HIDDEN IN PLAIN SIGHT

CAN CRYPTOGRAPHY HELP CRACK THE NEXT GENERATION OF NUCLEAR ARMS-CONTROL TREATIES?

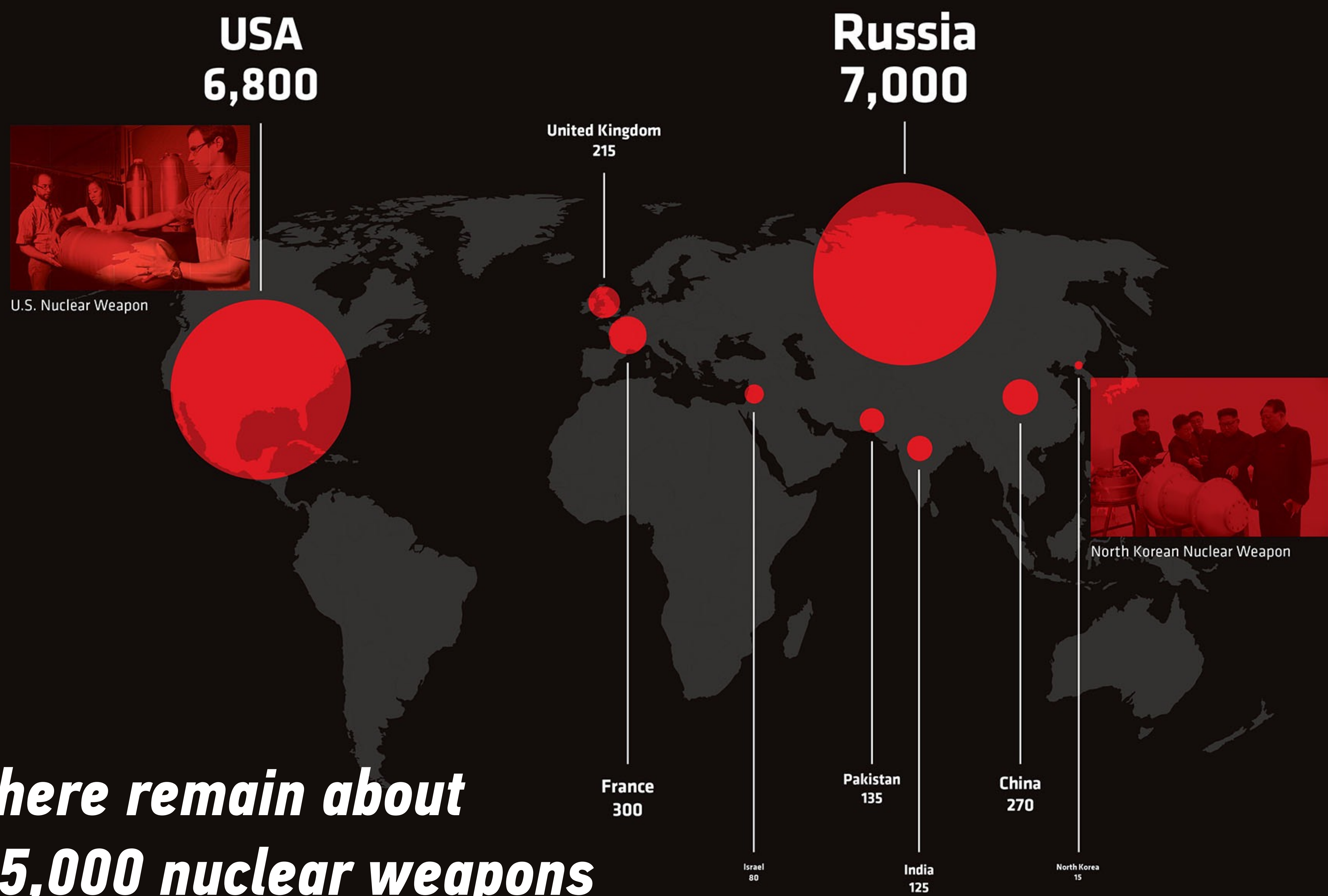
Alexander Glaser and Sébastien Philippe

Princeton University

Ruhr-Universität Bochum, November 17, 2017

Revision 3z

BACKGROUND



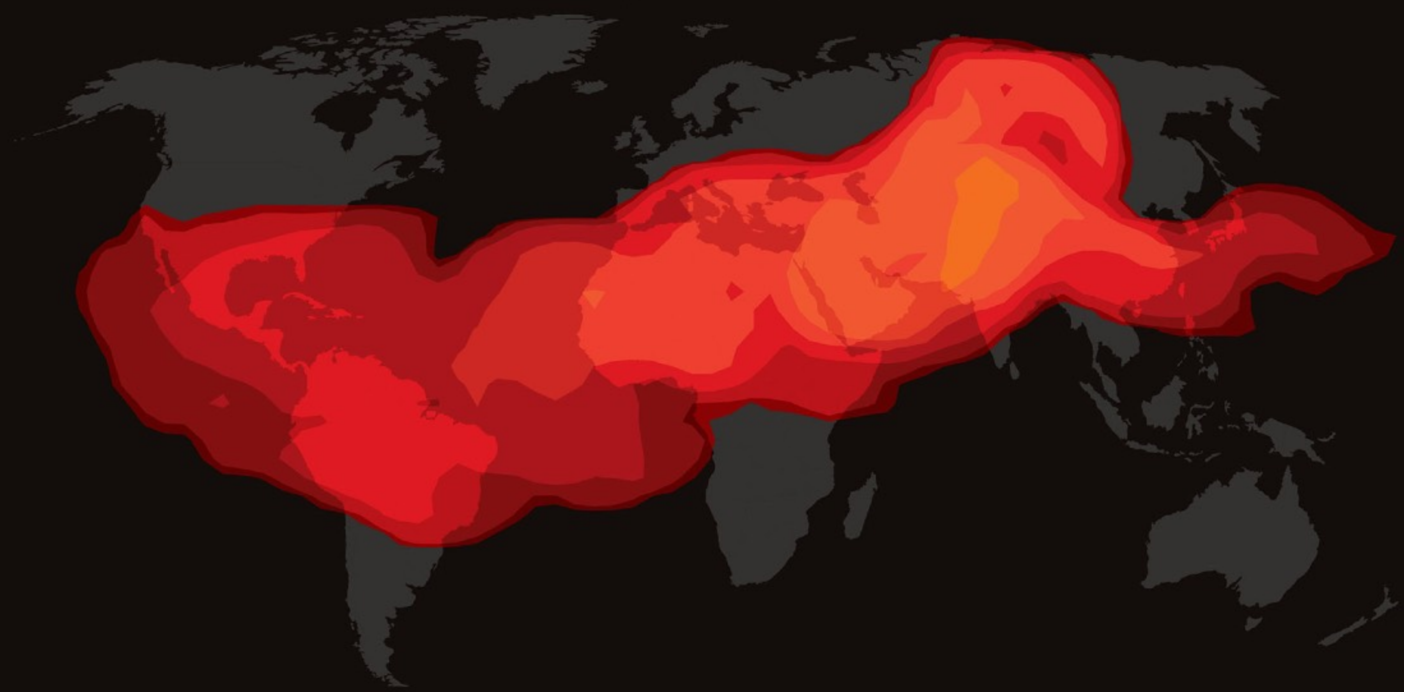
There remain about 15,000 nuclear weapons in the world today

Hans Kristensen and Robert Norris, Nuclear Notebook, Federation of American Scientists and thebulletin.org/nuclear-notebook-multimedia

Day 4: May 18th

Even a “limited” nuclear war has global environmental consequences

Day 7: May 21st

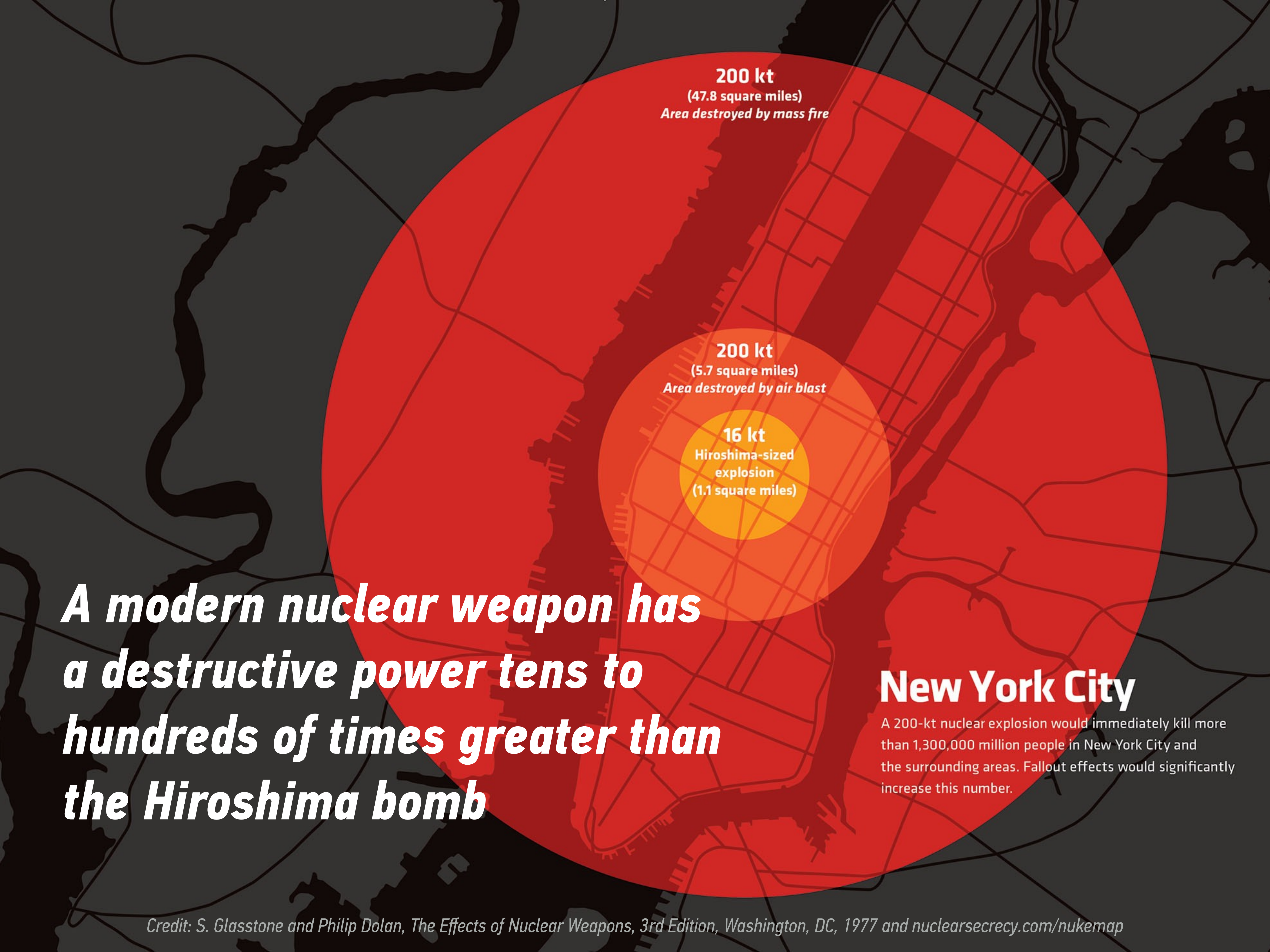


Smoke from a regional nuclear war between India and Pakistan

Black Carbon Absorption Optical Depth

1 0,7 0,5 0,3 0,1 0,07 0,05 0,03

Credit: Alan Robock and Luke Oman, climate.envsci.rutgers.edu/nuclear and www.atmos-chem-phys.net/7/2003/2007



A modern nuclear weapon has a destructive power tens to hundreds of times greater than the Hiroshima bomb

Credit: S. Glasstone and Philip Dolan, The Effects of Nuclear Weapons, 3rd Edition, Washington, DC, 1977 and nuclearsecrecy.com/nukemap

NUCLEAR WEAPON STOCKPILES, 2017

(ONLY ABOUT 20% ARE CAPTURED BY ARMS-CONTROL AGREEMENTS)

Country	Total warheads (peak)	Total warheads (2017)	Deployed warheads (strategic)
United States	31,255	**~ 6,800**	**1,393**
Russia	~ 40,000	**~ 7,000**	**1,561**
France	540	300	
United Kingdom	500	215	
China		270*	
Israel		80*	
India		110*	
Pakistan		120*	
North Korea		20*	

New START data as of October 2017

Adapted from Nuclear Notebook, fas.org/issues/nuclear-weapons/status-world-nuclear-forces *Estimate

WHAT'S NEXT FOR NUCLEAR ARMS CONTROL?

2015 STATEMENT BY JAMES MATTIS

"The nuclear stockpile must be tended to and fundamental questions must be asked and answered:

- *We must clearly establish the role of our nuclear weapons: do they serve solely to deter nuclear war? If so we should say so, and the resulting clarity will help to determine the number we need.*
- *Is it time to reduce the Triad to a Diad, removing the land-based missiles? This would reduce the false alarm danger.*
- *Could we re–energize the arms control effort by only counting warheads vice launchers?*
- *Was the Russian test violating the INF treaty simply a blunder or a change in policy, and what is our appropriate response?"*

General James N. Mattis, USMC (Ret.)
Former Commander, United States Central Command

Senate Armed Services Committee
Global Challenges and U.S. National Security Strategy
January 27, 2015

INTERNATIONAL PARTNERSHIP

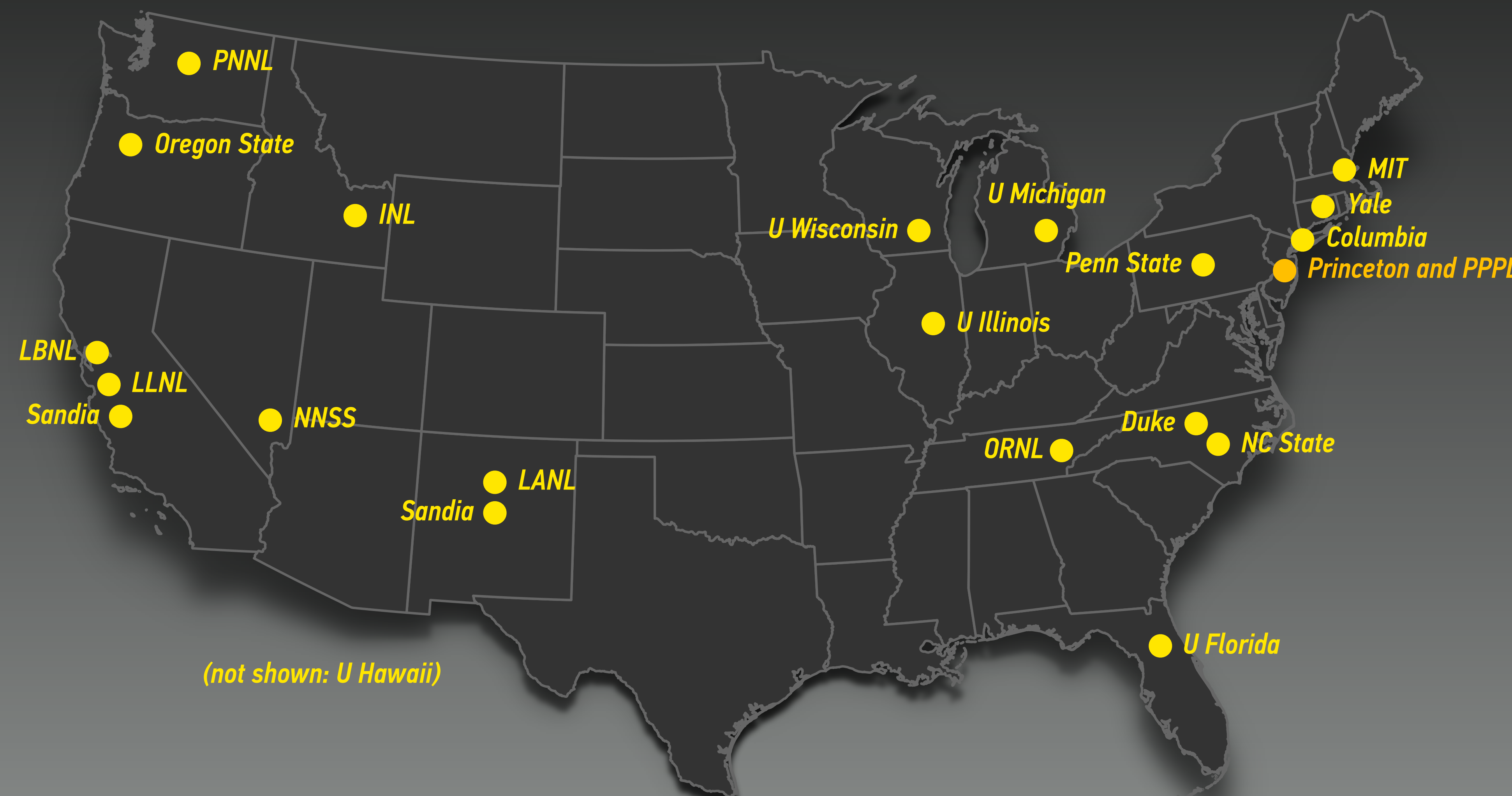
FOR NUCLEAR DISARMAMENT VERIFICATION

Established in 2015; currently 26 participating countries

Working Group One: “Monitoring and Verification Objectives” (chaired by Italy and the Netherlands)
Working Group Two: “On-Site Inspections” (chaired by Australia and Poland)
Working Group Three: “Technical Challenges and Solutions” (chaired by Sweden and the United States)

www.state.gov/t/avc/ipndv

CONSORTIUM FOR VERIFICATION TECHNOLOGY



Five-year project, funded by U.S. DOE, 13 U.S. universities and 9 national labs, led by U-MICH

Princeton participates in the research thrust on disarmament research
(and leads the research thrust of the consortium on policy)

WHAT IS TO BE VERIFIED?

THOUSANDS OF NUCLEAR WEAPONS

ARE CURRENTLY NON-DEPLOYED (i.e., IN RESERVE OR AWAITING DISMANTLEMENT)

W87/Mk-21 Reentry Vehicles in storage, Warren Air Force Base, Cheyenne, Wyoming
Photo courtesy of Paul Shambroom, www.paulshambroom.com

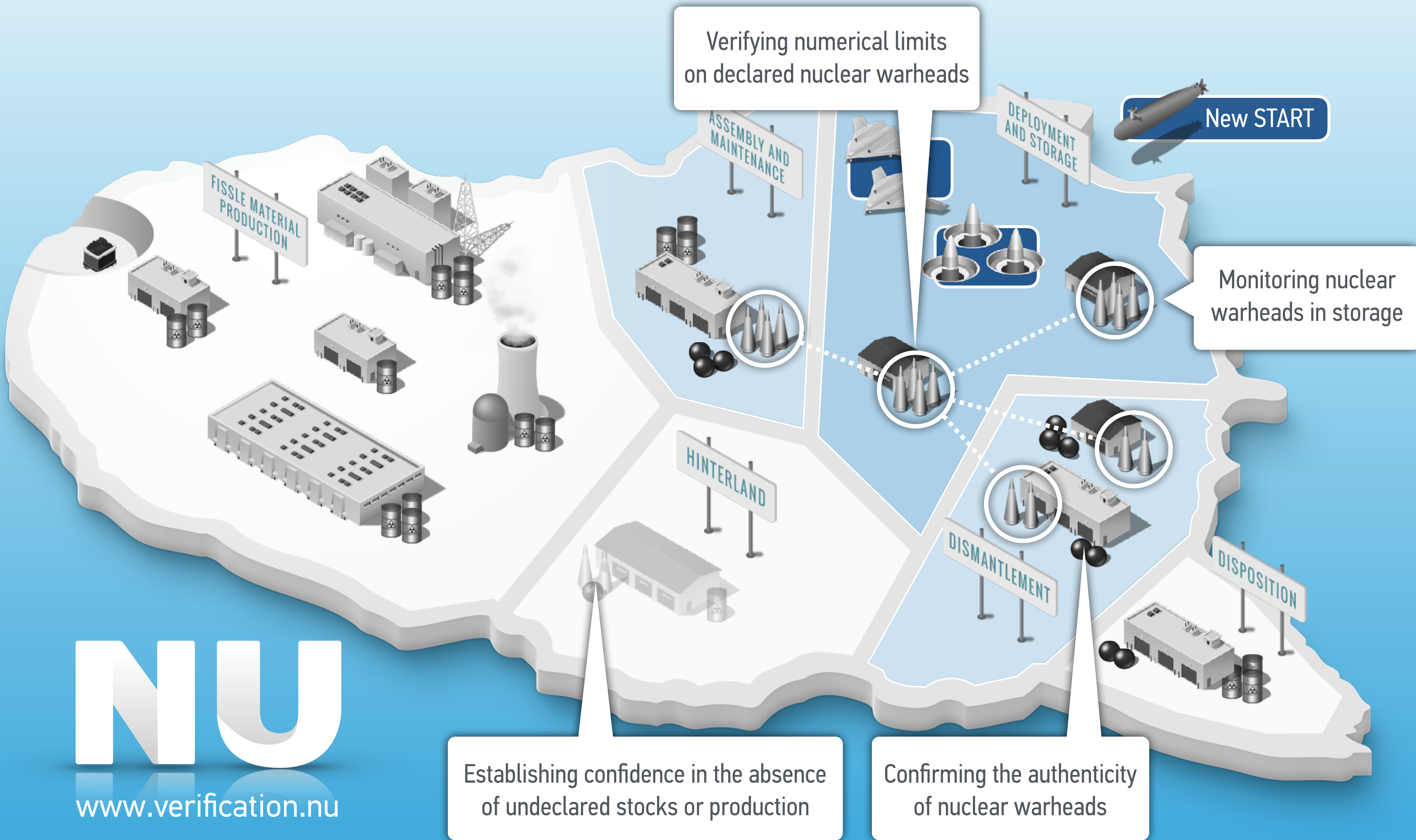
MAPPING NUCLEAR VERIFICATION

NU

www.verification.nu

Revision 3

VERIFICATION CHALLENGES OF DEEPER REDUCTIONS



www.verification.nu

Revision 3

WHY ARE WARHEAD INSPECTIONS SO HARD?

(AS SEEN FROM INSPECTOR'S PERSPECTIVE)

VERY LITTLE (IF ANY) INFORMATION ABOUT THE INSPECTED ITEM CAN BE REVEALED

Some information may be shared in advance, but no additional information during inspection

ADVERSARY/COMPETITOR HAS (DE FACTO) INFINITE RESOURCES

ADVERSARY/COMPETITOR MAY BE EXTREMELY MOTIVATED (TO DECEIVE INSPECTOR)

Stakes are very high (especially when the number of weapons drops below ~1,000)

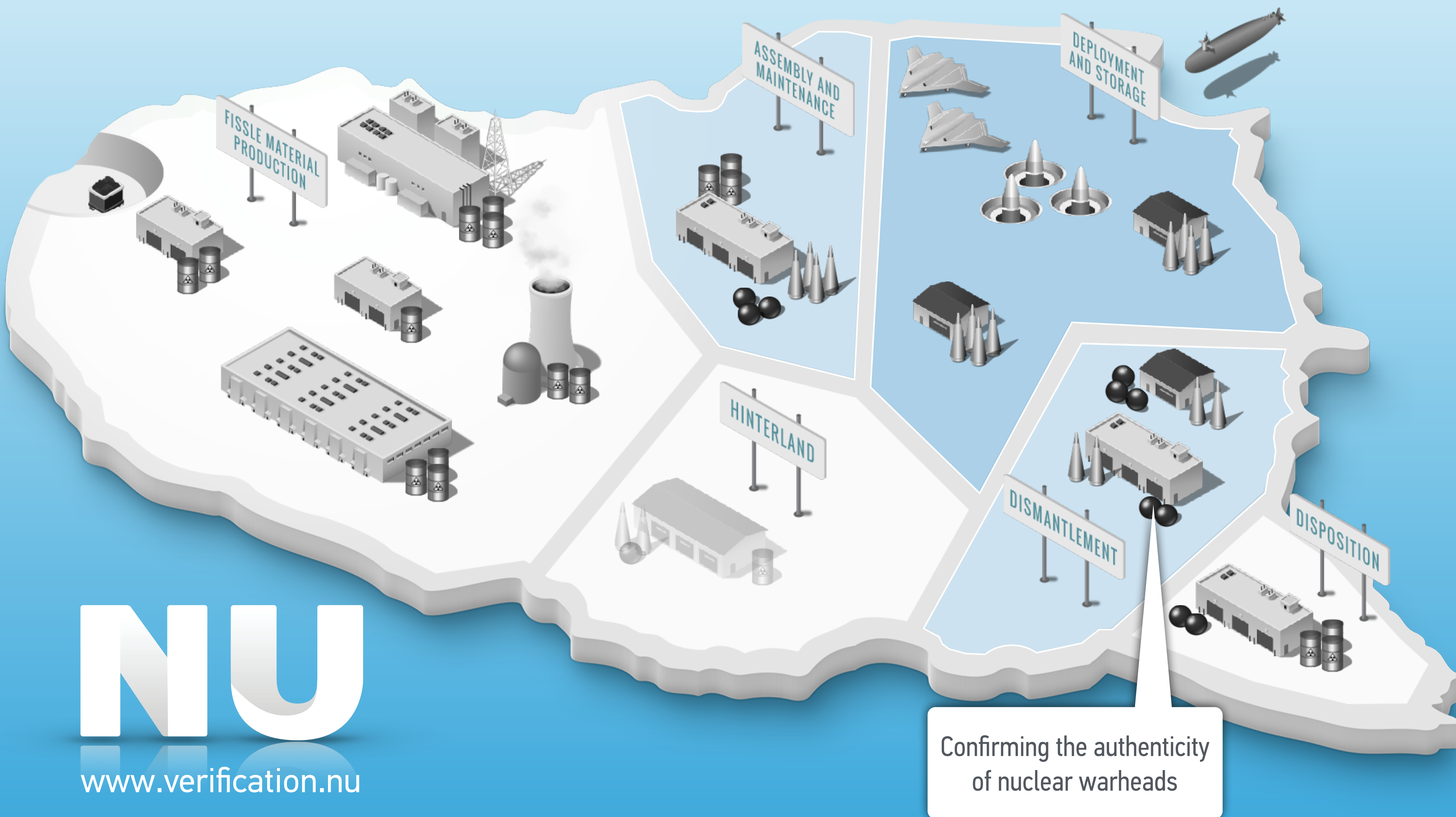
HOST HAS LAST OWNERSHIP OF INSPECTION SYSTEM <u>BEFORE</u> THE MEASUREMENT

(and inspector never again has access to system <u>after</u> the measurement is complete)

CONFIRMING THE AUTHENTICITY OF WARHEADS

(THE ORTHODOX APPROACH)

VERIFICATION CHALLENGES OF DEEP REDUCTIONS

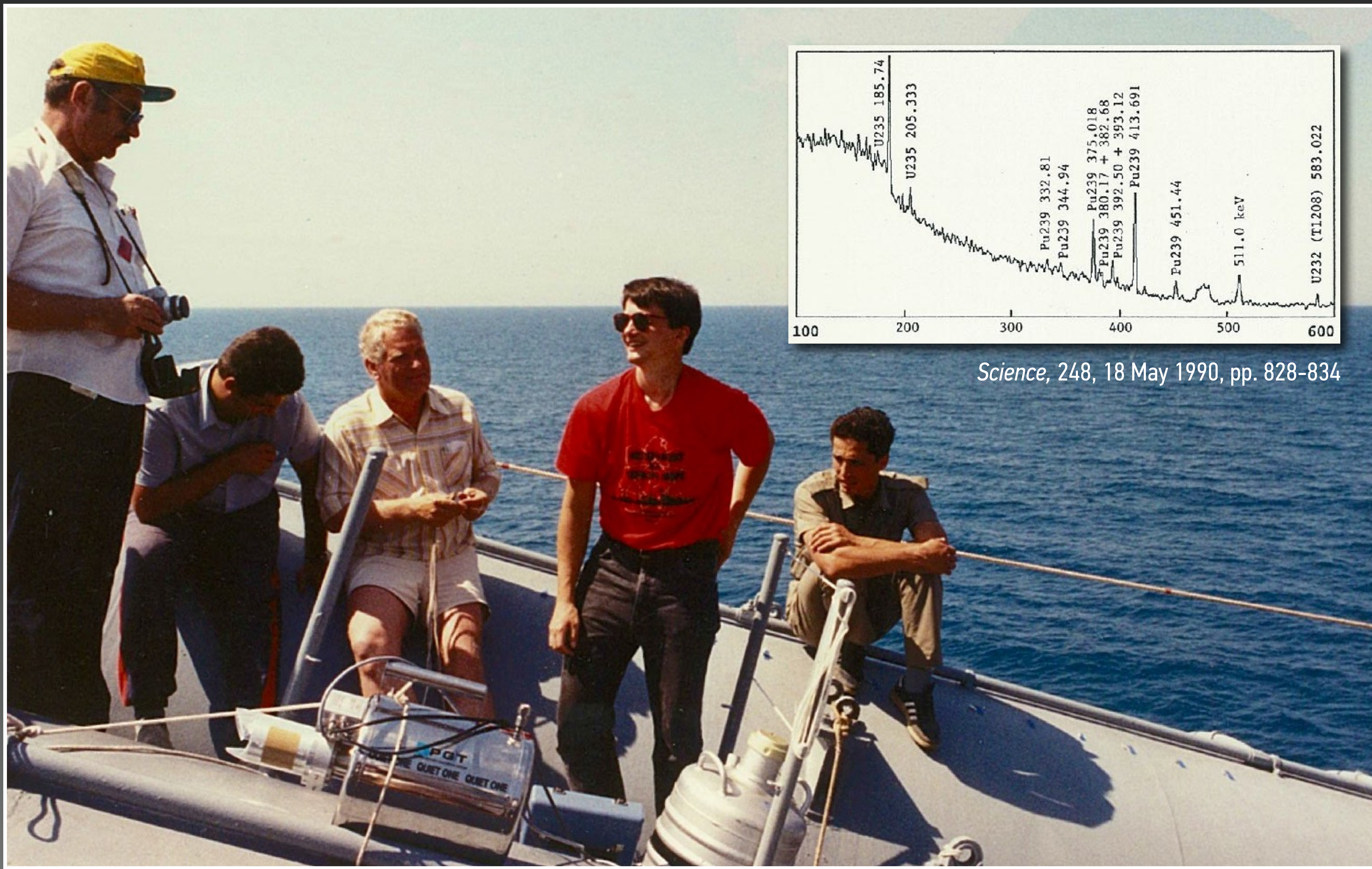


www.verification.nu

Revision 3

NUCLEAR WEAPONS HAVE UNIQUE SIGNATURES

BUT THEY ARE SENSITIVE AND CANNOT BE REVEALED TO INSPECTORS

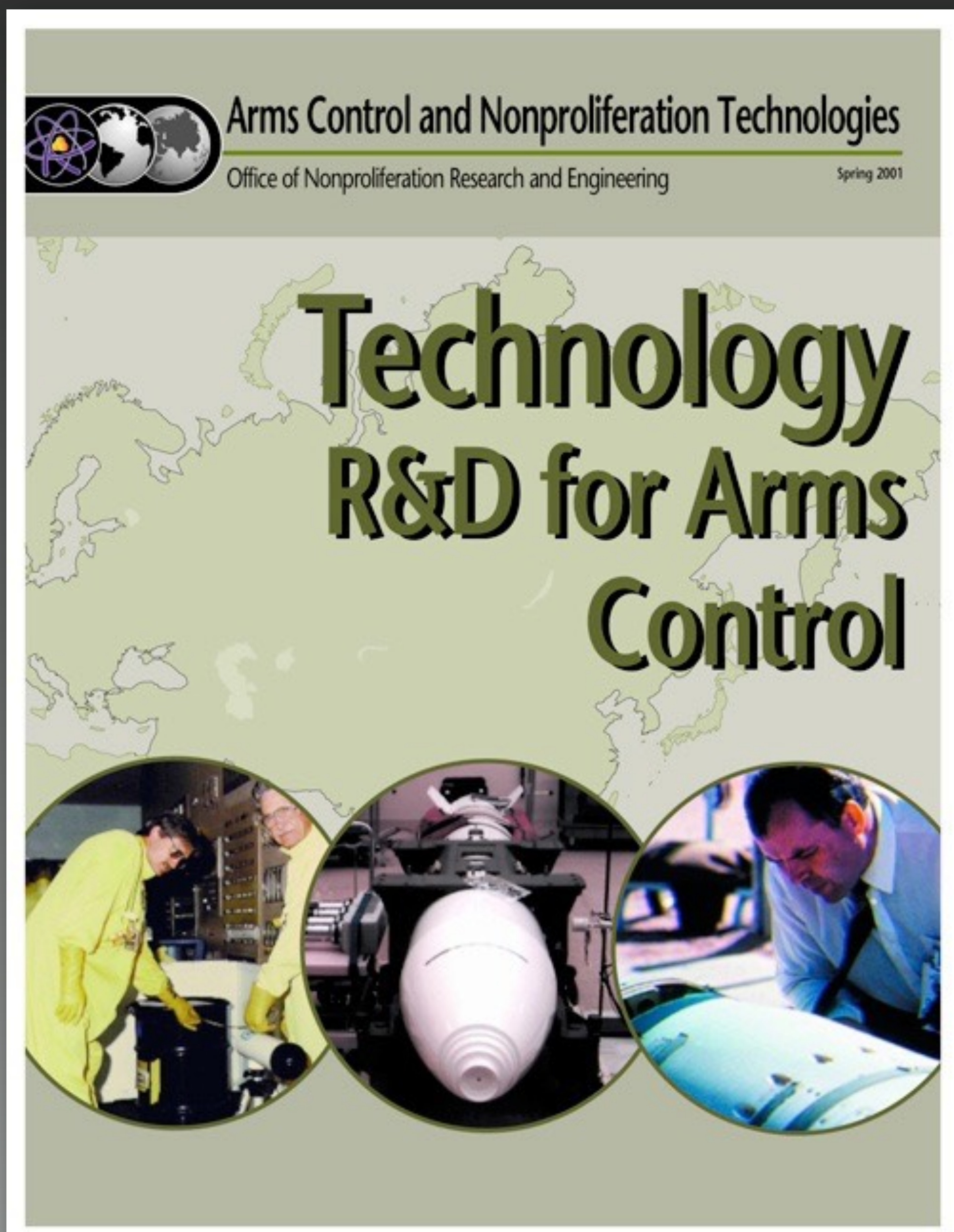


Science, 248, 18 May 1990, pp. 828-834

U.S. Scientists on a Soviet Cruiser in the Black Sea, 1989

NUCLEAR WARHEAD VERIFICATION

KEY CONCEPTS OF (PROPOSED) SYSTEMS



edited by D. Spears, 2001

ATTRIBUTE APPROACH

Confirming selected characteristics
of an object in classified form
(for example, the presence/mass of plutonium)

TEMPLATE APPROACH

Comparing the radiation signature
from the inspected item with a reference item
("golden warhead") of the same type

INFORMATION BARRIERS

Technologies and procedures that
prevent the release of sensitive nuclear information
(generally needed for both approaches)

THE ORTHODOX APPROACH

25 YEARS OF R&D ... BUT SO FAR NO WINNING TECHNOLOGY OR DESIGN

Inspection System developed as part of the Trilateral Initiative during a demonstration at Sarov
Source: Tom Shea

2nd Prototype of the Information Barrier developed as part of the UK-Norway Initiative
Source: ukni.info

Trusted Radiation Identification System (TRIS) developed by Sandia National Laboratories
Source: U.S. Department of Energy

Fundamental challenge: How can information barriers simultaneously be authenticated and certified, i.e., trusted by inspector team and host team at the same time?

HARDWARE TROJANS

STEALTHY MODIFICATIONS TO AN INTEGRATED CIRCUIT THAT ADD OR REMOVE FUNCTIONALITIES

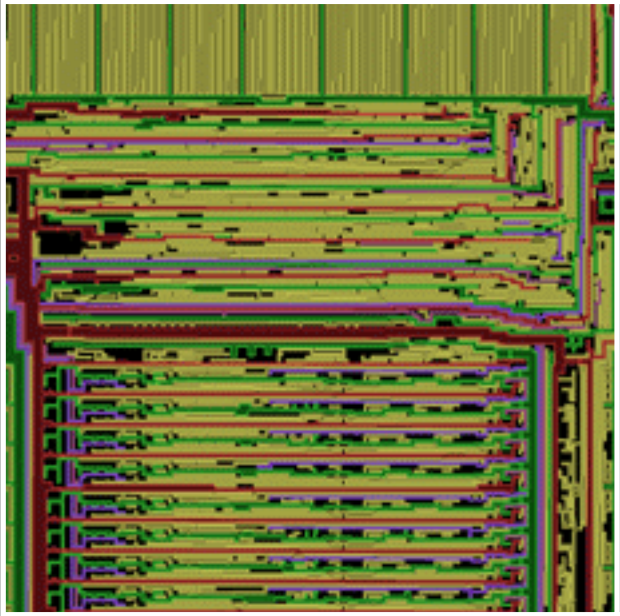
CAN YOU TRUST THIS CHIP?

Does the hardware meet the design specifications?

Does it perform as intended?

Insertion of trojan is possible at every stage of the product cycle

in particular, during design, manufacturing, assembly, and shipping (supply chain)



HARDWARE VERIFICATION CHALLENGES

Reproducibility is difficult; trojans can be triggered by aging mechanisms or environmental conditions; extremely hard for inspector to reproduce

Below transistor level: Terra Incognita; so far no solutions

G. T. Becker, F. Regazzoni, C. Paar, W. P. Burleson, “Stealthy dopant-level hardware Trojans,” *Journal of Cryptographic Engineering,* (4) 1, April 2014.

ONE (BIG) ISSUE REMAINS

NO POST-MEASUREMENT INSPECTION OF EQUIPMENT

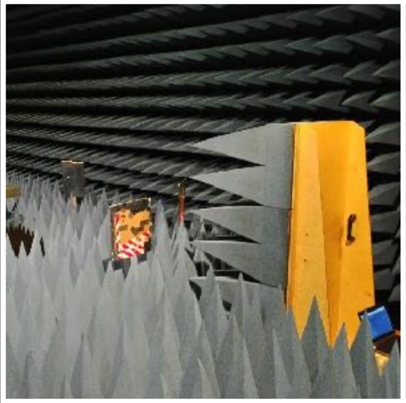
After all these years, no one has yet demonstrated either an attribute or template type system using a classified test object in such a way that specialists from the inspecting country can then [i.e., after the measurement] thoroughly examine and proof the measurement equipment."

James Fuller, October 2012

WHAT TO DO WHEN THERE REMAIN ENDURING CONCERNS ABOUT INFORMATION SECURITY

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 radically different verification approaches; for example, consider zero-knowledge protocols and develop alternatives to onsite inspections at certain sensitive facilities

REVEAL THE SECRET

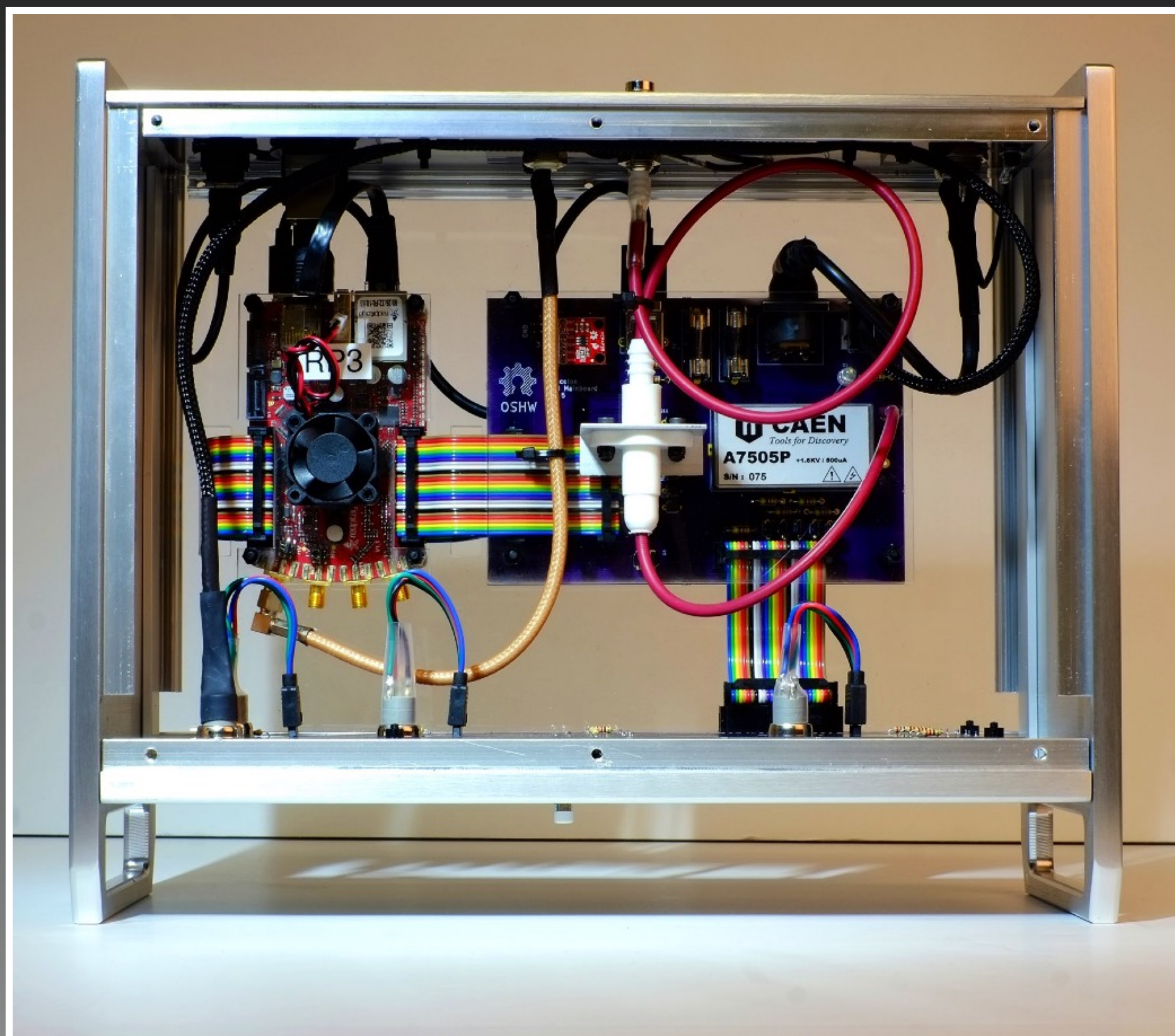
Requirement to protect sensitive information is typically the main reason for complexity of verification approaches; for example, mass of fissile material in a nuclear weapon

Source: Author (top and bottom), Christian Zenger (middle)

INFORMATION BARRIER EXPERIMENTAL & VINTAGE VERIFICATION

INFORMATION BARRIER EXPERIMENTAL

A PROTOTYPING PLATFORM FOR HARDWARE AND SOFTWARE CHALLENGES?

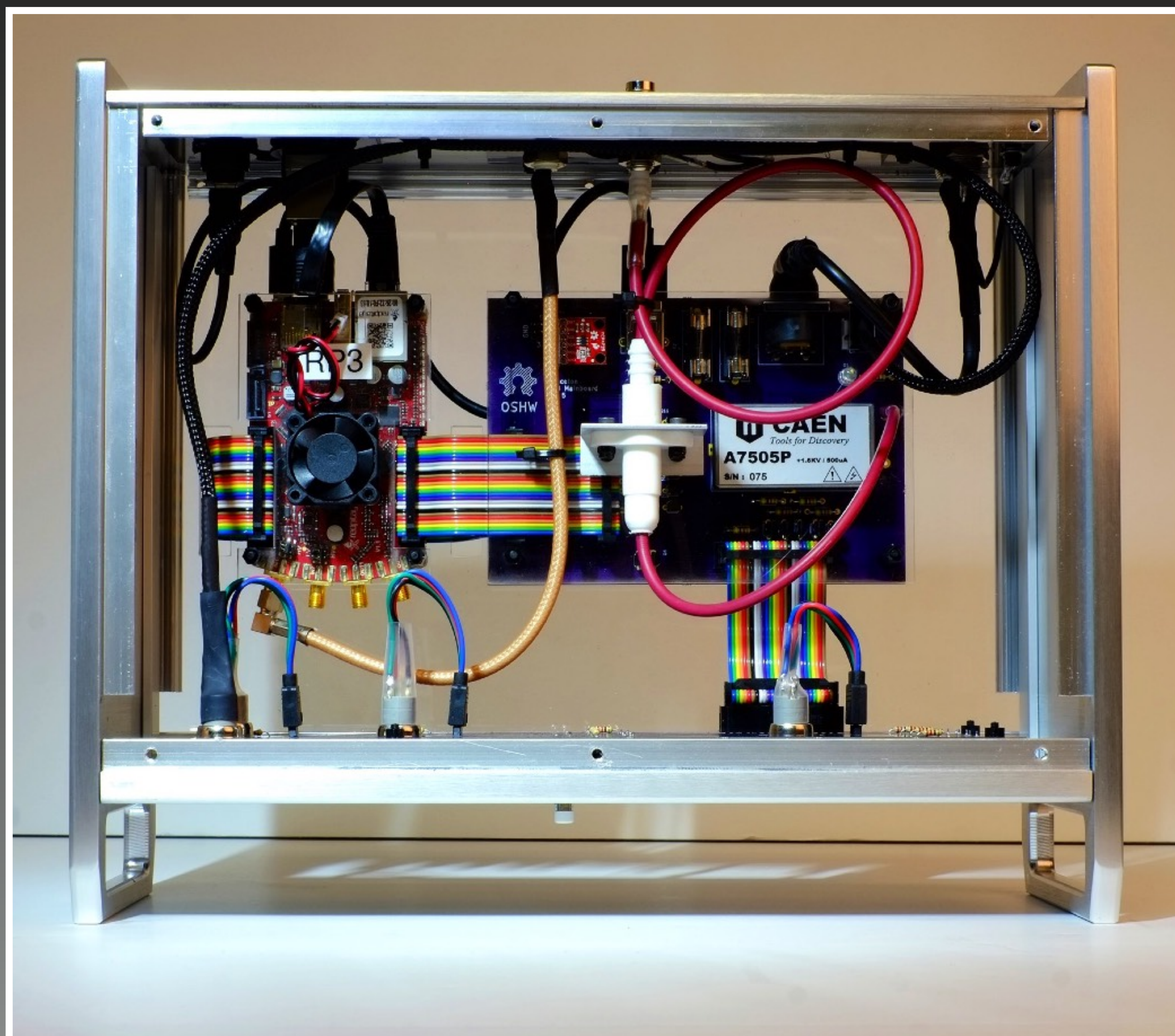


M. Kütt, M. Göttsche, and A. Glaser, "Information Barrier Experimental," *Measurement,* 114, 2018

M. Göttsche, J. Schirm, and A. Glaser, "Low-resolution Gamma-ray Spectrometry for an Information Barrier Based on a Multi-criteria Template-matching Approach," *Nuclear Instruments and Methods A,* 840, 2016, pp. 139–144

INFORMATION BARRIER EXPERIMENTAL

A PROTOTYPING PLATFORM FOR HARDWARE AND SOFTWARE CHALLENGES?



M. Kütt, M. Göttsche, and A. Glaser, "Information Barrier Experimental," *Measurement,* 114, 2018

M. Göttsche, J. Schirm, and A. Glaser, "Low-resolution Gamma-ray Spectrometry for an Information Barrier Based on a Multi-criteria Template-matching Approach," *Nuclear Instruments and Methods A,* 840, 2016, pp. 139–144

"VINTAGE VERIFICATION"

SIMPLE, WIDELY AVAILABLE, WELL UNDERSTOOD ELECTRONICS
(AND NEVER INTENDED FOR USE IN SECURITY APPLICATIONS)

(Talk at 34c3, December 2017)

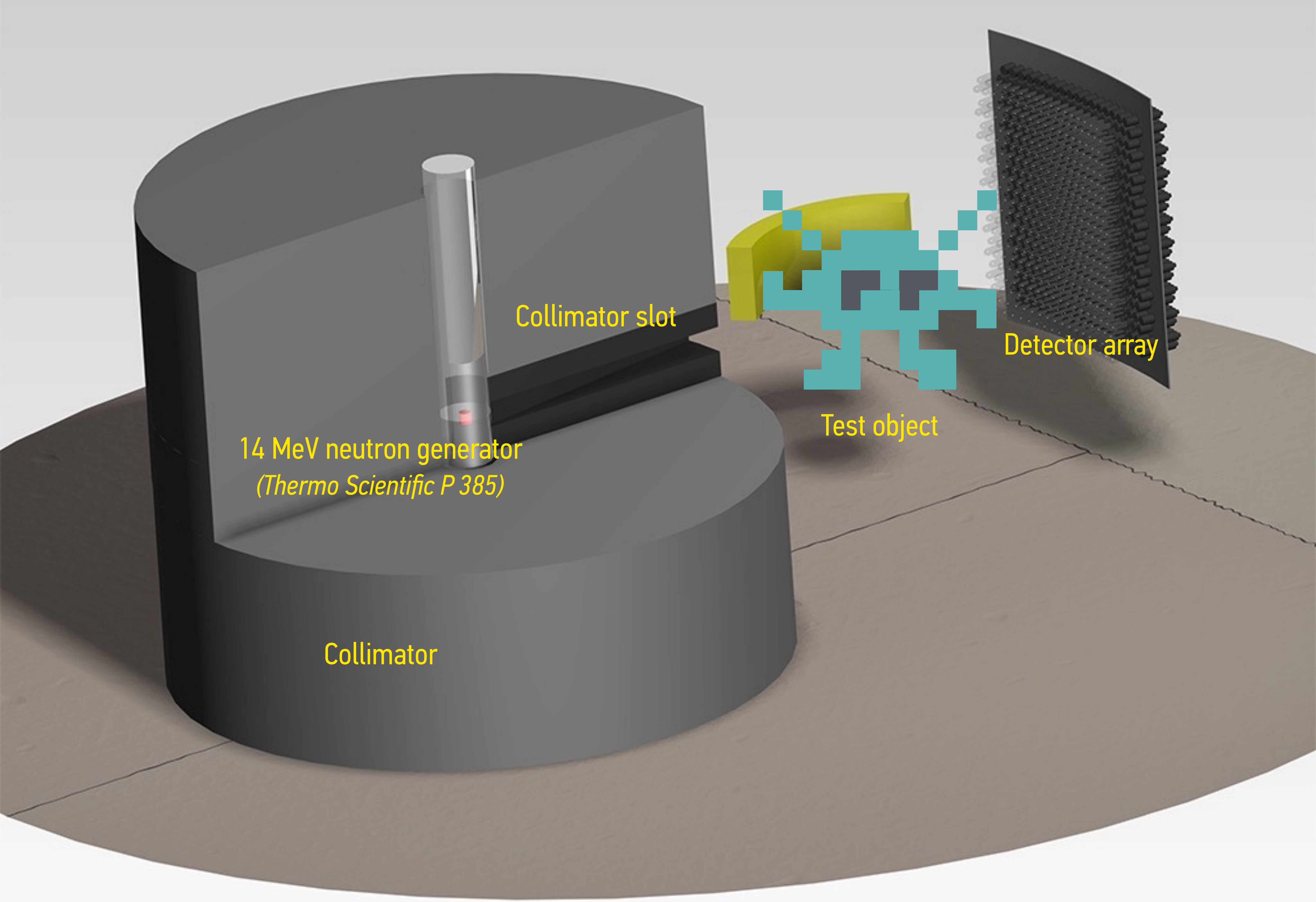
REINVENTING THE PROBLEM # EXAMPLE 1

ZERO-KNOWLEDGE NUCLEAR WARHEAD CONFIRMATION

PHYSICAL ZERO-KNOWLEDGE PROOFS

CAN WE SHOW TWO OBJECTS ARE IDENTICAL WITHOUT LEARNING WHAT THEY ARE?

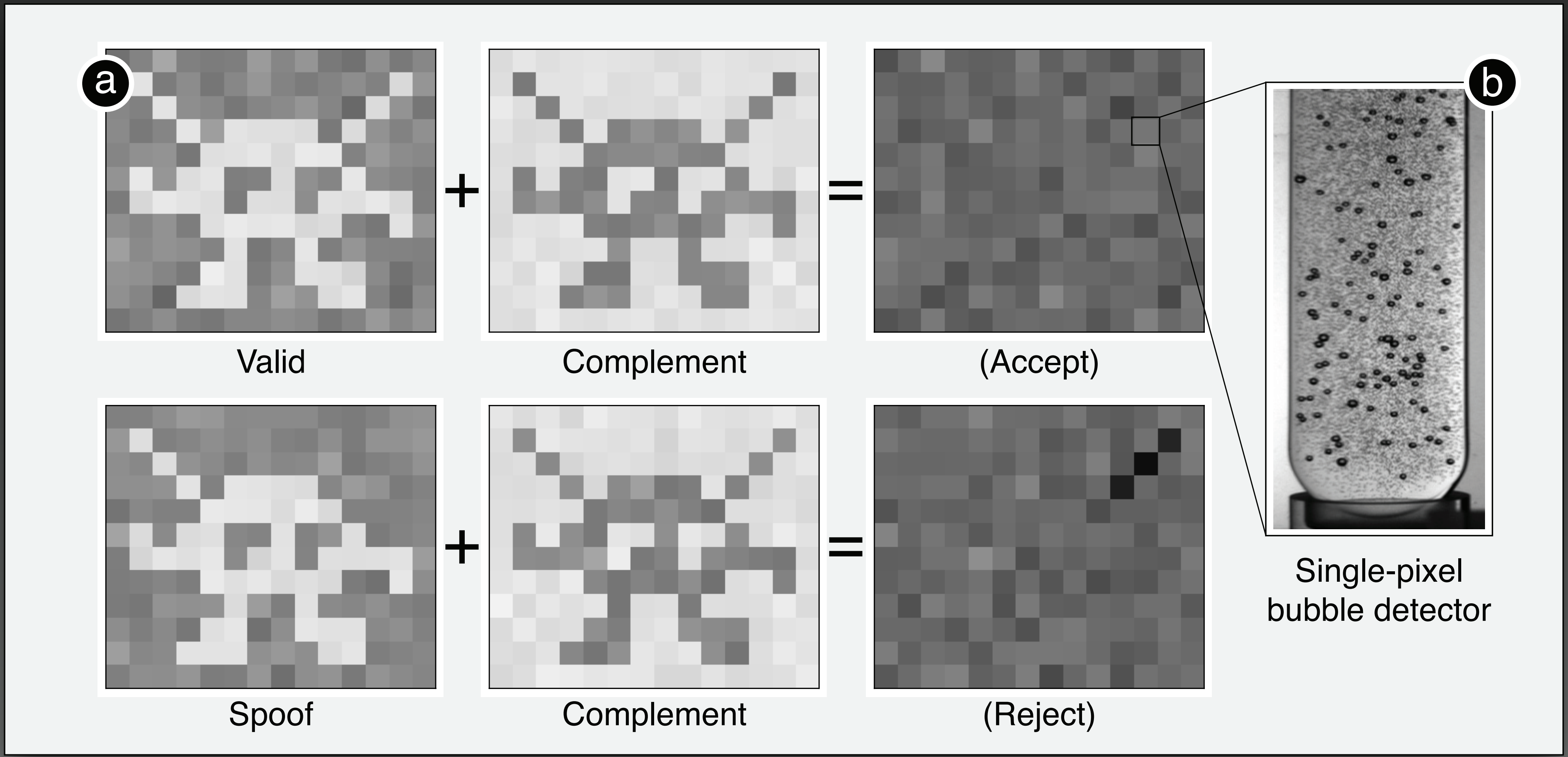
Bob wants to prove to Alice that two objects are "identical"
in a way that Alice gains no new knowledge about the objects themselves



A. Glaser, B. Barak, R. J. Goldston, “A Zero-knowledge Protocol for Nuclear Warhead Verification,” *Nature,* 510, 26 June 2014
S. Philippe, R. J. Goldston, A. Glaser, F. d’Errico, *Nature Communications,* 7, September 2016, www.nature.com/articles/ncomms12890

PHYSICAL ZERO-KNOWLEDGE PROOFS

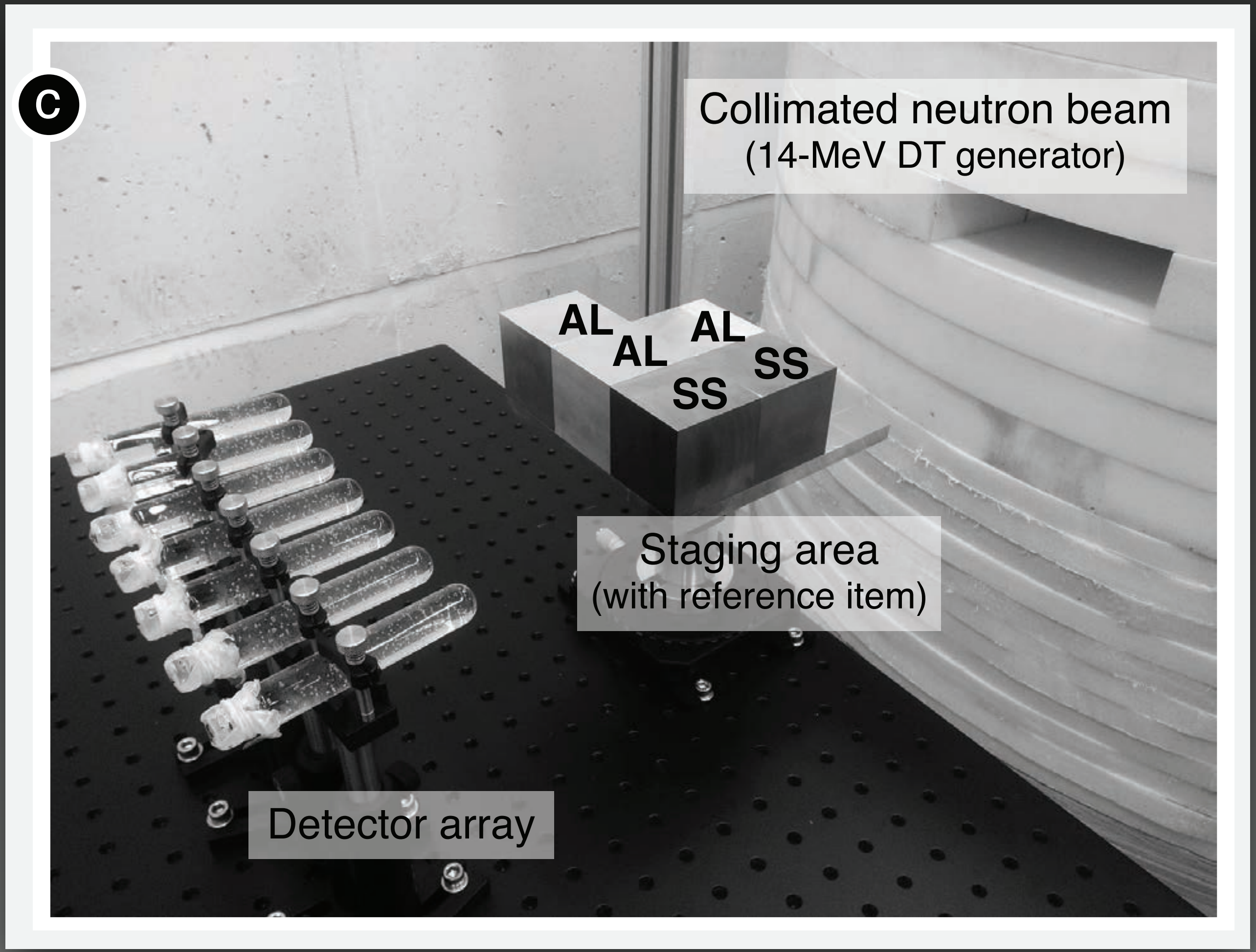
ZERO-KNOWLEDGE DIFFERENTIAL RADIOGRAPHY

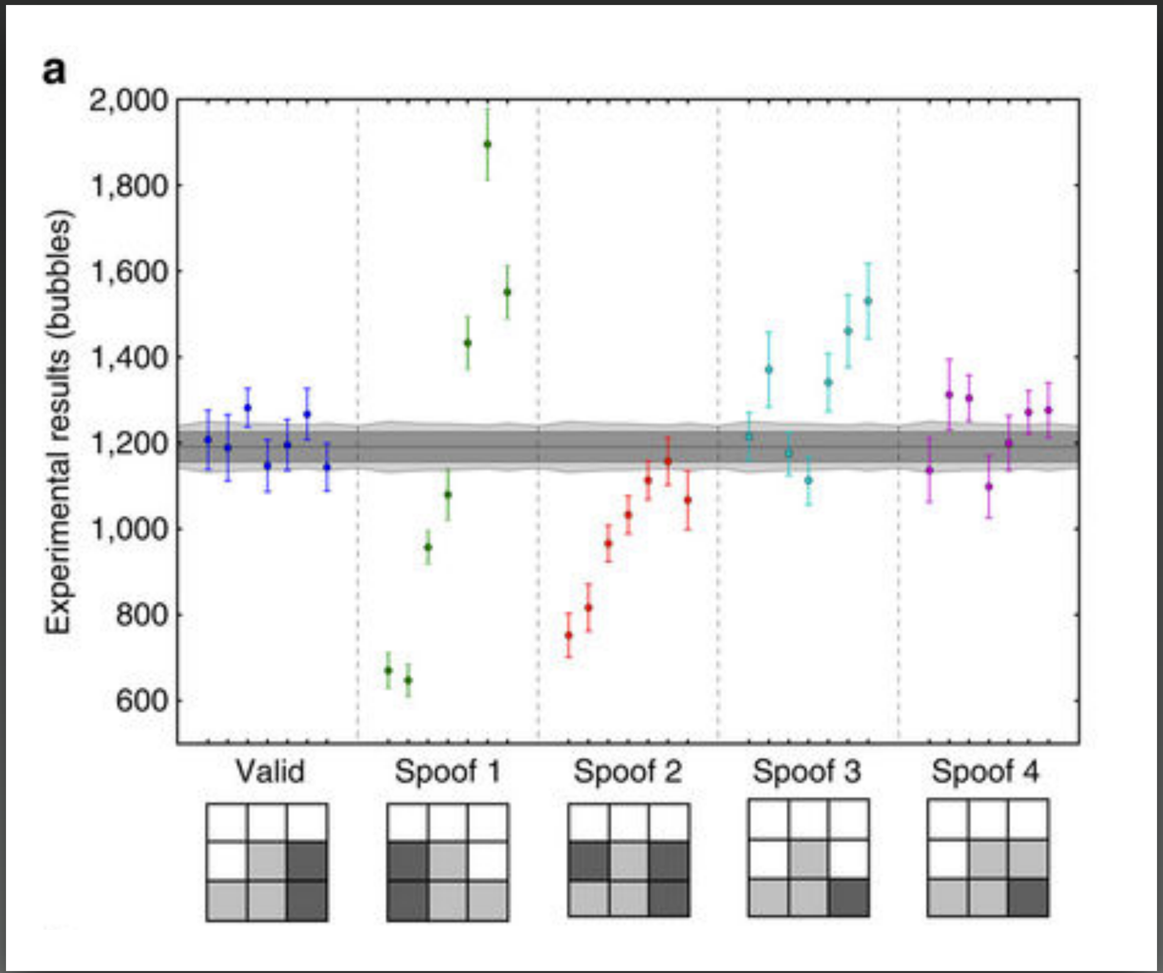


S. Philippe, R. J. Goldston, A. Glaser, F. d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification," *Nature Communications,* 7, September 2016, www.nature.com/articles/ncomms12890

PHYSICAL ZERO-KNOWLEDGE PROOFS

EXPERIMENTAL DEMONSTRATION AND RESULTS

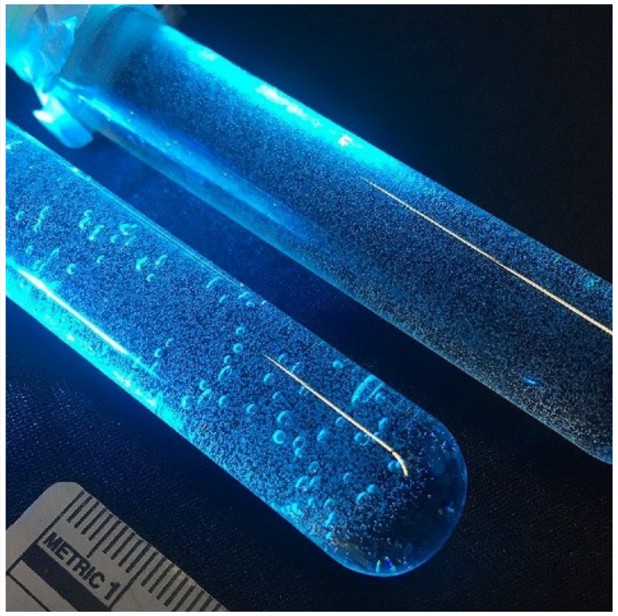




S. Philippe, R. J. Goldston, A. Glaser, F. d'Errico, "A physical zero-knowledge object-comparison system for nuclear warhead verification," *Nature Communications,* 7, September 2016, www.nature.com/articles/ncomms12890

SUPERHEATED EMULSIONS AS PUF-DETECTORS

OPEN PATH FOR TRUSTED MEASUREMENTS



AVOID DETECTOR-SIDE ELECTRONICS

Superheated emulsions are designed to be insensitive to γ-radiation and sensitive to neutrons with energy $E_n > E_{min}$

Tailor-made by Francesco d'Errico Research Group, Yale University.

HAVE PROPERTIES OF AN OPTICAL PHYSICALLY UNCLONABLE FUNCTION

Could allow host to review the data before the inspector sees it while giving the inspector confidence the data was not tampered with

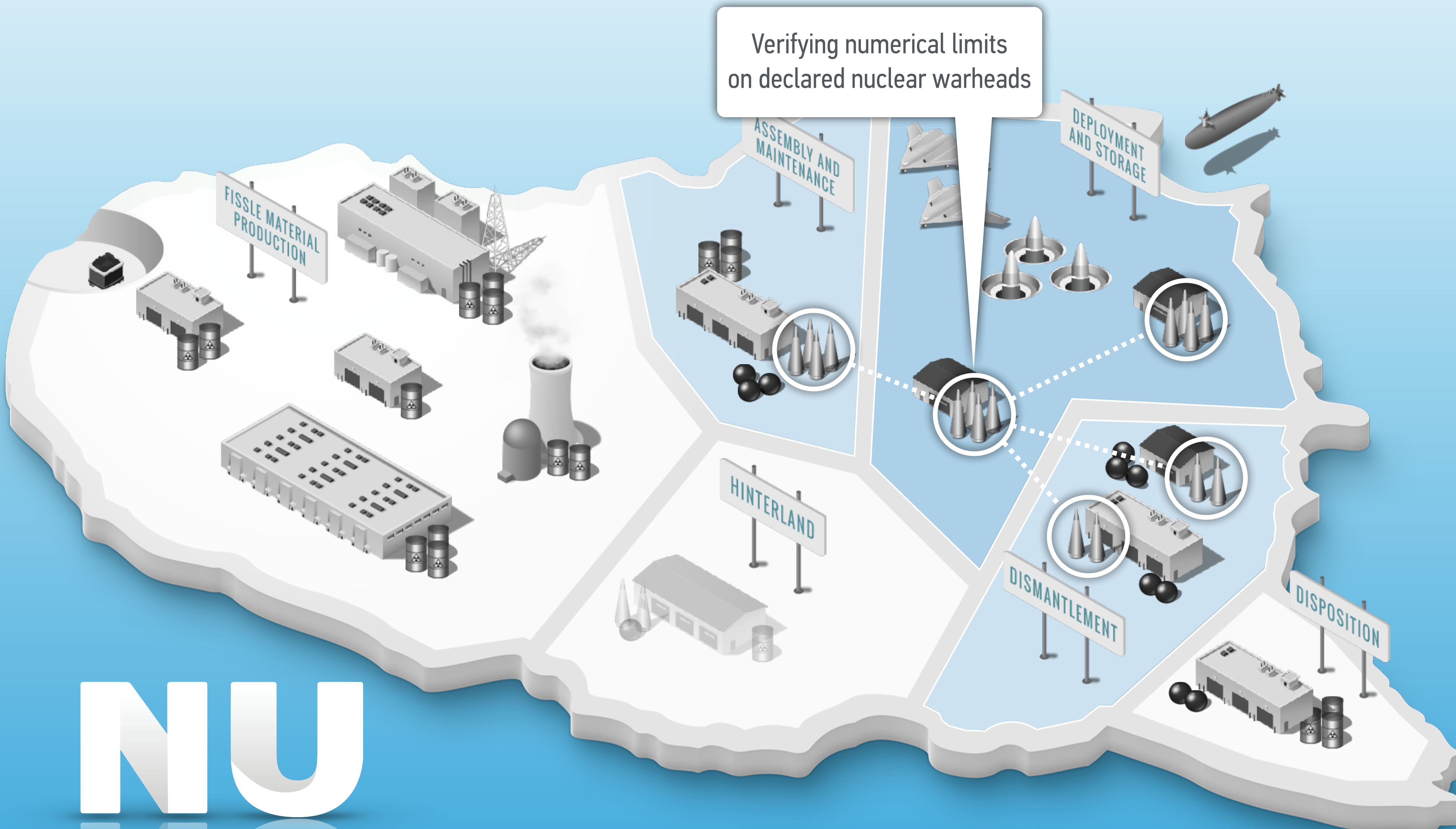
First experimental results are promising: detectors are unique objects, physically unclonable, and challenge response pairs are sensitive to neutron interaction

Source: Authors (Top: A. Glaser.; Bottom: Experimental Set-up, S. Philippe)

REINVENTING THE PROBLEM # EXAMPLE 2

CONFIRMING NUMERICAL LIMITS ON NUCLEAR WARHEADS

VERIFICATION CHALLENGES OF DEEP REDUCTIONS



NU

www.verification.nu

Revision 3

TAGGING

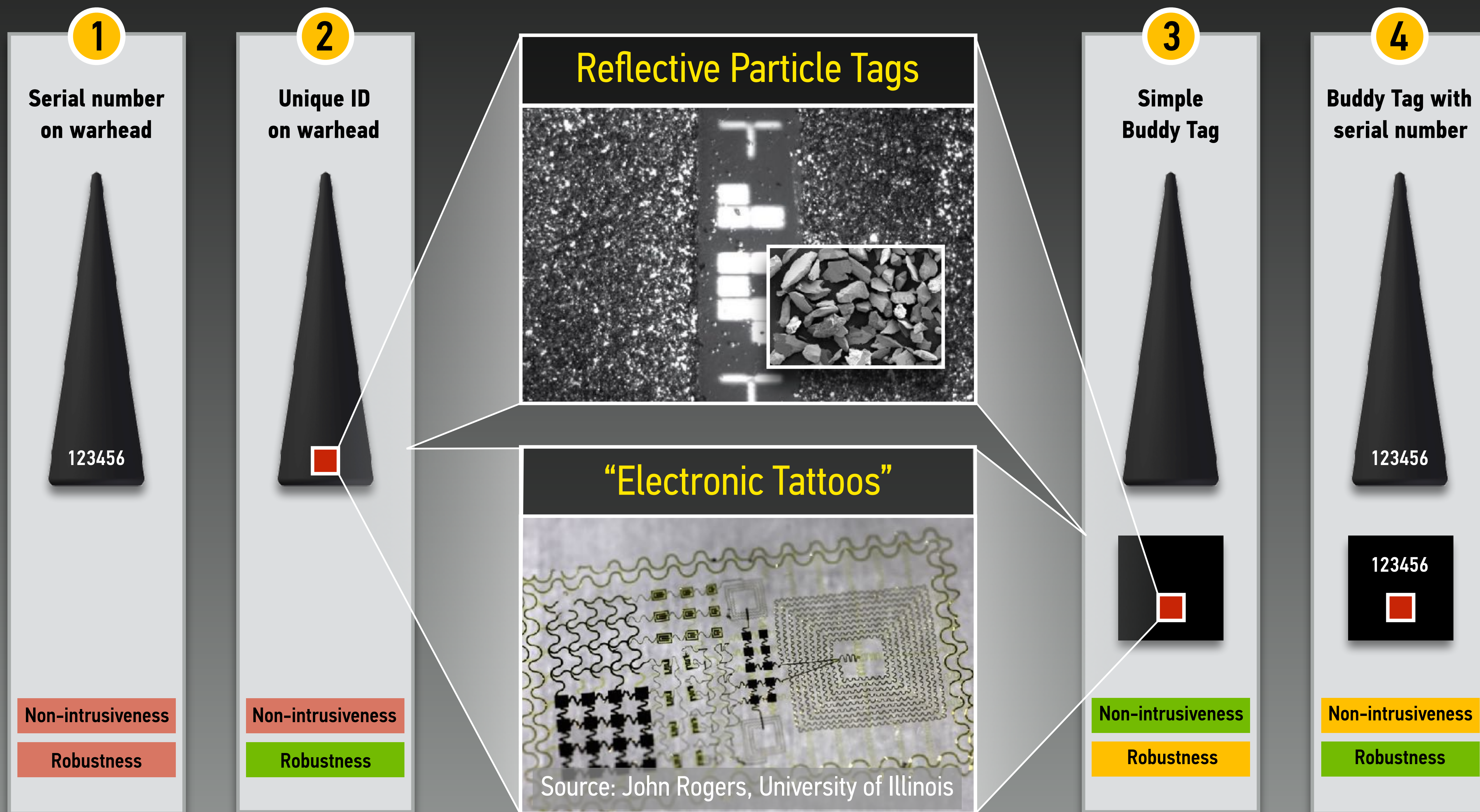
TRANSFORMING A “NUMERICAL LIMIT” INTO A “BAN ON UNTAGGED ITEMS”

Source: www.automoblog.net

Steve Fetter and Thomas Garwin, “Using Tags to Monitor Numerical Limits in Arms Control Agreements”
in Barry M. Blechman, ed., Technology and the Limitation of International Conflict, Washington, DC, 1989, pp. 33–54

VERIFYING NUMERICAL LIMITS OF DECLARED NUCLEAR WARHEADS

WARHEAD TAGGING OPTIONS



Reflective particle tag concept: A. Gonzales, *Reflective Particle Tag for Arms Control and Safeguards Authentication,* Sandia National Laboratories, 2004

Original buddy tag concept: S. E. Jordan, *Buddy Tag's Motion Sensing and Analysis Subsystem,* Sandia National Laboratories, 1991

AN ALTERNATIVE TO TAGGING: CRYPTOGRAPHIC ESCROW

```
ITEM 01: 67d97802b84a6db872aacc400a0f5eaeebcec52012503111891b0d1e89711605
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: bca49804e0b0da52df8f533d91d680e2681875211538dea4401277bc6cfa2e3
```

Declaration in hashed form (with one entry per item)

```
ITEM 01: 67d97802b84a6db872aacc400a0f5eaeebcec52012503111891b0d1e89711605
ITEM 02: b3c22af3a5f9ecc51c5cf6b4604e2bef191e4ceb305c6ef4a9589206e0bd7e62
ITEM 03: 8edd164eb3fd9116 SITE C :: W99 :: TIME 12345678 a562c8ffeefbc2fb
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: bca49804e0b0da52df8f533d91d680e2681875211538dea4401277bc6cfa2e3
```

Declaration with entries for Site C revealed

S. Philippe, A. Glaser and E. W. Felten, "Cryptographic Escrow of Nuclear Warhead Inventories for Early Commitment and Non-intrusive Verification," *Proceedings of the 58th INMM Annual Meeting*, 2017.

ESCROW CONSTRUCTION

FOR A GIVEN ITEM AND USING HASH FUNCTIONS

```
ITEM 999: b86d553666858d3c611884207c40b2eb3d9a3ac94a8cae9e4cd34deaa95ff589
```

```
digest_0 = sha256(m_0)
```

```
m_0 = {152441ff1a5b9f3f},
      {fe2b9cba3ef8d73e},
      {"type: w99", "site: air base 001", "status: stored”},
      {5a85ac7ef688d9aceec32b1ef3d5779add02989fa8161f65c86a306e2ad57e07}
```

```
digest_1 = sha256(m_1)
```

```
m_1 = {db91dc3900328ca2},
      {"serial: w99xyz1234", "pu: 4.000 94.000", "u: 15.000 97.000"}
```

Shown commitments (generated with the SHA-256 hash function) are for illustration purposes only; actual messages and digests may use a different commitment scheme

WAY FORWARD & NEXT STEPS

PREPARING FOR DEEPER REDUCTIONS AND MULTILATERAL NUCLEAR ARMS CONTROL

TAKING INFORMATION SECURITY SERIOUSLY

Jointly develop and demonstrate methods to confirm numerical limits on nuclear warheads and confirm their authenticity

Focus initially on non-intrusive approaches that are acceptable to all participants (but can accommodate “upgrades”)

THINKING OUTSIDE THE BOX

- Proof of knowledge and trusted sensors
- Next-generation data exchange (cryptographic escrow, blockchains)
- Involve broader crypto-community (hackathons)