DET Webinar Series
New Tools for Transparency, Verification, and Confidence Building
3 November 2021

Step-by-Step Warhead Data Exchange Methodology

William M. Moon
Nonresident Fellow, Stimson Center
Technical Team Lead, Center for Nonproliferation Studies (CNS) Research Project:
Verification of Nonstrategic Nuclear Warhead Stockpiles

Warhead Verification

- CNS study supported by Belgium, Denmark, Netherlands, Germany, and Sweden to examine verification of nonstrategic nuclear warheads.
- Arms control treaties limit delivery systems, no direct limits on warheads and none on nonstrategic warheads.
  - Warheads are small, mobile, difficult to detect and monitor;
  - On-site inspection is intrusive, raises safety and security concerns – no electronics, video;
  - Direct observation difficult, warheads stored in containers, made up of various components.

Designing a Warhead Data Exchange Methodology

- Need a way to “tag” and track warheads throughout their service life
  - without revealing sensitive information on design, composition, or performance;
  - without creating nuclear safety or security vulnerabilities;
  - without disrupting warhead operations.

Previous US-Russian Warhead Data Exchanges under CTR and Mil-to-Mil

- Cooperative Threat Reduction (CTR) program (1992-2013), US and Russia worked together to develop and implement warhead inventory management systems (AICMS & DIAMONDS).
- Inventory management systems track warheads by locations, movements, other transactions. CTR and Mil-to-Mil technical exchanges shared data such as:
  - Warhead storage, transport, and disassembly locations;
  - Warhead shipments conducted;
  - Component shipments;
  - Security check and inventory management audit procedures.
- Historical data of this kind is not as sensitive as design, composition, or performance, and can be exchanged.
- This data can be used to create a unique identifier, or “Warhead Passport,” for individual warheads. A unique, virtual tool to identify and track warhead transactions.

Using Cryptography to Share Data

- While historical data on warhead transactions may be shared, the US and Russia would not want to exchange a complete history of their warhead life cycles.
- Cryptography, however, can be used to create a unique “hash code” that represents the warhead passport, like a label, but does not contain any data.
  - A hash is a string of letters and digits generated from any dataset by a **hash function;**
  - a hash function **cannot be reversed** to get the original input data from a hash code;
  - **no two datasets will yield the same code** when run through the same hash function.
  - With hashes, individual warheads’ life cycle data can be cryptographically committed to the other side.
- Each country’s warhead inventory would be represented by an immutable ledger of warhead passport hash codes.

Notional Warhead Passport Updating Methodology

Passport ID Hash: 8df91ks83v0

Date/Time	Location	Status	Components	Operation	Personnel
11-11-2001 14:00	Departure from Assembly-1	Inactive	Primary (P), Secondary (S), Limited Lifetime Component (LLC), Permissive Action Link (PAL)	Transfer of Custody (TOC)	Escort-1
11-13-2001 06:15	Arrival RTP-1	Inactive	P, S, LLC, PAL	Rail to Road Transfer	Escort-1
…	…	…	…	…	…
01-02-2013 13:15	Central Storage Site-1	Active	P, S, LLC, PAL	Audit	Escort-4

Update 1 Hash: b1s5oe25am

01-08-2023 02:06	Central Storage Site-1	Scheduled for dismantlement	P, S, LLC, PAL	Designated for dismantlement	Escort-11	Previous hash: 8df91ks83v0

Update 2 Hash: a832j3msy1s

02-03-2023 12:40	RTP-5	Scheduled for dismantlement	P, S, PAL	Transportation	Escort-11	Previous hash: b1s5oe25am

Update 3 Hash: x98y1h3ni0

02-05-2023 18:57	Disassembly-3	Dismantled	P, S, PAL	TOC: Disassembly	Escort-11	Previous hash: a832j3msy1s

Each data update includes the previous hash in order to form a continuous and immutable chain of commitments

Step-by Step Data Exchange Methodology

- Baseline: the sides exchange a ledger of hash codes, representing the warhead inventory, that cryptographically commit data from nuclear warhead passports.
- Data Updates: the sides commit hashes representing all applicable warhead transactions within a specified timeframe.
- Data Challenges:
  - The observing party requests the host to “de-commit” or reveal a specific data element of a warhead passport;
  - The parties validate or confirm the data by running it through the hash function to ensure it produces the identical hash code.
- Data is revealed step-by-step, with each challenge revealing more data in order to build confidence in the individual warhead data and overall inventory. No current or projected data will be released.
- Since the challenges are samples of the overall inventory and may address any point in the history of a warhead’s life cycle, each de-committed data point increases confidence in the validity of the overall ledger.

Visualization of the Data Challenge Process

1. The host party derives a hash from a sensitive data entry

2. The hash is committed to the observing party

3. Later, the observing party may challenge the committed hash

4. The host party shares the original data entry

5. The verifying party also derives a hash and compares it to the hash committed by the host

- 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. **change word sensitive

Warhead Data Exchange Methodology as a Transparency, Verification, and Confidence-Building Tool

- Data Exchange concept is not intended as a comprehensive verification solution.
- Step-by-Step: US-Russian Joint exercise(s)/demonstration(s) should be conducted using notional data to further develop the concept in support of potential diplomatic discussions or agreement(s). CNS developing a table top demonstration.
- Enables the sides to build confidence in the data exchange process over time, thus creating a foundation for future verification.
- Could be applied to entire inventory, or any agreed sub-set of data such as deployed or non-deployed warheads, strategic, nonstrategic, warheads destined for dismantlement, or warheads at specific storage sites.