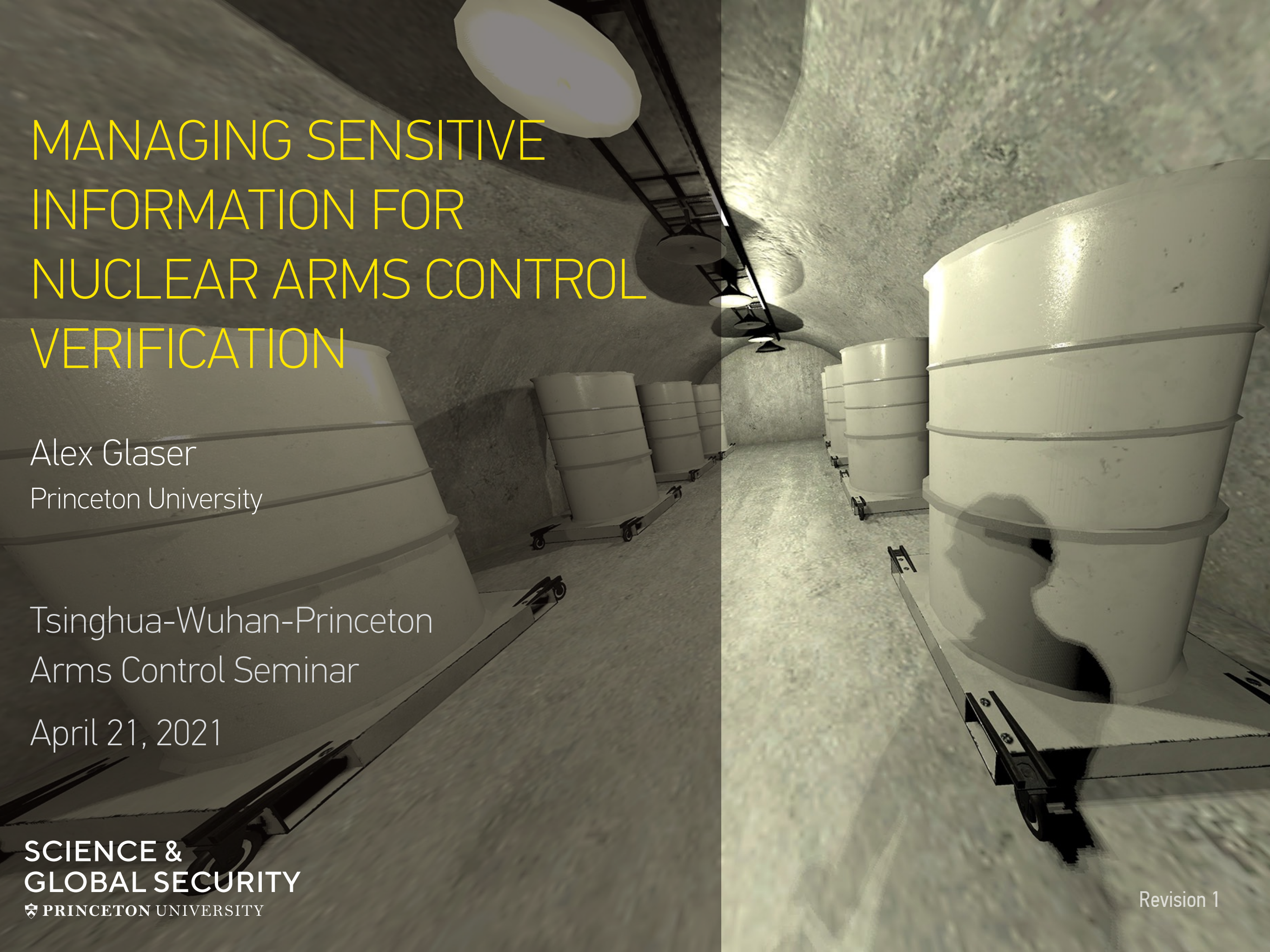




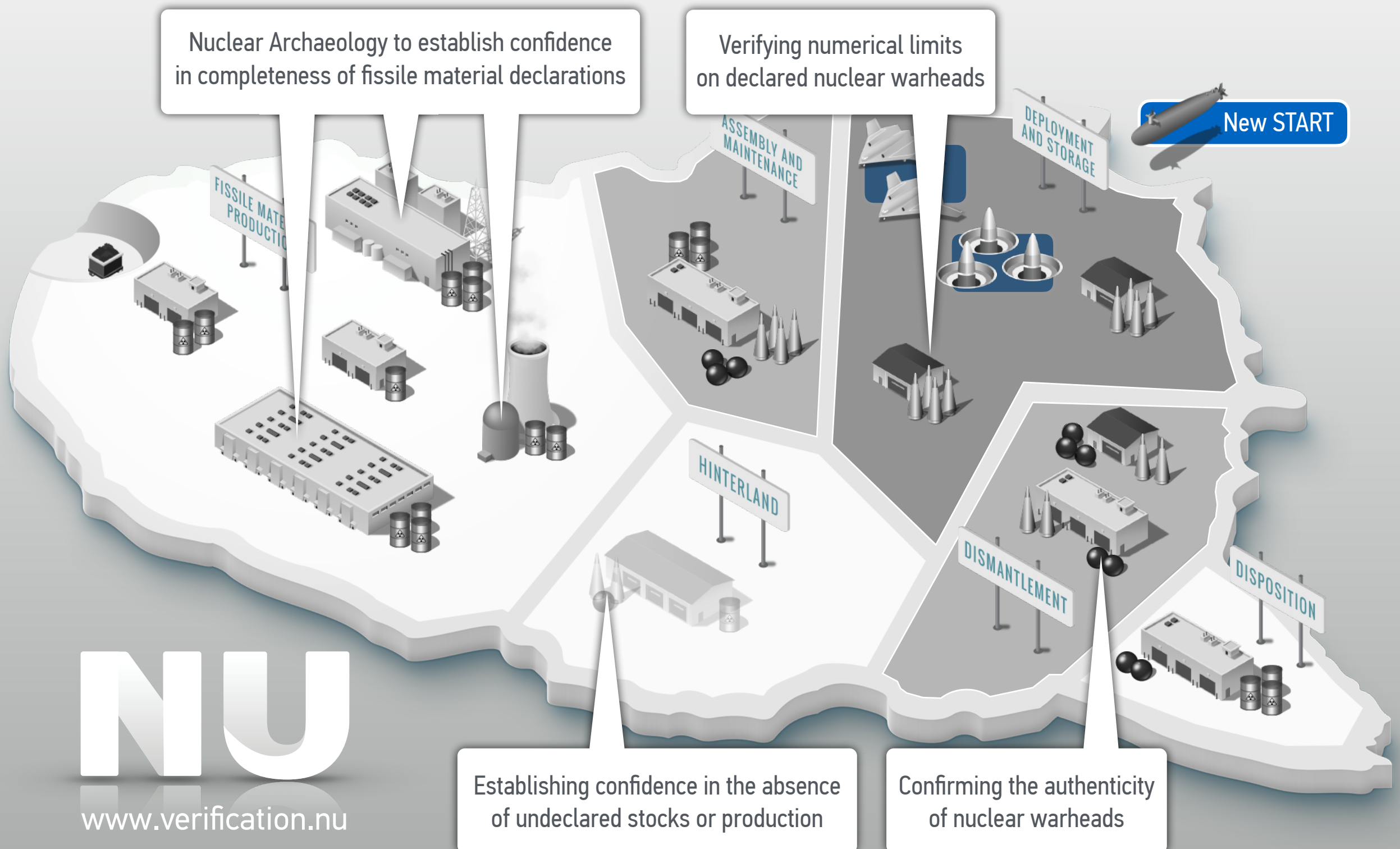
MANAGING SENSITIVE INFORMATION FOR NUCLEAR ARMS CONTROL VERIFICATION

Alex Glaser
Princeton University

Tsinghua-Wuhan-Princeton
Arms Control Seminar

April 21, 2021

VERIFYING DEEPER REDUCTIONS



DEALING WITH SECRETS

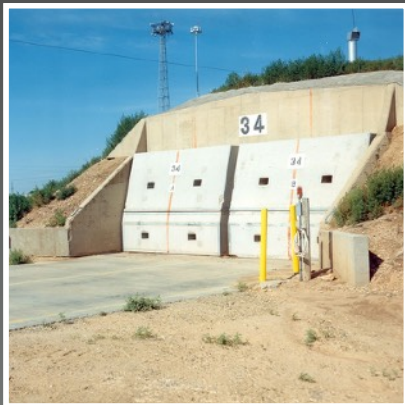
(Warheads and other classified nuclear components)

HOW NOT TO GIVE AWAY A SECRET



CONTINUE IMPROVING TECHNOLOGIES AND APPROACHES

Work on information barriers with a particular focus on certification and authentication; in particular, identify joint hardware and software development platforms



REINVENT THE PROBLEM: NEVER ACQUIRE SENSITIVE INFORMATION TO BEGIN WITH

Explore fundamentally different verification technologies and approaches; for example, develop alternatives to onsite inspections at certain sensitive facilities



REVEAL THE SECRET

Requirement to protect sensitive information is typically the main reason for complexity of verification approaches; for example, mass of fissile material in a nuclear weapon

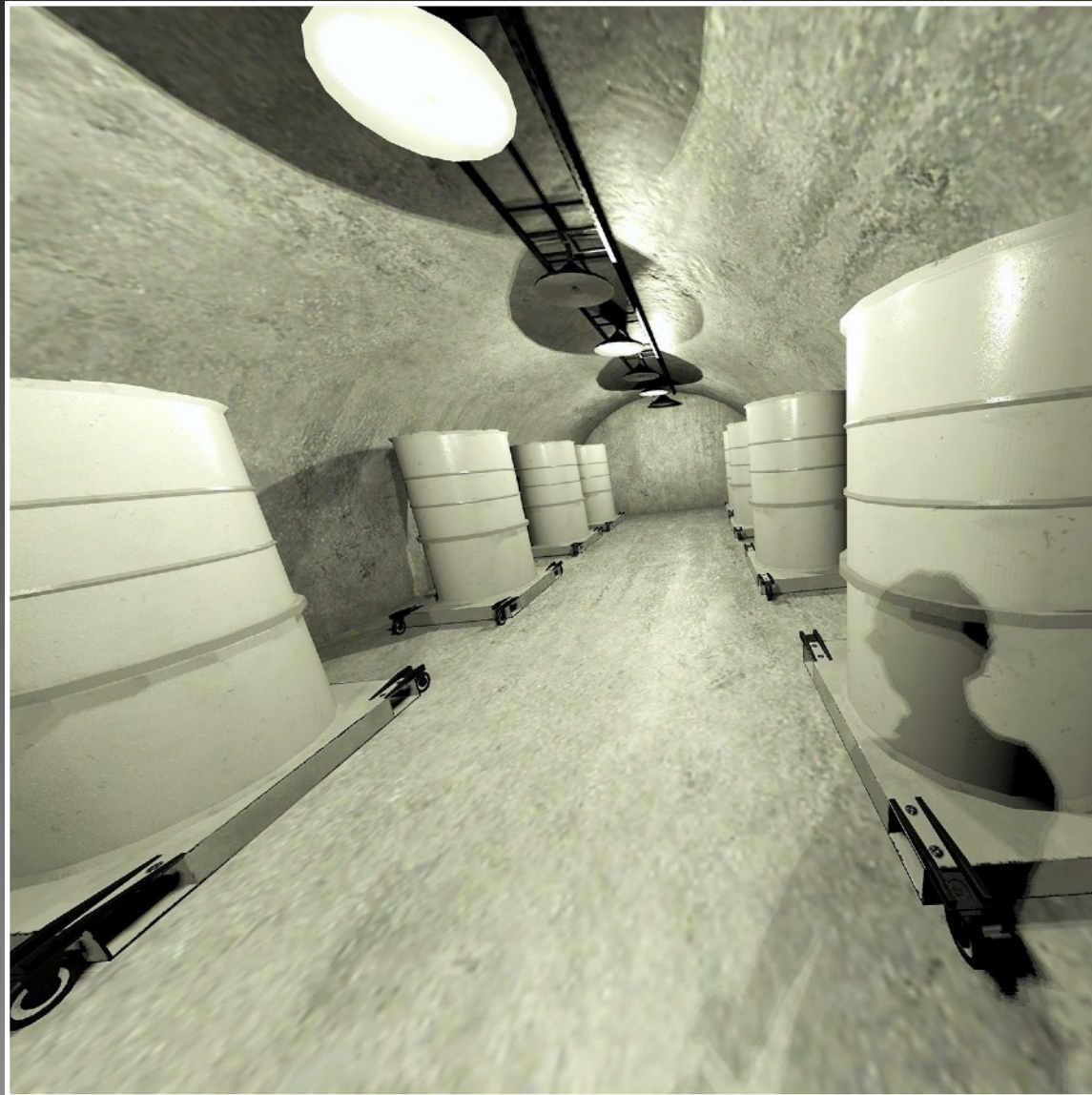
Source: Author (top and bottom), altave.com.br (middle)

REINVENTING THE PROBLEM

Example 1: Confirming Absence

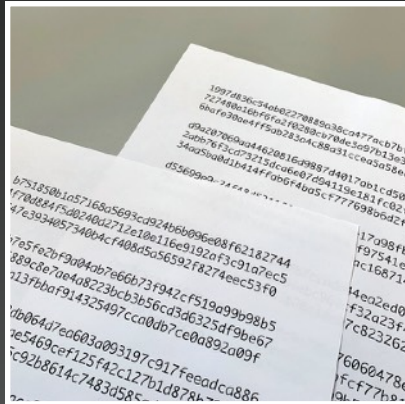
ABSENCE MEASUREMENTS

BUILDING ON EXPERIENCE WITH NEW START



Source (right): Randy Montoya, share-ng.sandia.gov/news/resources/news_releases/treaty_equipment

FEATURES OF AN ABSENCE REGIME



BASIC APPROACH

- Conduct routine & challenge inspections to confirm correctness of declarations
- Accept all items as treaty accountable that the host declared as such
- Only inspect other items present at site to confirm that they are indeed not accountable



RELEVANT VERIFICATION TECHNOLOGIES

- Simple radiation (neutron and/or gamma) detection equipment (only as needed)
- No information barriers required

For more, see: Radiation Detection Equipment: An Arms Control Verification Tool, DTRA, 2011



ADVANTAGES & SHORTCOMINGS

- Well established (as part of New START)
- Low risk of exposing sensitive information (if access can be facilitated/managed)
- Ambiguity could help address some security concerns of parties

Source: Author (top), www.idealvac.com (middle), and quad-nvp.info (bottom)

REINVENTING THE PROBLEM

Example 2: Secure Declarations

“PRIVACY-PRESERVING DECLARATIONS”

ITEM 01: 67d97802b84a6db872aacc400a0f5eaeabcec52012503111891b0d1e89711605
ITEM 02: b3c22af3a5f9ecc51c5cf6b4604e2bef191e4ceb305c6ef4a9589206e0bd7e62
ITEM 03: 0b277554264c8d00e81fb4b0af3f39f753146c8881ce093d7d45e8212cce95ac
ITEM 04: 4161814ef03933b605958325ca0aa3a3d9d2106f8f79b2c28cec5e75ea70266b
ITEM 05: f5c53f5c375c22f6e20554d5d7488f1cc678caa4fdc50aca77057c4755d7b12b
ITEM 06: fb28390a1b3db5db0fb44534a8a8c8716dccf64aa41828658b5fcadaf82b37c8
ITEM 07: 368bfb3e543c11dec2511b38e59dd4dadf7eb0ed87d3128d8f3f13c0b37073c5
ITEM 08: a1e89078ac797a3cfc8423965ca966645b62e2e212597e81b9c2a2e041778fd4
ITEM 09: f7618c3fead199ec24dcdbf6854d993330a8870c9e6a313d15d8fd988877f813
ITEM 10: 2abd37560821d1e5007a26c3ec0e25a16c46dcea5258605e0a2ef207ecf98520
ITEM 11: 9280cac30c39ea62daf66f082f2a574ae865308be5bb49cce11dabebf26a6a8c
ITEM 12: f7467d431353ce15dfe0dc6395e9e6a8806afd3222467ffb5eb1105bfa90bb31
ITEM 13: 023cc75fce0d55eb9cce5aa4b9f79d20d3da555c98048abfcc147c797a8db642
ITEM 14: 4108821ea003aaceefdb8c2d86126c33a5315b62043b36d5e612bc831e446896
ITEM 15: 340bcbda4afb3409f2d750f0a3ac029270a27e727c83650d8b6417d8153765a2
ITEM 16: bca49804e0b0da52df8f533d91d680e26818752111538dea4401277bc6cfa2e3

Declaration in hashed form (with one entry per item)

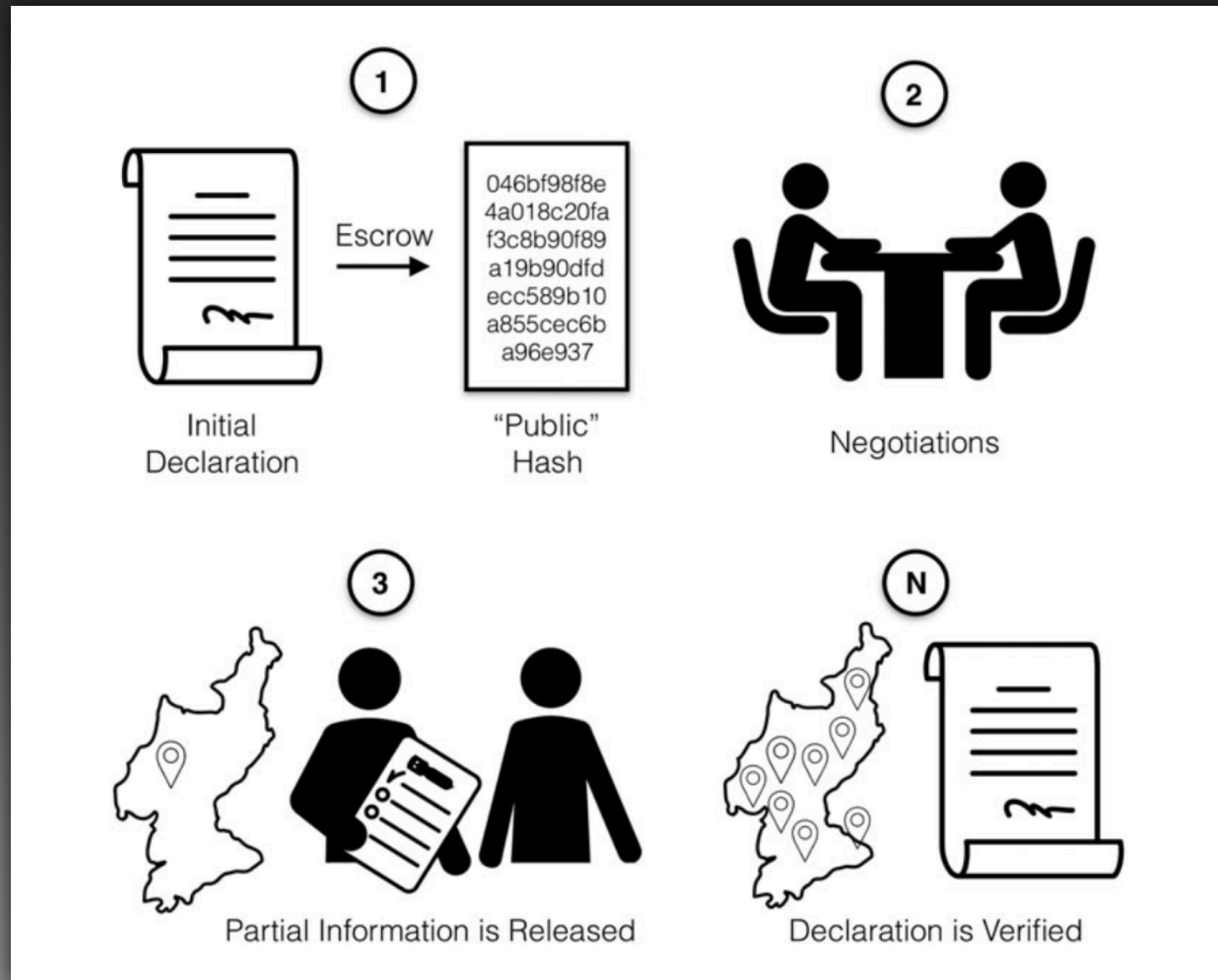
ITEM 01: 67d97802b84a6db872aacc400a0f5eaeabcec52012503111891b0d1e89711605
ITEM 02: b3c22af3a5f9ecc51c5cf6b4604e2bef191e4ceb305c6ef4a9589206e0bd7e62
ITEM 03: [8edd164eb3fd9116](#) SITE C :: W99 :: TIME 12345678 [a562c8ffefbc2fb](#)
ITEM 04: 4161814ef03933b605958325ca0aa3a3d9d2106f8f79b2c28cec5e75ea70266b
ITEM 05: f5c53f5c375c22f6e20554d5d7488f1cc678caa4fdc50aca77057c4755d7b12b
ITEM 06: fb28390a1b3db5db0fb44534a8a8c8716dccf64aa41828658b5fcadaf82b37c8
ITEM 07: 368bfb3e543c11dec2511b38e59dd4dadf7eb0ed87d3128d8f3f13c0b37073c5
ITEM 08: [25b78703bcbdcfa7](#) SITE C :: W99 :: TIME 12345678 [0e62292b6c2f98a3](#)
ITEM 09: [184702dc19247c56](#) SITE C :: W99 :: TIME 12345678 [6f2efeb7be00fc82](#)
ITEM 10: 2abd37560821d1e5007a26c3ec0e25a16c46dcea5258605e0a2ef207ecf98520
ITEM 11: [c02d3fee2ad8a77a](#) SITE C :: W99 :: TIME 12345678 [dfa54d7edc14494b](#)
ITEM 12: f7467d431353ce15dfe0dc6395e9e6a8806afd3222467ffb5eb1105bfa90bb31
ITEM 13: 023cc75fce0d55eb9cce5aa4b9f79d20d3da555c98048abfcc147c797a8db642
ITEM 14: 4108821ea003aaceefdb8c2d86126c33a5315b62043b36d5e612bc831e446896
ITEM 15: 340bcbda4afb3409f2d750f0a3ac029270a27e727c83650d8b6417d8153765a2
ITEM 16: bca49804e0b0da52df8f533d91d680e26818752111538dea4401277bc6cfa2e3

Declaration with entries for Site C revealed



“PRIVACY-PRESERVING DECLARATIONS”

(CONTINUED)



Sébastien Philippe, Alexander Glaser, and Edward W. Felten, “A Cryptographic Escrow for Treaty Declarations and Step-by-Step Verification”
Science & Global Security, 27 (1), 2019, scienceandglobalsecurity.org/archive/sgs27philippe.pdf

A PATH FORWARD

FOR NUCLEAR DISARMAMENT VERIFICATION



RETHINKING NUCLEAR DISARMAMENT VERIFICATION

Explore verification approaches that minimize access to treaty accountable items and avoid measurements on those

Consider approaches that offer “on-ramps,”
i.e., that start off simple and can accommodate “upgrades” later on



ABSENCE VERIFICATION & SECURE DECLARATIONS

Two complementary concepts that (together) could lay the basis for future (bilateral or multilateral) arms-control agreements that place limits on the total number of weapons in the arsenals

Source: IAEA (top, [flickr.com/photos/iaea_imagebank/albums/72157659464420989](https://www.flickr.com/photos/iaea_imagebank/albums/72157659464420989) and Randy Montoya (bottom)

