Demonstrating a Warhead Tracking System

CNS

MARCH 2023

Marshall L. Brown Jr.

Middlebury Institute *of* International Studies at Monterey
James Martin Center for Nonproliferation Studies

Demonstrating a Warhead Tracking System

Marshall L. Brown Jr.

James Martin Center of Nonproliferation Studies
Middlebury Institute of International Studies at Monterey

460 Pierce Street, Monterey, CA 93940, USA
Phone: +1 (831) 647-4154
Fax: +1 (831) 647-3519

www.nonproliferation.org www.middlebury.edu/institute

This work was performed under contract (19AQMM21P1817) with the U.S. Department of State.

Cover image: The Mk 7 was the first nuclear weapon that could be carried by aircraft either internally or externally. It was for use against hardened or underground targets, such as bunkers, command centers, and submarine pens. Source: www.atomicarchive.com.

Contents

Executive Summary

On December 13, 2022, CNS Technical experts provided a proof-of-concept demonstration of a new methodology for secure nuclear warhead data exchanges, which was funded by the Department of State's Verification Fund. Such a methodology would support a verifiable nuclear warhead arms control treaty or other measures addressing nuclear warheads. The Warhead Tracking System methodology is based in part on the extensive technical engagements on nuclear warhead inventory management systems, under the Cooperative Threat Reduction (CTR) Nuclear Security program, from the mid to late 1990s up until the CTR agreement expired in 2013. The unique characteristics of each individual warhead are represented by a string of data, which for the purposes of this methodology is called a "passport." These passports can be exchanged securely using cryptographic "hash codes" (commitments) and would be periodically updated to account for warhead movements and operations.

The technical team developed and presented notional US and Russian passports and showed how that data would be transformed into hash codes. Because neither side would be prepared to disclose all data on its nuclear warheads, this methodology includes a data challenge procedure that would require certain data to be divulged, which, if confirmed to be valid, would provide some assurance that other data represented by the hash codes are valid. The technical team also explained the use of a mathematical proof that could be used by the sides to determine whether the data in the hash codes was valid by checking if it followed a particular set of rules, without revealing the data itself. The next step in developing this methodology is to integrate it into a comprehensive verification protocol, which is the subject of a forthcoming V Fund project.

Attendees at this demonstration were from The White House, Departments of State, Energy and Defense, National Laboratories, National Academy of Sciences, and NGOs (total of 25). A number of questions were posed during the demonstration that the technical team will take into account in the continued development and evolution of this methodology.

The B83 bomb had an explosive force roughly 80 times greater than that of the Hiroshima bomb. Its job was to obliterate hardened military sites and command bunkers, including Moscow's. The Biden Administration has announced plans to retire the weapon. Source: https://www.nytimes.com/2022/11/17/science/retired-nuclear-bombs-b83.html.

Introduction to the Warhead **Verification Demonstration**

Senior CNS Fellow and Project Manager Miles Pomper welcomed the attendees and opened the meeting by describing the CNS Report, "Everything Counts: Building a Control Regime for Nonstrategic Nuclear Warheads in Europe". That report, which was designed to feed into the US-Russian strategic stability talks, was funded by Denmark, Germany, the Netherlands, Norway and Sweden. Pomper explained that most of the work on the report had occurred prior to the February 2022 Russian invasion of Ukraine, and that the subsequent breakoff of the strategic stability talks has shown that now is not the time for arms control negotiations. At the same time there are only three years before New START terminates, and a future treaty will need to address both strategic and non-strategic warheads – a requirement set forth in the Senate's Resolution of advice and consent to the ratification of the New START Treaty. In this respect, the technical verification system contained in that report - demonstrated at this meeting - remained relevant and could lead to the development of a protocol on verification for nuclear warheads.

Assistant Secretary of State for the Bureau of Arms Control, Verification, and Compliance (AVC) Mallory Stewart remarked that there is a lack of trust between the US and Russia at the present time, but that DOE and the national labs are doing good work on possible verification systems for arms

control purposes: what is needed is to have verification that is credible and practical. She noted favorably the possible use of cryptology in verification methodologies, such as what was to be demonstrated at this meeting and stated that the State Department's V Fund existed to fund this type of project.

Warhead Verification Demonstration

CNS Consultant and Technical Team Leader William Moon began the technical demonstration by explaining the basis for the proposed warhead tracking system: the use of historical location and logistics data that can be used to identify and track individual warheads, and the associated data challenge concept. His technical team, consisting of Dan Zhukov and Neil Perry, built two notional but realistic data bases of US and Russian ("Blue" and "Red") warhead inventories, each consisting of 25 different kinds of warheads, which would be used to demonstrate how this system could work. He emphasized that such a system could be used to apply to any warhead and would provide the status of individual warheads. This tracking system is based on how much is already known from the 1992-2013 CTR experience – how the Russians move their warheads, and much of the historical data has already been exchanged with the Russians during technical exchanges. With respect to other possible kinds of verification, Moon noted that radiation detection is too expensive and intrusive, and tagging individual warheads poses safety and security concerns and might involve revealing sensitive information on design, composition, and performance -- which neither side would accept.

The warhead tracking system would create a virtual tool that contains historical data on the logistics (location, status, movements, operations, escort personnel, and certain components) of all warheads. At the same time, only enough data to identify one warhead from another would be required: the sides would compile this data in the form of a warhead "passport." Such a form would be understandable to the Russians since they used such a system, although on paper rather than in virtual form when they developed their warhead inventory management system in cooperation with the US CTR program. By using cryptologic methods, the sides would not share the details of that data except by specific procedures and over time. Moon explained that there would be a baseline data exchange for all warheads, and subsequent periodic updates for individual warheads. An immediate advantage of this methodology was that, through a baseline exchange of such data, the total number of warheads would be known for each side's inventory. A "data challenge" procedure would be developed to reveal individual data elements from these "passports," enabling sides to learn new information and confirming what they think they already know. In making successful challenges the sides would gains confidence in the validity of the whole data exchange process. To conclude his introductory remarks, Moon stressed that this was not a complete verification system but would serve as the foundation for such a system by providing a methodology to track warheads over their lifetimes.

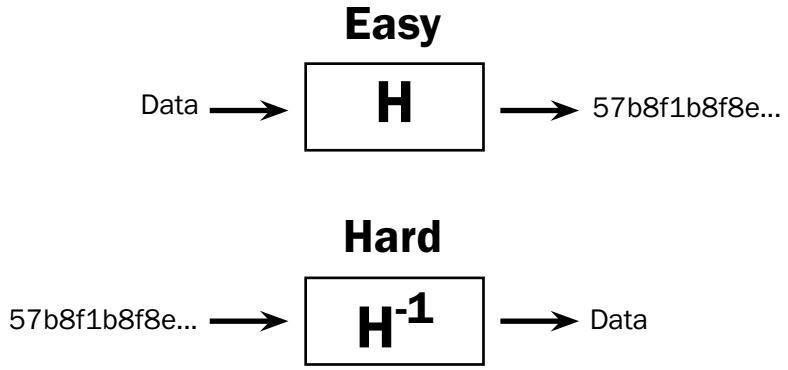
Moon described how a warhead "passport" – the compilation of logistical data on each warhead – would be created, and when a device would become accountable as a warhead: when the device is transferred from a production facility to the military and becomes part of the established inventory management system. Concerning whether the proposed methodology would apply to non-declared warheads, Moon clarified that, while this warhead tracking system would monitor only those declared, it would be difficult for a side to have a separate inventory management system to deal with non-declared warheads, but acknowledged that this issue would be addressed when a complete verification system was developed.

Moon, Zhukov. and Perry then discussed the notional US and Russian warhead passports, which were included in the briefing books provided to the attendees. They also described the codes used in the passports that apply to the location and status of warheads, noting that the operations would not be the same for both sides but that each side would be informed of what they signified, so that the status of a particular warhead would be known. A fundamental difference was the use of rail transport by the Russians (thus the identification of Rail Transfer Points was important) and air transport by the United States for transfer of warheads overseas, but in both cases these temporary locations might be susceptible to independent monitoring under a complete verification system.

Passport for Warhead #123 (Russian ALCM 2 Ukrainka)								
Date/Time	**Location**	**Status**	**Secondary Component**	**Limited Lifetime 1**	**Limited Lifetime 2**	**Operation Conducted**	**Personnel**	**Nonce Field**
09/10/2017 11:00	EADOT	RP	S02001	LLC102001	LLC202001	R11	EAD1	3eedc 2wsx
09/12/2017 08:00	EADOT	RI	S02001	LLC102001	LLC202001	R21	EAD1	0pp;;/8ik,888
09/15/2017 14:20	ER31K	RI	S02001	LLC102001	LLC202001	R322	R31K2	2wsxxdrt6
09/17/2017 01:30	ER31K	RI	S02001	LLC102001	LLC202001	R23	C312	77ujtt55ggg
09/17/2017 03:00	EC31K	RI	S02001	LLC102001	LLC202001	R311	C312	34gym,,8kik,,
09/18/2017 04:00	EC31K	RI	S02001	LLC102001	LLC202001	R25	C312	5tre34fddcv
09/18/2017 18:12	EC31K	RA	S02001	LLC102001	LLC202001	R16	C312	7rdxzsw345
09/25/2017 09:26	EC31K	RA	S02001	LLC102001	LLC202001	R43	C313	22W3TT&&
02/13/2018 13:25	EC31K	RA	S02001	LLC102001	LLC202001	R44	C314	vgv7^764
06/02/2018 16:20	EC31K	RA	S02001	LLC102001	LLC202001	R47	C315	XXDXTTVUG&
11/05/2018 05:05	EC31K	RA	S02001	LLC102001	LLC202001	R26	C312	9jnggh^51
11/05/2018 16:00	EA31U	RA	S02001	LLC102001	LLC202001	R311	A311	3u*7(Olmbb
11/07/2018 18:40	EA31U	RA	S02001	LLC102001	LLC202001	R25	A313	82WSXedc45,.
11/09/2018 23:42	EA31U	RA	S02001	LLC102001	LLC202001	R44	A313	&tr542$VBm
05/05/2019 05:20	EA31U	RA	S02001	LLC102001	LLC202001	R47	A314	{p;l88&&6hgv
12/27/2019 07:28	EA31U	RA	S02001	LLC102001	LLC202001	R44	A314	jjnhf461qa4dc
05/15/2020 19:39	EA31U	RA	S02001	LLC102001	LLC202001	R41	A312	OiJnuhb,.”/?
11/02/2020 08:08	EA31U	RA	S02001	LLC102001	LLC202001	R43	A312	OkmNBBh6fr4
11/11/2020 13:00	EA31U	RR	S02001	LLC102001	LLC202001	R12	A312	&**(uj*987dn
07/11/2021 10:10	EA31U	RS	S02001		LLC202001	R46	A315	88cnnshshcr4
09/11/2021 12:11	EA31U	RS	S02001			R46	A315	*nimjmmkol,2
02/05/2022 10:30	EA31U	RS	S02001			R26	A311	Ookm789
02/05/2022 21:00	ER31K	RS	S02001			R313	R31K1	2345tgy67uj
02/06/2022 09:30	EADOT	RS	S02001			R22	EAD1	543erfdvv
02/07/2022 19:30	EADOT	RS	S02001			R13	EAD1	Buuj4425789
02/07/2022 23:10	EADOT	RS	S02001			R14	EAD1	9jnnnbvc33SA
06/30/2022 08:00	EADOT	RM	S02001			R15	EAD1	7y&8Uhbhger

Perry discussed how the sides could exchange data on all warheads without sharing the information contained therein, since it was unlikely that either side would accept sharing all information about their nuclear warheads, for security reasons. This ability to exchange data while preserving security was accomplished through the development of cryptographic "hash codes" to create a unique, virtual identifier for each warhead, which represented the passport of each individual warhead. This hash code would be updated as the status of that warhead changed. It was explained that the hash code was like an envelope in which data was placed, and that data would be revealed only when, and if, that envelope was opened. And, when the envelope was opened, the data would be "proven" through an exchange of the hash codes proofs provided by the side that initially had provided the hash code: this would be part of the "data challenge" process. Importantly, the operation to produce hash codes from a given dataset is a one-way function, and it is practically impossible to reproduce the original data from the committed hash code that represents it – the envelope cannot be broken into. Perry added that Russia and the United States used different methodologies to produce hash codes, so for this project CNS developed a code that uses both methodologies. In this way, the sides would have confidence in the coding even if they did not trust each other's methodology.

A simplified visualization of how a hash function operates is shown below:



Moon explained that there would be frequent exchanges of hash codes representing updated data but that it would be for the sides to negotiate the notification timelines, noting that based on previous technical exchanges with the Russian Ministry of Defense it would probably be between 30 and 90 days after the particular activity or operation concluded. The data exchanges, both the initial baseline and subsequent data updates, would be provided to the respective NNRRCs.

Perry described another way the sides could evaluate the committed data (data in the hash code), without revealing any data. The Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) tool is a program that provides a mathematical proof that the data set represented by the hash code is a valid set of data based on an agreed set of parameters. This

tool would be used to determine whether the rules on what data goes into the passport and how it is formatted (before being committed) were being followed. The two sides would have to negotiate the specific rules to be tested. Perry and Moon reviewed the several dozen rules that were tested on the 50 passports by the CNS zk-SNARK tool.

The technical team then turned to the last piece of the warhead tracking system, the data challenge procedure, which would be used to reveal the original data represented by the committed hash codes and thus build confidence in the accuracy of the data used to generate the hash codes. Moon characterized this also as the first step in building a verification system. The team developed 50 different examples of data challenges and each data challenge would reveal more data, thus providing more confidence in the validity of the data exchanged between the sides. Moon remarked that even "old" intelligence could be used for data challenges, and he recalled the popular board game "Battleship", which permits the challenging side, as each "challenge" receives a positive or negative response, to obtain more information. Data challenges can be quite creative, and there is no requirement that the challenged party be informed of the information on which the challenge is based. An example was presented of a series of four data challenges, in which more data is provided with each subsequent challenge. All 50 data challenges were included in the notebooks provided to the participants.

A visualization of the data challenge process is shown below:

Visualization of the Data Challenge Process

1. The host party derives a hash from a passport entry or a notification
2. The hash is committed to the observing party
3. Later, the observing party issues a data challenge for the commitment
4. The host party decommits the original passport entry or notification and shares it along with a cryptographic proof
5. The observing party vallidates the decommitted data by using the proof to derive a hash and comparing it to the original commitment

- The cryptographic commitment is immutable: If there is any change in the original data entry between steps 1 and 4, the hash code derived in Step 5 will be different.
- Challenges can be designed to correlate with NTM or other known data points to further increase confidence in the data validity.

Before turning to Perry to demonstrate how hash codes could be validated as part of the data challenge procedure, Moon acknowledged that the warhead tracking system that he and his team had outlined was not a complete solution to warhead verification and would track only declared warheads. The next step would be to come up with a comprehensive verification protocol, although the parties could decide to start out with technical discussions,

which could address the entire inventory of warheads or just a subset, such as non-strategic nuclear warheads, or even just the warheads located at a particular site. What would also be needed, with respect to data challenge procedures, is the number of such challenges, their frequency, and their format. In addition, the frequency of data updates would need to be negotiated. As next steps, in terms of verification measures, one could consider video, displays in the open, and additional measures to detect non-declared warheads. He also emphasized the need to have some sort of bilateral entity, like New START's BCC, to address issues that arise in the implementation of the warhead tracking system.

At the conclusion of the demonstration, Moon emphasized two points that he wanted the attendees to consider:

1. A "step by step," or bottom-up approach, to developing an agreement dealing directly with warheads, taking into account the different warhead operational systems of the two sides. This would require extensive negotiations to settle issues or "trade-offs" before such a system could be implemented. Under this approach, the sides could agree to conduct technical discussions on developing a warhead tracking system before any political agreement addressing warheads was reached.

2. This warhead tracking system methodology could support a wide range of risk reduction as well as potential arms control applications. These could include some simple risk reduction measures such as enabling notifications of safety and security warhead movements that could reduce the risk of miscalculating that warhead movements are being conducted for warfighting purposes. It could also support a pullback of certain warheads from one or more locations as a risk reduction measure or could be used to monitor warheads at a particular site or region. All these possibilities could precede any talk of a freeze or reduction in stockpiles. One could also view the exchange of data on warheads to support deterrence by providing evidence of nuclear capabilities while at the same time contributing to stability by pointing out sub-elements of the stockpile that may be of most interest, such as identifying the actual numbers of warheads that may be active, inactive, reserve or scheduled for dismantlement at a particular time and date.

Former NATO Deputy Secretary General Rose Gottemoeller acknowledged the work at the national laboratories and in international organizations on monitoring warheads, adding that the team's focus on data exchange/notifications fills a gap. She noted the contribution of the Stanford cryptography community that developed the technical background for this warhead tracking system, and she indicated that she expected a lot of help from them.

The Honest John was the first nuclear-tipped rocket to be deployed by the United States Army. It was a simple, free-light rocket capable of delivering a nuclear warhead. Courtesy of William Moon.

Additional Comments and Questions Raised during the Warhead Verification Demonstration

Prior to the conclusion of the morning session, and during the afternoon session, which was devoted to in-depth discussion of the relevant technologies, a number of questions were raised based on the demonstration, which included:

1. Concerning the identification in the warhead "passport", of personnel involved in a particular operation, and its potential counterintelligence implications, Moon clarified that these would not show operational personnel and perhaps a photo would be taken of an escort, with an indication of the date/time/group.

2. Concerning red teaming this methodology, Moon responded that it would be necessary and would likely begin after the proof of concept.

3. Concerning data updates, how would items be treated that were outside the tracking system, and thus wouldn't it be necessary to start off with a treaty text, Moon responded that the warhead tracking system that was being demonstrated was just a building block.

4. Concerning the need for more robust monitoring, Moon responded that it would be needed, including monitoring for the absence of warheads, and not just of data exchange.

5. Concerning the negotiability of this system, it was noted that U.S policymakers would have to be convinced of its utility and to be informed on what the Russians, as well as the cryptography community, are doing. Moon indicated that the only connection at this point with the Russians is through the Russian Academy of Sciences, which did not involve discussions on cryptography. Perry added that there was some concern in the cryptography community that there could be access to the data via "back doors" but that there were ways of constructing the hash codes that help to alleviate these concerns. Concerning hash codes, the team acknowledged that there are different ways to build hash codes to address this but, as long as they work, they would be acceptable.

6. Concerning more robust monitoring, Moon noted that every aspect of a warhead's activity is registered, and that while there are no arms control

inspections being conducted at this time, inspections could be part of the next step in this project: a side could still do a lot without inspecting everything all the time – spot checking could be enough. He added that the sides previously conducted technical discussions on their respective warhead inventory management systems and that the data contained in the warhead passports is already tracked by those systems.

7. Concerning whether a side could cheat by switching warheads with items that are not warheads, it was noted that even training warheads and warhead containers are tracked by the Russians. Moon explained that the Russians do not open up containers to determine whether what is inside is a warhead or not: when a warhead is placed in a container, the Ministry of Defense's representative at the facility signs off on the transfer of custody, and the warhead is not taken out during transport or storage. He remarked that both sides already know how each side operates, although it is difficult to know what is in reserve or scheduled for destruction. In addition, the Russians may not have as many warheads on active status as does the U.S.

8. Concerning the number of data fields that would be contained in a warhead passport, there could be as few or as many as needed, which is why red-teaming would be useful.

9. Concerning a cheating scenario, whereby the Russians had a totally separate system to deal with non-declared systems, it would require that the Russians deconflict with the system for declared systems, and it would be difficult to do across the board. In any event, arms control means making it difficult to cheat, and additional measures would be necessary to prevent cheating altogether.

10. Concerning the need to have some external verification, which could include access or stand-off verification techniques, the team acknowledged that the sides would definitely have to negotiate such measures, and perhaps the use of hash codes to validate photographs.

11. Concerning whether the data points would evolve over time, Moon responded that some of the hash codes may not be divulged for years, and that this could be based on an agreement between the sides.

12. Concerning possible asymmetry in the data columns, it was recognized that this could present political issues on the U.S. side, and this was something that would have to be considered when agreeing upon the data to be provided.

13. Concerning the likely resistance of the Russians to what they might consider to be "verification tourism," which could include the idea of adding data points that would not be verified for years, it was suggested that the U.S, provide an estimate of the data that would be needed; Moon acknowledged that the data would not have to cover everything and would

be subject to negotiation. He added that the Russians might be interested in finding out, for example, whether certain U.S. warheads were active or inactive, and a data column identifying the status could indicate that.

14. Concerning the need for on-site inspection as part of a comprehensive verification methodology, Moon stated that such inspections will be needed but the warhead tracking system may not require as many on-site inspections as would be required without such a system.

15. Concerning data challenges, Moon remarked that the rules would be negotiated and that both sides would thus know what the rules were.

16. Concerning the need, from a policy-maker's viewpoint, to be convinced that the data is verifiable, and that the warhead tracking system would provide some tangible results, Moon noted that there would be NTM data, as well as the results of the data challenge, to demonstrate its validity, and while thousands of data points would be exchanged, he acknowledged that this was not a complete verification system – that was the next step.

Conclusion of the Meeting

The meeting concluded with the attendees expressing their appreciation for the demonstration by the technical team and their interest in seeing the results of the next step, the creation of a comprehensive verification protocol that includes the warhead tracking system.

Presentation at the James Martin Center for Nonproliferation Studies.

About the Author

Marshall L. Brown Jr. was the legal adviser to the US delegation during the negotiation of the Strategic Arms Reduction Treaty (START I), the Open Skies Treaty, the Comprehensive Nuclear-Test-Ban Treaty, the US-Poland missiledefense basing agreement, and the New Strategic Arms Reduction Treaty. He also participated in periodic implementation meetings for the Anti-Ballistic Missile Treaty, the Intermediate-Range Nuclear Forces (INF) Treaty, and START I, as well as in meetings on the Convention on Certain Conventional Weapons and in review conferences for the Biological and Toxin Weapons Convention and Chemical Weapons Convention. He served as attorney-adviser and assistant general counsel in the US Arms Control and Disarmament Agency, as force counsel in the Multinational Force and Observers (Sinai), and as attorney-adviser in the US State Department, from which he retired in 2010. Brown was also a co-author of Occasional Paper 55 *Everything Counts: Building a Control Regime for Nonstrategic Nuclear Warheads in Europe*.

nonproliferation.org

Middlebury Institute *of*
International Studies at Monterey
James Martin Center for Nonproliferation Studies