HOW TO DISMANTLE AN ATOMIC BOMB WITHOUT SPILLING THE BEANS

Information Security in Nuclear Warhead Verification

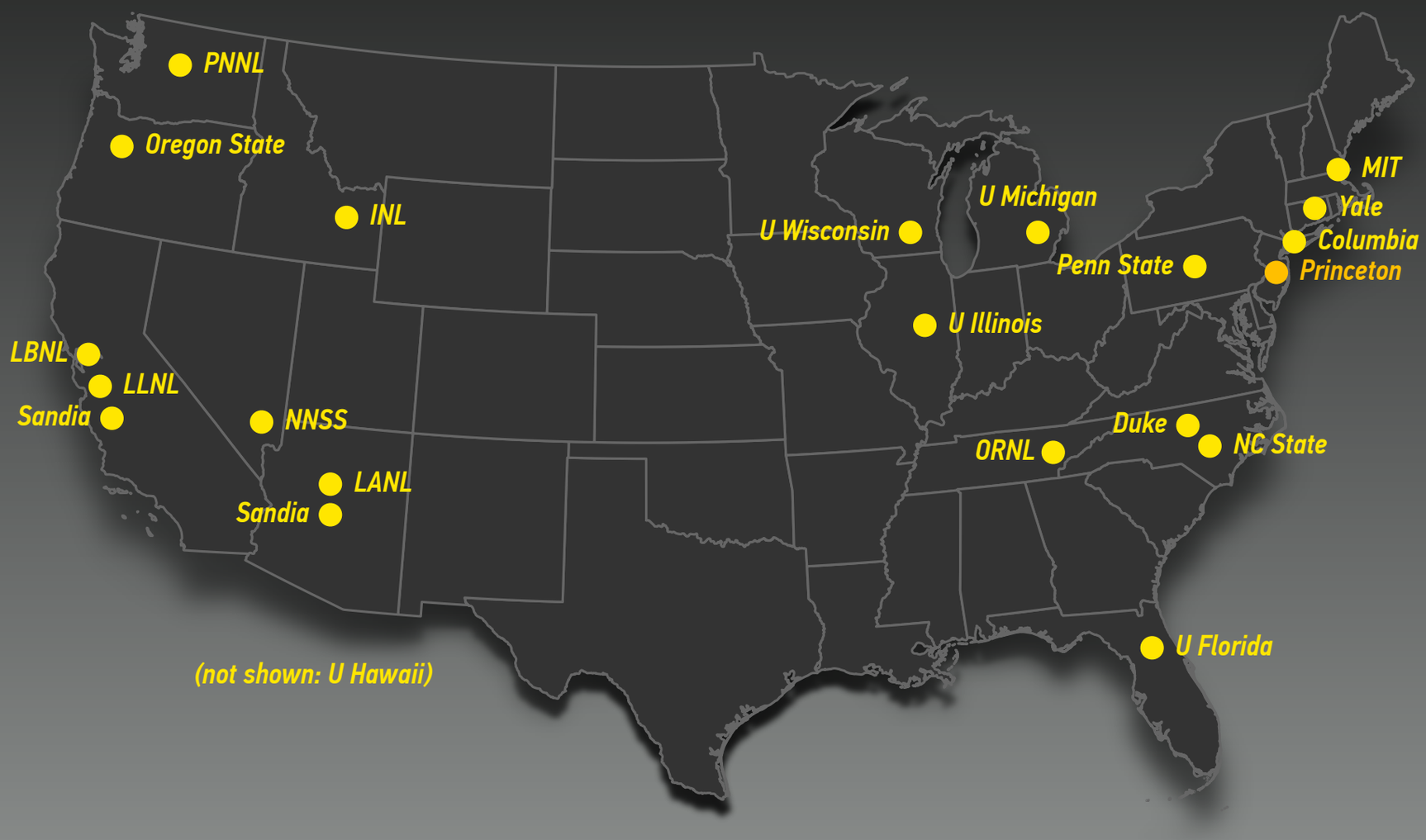
Alexander Glaser

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

University of Illinois at Urbana-Champaign
January 20, 2015

Revision 1

CONSORTIUM FOR VERIFICATION TECHNOLOGY



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

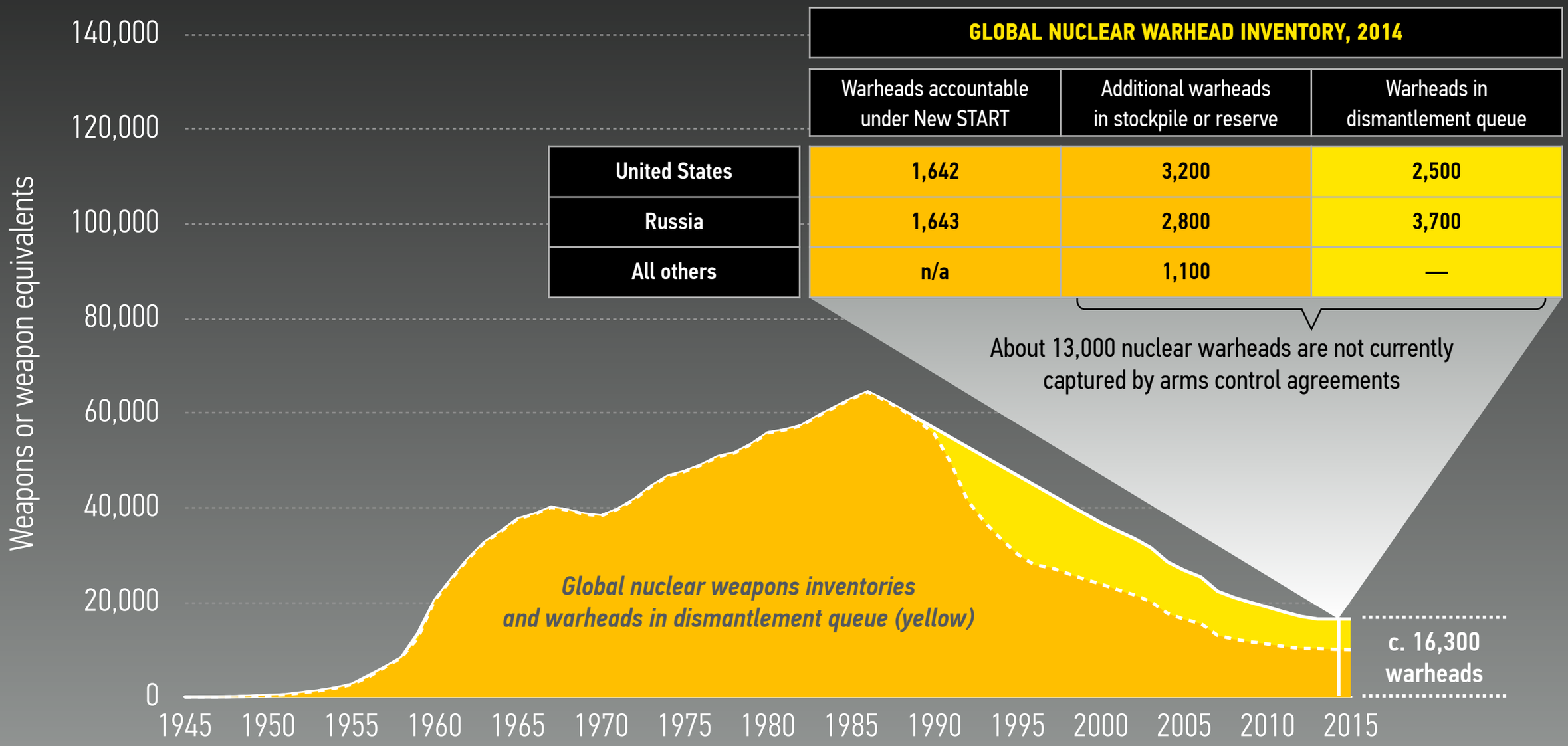
Princeton participates in the research thrust on disarmament research
(and leads the research thrust of the consortium on policy)

BACKGROUND

WARHEAD INVENTORIES AND VERIFICATION

GLOBAL NUCLEAR WEAPON INVENTORY

1945–2015



Hans M. Kristensen and Robert S. Norris, "Global Nuclear Weapons Inventories, 1945–2013," *Bulletin of the Atomic Scientists,* 69 (5), 2013, 75–81
U.S. Department of State; and H. M. Kristensen and R. S. Norris, "Worldwide Deployments of Nuclear Weapons, 2014," *Bulletin of the Atomic Scientists,* 70 (5), 2014

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

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

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

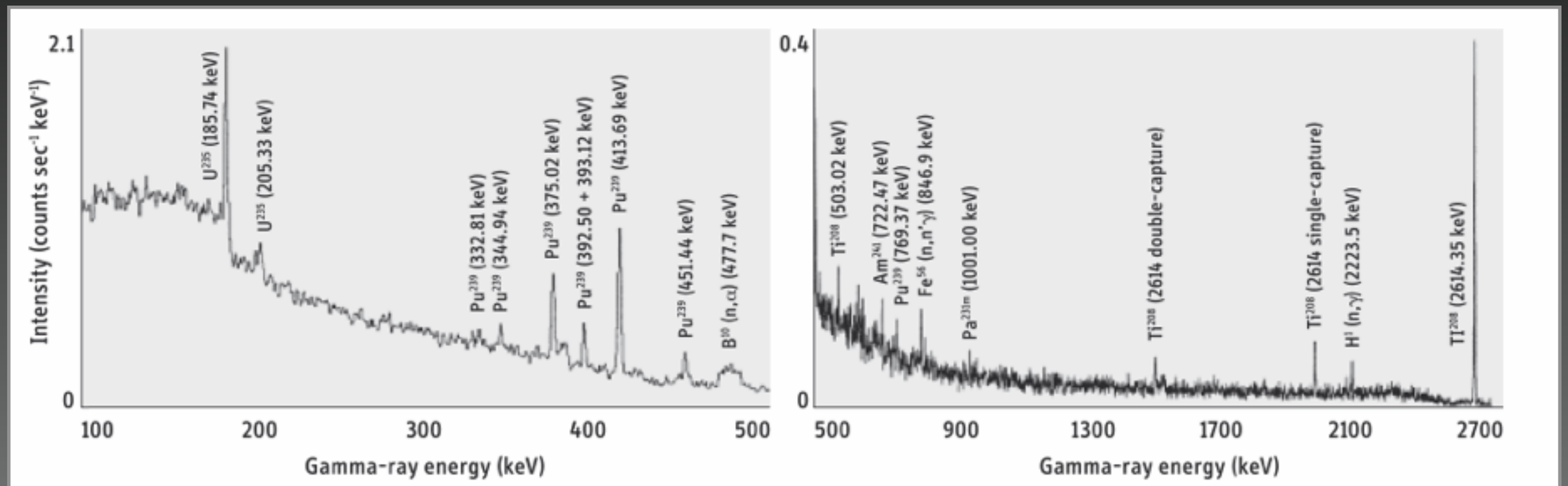
Source: U.S. Department of Energy (top) and U.S. Department of Defense, www.defenseimagery.mil (bottom)

WARHEAD AUTHENTICATION

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

NUCLEAR WEAPONS HAVE UNIQUE SIGNATURES

BUT MOST OF THEM ARE SENSITIVE AND CANNOT BE REVEALED TO INSPECTORS

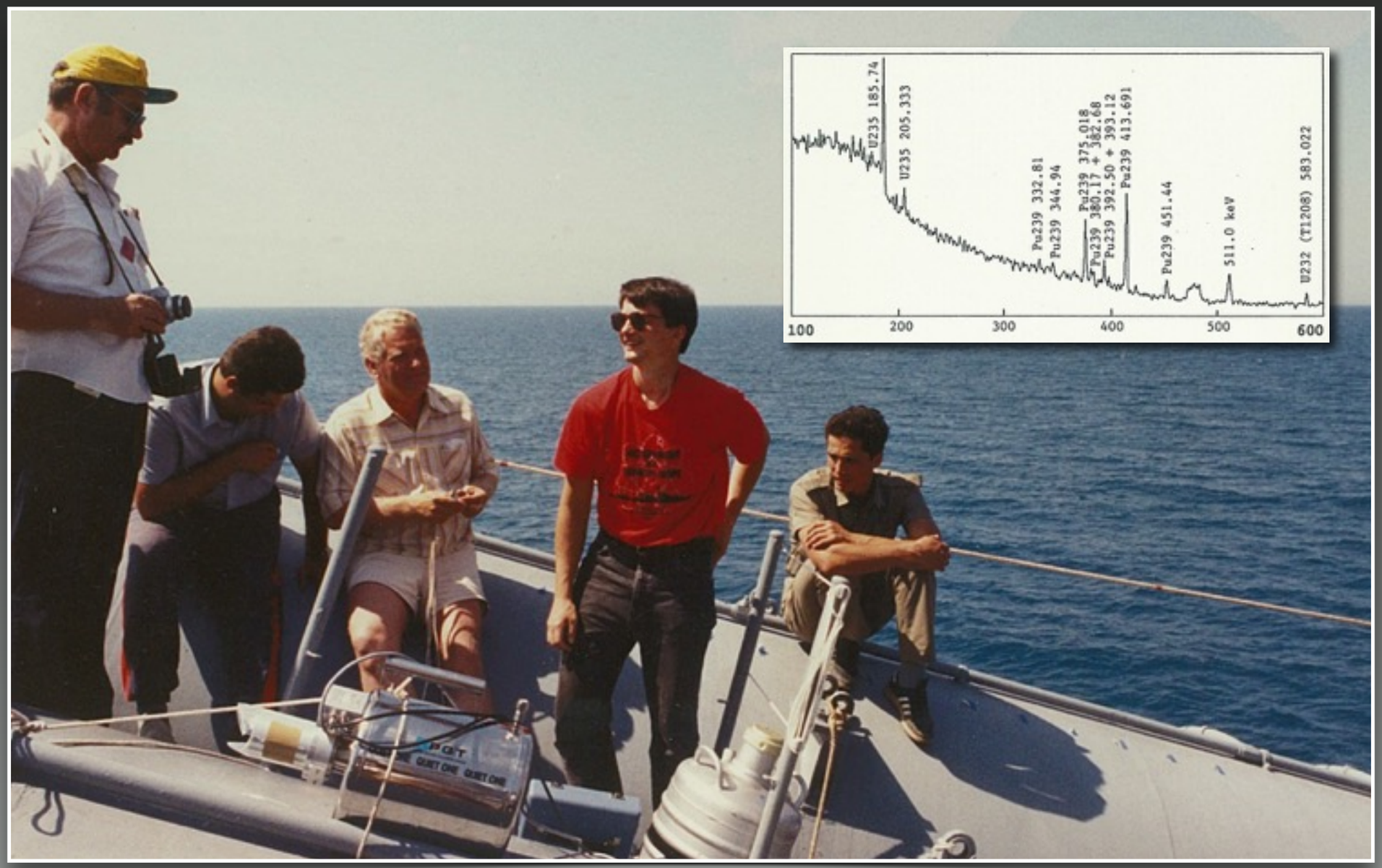


Gamma radiation spectrum from a Soviet warhead measured in 1989

Steve Fetter, Thomas B. Cochran, Lee Grodzins, Harvey L. Lynch and Martin S. Zucker
"Measurements of Gamma Rays from a Soviet Cruise Missile," Science, Vol. 248, 18 May 1990, pp. 828–834

NUCLEAR WEAPONS HAVE UNIQUE SIGNATURES

BUT MOST OF THEM ARE SENSITIVE AND CANNOT BE REVEALED TO INSPECTORS



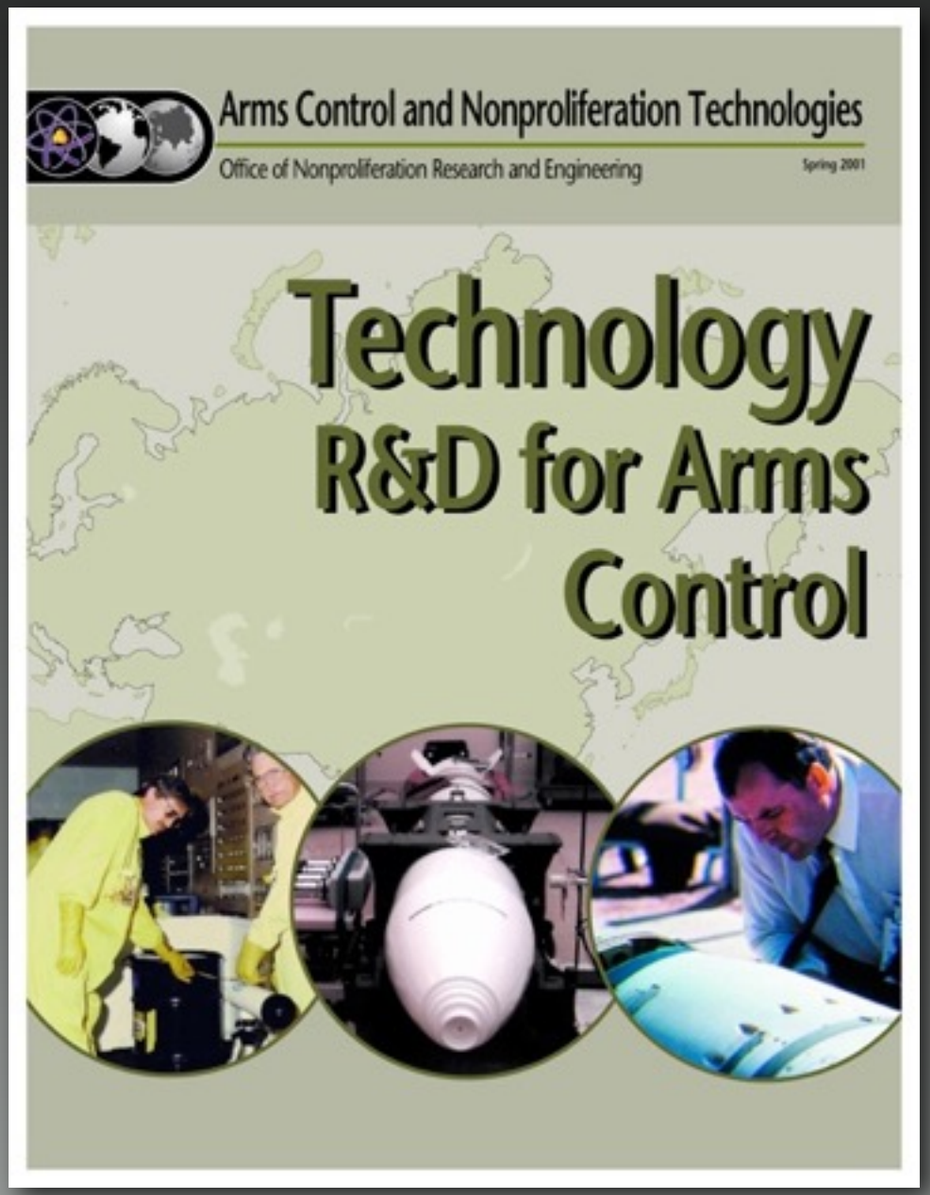
U.S. Scientists on a Soviet Cruiser in the Black Sea, 1989

INFORMATION SECURITY

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

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

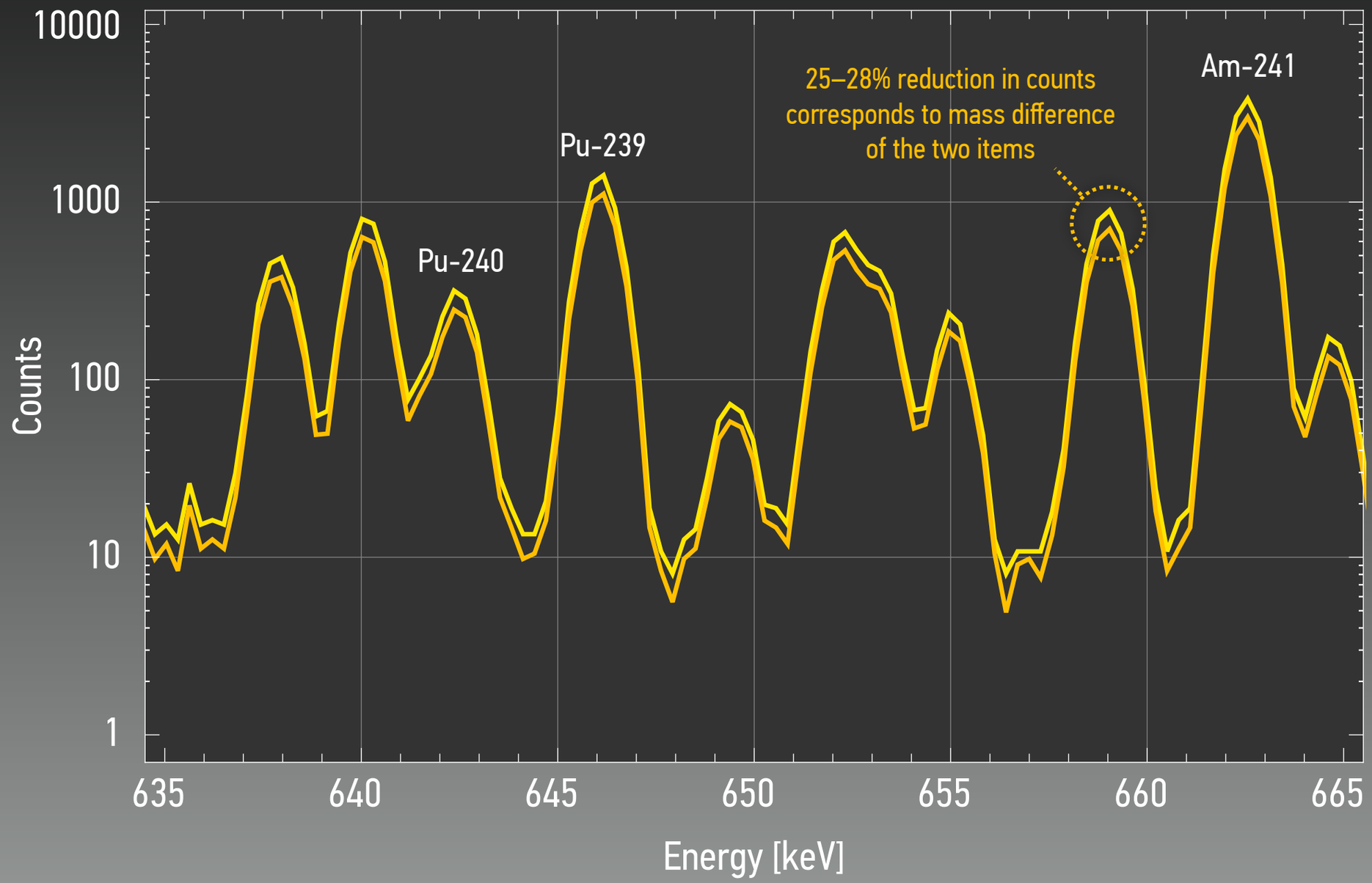
Comparing the radiation signature
from the inspected item with a reference item
("golden warhead") of the same type

INFORMATION BARRIERS

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

HIGH-RESOLUTION GAMMA SPECTRA

SIMULATED DATA FOR THIN SHELLS OF WEAPON-GRADE PLUTONIUM



Relative intensities of Pu-239, Pu-240, and Am-241 peaks can be used to estimate isotopics and age of the material
MCNP simulations by Janet Schirm and Alex Glaser

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.

EXAMPLE

PRINCETON / GLOBAL ZERO WARHEAD VERIFICATION PROJECT

PRINCETON / GLOBAL ZERO WARHEAD VERIFICATION PROJECT

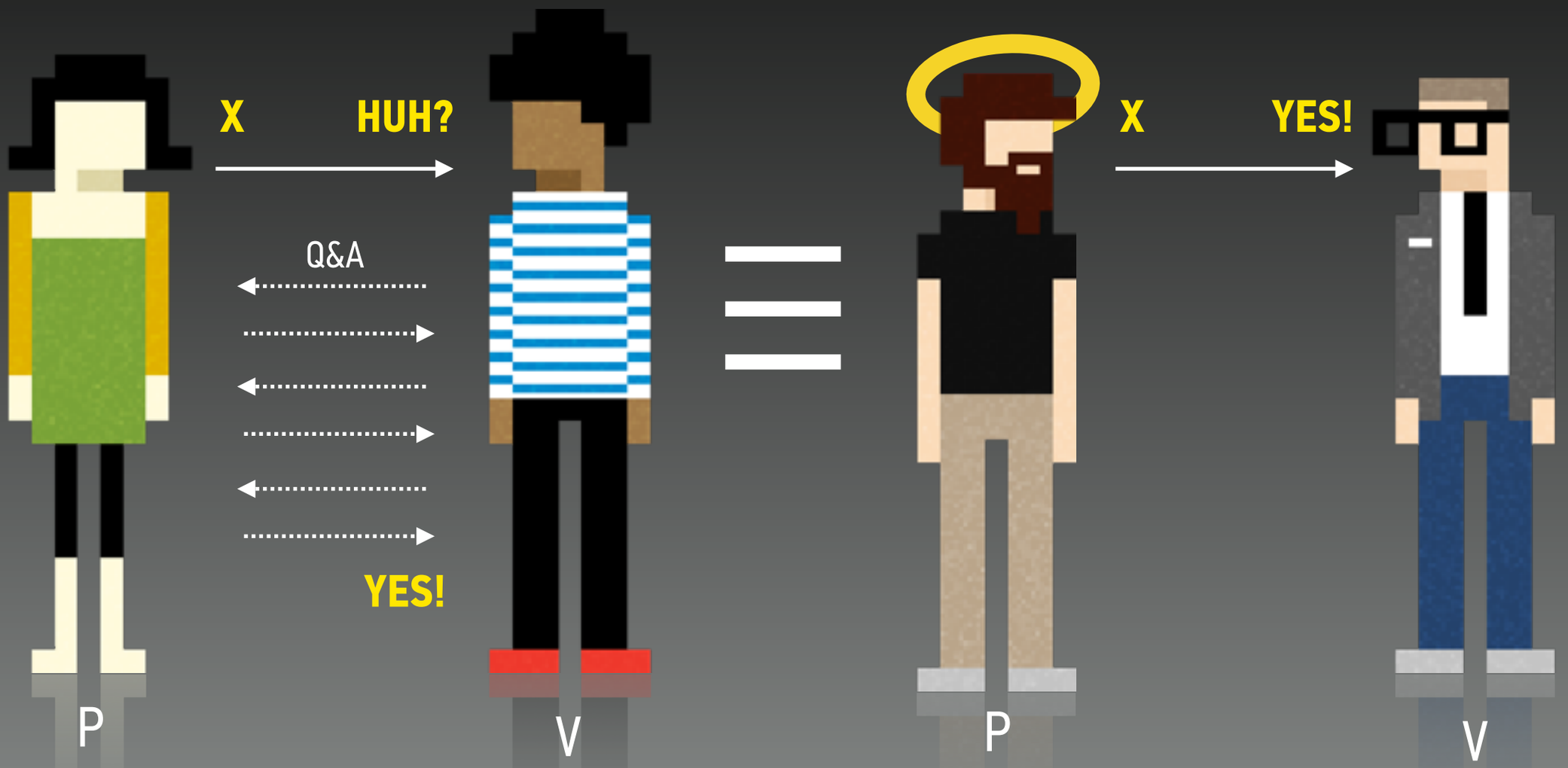
Princeton Plasma Physics Laboratory

GENERAL APPROACH

- 14.1-MeV neutrons for imaging
- Template approach
- Unclassified test objects
- Zero-knowledge interactive protocol
- Non-electronic detectors

So far, mostly simulated data;
experimental demonstration now underway

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 SUDOKU

DEMO

Concept and idea by Moni Naor, wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO

	5	
4		
		1

		2
9	3	
	7	

	8	6
2		3

2		
		6
7		9

		3
4		
		5

		5
	1	

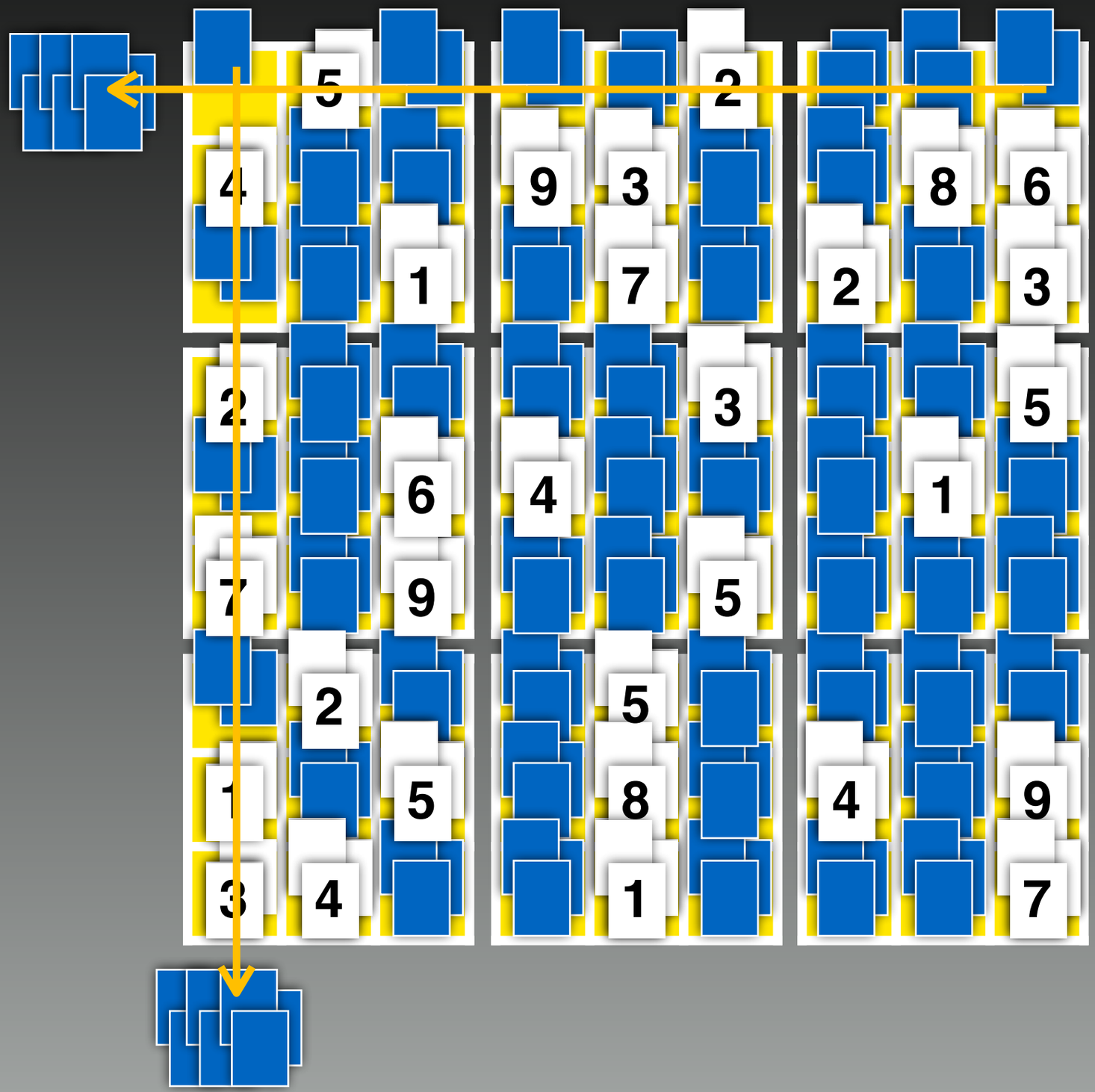
	2	
1		5
3	4	

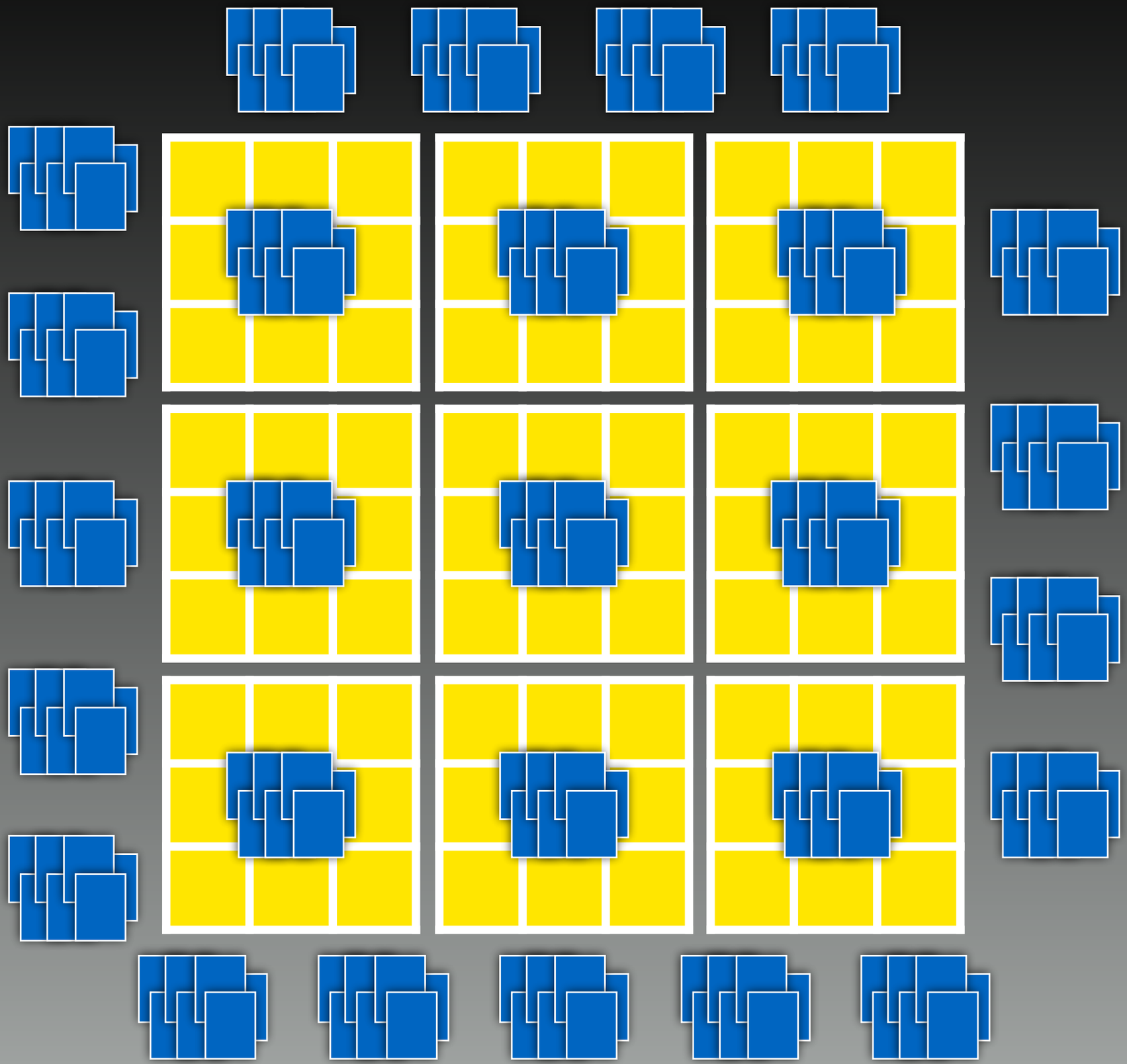
	5	
	8	
	1	

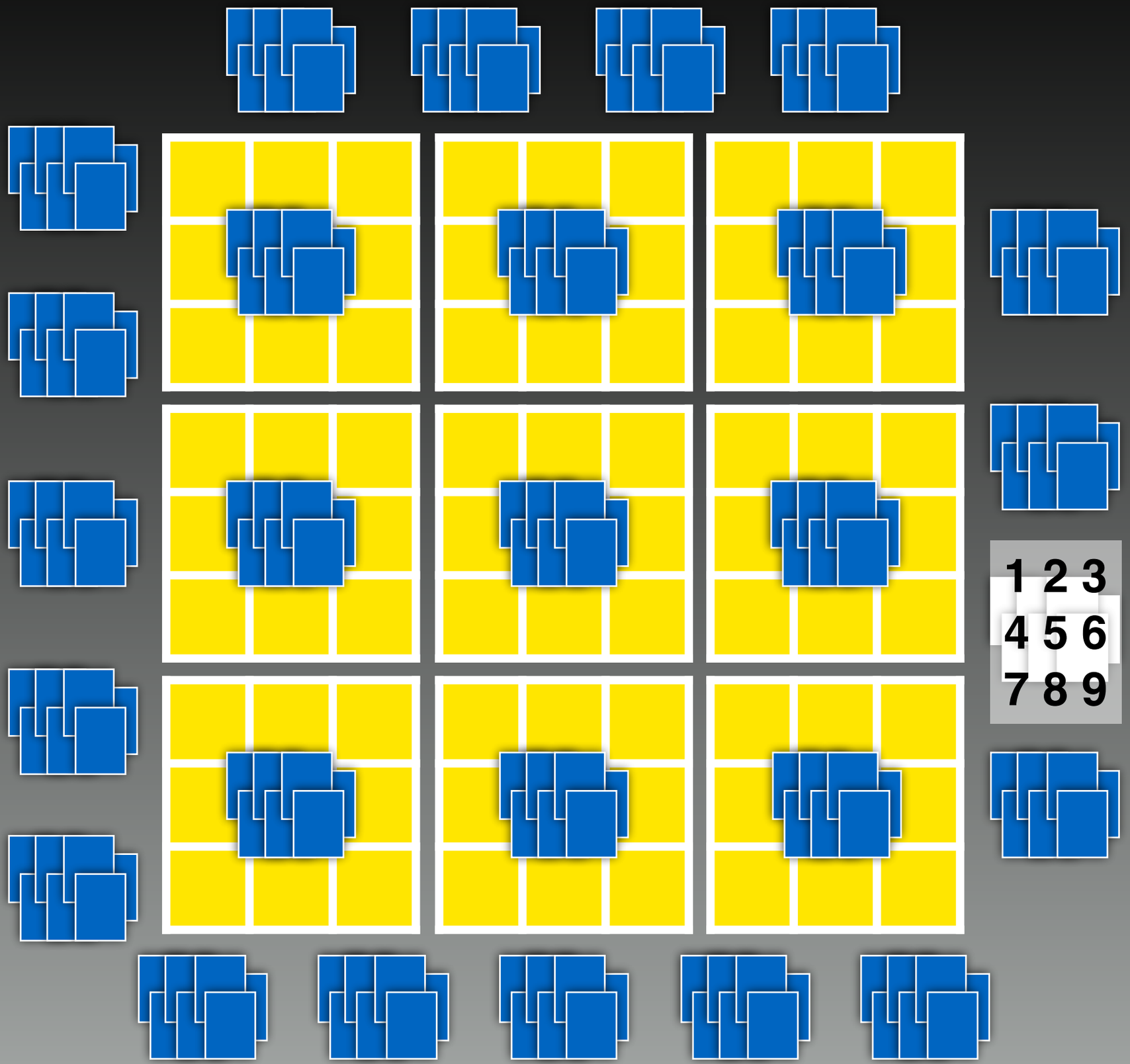
4		9
		7

	5			2				
4			9	3			8	6
		1		7		2		3
2				3				5
		6	4				1	
7		9			5			
	2			5				
1		5		8		4		9
3	4			1				7

	5			2				
4			9	3			8	6
		1		7		2		3
2					3			5
		6	4		5		1	
7		9						
	2			5				
1		5		8		4		9
3	4			1				7


5 2
4 9 3 8 6
1 7 2 3
2 3 5
6 4 1
7 9 5
2 5 8 4 9
1 5 4 8 1 7
3 4




1 2 3
4 5 6
7 8 9

"NUMBER OF MARBLES IN A CUP"

Peggy has two small cups each containing the same number of marbles. She wants to prove to Victor that both cups contain the same number of marbles without revealing to him what this number is.

BUBBLE DETECTORS OFFER A WAY TO IMPLEMENT THIS PROTOTOCL

AND AVOID DETECTOR-SIDE ELECTRONICS

Bubble detectors (BTI Technologies)

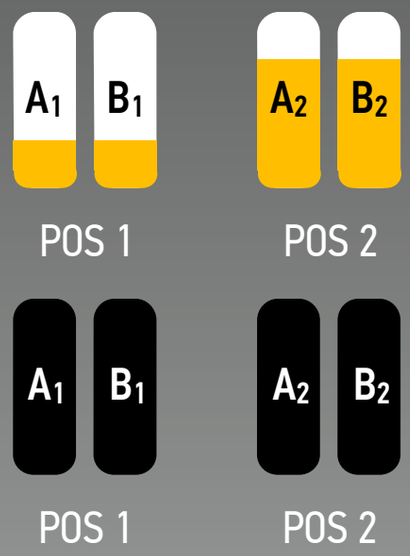
Optical readout

Detectors with different neutron-energy thresholds (no cutoff, 500 keV, 1 MeV, 10 MeV) allow measurements that are sensitive to different diversion scenarios

PROPOSED HARDWARE IMPLEMENTATION OF A ZERO-KNOWLEDGE PROTOCOL FOR NUCLEAR WARHEAD VERIFICATION

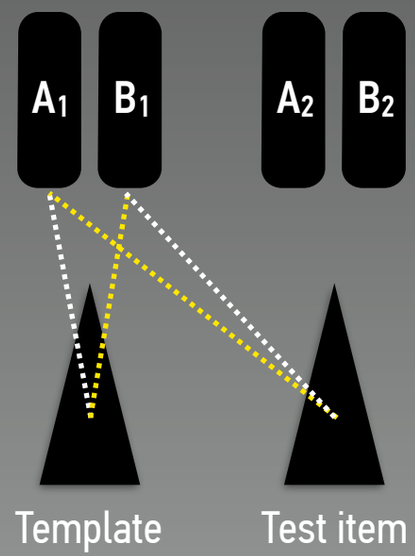
1

Host preloads secretly n pairs of bubble detectors with "negative" radiograph of the template



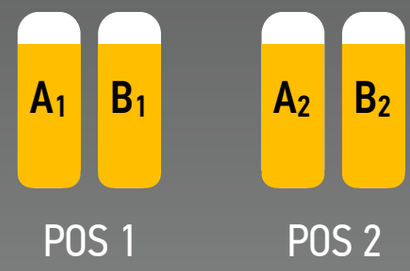
2

For every position, inspector chooses randomly, which detector (A_i, B_i) to use on reference or test item



3

After interrogation, inspector verifies all detectors contain the same bubble count



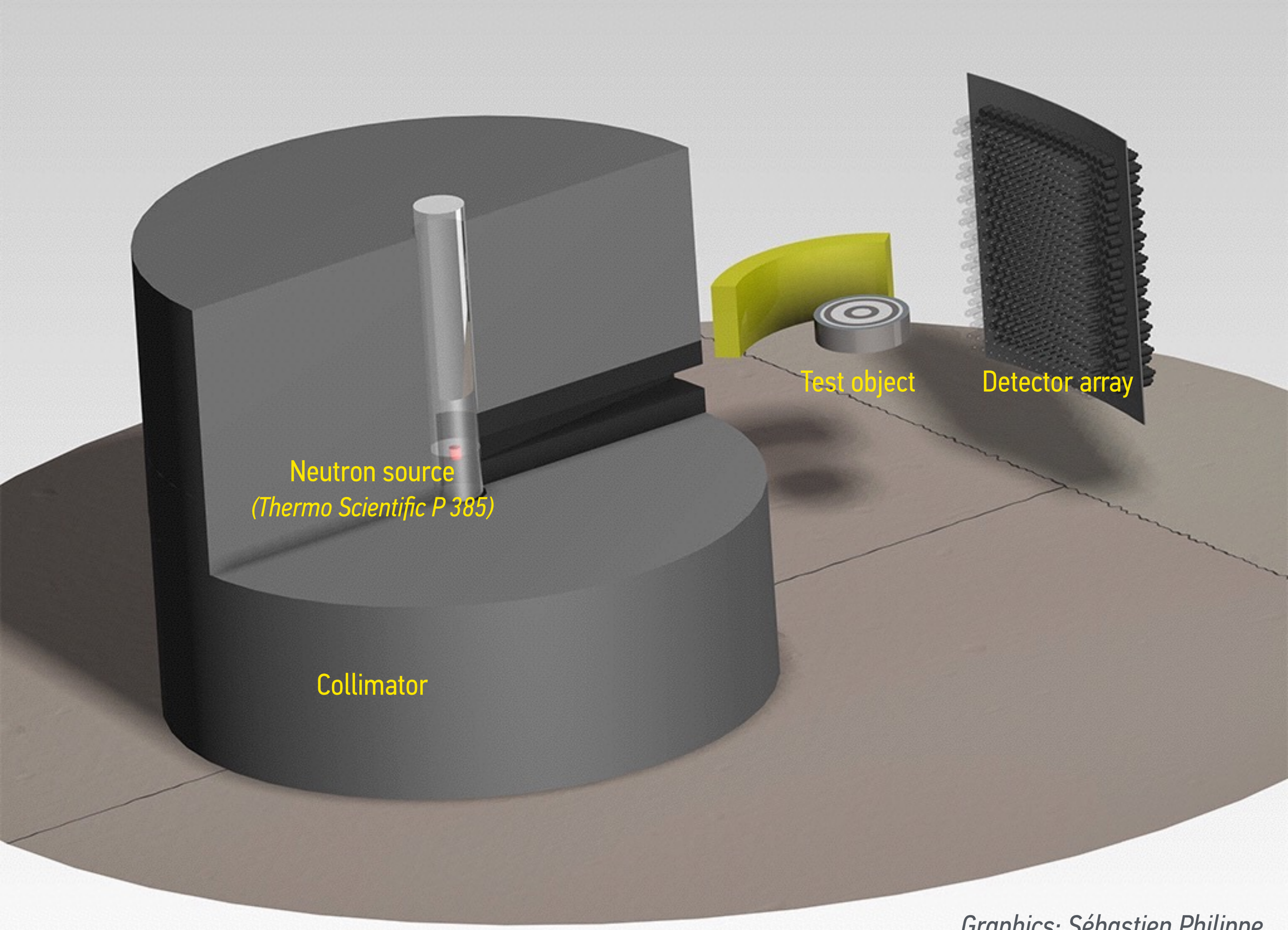
50% confidence after 1st round

...

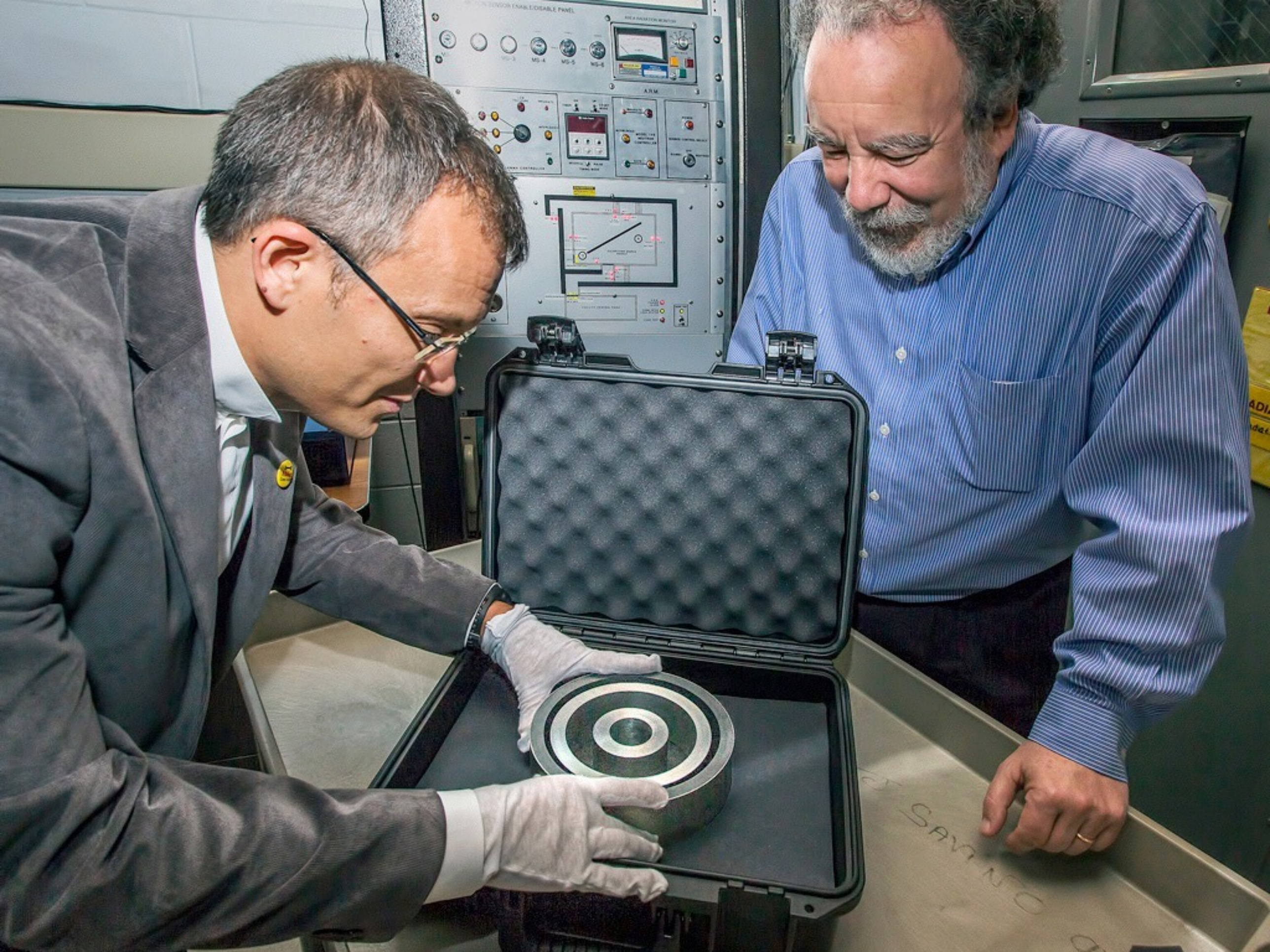
95% confidence after 5th round

WILL IT BLEND?

www.blendtec.com

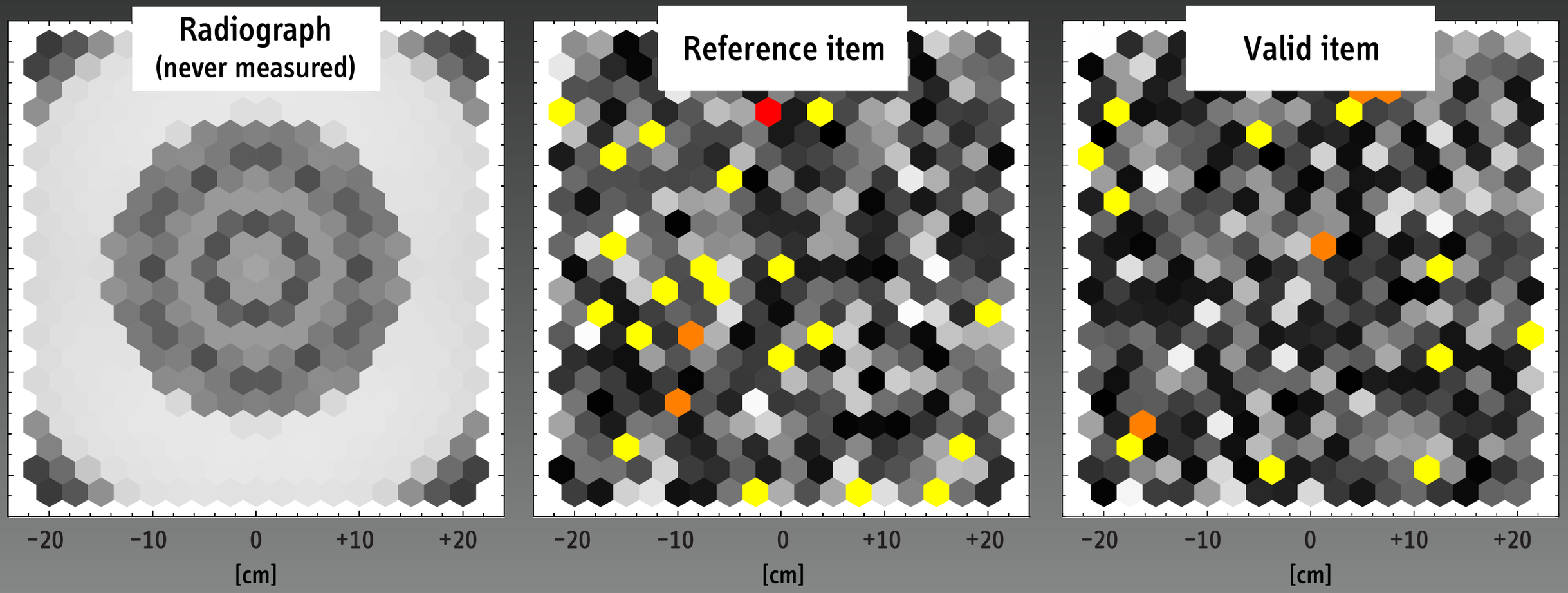


Graphics: Sébastien Philippe



ZERO-KNOWLEDGE VERIFICATION

AUTHENTICATING WARHEADS WITHOUT MEASURING CLASSIFIED INFORMATION

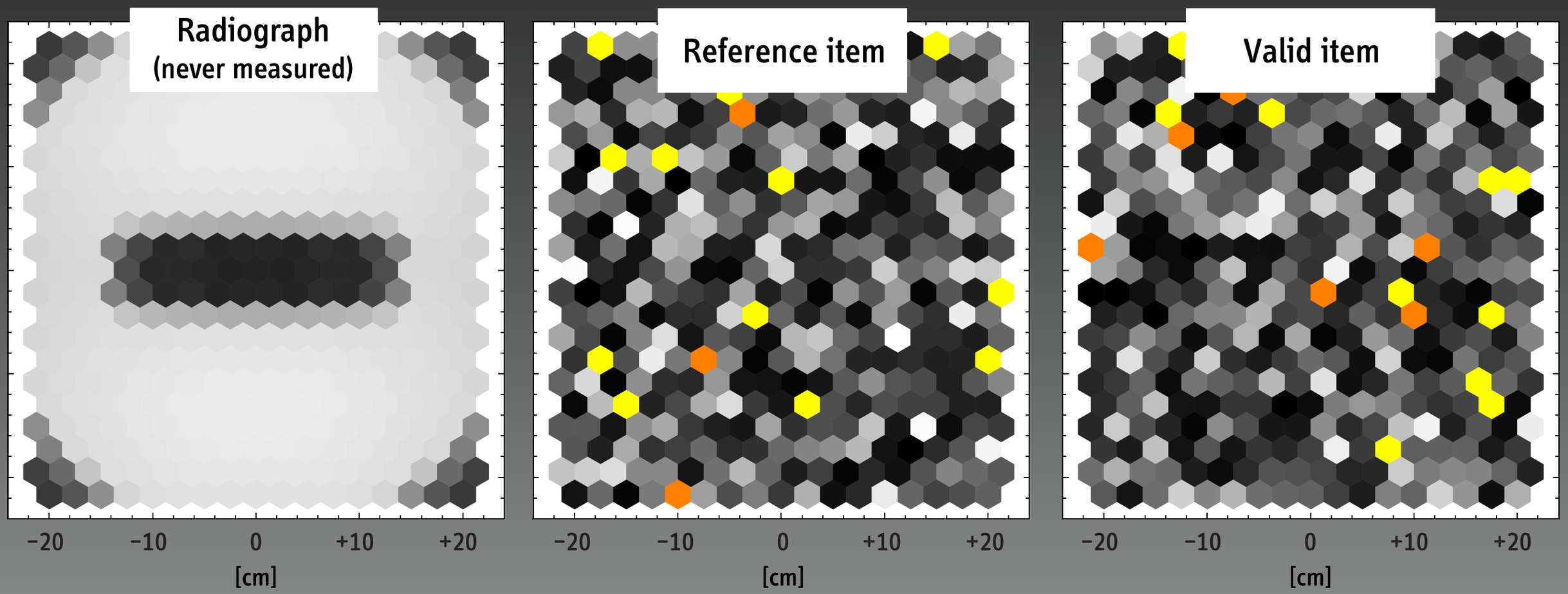


Simulated data from MCNP5 calculations, neutron energies > 10 MeV, N(max) = 5,000

A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502

ZERO-KNOWLEDGE VERIFICATION

AUTHENTICATING WARHEADS WITHOUT MEASURING CLASSIFIED INFORMATION

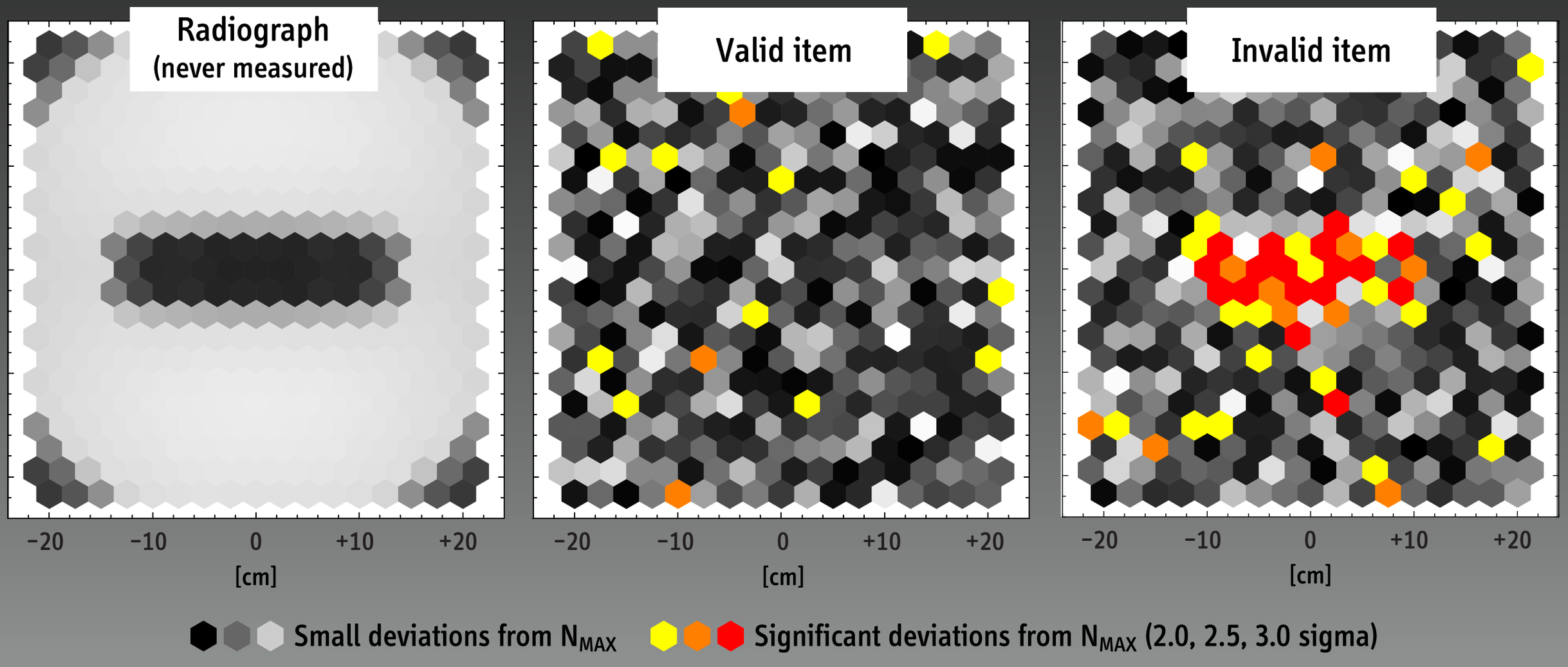


Simulated data from MCNP5 calculations, neutron energies > 10 MeV, N(max) = 5,000

A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502

ZERO-KNOWLEDGE VERIFICATION

AUTHENTICATING WARHEADS WITHOUT MEASURING CLASSIFIED INFORMATION

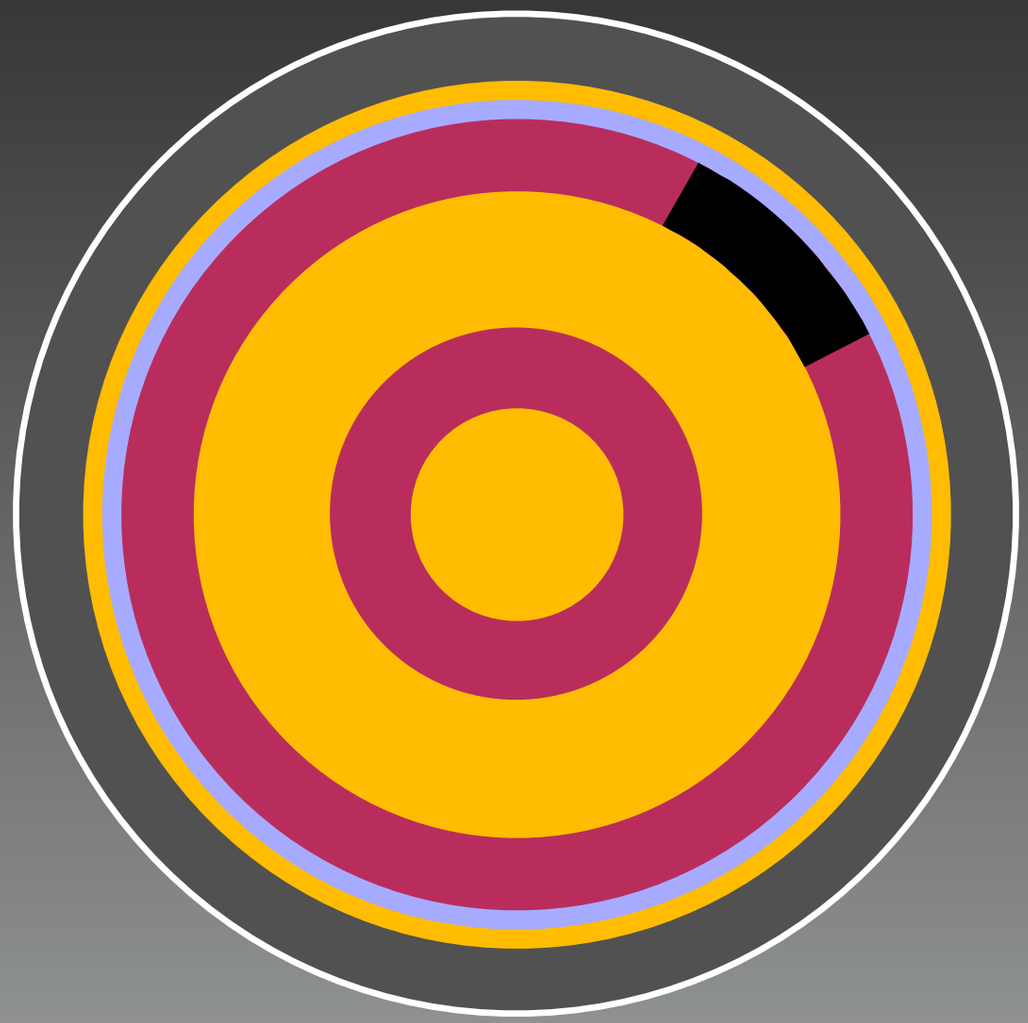


Simulated data from MCNP5 calculations, neutron energies > 10 MeV, N(max) = 5,000; invalid item: lead for tungsten

A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502

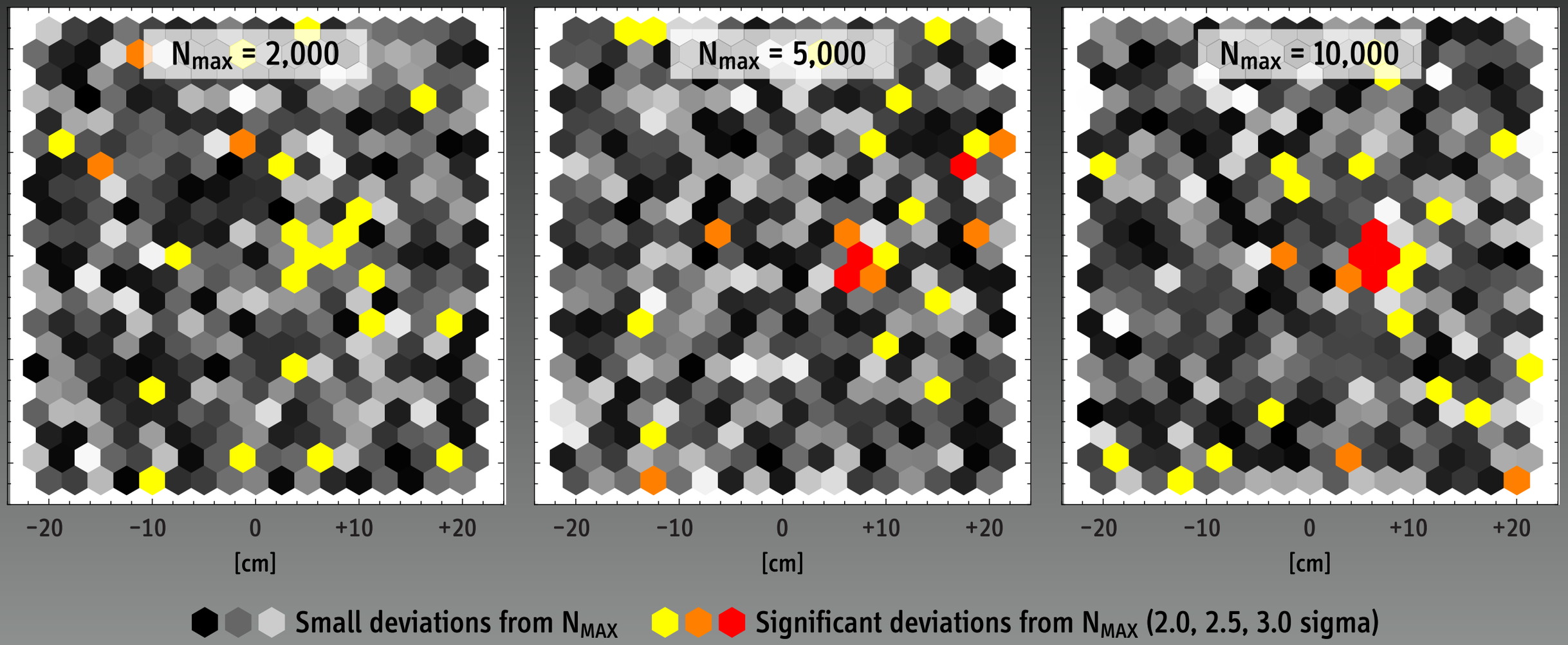
LOCAL TUNGSTEN DIVERSION

36-DEGREE SEGMENT OF OUTER TUNGSTEN RING (543 GRAMS, 7% OF TOTAL TUNGSTEN)



ZERO-KNOWLEDGE VERIFICATION

AUTHENTICATING WARHEADS WITHOUT MEASURING CLASSIFIED INFORMATION



543 grams of tungsten removed from outer ring of BTO; simulated data from MCNP5 calculations, neutron energies > 10 MeV

A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502

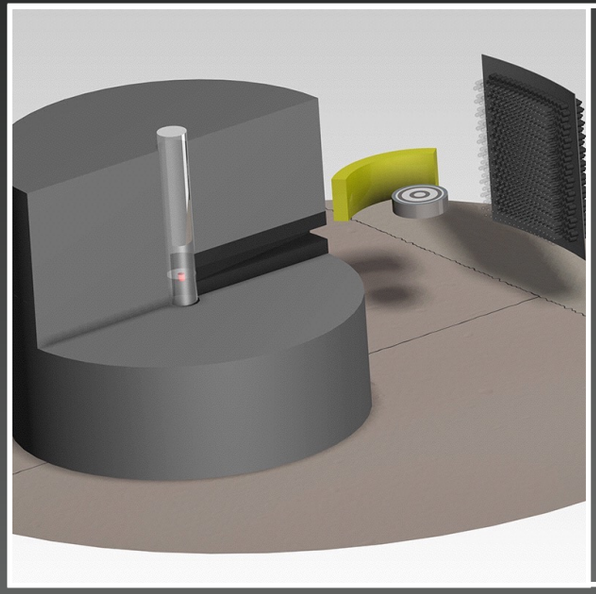

AMERICA'S ALL TIME
FAVORITE GAME
BATTLESHIP
IT'S A HIT
G-4
BATTLESHIP

PROBABILITIES FOR AN ITEM TO BE FLAGGED AS "INVALID"

N(max)	500	1,000	2,000	5,000	10,000	32,000
Valid item	≤ 5% (by design, in all cases)					
Full removal	> 99.9% (in call cases)					
Full substitution	77.7%	99.5%	> 99.9%	> 99.9%	> 99.9%	> 99.9%
Local removal	undetectable	15.7%	41.7%	94.6%	> 99.9%	> 99.9%
Local substitution	undetectable	undetectable	6.0%	11.7%	30.2%	95.5%

A. Glaser, B. Barak, R. J. Goldston, "A Zero-knowledge Protocol for Nuclear Warhead Verification," *Nature,* 510, 26 June 2014, 497–502

WAY FORWARD



DEMONSTRATING VIABILITY OF ZERO-KNOWLEDGE APPROACHES

- Experimental reproducibility of results
- Maximize bubble loading and confirm absence of bubble "aging"
- Two-color setting (e.g. 300 keV and 14 MeV neutrons)
  combined with different detector thresholds (e.g. 1 MeV and 10 MeV)

WARHEAD VERIFICATION: TAKING INFORMATION SECURITY SERIOUSLY

- Examine viability of "simple" inspection systems (gamma *and* neutron)
- Focus initially on non-intrusive verification approaches
  (i.e., acceptable to all participants, but designed to accommodate "upgrades")

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