INFORMATION SECURITY IN NUCLEAR WARHEAD VERIFICATION

Alexander Glaser

Department of Mechanical and Aerospace Engineering
and Woodrow Wilson School of Public and International Affairs
Princeton University

Workshop on New Technologies for Information Analysis to Support Non-Proliferation and Disarmament Verification
Vienna Center for Disarmament and Non-Proliferation
Vienna, December 12, 2014

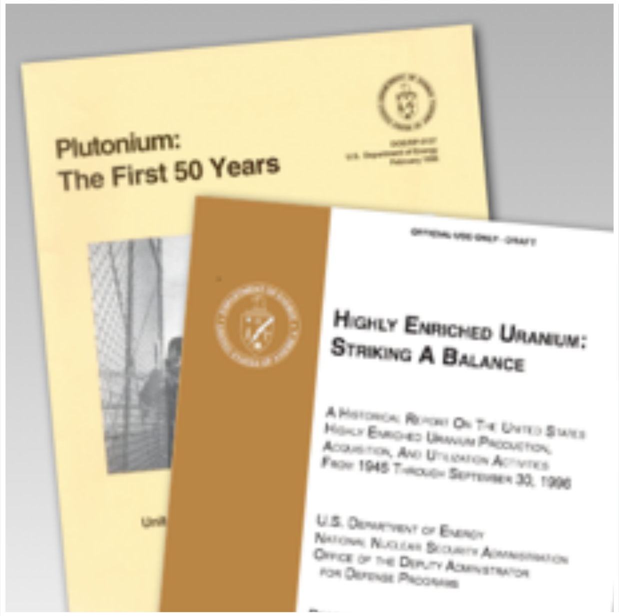
Revision 4

WHAT IS NEW HERE?

THE CHALLENGES OF DEEP REDUCTIONS AND MULTILATERAL NUCLEAR ARMS CONTROL

NEW TREATIES MAY LIMIT TOTAL NUMBER OF WEAPONS

- Would then also include (non-deployed) weapons in storage
- Need to prepare for the transition from bilateral to multilateral nuclear arms control agreements



Plutonium:
The First 50 Years

OFFICIAL USE ONLY - DRAFT

HIGHLY ENRICHED URANIUM:
STRIKING A BALANCE

A HISTORICAL REPORT ON THE UNITED STATES
HIGHLY ENRICHED URANIUM PRODUCTION,
ACQUISITION, AND UTILIZATION ACTIVITIES
FROM 1945 THROUGH SEPTEMBER 30, 1996

U.S. DEPARTMENT OF ENERGY
NATIONAL NUCLEAR SECURITY ADMINISTRATION
OFFICE OF THE DEPUTY ADMINISTRATOR
FOR DEFENSE PROGRAMS

NEW TREATIES MAY REQUIRE BASELINE DECLARATIONS

- Applies to both nuclear warhead (and fissile material) inventories
- How to bring in countries that currently consider these numbers sensitive?

Source: Paul Shambroom (top) and U.S. Department of Energy (bottom)

WHAT IS TO BE VERIFIED ?

VERIFICATION CHALLENGES OF NUCLEAR DISARMAMENT AT LOW NUMBERS

CORRECTNESS OF DECLARATIONS

- Warhead Counting

  Verify that numerical limit of declared items is not exceeded

- Warhead Authentication

  Verify authenticity of warheads prior to dismantlement

COMPLETENESS OF DECLARATIONS

- How to make sure that no covert warheads exist outside the verification regime?

Also (very) important, but not discussed here

Source: U.S. Department of Energy (top) and U.S. Department of Defense, www.defenseimagery.mil (bottom)

INFORMATION SECURITY

DEFENDING INFORMATION FROM UNAUTHORIZED ACCESS, DISCLOSURE, MODIFICATION, OR DESTRUCTION

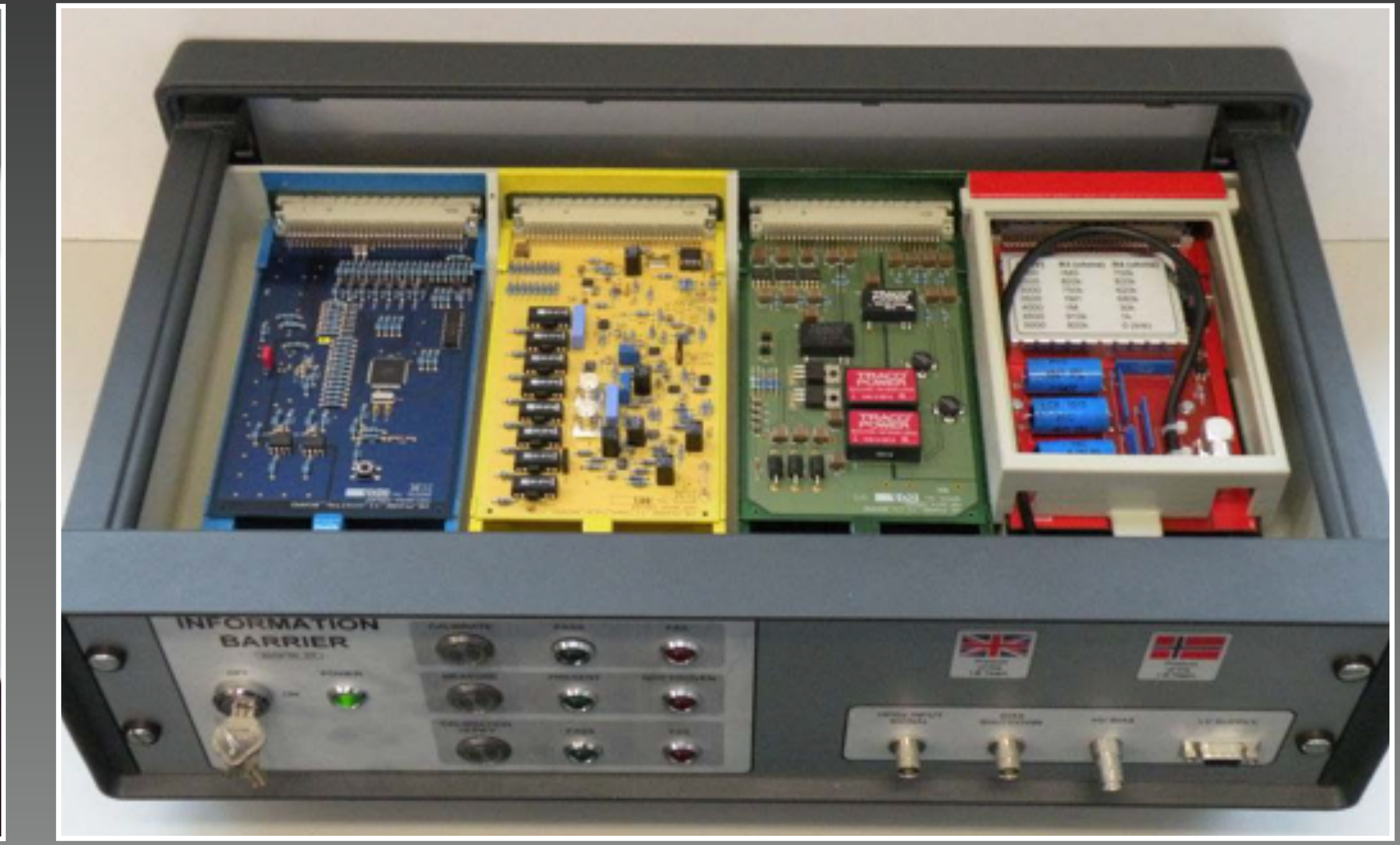
WARHEAD AUTHENTICATION AND VERIFIED WARHEAD DISMANTLEMENT

STANDARD APPROACHES PROTECT SENSITIVE INFORMATION WITH “INFORMATION BARRIERS”

(Classified information is “shielded” or “removed” during inspection)

Inspection System developed as part of the 1996–2002 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: David Chambers et al.

AN ALTERNATIVE APPROACH TO INFORMATION SECURITY

VERIFICATION PROTOCOLS AND MEASUREMENTS
THAT DO NOT ACQUIRE SENSITIVE INFORMATION IN THE FIRST PLACE

VERIFICATION CHALLENGE #1

WARHEAD COUNTING

TAGGING NUCLEAR WARHEADS

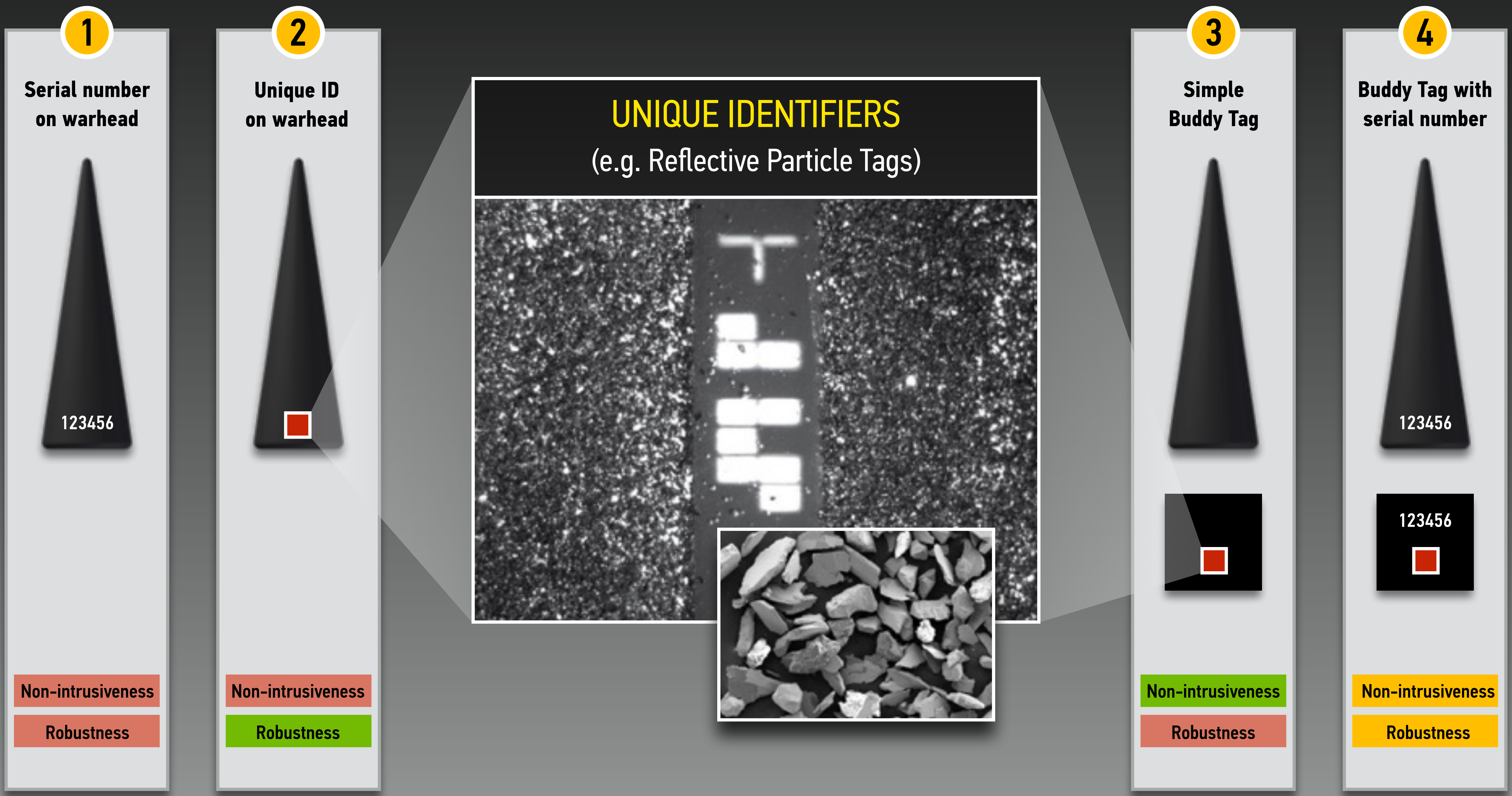
(TRANSFORMING A “NUMERICAL LIMIT” INTO A “BAN ON UNTAGGED ITEMS”)

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*

WARHEAD COUNTING OPTIONS

WITH VARIOUS LEVELS OF NON-INTRUSIVENESS AND ROBUSTNESS



1 Serial number on warhead

2 Unique ID on warhead

UNIQUE IDENTIFIERS
(e.g. Reflective Particle Tags)

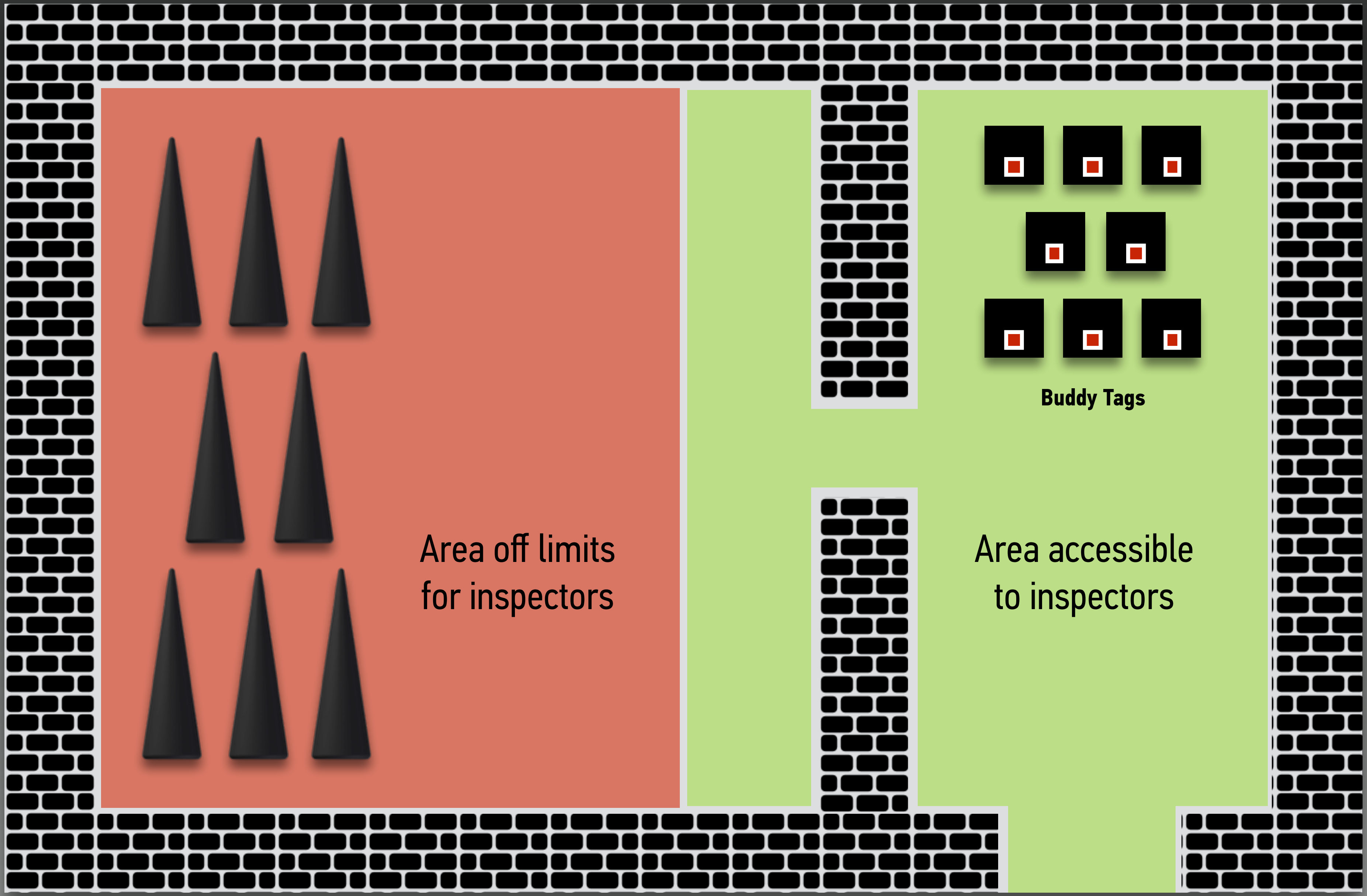
3 Simple Buddy Tag

4 Buddy Tag with serial number

Reflective particle tag concept: A. Gonzales, Reflective Particle Tag for Arms Control and Safeguards Authentication, Sandia National Laboratories, 2004
Buddy tag concept: S. E. Jordan, Buddy Tag's Motion Sensing and Analysis Subsystem, Sandia National Laboratories, 1991

OPTION FOR A MINIMALLY INTRUSIVE ONSITE INSPECTION

USING BUDDY TAGS WITHOUT DIRECT ACCESS TO TREATY ACCOUNTABLE ITEMS



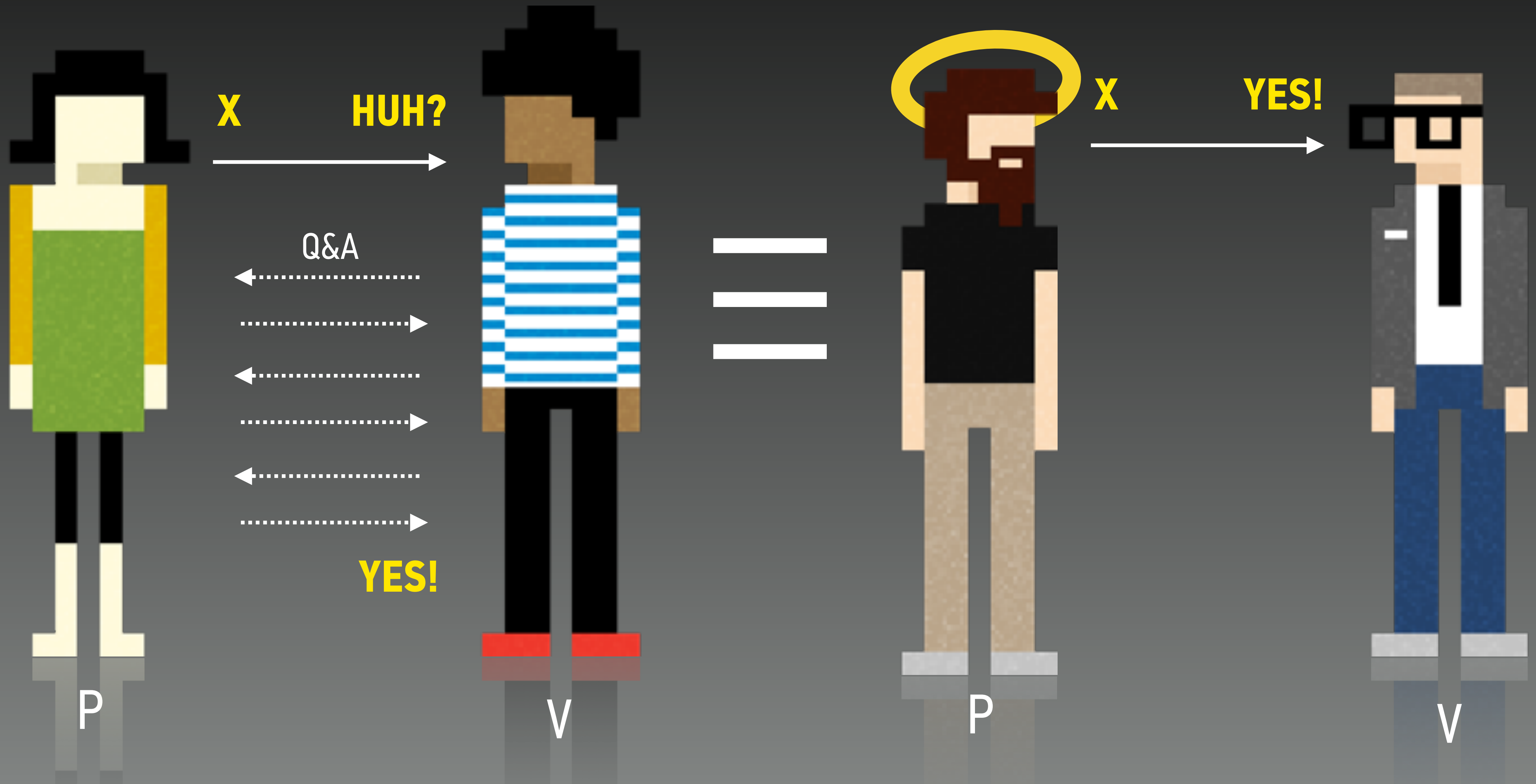
Hypothetical nuclear warhead storage facility

VERIFICATION CHALLENGE #2

WARHEAD AUTHENTICATION

(WILL YOU KNOW A NUCLEAR WEAPON WHEN YOU SEE ONE ?)

ZERO-KNOWLEDGE INTERACTIVE PROOFS



Zero-Knowledge Proofs: The prover (P) convinces the verifier (V) that s/he knows a secret without giving anything about the secret itself away

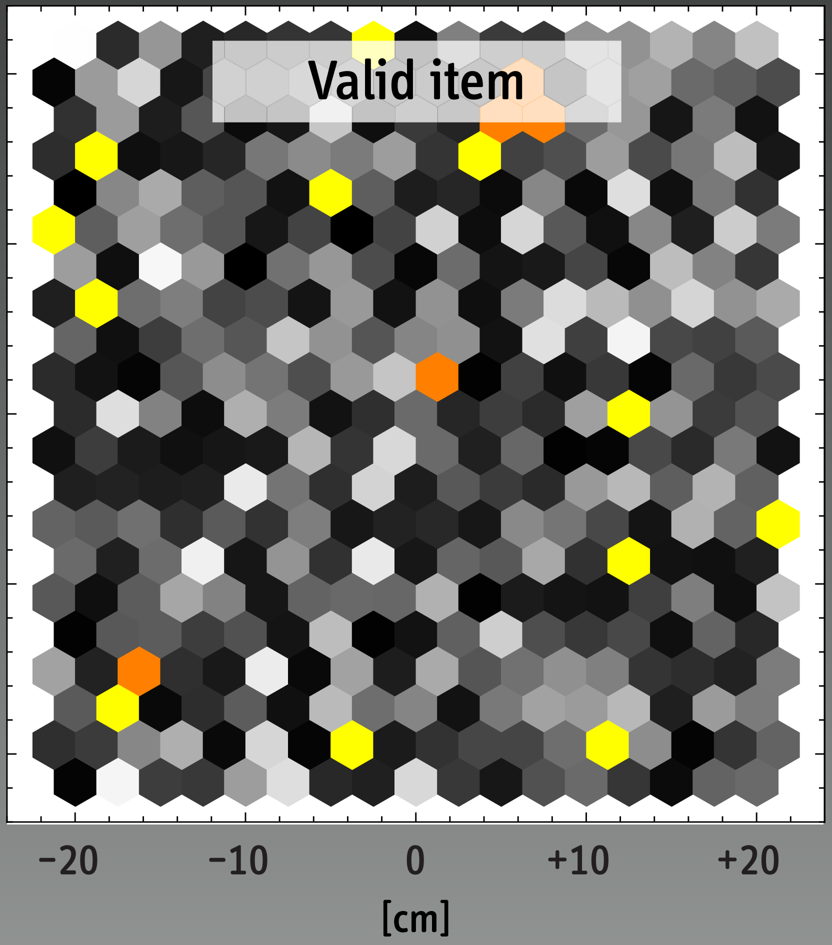
O. Goldreich, S. Micali, A. Wigderson, "How to Play ANY Mental Game," 19th Annual ACM Conference on Theory of Computing, 1987
Graphics adapted from O. Goldreich, *Foundations of Cryptography,* Cambridge University Press, 2001; and eightbit.me

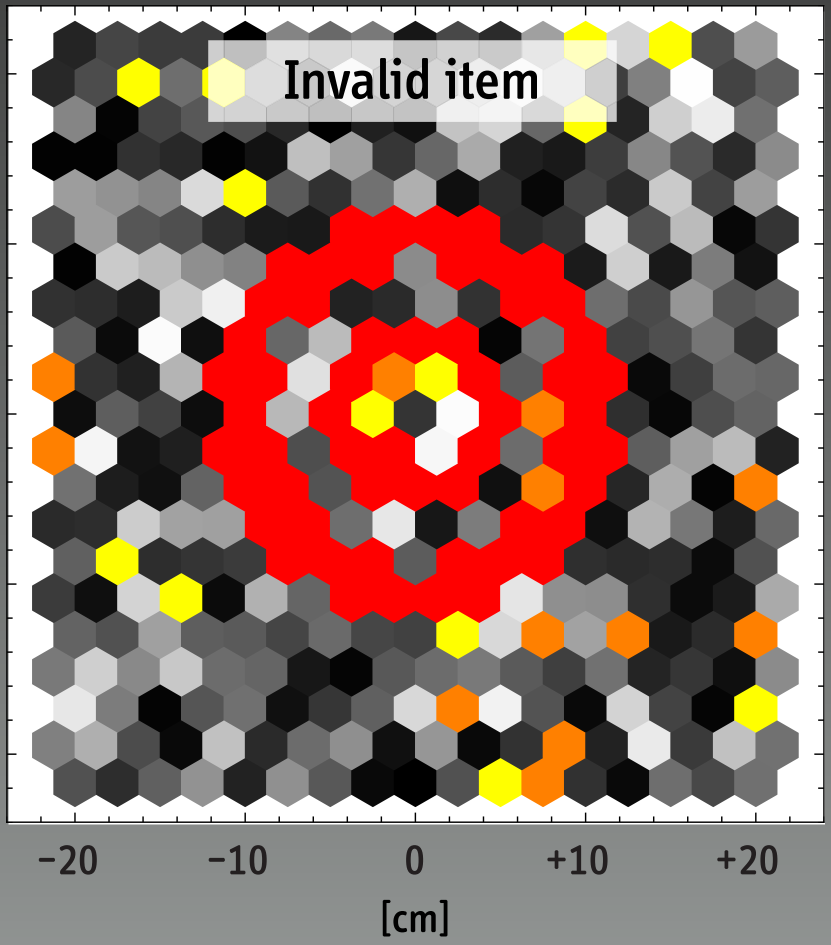
ZERO-KNOWLEDGE WARHEAD VERIFICATION

(AUTHENTICATING WARHEADS WITHOUT EVER MEASURING CLASSIFIED INFORMATION)

If the host is honest
and presents a valid warhead,
the inspector will only
see random noise

If the host tries to cheat
and presents a fake warhead,
non-random patterns will
become visible





A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502
See also: "Not-seeing is Believing," *Science,* 344 (6191), 27 June 2014, 1436–1437

WAY FORWARD

PREPARING FOR DEEP REDUCTIONS AND MULTILATERAL NUCLEAR ARMS CONTROL

TAKING INFORMATION SECURITY SERIOUSLY

- Jointly develop and demonstrate methods to count and authenticate nuclear warheads
- Focus initially on non-intrusive approaches that are acceptable to all participants (but can accommodate "upgrades")

THINKING OUTSIDE THE BOX

- Example 1: Virtual Environments

  Explore minimally intrusive inspection protocols; no sensitive information at risk
- Example 2: Modern Cryptography

  Explore concepts that do not acquire sensitive information (e.g. via zero-knowledge)

ACKNOWLEDGEMENTS

PRINCETON

Sébastien Philippe (PhD, MAE)
Robert J. Goldston (AST and PPPL)
Boaz Barak (Microsoft Research New England)
Charles Gentile (PPPL)
Mark Walker (PhD, WWS)

ELSEWHERE

Francesco d’Errico (Yale University)
Moritz Kütt (Technische Universität Darmstadt)
Tamara Patton (Vienna Center for Disarmament and Nonproliferation)

RESEARCH SUPPORTED BY

Global Zero
MacArthur Foundation
Carnegie Corporation of New York
U.S. Department of State
National Nuclear Security Administration, U.S. Department of Energy