared as a warhead as well.[407] Comparative measurement systems based on the template approach can be designed to be simpler and easier to authenticate and certify, but in traditional template verification systems, information barriers are still needed to protect the collected data.[408] These past efforts to develop template-based approaches include the Nuclear Material Identification System (NMIS) by the Oak Ridge National Laboratory; the Controlled Intrusiveness Verification Technology (CIVET) system, developed by the Brookhaven National Laboratory; the Trusted Radiation Identification System (TRIS) by the Sandia National Laboratories; and the Next Generation Trusted Radiation Identification System (NG-TRIS) by Sandia as well.[409] The development of these systems has also been driven by the need of nuclear weapons states to identify their own warheads.[410] These measurements systems have a demonstrated ability to distinguish between warhead and component types, but all of them rely on information barriers and as a Russian assessment of the CIVET system shows, important concerns about intrusions remain.[411] Particularly, the systems preserve the template data, which represents the classified warhead signature and thus needs to be protected throughout the verification process.[412]

---

[407] Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads."

[408] Peter Merkle et al., "Next Generation Trusted Radiation Identification System," *INMM 51st Annual Meeting* (2011), https://www.nti.org/media/pdfs/SNL-1_FINAL_INMM_2010_Next_Generation_Trusted_Radiation_System.pdf?_=1438113016.

Peter Marleau and Erik Brubaker, "An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System," *INMM 57th Annual Meeting* (2016): 2.

[409] Committee on International Security and Arms Control, National Research Council, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities,* 99.

Yan and Glaser, "Nuclear Warhead Verification: A Review of Attribute and Template Systems," 160.

[410] Committee on International Security and Arms Control, National Research Council, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities,* 99.

[411] Peter Vanier et al., "Study of the CIVET Design of a Trusted Processor for Non-Intrusive Measurements," INMM 42nd Annual Meeting (2001).

[412] National Nuclear Security Administration, "Highlights, February 2011," *Defense Nuclear Nonproliferation, Office of Nonproliferation and Arms Control* (2011), https://nnsa.energy.gov/sites/default/files/nnsa/inlinefiles/NIS%20February%202011%20Highlights.pdf, 5.

Most systems developed thus far have used gamma-ray or neutron spectra as the signature, but it would be possible to use other, non-nuclear characteristics as well.[413]

Novel verification protocols developed in the past several years have overcome the use of information barriers by employing physical measurement methods that inherently protect classified information.[414] These protocols employ physical cryptography to protect classified information, conforming to the idea of zero-knowledge proofs. Their strength in circumventing the use of information barriers by using the zero-knowledge property, however, has also created challenges that remain unsolved. First, while these novel approaches push the issue of information protection from electronic barriers to physical ones, all implementations thus far require the host to maintain some aspects of the measurement system secret in order to maintain the zero-knowledge property of the protocol. Second, all the current implementations of these protocols are based on template verification protocols, which rely on the use of an authentic reference warhead. Even if the measurements conclusively prove that the two compared items are identical, this result doesn't provide assurance of the authenticity of the reference warhead. This 'golden warhead' challenge remains the core challenge in all template verification systems, whether based on traditional or zero-knowledge protocols.

IV. General Idea of Zero-Knowledge Proofs in Cryptography

Goldwasser *et al.* introduced interactive proof systems for the first time in 1985, establishing a computational complexity measure that would determine how much additional knowledge is needed, apart from the end result, to prove a theorem to be true.[415] The insight was that interaction between

---

[413] Committee on International Security and Arms Control, National Research Council, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities,* 99.

[414] Philippe, Barak, and Glaser, "Designing Protocols for Nuclear Warhead Verification."

[415] Shafi Goldwasser, Silvio Micali, and Charles Rackoff, "The Knowledge Complexity of Interactive Proof-Systems," *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing* (1985): 291, https://groups.csail.mit.edu/cis/pubs/shafi/1985-stoc.pdf.

the prover and the verifier would allow this to be zero in an ideal case, constituting a zero-knowledge proof.[416] The main application of these proofs are in cryptographic protocols, which are communication mechanisms that ensure the confidentiality, authentication, and integrity of interactions in an insecure environment.[417] When cryptographic protocols employ zero-knowledge proofs, the authentication of a statement or other exchange of knowledge is done without revealing the underlying solution or any additional information.[418]

Three important properties apply to all zero-knowledge proofs – completeness, soundness, and zero-knowledge.[419] In the ideal case, these properties are fully true, but in non-ideal conditions they exist on a probabilistic distribution, defining a completeness error and a soundness error for the protocol.[420] Completeness refers to the fact that an honest verifier can always be convinced of the truthfulness of a genuinely true statement by an honest prover. Thus, with perfect completeness, the likelihood of false negatives is zero. Soundness, on the other hand, controls for false positives – if a statement is false, a cheating prover could not prove it to be true to an honest verifier. As with completeness, however, soundness is not necessarily perfect. Lastly, the zero-knowledge aspect certifies that even when cheating, the verifier cannot learn any information about a correct proof or from an honest prover.[421]

Commitment protocol is another important dimension of zero-knowledge proofs.[422] Here, the first party to an interaction commits to some value, which remains hidden to the second party

---

[416] Ibid.

[417] Ling Dong and Kefei Chen, *Cryptographic Protocol* (Beijing: Springer, 2012): 2.

[418] Goldwasser, Micali, and Rackoff, "The Knowledge Complexity of Interactive Proof-Systems," *ACM Symposium*, 188.

[419] Ronen Gradwohl et al., "Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles," *Lecture Notes in Computer Science* 4475 (2008): 2, https://guyrothblum.files.wordpress.com/2014/11/gnpr07.pdf.

[420] Ibid.

[421] Ibid.

[422] Ibid., 3.

throughout the proof process. After the proof has been completed, however, the two parties can decide to reveal or decommit the value. This enables the second party to learn the value and ensure that it was what was originally agreed. This leads to binding, meaning that after the second party knows the unique value, it is impossible for the first party to change it.[423]

V. Physical Zero-Knowledge Proofs

The concept of zero-knowledge proofs can also be applied to propositions relating to the physical world.[424] In this context, zero-knowledge proofs verify propositions about physical properties of objects without revealing any information apart from the true/false result. Physical zero-knowledge proofs can be carried out without the involvement of computers, only through human-aided implementation of the protocol in question. This is a key feature of the protocols, addressing the confidentiality and integrity issues that the involvement of computers may create. It is also possible to construct hybrid systems that are based on human-implemented systems that are also complemented by hardware, such as physical measurement systems. Only one of the parties has full access to the considered object and the measurement system, with the intent of keeping them out of bounds to the verifier but still being able to verify the obtained results.[425]

Physical zero-knowledge proofs can be formalized using Universally Composable (UC) security framework, under which a physical protocol is separated into a logical and physical layer.[426] The logical layer exists in a hybrid world, which is essentially a reduced and abstracted version of the real world. The physical measurements of the protocol only interact with the physical layer, but any

[423] Ibid.

[424] Ben Fisch, Daniel Freund, and Moni Naor, "Physical Zero-Knowledge Proofs of Physical Properties," *Proceedings from CRYPTO 2014: Advances in Cryptology* (2014): 313.

[425] Ibid., 315.

[426] Ibid., 316.

interaction at this level also creates an effect on the logical layer in the hybrid reality. The verifier has access only to this logical layer, but the universal composition property implies that the knowledge obtained from this layer also reflects the nature of the physical layer. Thus, the properties of zero-knowledge proofs – completeness, soundness, and zero-knowledge – can be computed at the level of the logical layer. As any statement that is valid on the logical level in the hybrid world is also valid in the physical world, the inspector also can be convinced of the correctness or incorrectness of the original proposition in the real world.[427]

VI. Application to Warheads

Applying the idea of physical zero-knowledge proofs to warhead verification could be instrumental for addressing the conflict between state interests in confidentiality and inspector concerns about transparency.[428] When applied in this context, the host state serves in the role of the prover, and the inspecting agent or agency conforms to the role of the verifier.[429] The nature of the propositions, relating to warhead properties, defines the conditions of the protocol and could theoretically represent either an attribute or template verification approach. Proving a proposition such as *"The fissile material at the core of this warhead has a ratio of* ^{240}Pu *to* ^{239}Pu *of less than 0.1 and thus represents an authentic warhead"* would represent an attribution statement, derived from the conditions defined in the Trilateral Initiative, and could be assessed using physical zero-knowledge proofs.[430] The

[427] Ibid.

[428] Goldwasser, Micali, and Rackoff, "The Knowledge Complexity of Interactive Proof-Systems," 291.

Uriel Feige, Amos Fiat, and Adi Shamir, "Zero-Knowldege Proofs of Identity," *Journal of Cryptology* 1 (1988): 77, http://s3-ap-southeast-1.amazonaws.com/erbuc/files/a60459e4-bcf1-421c-a3a5-9e8f79aa8be8.pdf.

Shafi Goldwasser, Silvio Micali, and Charles Rackoff, "The Knowledge Complexity of Interactive Proof-Systems," *SIAM Journal on Computing* 18, no. 1 (1989): 186, http://crypto.cs.mcgill.ca/~crepeau/COMP647/2007/TOPIC01/GMR89.pdf.

[429] Goldwasser, Micali, and Rackoff, "The Knowledge Complexity of Interactive Proof-Systems," *SIAM*, 186.

[430] Thomas Shea and Laura Rockwood, "Nuclear Disarmament: The Legacy of the Trilateral Initiative," *Deep Cuts Working Paper*, no. 4 (2015): 15, https://www.files.ethz.ch/isn/192450/DeepCuts_WP4_Shea_Rockwood_UK.pdf.

statement *"The radiographic signature of this warhead is statistically indistinguishable from that of a pre-authenticated warhead of the same type and thus the warhead is authentic,"* on the other hand, would refer to a template verification protocol and could similarly be proven using physical zero-knowledge proofs.[431]

The concept of physical zero-knowledge proofs from this abstract mathematical level has been demonstrated in practice using the template verification approach.[432] These proposals employ physical measurement systems that inherently protect the sensitive information contained by warheads. These measurement systems are non-electronic, which prevents interference and tampering with the system before, during, or after the measurement.[433] The approaches have been proven capable of achieving the principles of completeness, soundness, and zero-knowledge in the correct conditions.[434] As discussed earlier, the last principle only remains true if the host maintains honesty.[435] Thus, the zero-knowledge property requires the host to follow the procedure, but it is resistant to verifier cheating – no sensitive information can be leaked even if the verifier does not follow the protocol.[436]

VII. Neutron Radiographic Profile Comparison

The idea proposed by Glaser *et al.* from Princeton University employs differential measurements of the neutron radiographic profiles of warheads.[437] As was discussed in the previous

---

[431] Philippe, Barak, and Glaser, "Designing Protocols for Nuclear Warhead Verification," 7.

[432] Alex Glaser, Boaz Barak, and Rob Goldston, "A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol," *INMM 53rd Annual Meeting* (2012): 1, http://www.boazbarak.org/Papers/nuclear-zk.pdf.

[433] Sébastien Philippe, Robert Goldston, Alexander Glaser, and Francesco d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification," *Nature Communications* 7 (2016), http://www.nature.com/articles/ncomms12890.

[434] Philippe, Barak, and Glaser, "Designing Protocols for Nuclear Warhead Verification," 7.

[435] Goldwasser, Micali, and Rackoff, "The Knowledge Complexity of Interactive Proof-Systems," *SIAM,* 196.

[436] Ibid.

[437] Glaser, Barak, and Goldston, "A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol," 1.

Philippe, Goldston, Glaser, and d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification."

chapter, neutron radiographs are created by allowing neutrons to penetrate material and then measuring this transmission with detectors on the other side of the object. The system used in this approach does not record the neutron signatures of the two warheads being compared, but instead utilizes superheated emulsion detectors as a proxy for carrying out the comparison.[438] These emulsion detectors are made of superheated octafluorocyclobutane (C_4F_8) that are made to be sensitive to neutrons above 1 MeV, but insensitive to gamma radiation.[439] In addition, the emulsion detectors do not reveal information about neutron multiplicity, only about neutron fluence.[440] When neutrons that pass through the inspected object interact with the superheated emulsion, macroscopic bubbles are generated in the emulsion matrix.[441] This is because the matrix is in a meta-stable state and contains specific sites that can undergo vaporization when a small amount of energy enters the system, such as through a neutron.[442] Thus, the neutron radiographs of the warheads are manifested as 'bubbles' on the superheated emulsion detectors. These bubbles can be counted with magnetic resonance imaging or optical tomography, and the neutron count in each detector is reflected as a pixel in the final image.[443] The detectors can be certified at any point by using a calibrated neutron source, or using a test object to check the calibration data given by the host state.[444]

The neutron source used in the system is a 14 MeV collimated neutron beam, with a 4-minute exposure time that creates a maximum of 1,200 bubbles (N_{max}), with some variance inherent to the

---

438 Philippe, Goldston, Glaser, and d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification."

439 Ibid., 6.

440 Alexander Glaser, Boaz Barak, and Robert Goldston, "Toward a Secure Inspection System for Nuclear Warhead Verification Without Information Barrier," *INMM 54th Annual Meeting* (2013): 3.

441 Robert Goldston et al., "Zero Knowledge Warhead Verification: System Requirements and Detector Technologies," *INMM 55th Annual Meeting* (2014): 4.

442 S. G. Vaijapurkar, "The performance evaluation of gamma- and neutron-sensitive superheated emulsion (bubble) detectors," *Radiation Protection Dosimetry* 130 (2008): 286.

443 Goldston at al., "Zero Knowledge Warhead Verification: System Requirements and Detector Technologies," 1.

444 Glaser, Barak, and Goldston, "Toward a Secure Inspection System for Nuclear Warhead Verification Without Information Barrier," 3.

measurement system. This system is depicted in Figure 5.1. The 14 MeV neutrons were decided on the basis that these penetrating high-energy neutrons are sensitive enough for differences both in geometric conformation and material composition of the warhead.[445] Neutrons at this energy, however, may not be able to sufficiently distinguish between fissile and fissionable materials, but combining the use of 250 keV neutrons could solve this potential challenge.[446] The neutron source used was a deuterium-tritium neutron generator, which yields approximately 10^8 neutrons per second.[447] The exposure time is dependent on what the target number, N_{max}, of bubbles is, which also determines the confidence level in the experiment. The variance associated with the detectors is shown in Figure 5.2.

[445] Philippe, Goldston, Glaser, and d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification," 4.

[446] Goldston et al., "Zero Knowledge Warhead Verification: System Requirements and Detector Technologies," 1

[447] Philippe, Goldston, Glaser, and d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification," 6.

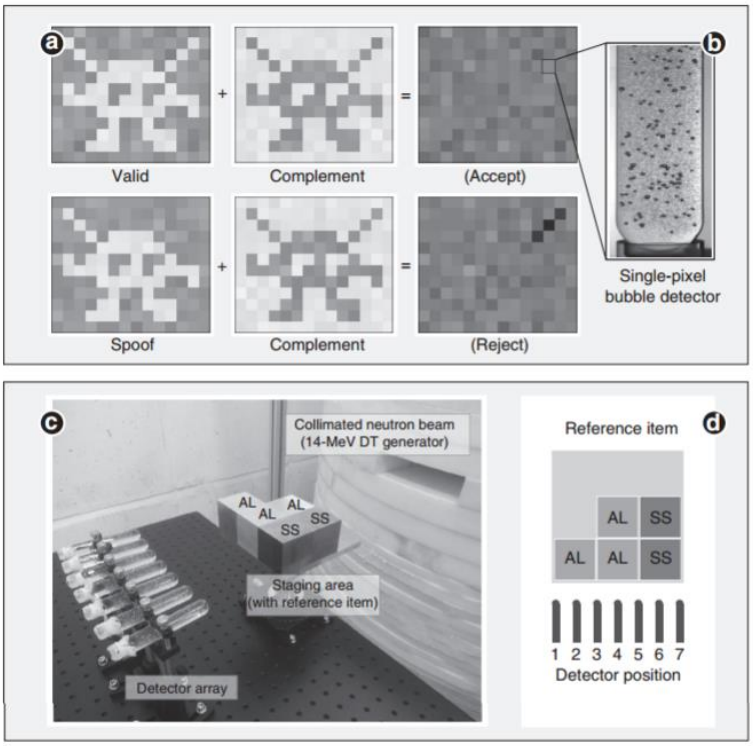

Figure 1 | Experimental realization of a physical zero-knowledge object comparison system. (**a**) Concept of zero-knowledge differential neutron radiography using superheated droplet detectors. Items are exposed to a neutron beam and their 2D transmission radiographs are recorded on detectors preloaded with the complement radiograph (including Poisson noise) of a reference item. If the item is valid (identical to the reference), the final radiograph is identical to the expected exposure if no object had been present (in the ideal implementation the root mean square deviation from the expected bubble count, N_{max}, is solely because of Poisson noise, $(N_{max})^{0.5}$). If the item is a spoof with an experimentally significantly different radiograph, some characteristic features appear in the final radiograph (the results are no longer zero-knowledge) and the inspector rejects the proof. Each pixel represents the bubble count from a single superheated droplet (bubble) detector. (**b**) Picture of an irradiated superheated droplet (bubble) detector. Some metastable droplets vapourized and expanded into macroscopic bubbles after a neutron interaction. The bubble count reflects the total fluence delivered to the detector. (**c**) One-dimensional experimental realization with superheated droplet detector array, reference item (black box hood not shown) on staging area and aperture of a 14 MeV collimated neutron beam. The set-up is placed in a room shielded with borated concrete walls. A fast neutron counter (not shown) monitored the source fluence along the axial direction. (**d**) Composition and pattern of the reference item with detector positions (AL, aluminium; SS, stainless steel).

Figure 5.1. The system design incorporates the principle of template approach (a), superheated emulsion detectors (b), neutron radiography (c), and positional variance (d). Source: Sébastien Philippe, Robert Goldston, Alexander Glaser, and Francesco d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification," *Nature Communications* 7 (2016), 3.

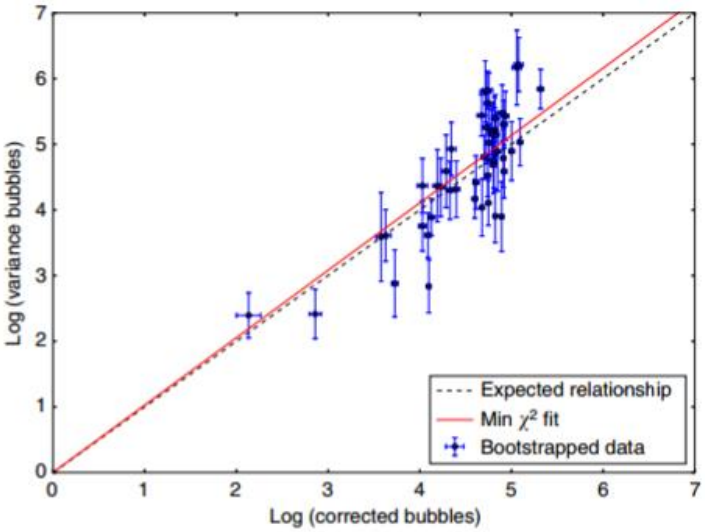

Figure 4 | Analysis of the superheated droplet detector variance. Plot of the logarithm of the variance versus the logarithm of the average number of true (corrected) bubbles. The data and one s.d. error bars were obtained by bootstrapping the corrected experimental results (1,000 samples per data point).

Figure 5.2. The variance associated with the superheated emulsion detectors. Source: Sébastien Philippe, Robert Goldston, Alexander Glaser, and Francesco d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification," *Nature Communications* 7 (2016), 6.

The fluence response function, f reflects the relationship between neutron interactions, whose number depends on the neutron fluence that arrived at the detector, and the resulting bubble count. This establishes the calibration of the equipment, which can be certified by the inspector at any point. After this, unique radiographs of warheads can be measured, determined by its configuration, shielding, and material properties, and with the measurements being dependent on the fluence response function. The complimentary radiographs can be created through an inverse of the fluence response function.[448]

[448] Ibid.

In the first stage of the protocol, the complement neutron radiograph of the reference warhead is preloaded into the detector.[449] This pre-loading phase is done privately by the host, without inspector access to the system. Next, the inspected warhead is irradiated, with the resulting signature being added to the preloaded detectors. If the two warheads are sufficiently similar – in the optimal case, identical – the inverse signature that was preloaded, and the newly measured signature, should complement each other and the end result should be essentially a blank reading, only reflecting the Poisson noise in the measurement environment. This is because the spread of neutrons is inherently governed by Poisson statistics, similar to many other physical measurement data.[450] Any deviation from this should be due to the statistical error in the measurement process, which can be corrected partially via calibration, or the small variance in the reference radiographs. The ability to repeat the measurements, however, allows the inspector to determine the acceptable margin for error for false positives and negatives.[451]

Experimental results from the verification approach are shown in Figures 5.3-5.6. Figure 5.3, panel a, shows the difference between a valid item and different diversion scenarios, and has been corrected for occultation, or the fact that some of the bubbles are hidden in the bubble counting process.[452] It is evident that the spoofs can be distinguished from the valid item, with each diversion scenario providing a different pattern. Panel b shows how the experimental results compare with the computational Monte Carlo simulations.

---

[449] Ibid.

[450] MIT Department of Physics, "Poisson Statistics," July 8, 2004, available at http://123.physics.ucdavis.edu/week_0_files/Poisson.pdf.

William Noonan, "Neutrons: It Is All in the Timing – The Physics of Nuclear Fission Chains and Their Detection," *Johns Hopkins Applied Technical Digest* 32, no. 5 (2014): 766, available at http://techdigest.jhuapl.edu/TD/td3205/32_05-Noonan.pdf.

[451] Philippe, Goldston, Glaser, and d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification."

[452] Ibid., 6.

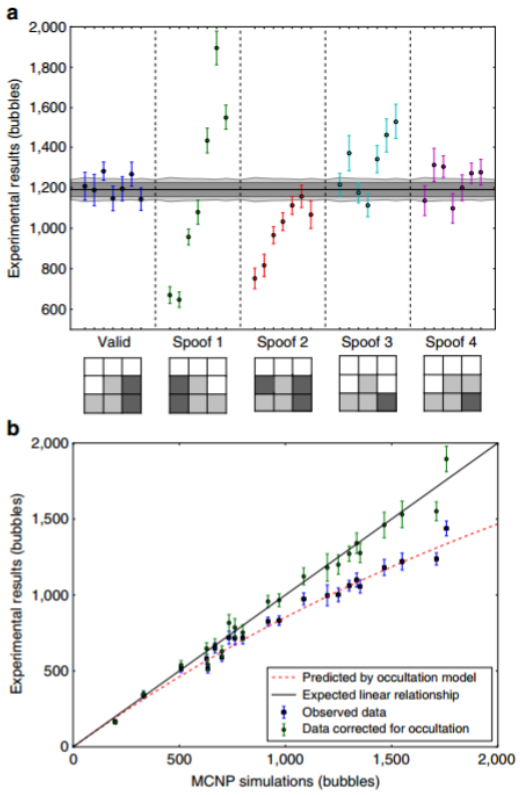

Figure 2 | Experimental evidence of a practical physical zero-knowledge proof. (**a**) Experimental results for the five inspection scenarios investigated (valid item and four spoofs denominated Spoof1 to Spoof4). The item patterns are represented for each scenario with white as empty, light grey as aluminium and dark grey as steel. The results are corrected for the nonlinear counting effect. Error bars represent one s.e.m. calculated at each detector position from the 10 measurements performed for each scenario and the calibration data (obtained from 10 measurements with no item). The light grey band around N_{max} represents the expected error from a valid item $(2N_{max}+N_{ref})^{0.5}$. The dark grey band corresponds to the minimum achievable value with N_{max} bubbles, $(N_{max})^{0.5}$. The test statistic $T=\sum_{i=1}^{7}\frac{(N-N_{max})^2}{2N_{max}+N_{ref}}$ was compared with a χ^2 distribution with 7 degrees of freedom, giving the following results for each scenario: Valid, $T=6.60$, $P=0.474$; Spoof 1, $T=453.35$, $P<10^{-16}$; Spoof 2, $T=132.72$, $P<10^{-16}$; Spoof 3, $T=87.80$, $P=3.\,10^{-16}$; Spoof 4, $T=17.88$, $P=0.013$. (**b**) Observed and deduced true bubble count, from all scenarios at every position with interposed objects, versus corresponding Monte Carlo simulations obtained from the computational model of the experiment. The red dashed curve is obtained from our bubble occultation model using the calibration data with no interposed objects (see Methods). Error bars represent one s.e.m. calculated from measurements and calibration data.

Figure 5.3. Experimental results from detector exposure (a) and comparison to Monte Carlo simulations (b). Source: Sébastien Philippe, Robert Goldston, Alexander Glaser, and Francesco d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification," *Nature Communications* 7 (2016), 5.

As was discussed before, neutron counts on the detectors can be reflected as pixels to form an image. This is reflected in Figure 5.4, where the resulting images of the detector arrays are shown. When the comparison of the reverse radiograph of the template (middle image) is subtracted from a valid item (left), only Poisson noise would be visible in the resulting comparison. If this reverse radiograph is compared to a significantly different spoof item, the resulting comparison will reflect this. These diversion scenarios are shown in Figure 5.5. These results show that any modifications to the reference or the inspected item, both in terms of configuration or material composition, could be detected. Importantly, the physical implementation of the system did not reveal the underlying information about identical items, reflecting the zero-knowledge nature of the system.[453]

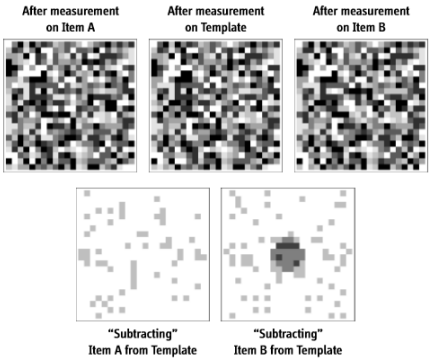

Figure 3: TOP: Status of detector arrays after measurements on a valid item (left), on the template (middle), and on an invalid item (right). As before exposure, all patterns are random, and inspectors can have full access to them. BOTTOM: After subtracting a pair of patterns, the data can be used to distinguish valid from invalid items. If a valid item is presented (left), the patterns are equivalent and only statistical noise is present; if an invalid item is presented, statistically significant differences appear. In this case, 800 grams of plutonium have been removed from the pit. 14 MeV neutrons, MCNP 5 simulations, 10 billion source neutrons.

Figure 5.4. The comparison of a valid and invalid item based on the template approach. Source: Alexander Glaser, Boaz Barak, and Rob Goldston, "A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol," *INMM 53rd Annual Meeting* (2012), 8.

[453] Ibid.

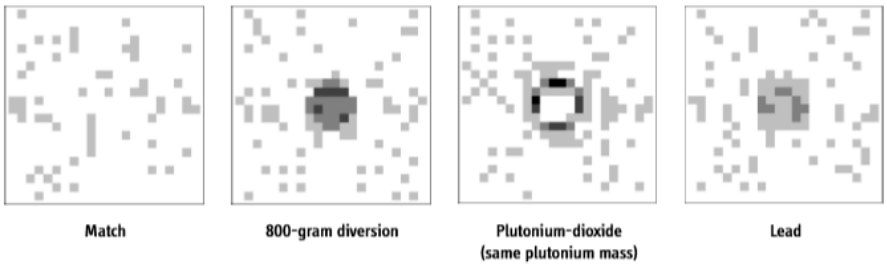

Figure 4: Different types of diversion scenarios can be distinguished using the proposed zero-knowledge protocol using modular arithmetic. MCNP 5 simulations.

Figure 5.5. The Monte Carlo simulation results from a match scenario and three diversion scenarios. Source: Alexander Glaser, Boaz Barak, and Rob Goldston, "A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol," *INMM 53rd Annual Meeting* (2012), 8.

Inspector and host interaction with the system is a critical dimension of the implementation of the approach.[454] After the preloading is done, the host must offer a certain number of pre-loaded detectors and their calibration data to the inspector, who randomly chooses which ones are used in the measurements. The rest can still be tested for their proper functionality. In addition, the protocol also involves several warheads that could be chosen for verification by the inspector. Since the host claims that all of the warheads are of the same type as the reference warhead(s), then any combination should result in a valid result. The randomization facilitated by these two choice conditions is intended to prevent the host from modifying the reference warhead such that it would match the warhead being verified. In addition, both parties are allowed to monitor the source neutron fluence to ensure that the agreed amount is being transmitted to the detector.[455] Overall, the zero-knowledge nature of the system is dependent on the host following the protocol, as the host must offer a warhead that matches the template in order to prevent any information from being revealed. If this is not the case, the

[454] Peter Marleau et al., "Zero Knowledge Protocol: Challenges and Opportunities," *INMM 56th Annual Meeting* (2015): 6.

[455] Philippe, Goldston, Glaser, and d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification."

resulting bubble count, N_{max}, will differ from the expected one, and may convey sensitive information.[456]

VIII. Isotopic Tomography Approach

A second implementation of a physical cryptographic system, proposed by Kemp *et al.* from the Massachusetts Institute of Technology, has important conceptual similarities with the approach proposed by Glaser *et al.*, but also clear differences. The approach is based on the proposition that if a warhead is identical, or sufficiently identical, to an authentic warhead configurationally, spatially, isotopically, and is otherwise comparable in macroscopic features, then it is an authentic warhead as well. While there can be microstructural differences that are not captured by these comparison points, it would be exceedingly difficult to manufacture a mock warhead that would only diverge from the authentic warhead at a microscopic level. Thus, the appropriate physical measurement system must be able to accurately determine these macroscopic features, but it does not need to distinguish microscopic structure.[457]

The system of choice is isotopic tomography, which allows the determination of the distribution of each isotope present in the warhead and creates a single-pixel radiograph of the template and inspected warheads, with the measurements taken at random orientations.[458] The measurement system is shown in Figure 5.6 and 5.7. The two signatures are created through three-dimensional information, but the reduction of the image conceals the actual spatial composition of the objects. The isotopic tomogram, depicting the warhead, is created through transmission nuclear-resonance fluorescence that employs a monoenergetic high-energy X-ray beam. In simulations of the

[456] Glaser, Barak, and Goldston, "Toward a Secure Inspection System for Nuclear Warhead Verification Without Information Barrier," 4.

[457] Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads."

[458] Ibid.

system, a bremsstrahlung X-ray source was used as a photon source, which is not ideal from the perspective of information processing or radiation dose, but other options are also available.[459]

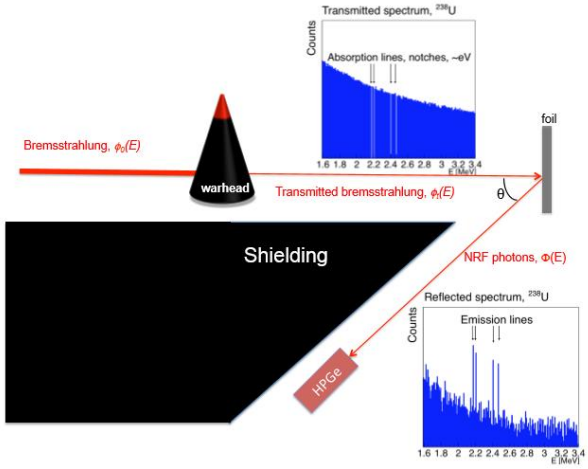

Figure 5.6. The system design in the Kemp et al. approach. Source: R. Scott Kemp et al., Figure S.3, "Supporting Information Physical Cryptographic Verification of Nuclear Warheads," for R. Scott Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads." *Proceedings of the National Academy of Sciences* 113 (2016): 8618–8623.

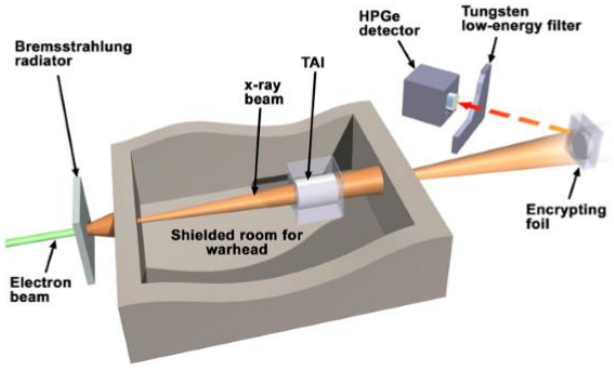

Fig. 1. Schematic of measurement apparatus. TAI is the treaty accountable item, either the template nuclear warhead or candidate warhead and its packaging.

Figure 5.7. The system design in the Kemp et al. approach. Source: R. Scott Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads," *Proceedings of the National Academy of Sciences* 113 (2016): 8619.

[459] Bremsstrahlung or 'braking' radiation refers to x-rays generated when decelerating electrons (for example, those hitting a metal) emit electromagnetic radiation.

The warhead contains a large number of nuclei from different elements, each of which will absorb photons of certain energy from the beam, based on their unique absorption spectrum. These spectra are unique to each isotope and can thus be used to identify each material. The confluence of these interactions between the beam and the warhead materials, reflected as absorption lines in the beam spectrum, depends on the structural and isotopic features of the warhead.[460] When these measurements are repeated at different orientations, the overall geometry of the warhead is produced. This information contained in the beam, however, is not directly collected by the measurement system, as it would reveal the warhead structure. The beam travels through foils, which are composed of the isotopes of interest at different concentration levels and thus also interact with the beam. Some of the photons in the beam are still at energy levels that can be absorbed by the foil nuclei, if a resonant isotope is present. When the excited foil nuclei return to the ground state, a gamma ray is emitted. This nuclear-resonance fluorescence, which is a function of both the warhead and foil characteristics, is detected by high-purity germanium (HPGe) detectors and constitutes the final, unclassified results. Using the same foil, but measuring different items, thus enables the comparison of these results and determines whether or not the objects are identical.[461]

Sensitive information is inherently protected by the system, as long as the composition of the foil remains secret.[462] Thus, the foil serves the role of a one-time-pad physical encryption key. The foil is created by the host, who maintains possession of the device throughout the measurement process and discards it after the process has been completed. The foils should contain a minimum level of all agreed isotopes and thus produce a minimum signal in the final results, which allows the inspector to certify the sensitivity of the foil. The inspector leads the measurement process and defines the specific

[460] Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads."

[461] Ibid.

[462] Ibid.

measurement orientations, which constitutes one obstacle to cheating from the host side.[463] In this method, similar to the previously described neutron-based approach, confidence can be built through having a large number of reference and inspected warheads available from which the inspector will choose.

Simulations of the system illustrate that it is able to detect several spoof scenarios, including some that may be indiscernible through other radiological techniques.[464] In general, information protection is inherent to the physical processes used by the system, but some concerns remain about the inspector's ability to discern estimations of the foil or the warhead's composition. These can be managed through different physical and mathematical approaches, enabling a level of confidence that is acceptable in practical conditions. The system has not been demonstrated in a real setting, however, which creates both opportunities and challenges.

One important concern in this approach is that the foil, or the physical cryptographic key, is completely inaccessible to the verifier. Compared to the previous approach, which constructed a physical template through the superheated emulsion detectors, this does not provide anything tangible for the inspector to assess after the measurement. This could be a concern, if the inspector wanted to certify that no interference had taken place during the process.

A critical challenge in both the Glaser *et al.* and Kemp *et al.* approaches is that the template and the instrumentation becomes inaccessible to the inspector after they have been prepared for measurement.[465] Both ideas pre-load the measurement system with sensitive information, which also rules out inspector access to the system after the measurement has been completed. In the Glaser *et*

[463] Ibid.

[464] Ibid.

[465] Marleau and Brubaker, "An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System," 1.

al. proposal, the host preloads a reverse radiographic signature to the detector, which is not revealed to the inspector. Furthermore, the positive result would be a null result within a certain margin of error, which would not allow the inspector to understand what the starting point was. In the Kemp *et al.* proposal, the host constructs the foil and maintains its composition as a secret throughout the experiment, discarding it after use. These approaches make it impossible for the inspector to authenticate the template or the measurement system after the conclusion of the measurement process.[466]

IX. Two-Dimensional Imaging Approach

A third approach developed by Marleau *et al.* at the Sandia National Laboratories intends to solve this challenge by not preloading the system with any sensitive information.[467] This would allow the inspector to authenticate the instrumentation post-measurement, which would provide confidence that there was no interference during the measurement process. The system still conforms to the principle of zero-knowledge proofs by not measuring sensitive information during the process. A key difference to the previous approaches is also that the blank result is maintained throughout the dynamic measurement process, as opposed to only becoming evident at the end. This could enable the verifier to interact with the system during the measurement process, not only in assessing the end results.[468]

The system combines a two-dimensional time-encoded imaging (2D-TEI) system and a neutron-emitting source to create a high-resolution radiograph of the items under measurement.[469] This system is shown in Figure 5.8. This measurement concept is referred to as CONFIDANTE

[466] Ibid.

[467] Ibid., 2.

[468] Ibid., 3.

[469] Ibid.

(CONfirmation using a Fast-neutron Imaging Detector with Anti-image NULL-positive Time Encoding), highlighting the fact that no information barriers are needed in the measurement process. The 2D-TEI is a cylindrical coded mask, composed of high density polyethylene, that rotates around the item under measurement. In the center, there are one or more deep liquid scintillator cells, which serve as the detector pixel. These pixels are time-encoded, with the rate being modulated by the mask rotation. Here, the information about the radiation fields produced by the warheads is composed into the coded mask, which is essentially a manifestation of the warhead design and composition.[470] This is shown in Figure 5.9.

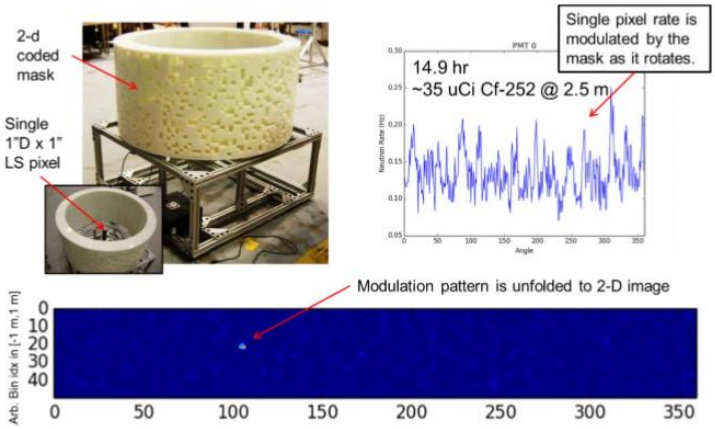

Figure 1 – The proof-of-concept time encoded imager (upper left) consists of a single 1" diameter by 1" deep liquid scintillator cell surrounded by a rotating cylindrical high density polyethylene coded mask. The modulated neutron detection rate (upper right) has the entire 2-dimensional field of view encoded in its pattern. The Maximum Likelihood Expectation Maximization (MLEM) unfolded image is shown (bottom).

Figure 5.8. The system design for the Marleau et al. approach. Source: Peter Marleau and Erik Brubaker, "An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System," *INMM 57th Annual Meeting* (2016): 3.

[470] Ibid., 4.

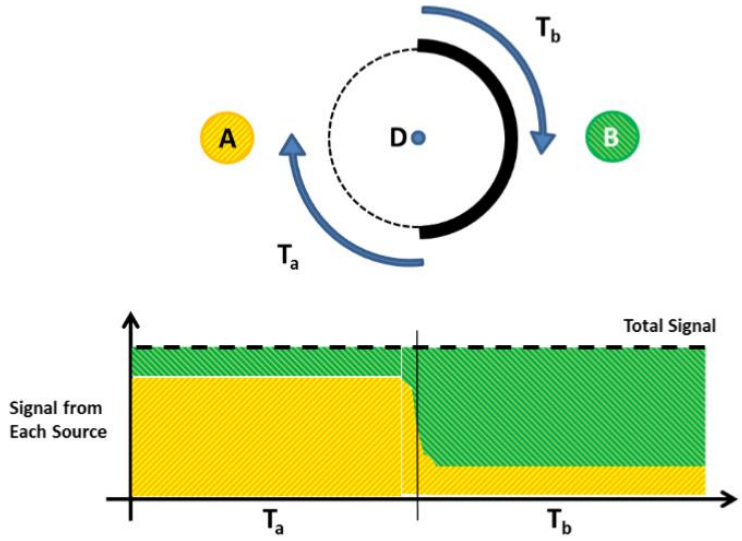

Figure 2 – (Top) Top view of an illustration of the proposed concept using the simplest example of a mask designed with one half as the anti-mask of the other. (Bottom) If A and B are identical, then the sum of signals (y-axis) will be constant as a function of rotation angle (x-axis) even though the contributions from A and B vary.

Figure 5.9. The principle of the two-dimensional imaging system. Source: Peter Marleau and Erik Brubaker, "An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System," *INMM 57th Annual Meeting* (2016): 5

Similar to the Glaser *et al.* method, the system protects sensitive information by superimposing the reverse measurement result of the reference warhead with the measurements obtained from the inspected warhead.[471] The reverse result has the opposite modulation from the other result. In practice, the comparison is carried out by constructing the mask out of two parts, with the first half of the mask pattern being the anti-mask of the reference warhead and the second half the mask of the inspected warhead. The cylindrical mask is placed between the two warheads under measurement. As the cylindrical mask rotates, the signals are superimposed, with the contributions from each direction varying as a function of the measurement angle. Since the signals from the two warheads are complements of each other, the resulting signal should always be the same (blank) independent of the

[471] Ibid.

rotation angle. The resulting signal should only reflect random noise that is inherent to any physical measurement system.[472]

Modeling this system with two identical items creates a count value distribution that is similar to expected random noise (Poisson noise).[473] The variance between the noise in the measurement results and an ideal Poisson distribution is reflected in the Feynman Y value, which essentially measures how Poisson-like the noise is. In the ideal case, where the noise consists only of statistical noise, the Feynman Y value should be zero. Experimentally, comparing two identical items produces a result very close to that.[474] Experimental results of the system are shown in Figures 5.10 and 5.11. Knowledge of the count distribution, however, would not allow the reconstruction of the original source distributions, since the signal is a summation of complements. This is only true, however, if the two measured items are identical and symmetrically aligned. In the case that only one item is present, or that the two measured items are very different in configuration, it is possible to infer the source configurations based on the measurement data. This may create the risk of information disclosure, including in situations where two identical warheads are improperly situated vis-à-vis the cylinder.[475] Thus, the count distribution may need to be modified through sequestration or other means to prevent any information being accidentally or purposefully revealed in the process.[476]

[472] Ibid.

[473] Ibid., 6.

[474] Ibid., 8.

[475] Ibid., 9.

[476] Ibid.

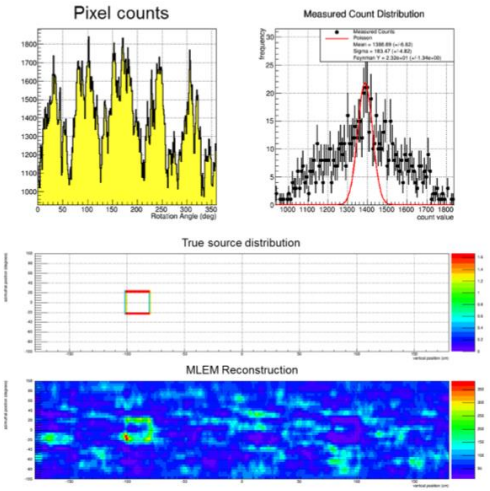

Figure 3 – Results from a simulation of a single object centered at (-90, 0). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top, left panel. The red line is the expectation if the distribution were consistent with purely statistical (Poisson) noise. (Center) The true source distribution used to generate the pixel count values in the top, left panel. A total of 1e6 events were generated. The y-axis is the vertical position in centimeters and the x-axis is the azimuthal angle in degrees. (Bottom) An MLEM reconstruction of the source distribution using the pixel count distribution in the top, left panel. The axes are identical to the center panel.

Figure 5.10. Simulation results. Source: Peter Marleau and Erik Brubaker, "An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System," *INMM 57th Annual Meeting* (2016): 6.

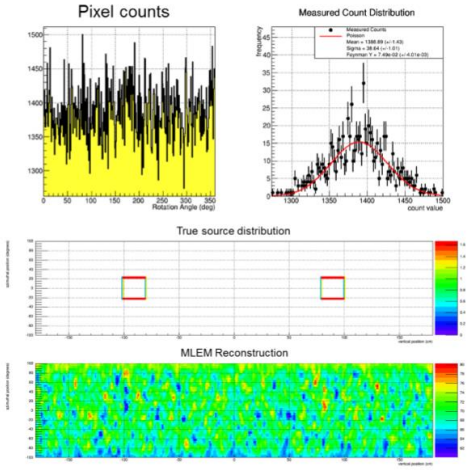

Figure 4 – Results from a simulation of a two identical objects centered at (-90, 0) and (90, 0). (Top, left) The pixel counts as a function of rotation angle for the source distribution shown in the center panel. (Top, right) A histogram of the pixel count values for each rotation angle bin in the top, left panel. The red line is the expectation if the distribution were consistent with purely statistical (Poisson) noise. (Center) The true source distribution used to generate the pixel count values in the top, left panel. A total of 1e6 events were generated. The y-axis is the vertical position in centimeters and the x-axis is the azimuthal angle in degrees. (Bottom) An MLEM reconstruction of

Figure 5.11. Simulation results. Source: Peter Marleau and Erik Brubaker, "An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System," *INMM 57th Annual Meeting* (2016): 7.

One benefit of the system design is also that it serves as a full imaging system, capturing all radiation sources in the measurement environment.[477] This creates an opportunity for the inspector to control the measurement conditions, for example by inserting an additional radiation source that can be checked during the result analysis. When the source is placed symmetrically with respect to the two measured items, it does not interfere with their comparison, but adds an additional measurement result. The system function, thus, could be authenticated through this control radiation source. Other aspects of the system also support authentication by the inspector, including that the system is accessible before and after the measurement is done, since no information about the test items is pre-loaded into the system.[478]

Both of these system characteristics also lend confidence to the host's certification assessment. If the total signal strength measured by the system is considered to be sensitive, the host could be allowed to place an additional radiation source, whose value is only known by the host, above the detector pixel and thus offset the measurement signal such that the contributions from the two measured items would remain confidential.[479]

X. Authenticating the Reference Warhead

These physical cryptographic protocols based on the zero-knowledge property do not rely on electronic information barriers that can be impossible to authenticate for the verifier.[480] Thus, they are able to solve one of the key challenges that all previous verification systems, both attribute- and template-based, have faced. Physical cryptographic verification systems inherently protect sensitive information based on the measurement technologies employed in the protocols, which never measure

[477] Ibid., 10.

[478] Ibid., 13.

[479] Ibid.

[480] Philippe, Barak, and Glaser, "Designing Protocols for Nuclear Warhead Verification," 3.

the sensitive information itself.[481] Proper design can ensure easy certification and authentication of the systems for all parties involved and can theoretically be implemented with any equipment, making the issue of host- or verifier-supply insignificant.[482]

The most significant challenge with the current implementations of physical cryptographic verification approaches, as with all template-based verification systems, relates to the question of trusting the reference warhead.[483] In all forms of template verification, an authentic 'golden warhead' must be established, allowing the comparison of this reference to an item under inspection.[484] When considering this challenge, one important question relates to terminology. In the traditional template approach literature, the reference *measurement*, not the item, is considered as the template. In the context of warhead verification, this would translate to considering the radiological signature or other measurement result of the warhead as the template, not the physical reference warhead itself.[485]

Neither the Glaser *et al.* or Kemp *et al.* proposals, however, establish a template in the same way as traditional template verification systems do.[486] The Glaser *et al.* approach uses the preloaded reverse radiographs as templates of a different kind, but as discussed earlier, those are not accessible or authenticable to the inspector. The preload data is classified, in the same sense as a template behind an information barrier. The Kemp *et al.* approach does not establish anything comparable to a template – the reference warhead is always used as the template. This makes maintaining continuity of

[481] Ibid., 9.

[482] Ibid..

[483] Marleau et al., "Zero Knowledge Protocol: Challenges and Opportunities," 5.

[484] Ibid.

[485] Ibid.

[486] Marleau and Brubaker, "An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System," 2.

knowledge of the reference warhead essential for the protocols, since the legitimacy of the comparison is contingent on the warhead's authenticity.

The Marleau *et al.* proposal does not preload any sensitive information to the system and thus enables the inspector access to the instrumentation at all times, but it also circumvents the establishment of a traditional template.[487] This approach is very similar to Glaser *et al.* in the sense that a measurement and its complement are compared to each other, with a confirmatory result being a blank. The challenge with these approaches, however, is that the inspector cannot access the data that produced this result – it only confirms that the reference item was identical to the inspected item. This, of course, is the core idea of zero-knowledge protocols and allows the protection of sensitive information. On the other hand, it also prevents the assessment of the authenticity of the reference warhead.

Several ideas have been proposed for ensuring the authenticity of the reference warhead. The inspector could be allowed to select the reference warhead from active delivery systems, as states would be highly unlikely to deploy counterfeit warheads in these conditions and undermine the weapons' deterrent capability.[488] Deception mechanisms are still conceivable, for example a situation where the host state learns beforehand which actively deployed warheads would be selected as templates and can replace them with blanks. Furthermore, this template selection mechanism could not be used for non-strategic nuclear warheads deployed in dual-capable systems, or those located in storage. Chain of custody methods could be one possible solution, but states may be unwilling to allow this level of access to their critical defense facilities and information.[489] As discussed in a previous

[487] Ibid.

[488] Philippe, Goldston, Glaser, and d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification."

Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads."

[489] Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads."

chapter, START I and New START contained provisions for verifying the non-nuclear nature of warheads through radiological measurements, but confidentiality concerns prevented more intrusive measurements on nuclear warheads.

XI. Future Directions

The fundamental assumption in zero-knowledge verification protocols is that no information should be released, or even measured, beyond the validity of the proposition under consideration. This property makes it inherently impossible to infer anything about the reference warhead. Would it be possible to allow some measurement information to be accessible to the verifier, however, for the purpose of authenticating the reference warhead? Relaxing the condition of zero-knowledge could open new opportunities for solving the 'golden warhead' challenge. Verification protocols that rely on electronic information barriers aim to do this by allowing the measurement of classified information, but then concealing it behind a trusted information barrier and only displaying an unclassified result.[490] This gain in the legitimacy of the measurement results, however, comes with the increased vulnerability to intricate spoofing attempts from either the host or the verifier.[491] Thus, both mechanisms of information integrity have inherent tradeoffs. Creating a verification system that would integrate both the attribute approach and the template approach could be one potential way to balance the different advantages and obstacles.[492]

As mentioned earlier, the core criteria for selecting the methods used in verification protocols should be the questions they are able to answer, either alone or in parallel with other verification

[490] Yan and Glaser, "Nuclear Warhead Verification: A Review of Attribute and Template Systems."

[491] Philippe, Barak, and Glaser, "Designing Protocols for Nuclear Warhead Verification," 9.

[492] Committee on International Security and Arms Control, National Research Council, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities,* 100.

mechanisms.[493] This informational value can justify the use of a particular mechanism, but this justification must be perceived as legitimate by all involved parties in the treaty. Reflecting back to mechanisms based on information barriers, their ability to provide information about the legitimacy of the measurement result – potentially, that a warhead is authentic based on the parameters defined by the verifier – could be a justification for involving this approach in authenticating the reference warhead. Integrating some form of measurement of the reference warhead behind an information barrier to a physical zero-knowledge verification protocol, thus, could be a powerful way of solving the 'golden warhead' challenge.

The question is, then, what should be measured about the reference warhead to establish confidence in its authenticity. These forms of information can be categorized in three groups – basic information, quantitative information, and disarmament information.[494] In the Trilateral Initiative, the United States and Russia followed a modest and careful approach, essentially establishing the lowest common denominator in deciding what characteristics could be determined. They agreed to measure three attributes that would provide basic information about the warheads and thus provide assurance of warhead authenticity: whether fissile material was present; whether its isotopic composition was typical for nuclear weapons; and whether the mass of the fissile material was above a minimum threshold, defined by the context where it was deployed.[495]

These attributes, however, only establish basic information about the warhead and remain at the lowest ladder of informational value. A further step into certifying the authenticity of a warhead would be using measurement approaches that provide quantitative information about the fissile

[493] Private communication with Dr. Thomas Shea, current affiliation with the Federation of American Scientists. Cited with permission.

[494] Ibid.

[495] Ibid.

material: the establishment of the exact mass of the material; or certification that the mass is within certain limits.[496] Going beyond fissile material, the last category of questions would probe into the fundamental characteristics of 'warheadedness': whether the object contains core nuclear weapons components, such as the physics package, pits, or secondaries; and whether the specific model of these components can be identified and confirmed.[497]

Negotiating the levels and characteristics that could be determined to authenticate the reference warhead will be an important, but challenging task. Nuclear weapons states have highly divergent classification standards in relation to their nuclear capabilities, as well as different decision-making mechanisms for determining what can and cannot be considered. If something is considered acceptable by policy-makers, different declassification procedures may be needed before the reference warhead authentication provision could be included in a verification protocol. The history of declassification actions related to restricted information about the U.S. nuclear capabilities provides an important example of shifts in classification considerations.[498] This collection of unclassified characteristics and information about warheads could be used as a basis for negotiating authentication measures for the reference warhead used in verification protocols. These authentication measures could be based on warhead signatures established from radiation measurements, with the declassified characteristics offering several options for consideration.[499]

One potential mechanism would be to establish a database of the radiation signatures of the state's declared types of warheads, which would be then used in the process of authenticating the reference warheads used in the inspection process. This is not entirely unprecedented, the United

[496] Ibid.

[497] Ibid.

[498] U.S. Department of Energy, "Restricted Data Classification Results 1946 to the Present (RDD-8)."

[499] Ibid.

States has engaged in collecting a comprehensive database of its nuclear warhead and component signatures with a potential disarmament verification purpose in mind.[500] Starting in 2012, this has been done in collaboration with the United Kingdom in the form of a modeling and measuring campaign that intends to establish a comprehensive signature database of warheads and components.[501] The effort seems to be ongoing, having been iterated in the 2015 NPT Review Conference.[502] Expanding dialogue on this effort to other nuclear weapons states could be the next step. A potential starting point for implementation could also be the collection of partial signatures of the warhead types that would first come under arms reduction negotiations.[503]

This mechanism would create similar concerns as with all previous attribute-based verification approaches. While states may be compelled to relax their classification protocols related to certain nuclear warhead characteristics to enable the authentication of the reference warhead and its type, they would still seek mechanisms to maintain restriction of this information and only allow its disclosure under necessary and legitimate conditions. This would entail the use of a secure arrangement that would allow the information to flow between a protected and an open state. The base case would be that the information is concealed, but under certain managed access conditions during reference warhead authentication, it could be disclosed to authorized officials. In the most optimal case, the

---

[500] National Nuclear Security Administration, "Joint U.S.-U.K. Report," 24.

United States Department of State, "Report of the United States of America Pursuant to Actions 5, 20, 21 of the 2010 Nuclear Non-Proliferation Treaty Review Conference Final Document," *2010 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons*, http://www.state.gov/documents/organization/225576.pdf, 12.

[501] National Nuclear Security Administration, "Joint U.S.-U.K. Report," 24.

[502] United States Department of State, "Report of the United States of America Pursuant to Actions 5, 20, 21 of the 2010 Nuclear Non-Proliferation Treaty Review Conference Final Document," *2015 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons,* http://www.un.org/en/conf/npt/2015/pdf/NPT-CONF2015-38.pdf, 25.

[503] Committee on International Security and Arms Control, National Research Council, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities,* 5.

warhead signature data would never be directly accessed in the reference warhead authentication process.

If a warhead signature was established through radiographic measurements, one potential approach to hide sensitive design information would be to blur or defocus the radiograph's spatial resolution.[504] Some measurement data in combination with image-reconstruction algorithms, however, could allow the regeneration of the high-resolution version of the signature if the signal-to-noise ratio was sufficient.[505] Other image reduction techniques could be considered to transform the measurement data only contain non-sensitive features, such as histogram comparison, material recognition, and active/passive pixel correlation.[506] Other alternative imaging information protection techniques include controlled image formation and constrained image analysis, neither of which constructs a full image in the traditional sense through the available imaging data.[507]

Modern cryptography contains several concepts that could prove useful for this challenge, basing their security on mathematical operations.[508] Kemp *et al.* implemented the idea of a physical encryption key in the verification protocol, but only on the side of the host.[509] The classified foil, whose composition is only known to the host, serves as a physical encryption key that allows the decryption of the measurement data.[510] Cryptographic protocols, however, have established a much wider range of ways to use encryption keys and other mechanisms in protecting sensitive information.

---

[504] S. Drell et al., "Verification Technology: Unclassified Version," *JASON Report* (1990), http://fas.org/irp/agency/dod/jason/verif.pdf, 99.

[505] Ibid.

[506] Allen Seifert et al., "Imaging for Dismantlement Verification: Information Management and Analysis Algorithms," *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment,* Vol. 662 (2012): 81.

[507] Allen Seifert et al., "Outcomes of a Workshop on Techniques for Information Protection of Imaging Information," *INMM 57th Annual Meeting* (2016): 3.

[508] Seifert et al., "Outcomes of a Workshop on Techniques for Information Protection of Imaging Information," 3.

[509] Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads."

[510] Ibid.

In the context of warhead verification, an encryption key that allowed the inspector to certify the underlying data could be a critical confidence-building mechanism, potentially allowing the indisputable authentication of the reference warhead.[511] Novel concepts in modern cryptography include arrangements such as digital signatures, physically unclonable functions, and quantum key distribution.[512] In the context of zero-knowledge cryptographic protocols, different physical and non-physical protection techniques have also been suggested.[513] Evaluation of fully homomorphic encryption has been initiated in the specific context of arms control, but overall, the consideration of all of these cryptographic information protection mechanisms are at very elementary stages.[514]

One interesting analogy to the challenge of reference warhead authentication are biometric authentication systems, which face several similar challenges as the radiological signature system under discussion. Biometric verification systems are based on template databases of different physical signatures or characteristics, such as fingerprints or iris scans, which are used to uniquely identify individuals.[515] These systems are designed to manage nonuniform and irregular data and tolerate some level of error in the measurements, as the physical signatures obtained from individuals can vary depending on the measurement conditions.[516] This is done by employing mechanisms such as secure sketches and fuzzy extractors, which allow the valid identification of nonuniform inputs.[517] A very similar challenge would also be faced when matching the reference warhead to its type in the database,

---

[511] Marleau et al., "Zero Knowledge Protocol: Challenges and Opportunities," 5.

[512] Juan Garay and Rosario Gennaro, eds., "Advances in Cryptology – CRYPTO 2014," *34th Annual Cryptology Conference, Proceedings,* Santa Barbara, CA, USA, August 17-21, 2014.

[513] Ben Fisch, "Physical Zero-Knowledge Proofs of Physical Properties," *TCC Rump Session* (2014), https://www.iacr.org/workshops/tcc2014/rump-slides/physical_zk_tcc.pdf, 5.

[514] Seifert et al., "Outcomes of a Workshop on Techniques for Information Protection of Imaging Information," 5.

[515] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," in *Proceedings from EUROCRYPT 2004: Advances in Cryptology* (2004): 2, http://crypto.di.uoa.gr/class/Kryptographia/Metaptychiakoi_2015_files/DRS04.pdf.

[516] Ibid.

[517] Ibid.

as any physical measurement will contain some level of uncertainty. In addition, the reference warheads are not necessarily perfect matches to their legitimate references, as warheads of the same type may have small differences due to irregularities in the production process or other factors.[518]

Another critical similarity is that the template measurements are highly sensitive and would need to be securely protected in the database. With biometric data, the risk is that the information from the database is stolen and could be used for false identification, or that an artificial biometric data point is constructed such that it matches one of the templates.[519] The signature measurement data obtained from warheads could reveal sensitive design information that could be exploited by adversaries, or reveal weaknesses about the state's defense capabilities. In biometric systems, this challenge is addressed through private verification mechanisms. These systems do not make comparisons of the original data, but instead employ cryptographic one-way functions to transform all inputs to the system. The database stores the transformed template, as opposed to the original, and compares the measurement data after it has been processed by this same function. Thus, even if data is disclosed, it cannot be used as long as the cryptographic function remains unknown. In addition to the raw measurements, helper data is also collected in the database creation phase that can be used to derive the same unique string from the input, such as a fingerprint, even if the measurement is not perfectly the same. This involves processes such as information reconciliation and privacy amplification, which handle the inaccuracy and randomness in the measurement data. Overall, biometric verification systems represent secure mechanisms to accurately authenticate data containing

[518] Philippe, Barak, and Glaser, "Designing Protocols for Nuclear Warhead Verification," 4.

[519] Jean-Paul Linnartz, "A Communication-Theoretical View on Secret Extraction," in *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, ed. Pim Tuyls et al. (London: Springer, 2007), 67.

some level of uncertainty, while protecting the underlying sensitive information from abuse or dishonest verifiers.[520]

In the context of a radiation signature database, similar cryptographic mechanisms could be used to encrypt the input measurements, protecting the information even if leaked.[521] As discussed earlier, some work has already been done in exploring these methods in the context of protecting information obtained from warheads.[522] The process described above for biometric authentication systems is only a simplified example of the involved processes, but more advanced mechanisms are also under development. Ongoing research is exploring concepts such as threshold homomorphic encryption schemes, where only binary biometric templates are stored and the verification process does not involve accessing the original template measurement data.[523] The processes used in these approaches also protect the templates against malicious database owners, which is a critical shortcoming in previous approaches. Overall, biometric authentication systems offer an important real-world analogy to the challenge of authenticating the reference warhead and could offer a direction for future study.

Trust in the integrity and confidentiality of nuclear disarmament verification is a critical precipitating factor that allows states to engage in disarmament. One of the most important dimensions of this trust is information protection – how well states consider their sensitive or classified information to be protected in all the complex stages of the process. The risks of unauthorized access and illegitimate disclosures can emerge both from the technologies utilized, as well as the human interaction with these systems. Verification protocols founded on physical zero-knowledge proofs

---

[520] Ibid., 77.

[521] Ibid., 69.

[522] Seifert et al., "Outcomes of a Workshop on Techniques for Information Protection of Imaging Information," 3.

[523] Cagatay Karabat et al., "THRIVE: threshold homomorphic encryption based secure and privacy preserving biometric verification system," *EURASIP Journal on Advances in Signal Processing* 71 (2015): 1.

would be an instrumental contribution to addressing these verification concerns. Their successful development and implementation could precipitate a paradigm shift in disarmament treaty architecture, enabling agreements that limit individual warheads. Conceptually, the veil that physics provides to these approaches enables inherent secrecy, but this lack of transparency also prevents trust-building.

The critical prevailing challenge in these template-based protocols is the authentication of the reference warheads. Confidence in the authentication process establishes the foundations of trust in the entire verification mechanism, which is why it is imperative to identify effective mechanisms to securely verify the authenticated standard.[524] The establishment of a warhead signature database that contains a comparison point for each warhead type could be one option, among others. These approaches, however, would require the zero-knowledge property of these verification approaches to be relaxed. Different concepts from modern cryptography could provide ideas for solving the subsequent challenges relating to the protection of sensitive information, as biometric authentication systems have demonstrated in practice.

Even though the prospects for further reductions in the near term are bleak, it is essential to invest and engage in this fundamental research now to create new verification tools and confidence-building assets for when political interests become aligned with disarmament goals. Critically, this process must be carried out in collaboration with all states with nuclear weapons capabilities, especially those that have thus far been isolated from the international nuclear policy architecture and security collaboration. Future verification conditions are likely to engage new states, address novel categories of nuclear weapons, and target much lower arsenal sizes, all of which create unique pressures for the verification mechanisms employed. Having the capacity to confidently authenticate, track, and

[524] Marleau et al., "Zero Knowledge Protocol: Challenges and Opportunities," 9.

dismantle individual warheads will become the priority in these conditions. The failure to develop sufficient readiness for these new verification requirements could become a significant barrier for future disarmament efforts.

Conclusion

The challenge of warhead authentication is an illustrative example of a verification issue where the current lack of technical capabilities has prevented certain measures of arms control from being implemented, and where a breakthrough in verification technologies could have a significant impact in shifting the dynamics of the political discussions. This illuminates how the theoretical processes discussed in the first chapter are manifested in practice. The development of zero-verification approaches would eliminate the technical argument that warhead reductions cannot be verified with a high level of accuracy, or that the verification process would reveal classified information and therefore threaten national security.[525] Thus, these novel verification capabilities would influence the arguments available both to arms control opponents and proponents, facilitating new treaty architecture options for further warhead reductions.

It must be recognized that novel verification technologies, such as zero-knowledge verification approaches, will not be a panacea for making arms control possible. Changes in the available verification capabilities cannot single-handedly make an arms control agreement possible, in the absence of political will. They can, however, shift the dynamics of the negotiations by changing the arguments available to the different stakeholders and creating new, feasible verification options. This is where the importance of verification technologies lies – they can increase the likelihood of achieving an agreement in verification provisions, and thus enhance the prospects of future rounds of arms control.

---

[525] These arguments were visible, for example, in the U.S.-Russian transparency and irreversibility dialogue between 1994 and 1995. (Source: Steven Pifer, "The Next Round: The United States and Nuclear Arms Reductions After New START," *Brookings Institution, Arms Control Series Paper 4* (2010): 31, available at https://www.brookings.edu/wp-content/uploads/2016/06/12_arms_control_pifer.pdf; also see Eugene Miasnikov, "Non-strategic Nuclear Weapons in Europe: Possible Scope and Conditions for Information Sharing, Transparency Measures and Verification," *presented at the Warsaw Workshop: Prospects for Information Sharing and Confidence Building on Non-Strategic Nuclear Weapons in Europe* (2013), 3, available at https://www.pism.pl/files/?id_plik=12843.)

This is why the development of novel verification capabilities is important. Even if the new verification capabilities are never fully implemented in an arms control agreement, their existence matters, because these new capabilities can both open the dialogue on new treaty architecture options, as well as shape the political dynamics of the treaty negotiations themselves. In the case of warhead authentication methods relying on zero-knowledge proofs, these mechanisms may be implemented jointly with an authentication system relying on the attribute approach, or otherwise be combined with verification mechanisms that do not rely on ideas drawn from physical cryptography. Even if this new innovation in warhead authentication methods was not implemented in its full capacity, the development of this verification approach would have an impact by allowing policymakers to envision the possibilities of verifying the next stages in warhead reductions, and by shaping the dialogue on these next steps in arms control.

No verification option will be perfect, and there will always be gaps in confidence about compliance, which can be operationalized by the opponents of arms control. As was discussed in the first chapter, however, other factors and processes can help compensate for these gaps in technical capabilities. Iterated interactions are one important reason why even imperfect verification capabilities can be sufficient for facilitating cooperation on arms control. Furthermore, as Figure 2 in the first chapter demonstrated, each larger verification challenge can be disaggregated into separate, specific challenges. Warhead authentication, for example, is only one of the challenges related to verifying disarmament agreements that focus on individual warheads, among other challenges that include tracking the warheads, managing access to the dismantlement facilities, and detecting undeclared warhead stockpiles. It is not necessary to have all of the verification challenges solved before negotiations can begin, because solutions in one of the areas can compensate for less progress in another one. In this view, a feedback loop also exists in the way that these different segments of the greater verification issue interact with each other. When combined with the fact that the negotiating

dynamics themselves also help fill the technical gaps that may remain, it is possible to envision how progress can be driven by incremental enhancements in the available technical verification capabilities.

The current political environment with respect to future reductions in nuclear arsenals remains challenging. In terms of further bilateral reductions between the United States and Russia, the domestic political context in both states is currently dire and the relations between the countries are tense. In discussions after New START was established, Russia has maintained that the next round of warhead reductions should be carried out multilaterally, calling for other nuclear weapons states to become involved.[526] Other states, however, have argued that further progress must be made in the U.S.-Russia context before any discussions about the multilateralization of the process. As the United States and Russia continue to hold approximately 90% of the global nuclear weapons stockpile, this assertion has clear legitimacy.[527]

It is conceivable, however, to engage the other nuclear weapons states in efforts that may fall short of substantive reductions in their nuclear weapons arsenals, but would still contribute to enhancing the future prospects of multilateral warhead reductions. Engagement in technological development is one important dimension of this, including in the context of the verification capabilities discussed in this thesis, and those referred to in Figure 2 in the first chapter. Other important dimensions for engagement include the development of common definitions about nuclear weapons terminology; discussing how non-nuclear weapons states could become involved; what role multilateral institutions, such as the IAEA, will have in multilateral disarmament; and other important aspects that remain to be contested.[528] The P5 states have already engaged in developing a framework

[526] Nuclear Threat Initiative, "Russia Insists on Multilateral Nuclear Arms Control Talks," May 28, 2013, accessed April 19, 2017, http://www.nti.org/gsn/article/russia-insists-next-round-nuke-cuts-be-multilateral/.

[527] Arms Control Association, "Nuclear Weapons: Who has What at a Glance."

[528] Robert Norris and Hans Kristensen, "Global nuclear weapons inventories, 1945–2010," *Bulletin of the Atomic Scientists* 66, no. 4 (2010): 82.
Hanne Kofstadmoen and Ole Reistad, "The Role of IAEA in Multilateral Nuclear Disarmament Verification," *IAEA*

of definitions, the *P5 Glossary of Key Nuclear Terms*, but more work remains to be done in developing a common language about nuclear arms control, for example with respect to tactical nuclear weapons.[529] Ultimately, as a first step towards multilateral arsenal reductions, the other nuclear weapons states could halt the buildup of their nuclear forces and engage in discussions about the pace and proportion of eventual warhead reductions.[530]

Transparency is one critical dimension where progress can be pursued now. The P5 nuclear weapons states, as well as the non-NPT nuclear weapons states, are in a position to take further steps towards disclosing information about their nuclear arsenals, stockpiles of fissile material, and other aspects of their nuclear weapons programs.[531] These transparency measures will be important steps in the path towards multilateral nuclear disarmament, which requires the facilitation of trust between nuclear weapons states, as well as with the rest of the international community.[532] At the moment, the P5 states take very different approaches to transparency, with the United States providing quite detailed information about current warhead numbers, whereas other P5 providing little, if any, information.[533] This highlights the fact that decisions about transparency, and its relation to security, are fundamentally subjective. Thus, the challenge is finding the avenues for transparency that states

---

Safeguards Syposium 2010, available at https://www.iaea.org/safeguards/symposium/2010/Documents/PapersRepository/280.pdf.

Chalmers, "The IAEA and Nuclear Disarmament Verification: A Primer."

[529] P5 Working Group on the Glossary of Key Nuclear Terms, *P5 Glossary of Key Nuclear Terms* (Beijing: China Atomic Energy Press, 2015), available at https://www.state.gov/documents/organization/243287.pdf.

Micah Zenko, *Toward Deeper Reductions in U.S. and Russian Nuclear Weapons* (New York: Council on Foreign Relations, 2010), 11.

[530] Norris and Kristensen, "Global nuclear weapons inventories, 1945–2010," 82.

[531] Steven Pifer and James Tyson, "Third-Country Nuclear Forces and Possible Measures for Multilateral Arms Control," *Brookings Institution, Arms Control and Non-Proliferation Series Paper* 12 (2016): 2.

[532] First Preparatory Committee for the 2015 NPT Review Conference, "Transparency of nuclear weapons: the Non-Proliferation and Disarmament Initiative: Working paper submitted by Australia, Canada, Chile, Germany, Japan, Mexico, the Netherlands, Poland, Turkey and the United Arab Emirates," (NPT/CONF.2015/PC.I/WP.12), available at http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/prepcom12/documents/WP12.pdf.

[533] U.S. Department of State, "Transparency in the U.S. Nuclear Weapons Stockpile," available at https://2009-2017.state.gov/t/isn/npt/statements/241165.htm.

find acceptable and that do not lead to unwelcome tradeoffs with security. The verification approaches discussed in this thesis do this in the context of warhead authentication, which is a later-stage process, but progress needs to be made in earlier stages as well. Conceiving ways to prevent information disclosure about stewardship practices, military facilities, and other sensitive aspects of the operations of states' nuclear enterprises will be important for making nuclear weapons states more willing to engage in transparency measures, paving the way for their involvement in verification processes.

Future stages of nuclear disarmament will be more challenging than the efforts undertaken in the past, for the reasons discussed in this thesis: addressing lower numbers of warheads, where uncertainty becomes riskier; considering new categories of weapons under limitations, where past verification approaches will become impossible; and involving other nuclear weapons states, who see verification in a different light and may have less advanced capabilities in national technical means. Especially when thinking about the 'hardest' cases of nuclear disarmament, such as between India and Pakistan or with Israel, concerns about the tradeoffs between secrecy and transparency will become prioritized. Especially in these types of conditions, novel verification capabilities can make or break future prospects for arms control.

Important future work needs to be done on the technical side of the verification challenges discussed in this thesis, as well as on other prevailing verification issues. In addition to this technical development work, the political dynamics discussed in the first chapter will require more research. One important question for future investigation is how changes in norms and perceptions about scientific knowledge, particularly among political elites and leaders, influences the impact of the dynamics discussed in the first chapter. In a world where scientific expertise is being contested, and 'alternative facts' are understood as a part of reality, how is the influence that science and technology has on public policy modified? As has been discussed in this thesis, technologies are often politicized,

but this phenomenon of politicization becomes more complex when our understanding of what constitutes a scientific fact is distorted.

Ultimately, nuclear weapons states' decisions to disarm their nuclear capabilities are going to be shaped by a range of strategic, political, and other factors both at the domestic and international levels. As has been illuminated in this thesis, however, verification capabilities can play a part in shaping the dynamics of the states' decision-making processes, especially if and when they engage in direct negotiations over disarmament efforts. Looking into the future, the technical development of verification capabilities can be an important path towards making multilateral negotiations on warhead reductions possible, in parallel with other confidence-building measures among the nuclear weapons states and with the rest of the international community.

-

Bibliography

2005 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons. "Nuclear disarmament and reduction of the danger of nuclear war: Working paper submitted by China." (NPT/CONF.2005/WP.2).

———. "Nuclear Disarmament: Working paper submitted by Canada," (NPT/CONF.2005/WP.38).

———. "Transparency, verification and irreversibility: essential principles in the process of nuclear disarmament: Working paper by the Republic of Cuba." (NPT/CONF.2005/WP.24).

———. "Working paper on nuclear disarmament for Main Committee I: Recommendations submitted by New Zealand on behalf of Brazil, Egypt, Ireland, Mexico, South Africa and Sweden as members of the New Agenda Coalition." (NPT/CONF.2005/WP.27).

———. "Verification of nuclear disarmament: final report on studies into the verification of nuclear warheads and their components: Working paper submitted by the United Kingdom of Great Britain and Northern Ireland," (NPT/CONF.2005/WP.1), http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2005/wp/wp1.pdf.

———. "Working paper on disarmament and non-proliferation education Submitted by Egypt, Hungary, Japan, Mexico, New Zealand, Peru, Poland and Sweden." (NPT/CONF.2005/WP.30) http://www.mofa.go.jp/policy/un/fmv0504/npt4.pdf.

Arms Control Association. "Nuclear Weapons: Who Has What at a Glance." Updated January 2017, available online from https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat.

———. "Iraq: A Chronology of UN Inspections." October 1, 2002. https://www.armscontrol.org/act/2002_10/iraqspecialoct02.

———. "U.S.-Russian Nuclear Arms Control Agreements at a Glance." April 2014. https://www.armscontrol.org/factsheets/USRussiaNuclearAgreementsMarch2010

Avenhaus, Rudolf, Nicholas Kyriakopoulos, Michel Richard, and Gotthard Stein. *Verifying Treaty Compliance: Limiting Weapons of Mass Destruction and Monitoring Kyoto Protocol Provisions.* Berlin: Springer, 2006.

Axelrod, Robert. *The Evolution of Cooperation*. New York: Basic Books, 1981.

Berger, Harold. *Neutron Radiography*. Amsterdam: Elsevier Pub. Co., 1965.

Braibant, Sylvie, Giorgio Giacomelli, and Maurizio Spurio. *Particles and Fundamental Interactions: An Introduction to Particle Physics*. Verlag: Springer, 2009.

Broad, William. "Web Archive Is Said to Reveal a Nuclear Primer." *New York Times*, November 3, 2006. http://www.nytimes.com/2006/11/03/world/middleeast/03cnd-documents.html.

Burr, William. "The Secret History of The ABM Treaty, 1969-1972." *National Security Archive Electronic Briefing Book No. 60*. http://nsarchive.gwu.edu/NSAEBB/NSAEBB60/index2.html.

Byrd, Donald. "Zeno's "Achilles and the Tortoise": Paradox and the Infinite Geometric Series." February 2010, revised December 2012. http://homes.soic.indiana.edu/donbyrd/Teach/Math/Zeno+Footraces+InfiniteSeries.pdf.

Camp, Chris. "Why No One Will Ever Build Another Nagasaki Type Bomb." *Arms Control Wonk*, July 15, 2014. http://www.armscontrolwonk.com/archive/604623/why-no-one-will-ever-build-another-nagasaki-type-bomb/.

Chalmers, Hugh. "The IAEA and Nuclear Disarmament Verification: A Primer." *VERTIC Research Reports,* No. 11 (2015). http://www.vertic.org/media/assets/Publications/VM11%20WEB.pdf.

Cliff, David, Hassan Elbahtimy and Andreas Persbo. "Verifying Warhead Dismantlement: Past, Present, Future." *VERTIC Research Reports*, Number 9, September 2010. http://www.vertic.org/media/assets/Publications/VM9.pdf.

Comley, Christine et al. "Confidence, Security, and Verification: The Challenge of Global Nuclear Weapons Arms Control." *Atomic Weapons Establishment*, AWE/TR/2000/001. http://fissilematerials.org/library/awe00.pdf.

Committee on International Security and Arms Control, National Research Council. *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities.* Washington D.C.: National Academies Press, 2005.

Congress of the United States. "Verification Technologies: Measures for Monitoring Compliance with the START Treaty." Office of Technology Assessment (1990). http://govinfo.library.unt.edu/ota/Ota_2/DATA/1990/9029.PDF.

Corson, James. "Overview of Nuclear Weaponry." *University of Virginia, Metals in Medicine and the Environment*, accessed March 26, 2017. http://faculty.virginia.edu/metals/cases/corson3.html.

Coster-Mullen, John. *Atom Bombs: The Top Secret Story of Little Boy and Fat Man*. Coster-Mullen, 2009.

Cottingham, W. N. and D.A. Greenwood. *An Introduction to Nuclear Physics*. Cambridge: Cambridge University Press, 2004.

Das, Ashik and Thomas Ferbel. *Introduction to Nuclear and Particle Physics* (2nd Edition). Singapore: World Scientific Publishing, 2003.

Das, Ashik and Thomas Ferbel. *Introduction to Nuclear and Particle Physics* (2nd Edition) (Singapore: World Scientific Publishing, 2003).

DeSutter, Paula. "Completion of Verification Work in Libya." *United States Department of State*. September 22, 2004. https://2001-2009.state.gov/t/vci/rls/rm/2004/37220.htm.

DeVolpi, Alexander. "Tagging and Fissile Material Verification Concepts for Nuclear Warhead Dismantlement." *INMM 31st Annual Meeting* (1990).

Digital National Security Archive. "Gun-assembly nuclear weapon." *Nuclear History I, 1955-1968,* accessed March 25, 2017, retrieved from http://ccl.idm.oclc.org/login?url=http://search.proquest.com/docview/1679150818?accountid=10141.

Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith. "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data." In *Proceedings from EUROCRYPT 2004: Advances in Cryptology* (2004). http://crypto.di.uoa.gr/class/Kryptographia/Metaptychiakoi_2015_files/DRS04.pdf.

Dong, Ling and Kefei Chen. *Cryptographic Protocol*. Beijing: Springer, 2012.

Drell, S. et al. "Verification Technology: Unclassified Version." *JASON Report* (1990). http://fas.org/irp/agency/dod/jason/verif.pdf.

Feige, Uriel, Amos Fiat, and Adi Shamir. "Zero-Knowldege Proofs of Identity." *Journal of Cryptology* 1 (1988): 77-94. http://s3-ap-southeast-1.amazonaws.com/erbuc/files/a60459e4-bcf1-421c-a3a5-9e8f79aa8be8.pdf.

Feshbach, Murray. *National Security Issues of the USSR*. New York: Springer, 1987.

Fetter, Steve et al. "Detecting Nuclear Warheads." In *Reversing the Arms Race: How to Achieve and Verify Deep Reductions in the Nuclear Arsenals*, edited by Frank von Hippel and R. Z. Sagdeev. New York: Gordon and Breach Science Publishers, 1990.

Fetter, Steve et al. "Detecting Nuclear Warheads." *Science & Global Security* 1 (1990): 225–302.

Fetter, Steve et al. "Gamma-Ray Measurements of a Soviet Cruise-Missile Warhead." *Science* 248, issue 2957 (1990): 828-834.

Fetter, Steve. "A Comprehensive Transparency Regime for Warheads and Fissile Materials." *Arms Control Association*, January 1, 1999. https://www.armscontrol.org/act/1999_01-02/sfjf99.

First Preparatory Committee for the 2015 NPT Review Conference. "Transparency of nuclear weapons: The Non-Proliferation and Disarmament Initiative: Working paper submitted by Australia, Canada, Chile, Germany, Japan, Mexico, the Netherlands, Poland, Turkey and the United Arab Emirates." (NPT/CONF.2015/PC.I/WP.12), available at http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/prepcom12/documents/WP12.pdf.

Fisch, Ben, Daniel Freund, and Moni Naor. "Physical Zero-Knowledge Proofs of Physical Properties." *Proceedings from CRYPTO 2014: Advances in Cryptology* (2014): 313-336.

Fuller, J.L. and J.K. Wolford. "Information Barriers." *Symposium on International Safeguards: Verification and Nuclear Material Security, 2001, Proceedings*. http://www-pub.iaea.org/MTCD/publications/PDF/ss-2001/PDF%20files/Session%2017/Paper%2017-01.pdf.

Fuller, James. "Verification on the Road to Zero: Issues for Nuclear Warhead Dismantlement." *Arms Control Association*, December 5, 2010. https://www.armscontrol.org/act/2010_12/%20Fuller.

Gaines, L.L. *Start II: Thinking One Move Ahead.* Washington D.C.: United States Department of Energy, Argonne National Laboratory, 1991.

Gallagher, Nancy. "The Design of Verification Regimes." In *Nuclear Proliferation in South Asia: The Prospect for Arms Control*, edited by Stephen Cohen (Boulder: Westview Press, 1991).

———. *The Politics of Verification.* Baltimore: Johns Hopkins University Press, 2003.

Garay, Juan and Rosario Gennaro, eds. "Advances in Cryptology – CRYPTO 2014." *34th Annual Cryptology Conference, Proceedings,* Santa Barbara, CA, USA, August 17-21, 2014.

Garwin, Richard. "Technologies and Procedures to Verify Warhead Status and Dismantlement." *SIPRI Workshop* (2001). https://fas.org/rlg/010208-sipri.htm.

Glaser, Alexander, Boaz Barak, and Rob Goldston. "A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol." *INMM 53rd Annual Meeting* (2012). http://www.boazbarak.org/Papers/nuclear-zk.pdf.

———. "Toward a Secure Inspection System for Nuclear Warhead Verification Without Information Barrier." *INMM 54th Annual Meeting* (2013).

Glaser, Alexander, Sébastien Philippe, and Francesco d'Errico, "Zero-Knowledge Differential Isotopic Comparison of Special Nuclear Materials." *INMM 57th Annual Meeting* (2016).

Goldston, Robert et al. "Zero Knowledge Warhead Verification: System Requirements and Detector Technologies." *INMM 55th Annual Meeting* (2014).

Goldwasser, Shafi, Silvio Micali, and Charles Rackoff. "The Knowledge Complexity of Interactive Proof-Systems." *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing* (1985). https://groups.csail.mit.edu/cis/pubs/shafi/1985-stoc.pdf.

Goldwasser, Shafi, Silvio Micali, and Charles Rackoff. "The Knowledge Complexity of Interactive Proof-Systems." *SIAM Journal on Computing* 18, no. 1, (1989): 186-208. http://crypto.cs.mcgill.ca/~crepeau/COMP647/2007/TOPIC01/GMR89.pdf.

Gradwohl, Ronen et al. "Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles." *Lecture Notes in Computer Science* 4475 (2008). https://guyrothblum.files.wordpress.com/2014/11/gnpr07.pdf.

Haas, Eckhard, Alexander Sukhanov, and John Murphy. "Trilateral Initiative: IAEA Authentication and National Certification of Verification Equipment for Facilities with Classified Forms of Fissile Material." *Symposium on International Safeguards: Verification and Nuclear Material Security, 2001, Proceedings.* http://www-pub.iaea.org/MTCD/publications/PDF/ss-2001/PDF%20files/Session%2017/Paper%2017-04.pdf.

Heinonen, Olli. "Verifying the Dismantlement of South Africa's Nuclear Weapons Program." http://belfercenter.ksg.harvard.edu/files/Verifying%20the%20Dismantlement%20-%20Heinonen%20Chapter%208.pdf.

Herrera, Geoffrey. *Technology and International Transformation*. New York: SUNY Press, 2006.

IAEA General Conference, 36th Regular Session. "South Africa's Nuclear Capabilities." (GC(XXXV)/RES/567). https://www.iaea.org/About/Policy/GC/GC36/GC36Documents/English/gc36-1015_en.pdf.

IAEA General Conference, 37th Regular Session. "The Denuclearization of Africa." (GC(XXXVII)/1075). https://www.iaea.org/About/Policy/GC/GC37/GC37Documents/English/gc37-1075_en.pdf.

Institute for Science and International Security. "Chapter 10: International Verification." Available at http://isis-online.org/uploads/isis-reports/documents/Chapter_10_International_Verification_Mechanisms_april_1_2016.pdf.

International Atomic Energy Agency. "IAEA Verification of Libya's Nuclear Programme." March 10, 2004. https://www.iaea.org/newscenter/news/iaea-verification-libyas-nuclear-programme.

Karabat, Cagatay et al. "THRIVE: threshold homomorphic encryption based secure and privacy preserving biometric verification system." *EURASIP Journal on Advances in Signal Processing* 71 (2015).

Kemp, R. Scott et al. "Physical Cryptographic Verification of Nuclear Warheads." *Proceedings of the National Academy of Sciences* 113 (2016): 8618–8623.

Kemp, R. Scott et al. "Supporting Information Physical Cryptographic Verification of Nuclear Warheads," for R. Scott Kemp et al., "Physical Cryptographic Verification of Nuclear Warheads." *Proceedings of the National Academy of Sciences* 113 (2016): 8618–8623, http://www.pnas.org/content/suppl/2016/07/13/1603916113.DCSupplemental/pnas.1603916113.sapp.pdf.

Kofstadmoen, Hanne and Ole Reistad. "The Role of IAEA in Multilateral Nuclear Disarmament Verification." IAEA Safeguards Syposium 2010, available at https://www.iaea.org/safeguards/symposium/2010/Documents/PapersRepository/280.pdf.

Kondratov, Sergey, et al. "AVNG System Demonstration." INMM 51st Annual Meeting (2011). http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-10-02620.

Kristensen, Hans and Robert Norris. "Status of World Nuclear Forces." *Federation of American Scientists*, accessed March 2, 2017, available at https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/.

Kryukov, Vyacheslav et al. "Trusted Processor: A Result of the Evolution of Information Barrier Technologies." *INMM 48th Annual Meeting* (2007).

Linnartz, Jean-Paul. "A Communication-Theoretical View on Secret Extraction." In *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, ed. Pim Tuyls et al. London: Springer, 2007.

Lodal, Jan. "Verifying Salt." *Foreign Policy*, No. 24 (1976).

Loehrke, Benjamin. "A nuke by any other name." *Bulletin of the Atomic Scientists*, May 12, 2012. http://thebulletin.org/nuke-any-other-name.

Logan, Jonothan. "The Critical Mass." *American Scientist* 84 (1996): 263-277.

MacArthur, D.W. and R. Whiteson. "Information Barriers in the Trilateral Initiative: Conceptual Description." *Los Alamos National Laboratory*. 1998. https://www.nti.org/media/pdfs/Whiteson_MacArthur_1998_IBs_in_the_Trilateral_Initiative_-_Conceptual_Design.pdf?_=1439480184

MacArthur, D.W. et al. "The Effects of Information Barrier Requirements on the Trilateral Initiative Attribute Measurement System (AVNG)." *INMM 42nd Annual Meeting* (2001).

Marleau, Peter and Erik Brubaker. "An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System." *INMM 57th Annual Meeting* (2016).

Merkle, Peter et al., "Next Generation Trusted Radiation Identification System." *INMM 51st Annual Meeting* (2011). https://www.nti.org/media/pdfs/SNL-1_FINAL_INMM_2010_Next_Generation_Trusted_Radiation_System.pdf?_=1438113016.

Miles, Aaron. "Adaptive Warhead Limits for Further Progress on Strategic Arms Control." *Real Clear Defense*, February 7, 2017. http://www.realcleardefense.com/articles/2017/02/07/progress_on_strategic_arms_control_110760.html.

MIT Department of Physics. "Poisson Statistics." July 8, 2004, available at http://123.physics.ucdavis.edu/week_0_files/Poisson.pdf.

Miasnikov, Eugene. "Non-strategic Nuclear Weapons in Europe: Possible Scope and Conditions for Information Sharing, Transparency Measures and Verification." *Presented at the Warsaw Workshop: Prospects for Information Sharing and Confidence Building on Non-Strategic Nuclear Weapons in Europe* (2013). Available at https://www.pism.pl/files/?id_plik=12843.

Mitchell, Dean and Keith Tolk. "Trusted Radiation Attribute Demonstration System." *INMM 41st Annual Meeting* (2000). http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/32/016/32016771.pdf.

Murphy, Chantell and James Doyle Johnson. "Recovering START Institutional Knowledge." *INMM 52nd Annual Meeting* (2011).

National Nuclear Security Administration. "Highlights, February 2011." *Defense Nuclear Nonproliferation, Office of Nonproliferation and Arms Control* (2011). https://nnsa.energy.gov/sites/default/files/nnsa/inlinefiles/NIS%20February%202011%20Highlights.pdf.

———. "Joint U.S.-U.K. Report on Technical Cooperation for Arms Control." D*efense Nuclear Nonproliferation, Office of Nonproliferation and Arms Control* (2015). https://nnsa.energy.gov/sites/default/files/Joint_USUK_Report_FINAL.PDF.

Noonan, William. "Neutrons: It Is All in the Timing – The Physics of Nuclear Fission Chains and Their Detection." Johns Hopkins Applied Technical Digest 32, no. 5 (2014): 762-773, available at http://techdigest.jhuapl.edu/TD/td3205/32_05-Noonan.pdf

Norris, Robert and Hans Kristensen. "Global nuclear weapons inventories, 1945–2010." Bulletin of the Atomic Scientists 66, no. 4 (2010): 77-83.

Nuclear Threat Initiative. "Libya." Last updated April, 2015. http://www.nti.org/learn/countries/libya/.

———. "Nuclear Disarmament Timeline." http://www.nti.org/analysis/articles/nuclear-disarmament-timeline/

———. "Russia Insists on Multilateral Nuclear Arms Control Talks." May 28, 2013, accessed April 19, 2017, http://www.nti.org/gsn/article/russia-insists-next-round-nuke-cuts-be-multilateral/.

———. "Treaty Between the United States of America and the Union of Soviet Socialist Republics on Strategic Offensive Reductions (START II)." Updated October 26, 2011.

http://www.nti.org/learn/treaties-and-regimes/treaties-between-united-states-america-and-union-soviet-socialist-republics-strategic-offensive-reductions-start-i-start-ii/.

———. "Treaty Between the United States of America and the Union of Soviet Socialist Republics on Strategic Offensive Reductions (START II)." Updated October 26, 2011. http://www.nti.org/learn/treaties-and-regimes/treaty-between-united-states-america-and-union-soviet-socialist-republics-strategic-offensive-reductions-start-ii/.

———. "Verifying Baseline Declarations of Nuclear Warheads and Materials," *Innovating Verification Series*, July 2014, http://www.nti.org/media/pdfs/WG1_Verifying_Baseline_Declarations_FINAL.pdf?_=1405443895.

Office of the Secretary of State. "Memorandum for the President: SALT Verification." August 7, 1978. http://nsarchive.gwu.edu/NSAEBB/NSAEBB231/doc14c.pdf.

Peter Marleau et al. "Zero Knowledge Protocol: Challenges and Opportunities." *INMM 56th Annual Meeting* (2015).

Philippe, Sébastien, Boaz Barak, and Alexander Glaser. "Designing Protocols for Nuclear Warhead Verification." *INMM 56th Annual Meeting* (2015). http://www.princeton.edu/~aglaser/PU104-Philippe-Barak-Glaser-2015.pdf.

Philippe, Sébastien, Robert Goldston, Alexander Glaser, and Francesco d'Errico. "A physical zero-knowledge object-comparison system for nuclear warhead verification." *Nature Communications* 7 (2016). http://www.nature.com/articles/ncomms12890.

Pifer, Steven and James Tyson. "Third-Country Nuclear Forces and Possible Measures for Multilateral Arms Control." *Brookings Institution, Arms Control and Non-Proliferation Series Paper* 12 (2016).

Pifer, Steven. "The Next Round: The United States and Nuclear Arms Reductions After New START." Brookings Institution, Arms Control Series Paper 4 (2010). Available at https://www.brookings.edu/wp-content/uploads/2016/06/12_arms_control_pifer.pdf.

———. "U.S. Military Advantages and the Future of Nuclear Arms Control." *Heinrich Boell Stiftung*, October 10, 2013. https://www.boell.de/en/2013/12/20/us-military-advantages-and-future-nuclear-arms-control.

Pomper, Miles, Nikolai Sokov, and William Potter. "Breaking the U.S.-Russian deadlock on nonstrategic nuclear weapons." *Bulletin of the Atomic Scientists*, December 4, 2009. http://thebulletin.org/breaking-us-russian-deadlock-nonstrategic-nuclear-weapons.

Putnam, Robert. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42 (1988): 427-460.

P5 Working Group on the Glossary of Key Nuclear Terms. P5 Glossary of Key Nuclear Terms (Beijing: China Atomic Energy Press, 2015), available at https://www.state.gov/documents/organization/243287.pdf.

Reed, Bruce Cameron. *The Physics of the Manhattan Project*. New York: Springer, 2015.

Riechelson, Jeffrey. "Declassifying the "Fact of" Satellite Reconnaissance." *National Security Archive Electronic Briefing Book* No. 231. http://nsarchive.gwu.edu/NSAEBB/NSAEBB231/.

Riechelson, Jeffrey. "Iraq and Weapons of Mass Destruction." *National Security Archive Electronic Briefing Book* No. 80. http://nsarchive.gwu.edu/NSAEBB/NSAEBB80/.

Rose, Frank. "Closing Remarks to the 4th Plenary Meeting of the International Partnership for Nuclear Disarmament Verification (IPNDV)." November 3, 2016. https://2009-2017.state.gov/t/avc/rls/264081.htm.

Second Preparatory Committee for the 2000 NPT Review Conference, "Verification of nuclear disarmament: First interim report on studies into the verification of nuclear warheads and their components: Working paper submitted by the United Kingdom of Great Britain and Northern Ireland," (NPT/CONF.2005/PC II/WP.1). http://www.acronym.org.uk/old/archive/npt/03wp1.htm.

Seifert, Allen et al. "Imaging for Dismantlement Verification: Information Management and Analysis Algorithms." *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, Vol. 662 (2012).

Seifert, Allen et al. "Outcomes of a Workshop on Techniques for Information Protection of Imaging Information." *INMM 57th Annual Meeting* (2016).

Shea, Thomas and Laura Rockwood. "IAEA Verification of Fissile Material in Support of Nuclear Disarmament." *Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School*, May 2015. http://www.belfercenter.org/sites/default/files/legacy/files/iaeaverification.pdf.

———. "Nuclear Disarmament: The Legacy of the Trilateral Initiative." *Deep Cuts Working Paper*, No. 4 (2015). https://www.files.ethz.ch/isn/192450/DeepCuts_WP4_Shea_Rockwood_UK.pdf.

Shea, Thomas. "The Trilateral Initiative: A Model for The Future?" *Arms Control Association*, June 11, 2008. https://www.armscontrol.org/act/2008_05/PersboShea.asp%23Sidebar1

———. "The Trilateral Initiative: IAEA Verification of Weapon-Origin Plutonium in the Russian Federation and the United States." *International Atomic Energy Agency Safeguards Symposium*, October 2014. https://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000334.pdf.

Squassoni, Sharon. *Disarming Libya: Weapons of Mass Destruction*. Washington D.C.: Library of Congress, Congressional Research Service, 2006.

———. "Iraq: U.N. Inspections for Weapons of Mass Destruction." *Report for Congress*, March 28, 2003. http://fpc.state.gov/documents/organization/19436.pdf.

Sublette, Carey. "Gun Assembly." *Nuclear Weapons Archive*, accessed March 25, 2017, http://nuclearweaponarchive.org/Library/Gun.html

———. "Implosion Assembly." *Nuclear Weapons Archive*, accessed March 25, 2017. http://nuclearweaponarchive.org/Library/Implsion.html.

———. "The W88 Warhead." *Nuclear Weapons Archive*, accessed March 25, 2017. http://nuclearweaponarchive.org/Usa/Weapons/W88.html.

———. "Thermonuclear Weapons Design." *Nuclear Weapons Archive*, accessed March 26, 2017, http://nuclearweaponarchive.org/Nwfaq/Nfaq4-5.html.

Takigava, Noboru and Kouhei Washiyama. *Fundamentals of Nuclear Physics*. Tokyo: Springer, 2017.

Taylor, Theodore. "Third Generation Nuclear Weapons." *Scientific American* 256, no. 4 (1987): 30-39.

The White House. "Background Information: START II Ratification." January 26, 1996. http://fas.org/nuke/control/start2/docs/strtrat.htm.

Third Preparatory Committee for the 2000 NPT Review Conference. "Verification of nuclear disarmament: second interim report on studies into the verification of nuclear warheads and their components: Working paper submitted by the United Kingdom of Great Britain and

Northern Ireland." (NPT/CONF.2005/PC.III/WP.3). http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/prepcom04/papers/wp3.pdf.

Tolk, Keith et al. "Trusted Processor: A Result of the Evolution of Information Barrier Technologies." *INMM 48th Annual Meeting* (2007).

Tuckerman, Mark. "CHEM-UA 127: Advanced General Chemistry I." *New York University*. http://www.nyu.edu/classes/tuckerman/adv.chem/lectures/lecture_22/lecture_22.pdf.

Tulliu, Steve and Thomas Schmalberber. *Coming to Terms with Security: A Lexicon for Arms Control, Disarmament and Confidence-Building* (Geneva: United Nations Institute for Disarmament Research, 2003). https://www.files.ethz.ch/isn/92883/Full-text.pdf

Union of Concerned Scientists. "How Do Nuclear Weapons Work?" Last modified September 30, 2016, accessed March 27, 2017. http://www.ucsusa.org/nuclear-weapons/how-do-nuclear-weapons-work#.WNXvrjvytPY.

———. "Verification of New START." July 2010. http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/inspection-fact-sheet-1.pdf.

United Nations General Assembly, 71st Session. *General and complete disarmament: taking forward multilateral nuclear disarmament negotiations*, 2016 (A/C.1/71/L.41), available from http://www.un.org/ga/search/view_doc.asp?symbol=A/C.1/71/L.41.

United Nations General Assembly, 65th Plenary Meeting. "Implementation of the Declaration on the Denuclearization of Africa: Nuclear capability of South Africa." (A/RES/46/34A), http://www.un.org/documents/ga/res/46/a46r034.htm.

United Nations Institute for Disarmament Research and the Verification Research, Training and Information Centre (VERTIC). *Coming to Terms with Security: A Handbook on Verification and Compliance*. London: VERTIC, 2003.

United Nations Security Council. "Note by the Secretary-General." October 8, 1997. http://nsarchive.gwu.edu/NSAEBB/NSAEBB80/wmd07.pdf.

United States Congress. *Nuclear Safeguards and the International Atomic Energy Agency*. Washington, DC: U.S. Government Printing Office, 1995. https://www.princeton.edu/~ota/disk1/1995/9530/9530.PDF.

———. "Verification Technologies: Measures for Monitoring Compliance with the START Treaty." *Office of Technology Assessment* (1990). http://govinfo.library.unt.edu/ota/Ota_2/DATA/1990/9029.PDF.

United States Department of Defense. "New START: Article-by-Article Analysis Telemetry Annex." *Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.* http://www.acq.osd.mil/tc/treaties/NST/Art%20By%20Art/art_telemetry_annex.htm.

———. "Strategic Arms Reduction Treaty (START I): Executive Summary." *Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.* http://www.acq.osd.mil/tc/treaties/start1/execsum.htm.

———. "Strategic Arms Reduction Treaty (START II): Heavy Bomber Protocol." *Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.* http://www.acq.osd.mil/tc/treaties/start2/start2_prot_bomber.htm.

United States Department of Energy. "Restricted Data Declassification Decisions: 1946 to the Present (RDD-8)." *Office of Health, Safety and Security, Office of Classification*, January 1, 2002. https://fas.org/sgp/othergov/doe/rdd-8.pdf.

United States Department of State. "Action Memorandum, January 13, 1972." Available at http://nsarchive.gwu.edu/NSAEBB/NSAEBB60/abm29.pdf.

———. "Annex 15: Procedures for the Use of Radiation Detection Equipment." *START Treaty.* http://www.state.gov/documents/organization/27380.pdf.

———. "Fact Sheet: Telemetry." *Bureau of Verification, Compliance, and Implementation*. April 8, 2010. http://www.state.gov/t/avc/rls/139904.htm.

———. "Fact Sheet: Transparency in the U.S. Nuclear Weapons Stockpile." https://2009-2017.state.gov/documents/organization/241377.pdf.

———. "International Partnership for Nuclear Disarmament Verification (IPNDV)." http://www.state.gov/t/avc/ipndv/.

———. "International Partnership for Nuclear Disarmament Verification (IPNDV)." http://www.state.gov/t/avc/ipndv/.

———. "Report of the United States of America Pursuant to Actions 5, 20, 21 of the 2010 Nuclear Non-Proliferation Treaty Review Conference Final Document." *2010 Review Conference of the*

Parties to the Treaty on the Non-Proliferation of Nuclear Weapons. http://www.state.gov/documents/organization/225576.pdf.

———. "Report of the United States of America Pursuant to Actions 5, 20, 21 of the 2010 Nuclear Non-Proliferation Treaty Review Conference Final Document." *2015 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons*. http://www.un.org/en/conf/npt/2015/pdf/NPT-CONF2015-38.pdf.

———. "Strategic Arms Limitations Talks/Treaty (SALT) I and II." *Office of the Historian.* Available online at https://history.state.gov/milestones/1969-1976/salt.

———. "The New START Treaty: An Overview of the Verification Regime." *P5 Conference, Geneva, Switzerland*. http://www.state.gov/documents/organization/208183.pdf.

———. "Transparency in the U.S. Nuclear Weapons Stockpile." Available at https://2009-2017.state.gov/t/isn/npt/statements/241165.htm.

———. "Treaty on the Non-Proliferation of Nuclear Weapons." *U.S. Delegation to the 2010 Nuclear Nonproliferation Treaty Review Conference.* http://www.state.gov/documents/organization/141503.pdf.

United States National Security Council. "Memorandum for the Members of the Verification Panel: Preparations for Next Round of SALT." December 30, 1969. http://nsarchive.gwu.edu/nukevault/ebb281/6A.PDF.

———. "National Security Decision Directive Number 65: Establishment of National Security Council Arms Control Verification Committee." 1982. https://reaganlibrary.archives.gov/archives/reference/Scanned%20NSDDs/NSDD65.pdf

Vaijapurkar, S. G. "The performance evaluation of gamma- and neutron-sensitive superheated emulsion (bubble) detectors." *Radiation Protection Dosimetry* 130 (2008): 285-290.

Vanier, Peter et al. "Study of the CIVET Design of a Trusted Processor for Non-Intrusive Measurements." *INMM 42nd Annual Meeting* (2001).

VERTIC. "About VERTIC." http://www.vertic.org/pages/homepage/about/about-vertic.php.

———. "Confidentiality and Verification: the IAEA and OPCW." *Trust & Verify* No. 114. May-June 2004. http://www.vertic.org/media/assets/TV114.pdf.

———. "Verifying Libya's Nuclear Disarmament." *Trust & Verify* No. 112. January-February 2004. http://www.vertic.org/media/assets/TV112.pdf.

von Baeckmann, Adolf, Garry Dillon, and Demetrius Perricos. "Nuclear Verification in South Africa." *IAEA Bulletin 1/1995: National Reports.* https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull37-1/37105394248.pdf.

von Hippel, Frank. "Verification of Nuclear Warheads and Their Dismantlement: A Joint American-Soviet Study." INMM 31st Annual Meeting (1990).

Waltz, Kenneth. *Theory of International Politics.* Reading, MA: Addison-Wesley Pub. Co., 1979.

Wellerstein, Alex. "Kilotons per Kilogram." Restricted Data: The Nuclear Secrecy Blog, December 23, 2013, http://blog.nuclearsecrecy.com/2013/12/23/kilotons-per-kilogram/.

———. "Secrecy, Verification, and Purposeful Ignorance." Restricted Data: The Nuclear Secrecy Blog, September 23, 2016. http://blog.nuclearsecrecy.com/2016/09/23/secrecy-verification-purposeful-ignorance/.

Winner, Langdon. "Do Artifacts Have Politics?" *Daedalus* 109 (1980): 121-136.

Woolf, Amy. *Monitoring and Verification in Arms Control.* Washington D.C.: Library of Congress, Congressional Research Service, 2011. https://www.fas.org/sgp/crs/nuke/R41201.pdf.

———. *Nonstrategic Nuclear Weapons*. Washington D.C.: Library of Congress, Congressional Research Service, 2016. Available at https://www.fas.org/sgp/crs/nuke/RL32572.pdf.

Wuest, C. R. "The Challenge for Arms Control Verification in the Post-New START World." *Lawrence Livermore National Laboratory*, July 16, 2012. https://www.nti.org/media/pdfs/Wuest_2012_The_Challenge_for_Arms_Control_Verification_in_the_Post_New_START_World.pdf.

Yan, Jie and Alexander Glaser. "Nuclear Warhead Verification: A Review of Attribute and Template Systems." *Science & Global Security* 23 (2015): 157–170. http://scienceandglobalsecurity.org/archive/sgs23jieyan.pdf.

Zenko, Micah. *Toward Deeper Reductions in U.S. and Russian Nuclear Weapons*. New York: Council on Foreign Relations, 2010.

"SALT II and the Growth of Mistrust." *Transcript of the Proceedings of the Musgrove Conference of the Carter-Brezhnev Project*. May 7-9, 1994. http://nsarchive.gwu.edu/carterbrezhnev/C-B%20-%20SALT%20II%20-%20Musgrove%20master%20transcript.pdf.

"Security Dialogue Discussions, Moscow, Russia, December 15, 2008." January 14, 2009. https://search.wikileaks.org/plusd/cables/09MOSCOW68_a.html