Zero-Knowledge Arms Control:

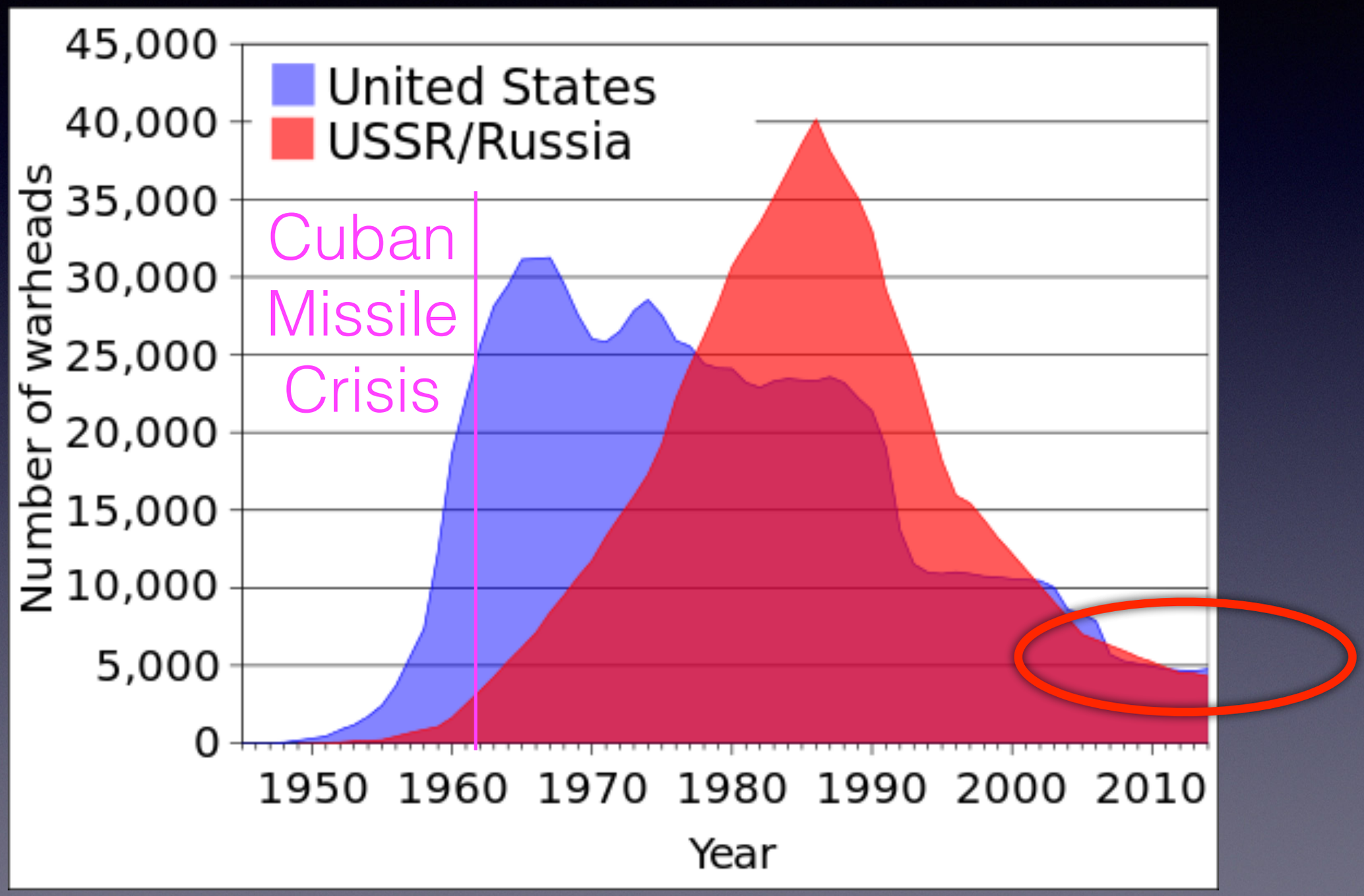
Proving a Warhead is Real While Learning Nothing about it

Rob Goldston, PPPL Director (1997 - 2009)
Prof. of Astrophysical Sciences
Affiliated Faculty, WWS Program on Science and Global Security

Other team members: Prof. Alex Glaser, P.U.,
Dr. Boaz Barak, Microsoft Research, New England
Sebastien Philippe, P.U. Graduate Student
Francesco D'Errico, Yale University

PPPL

The World has Fewer, but Still Far Too Many, Nuclear Warheads



Federation of American Scientists

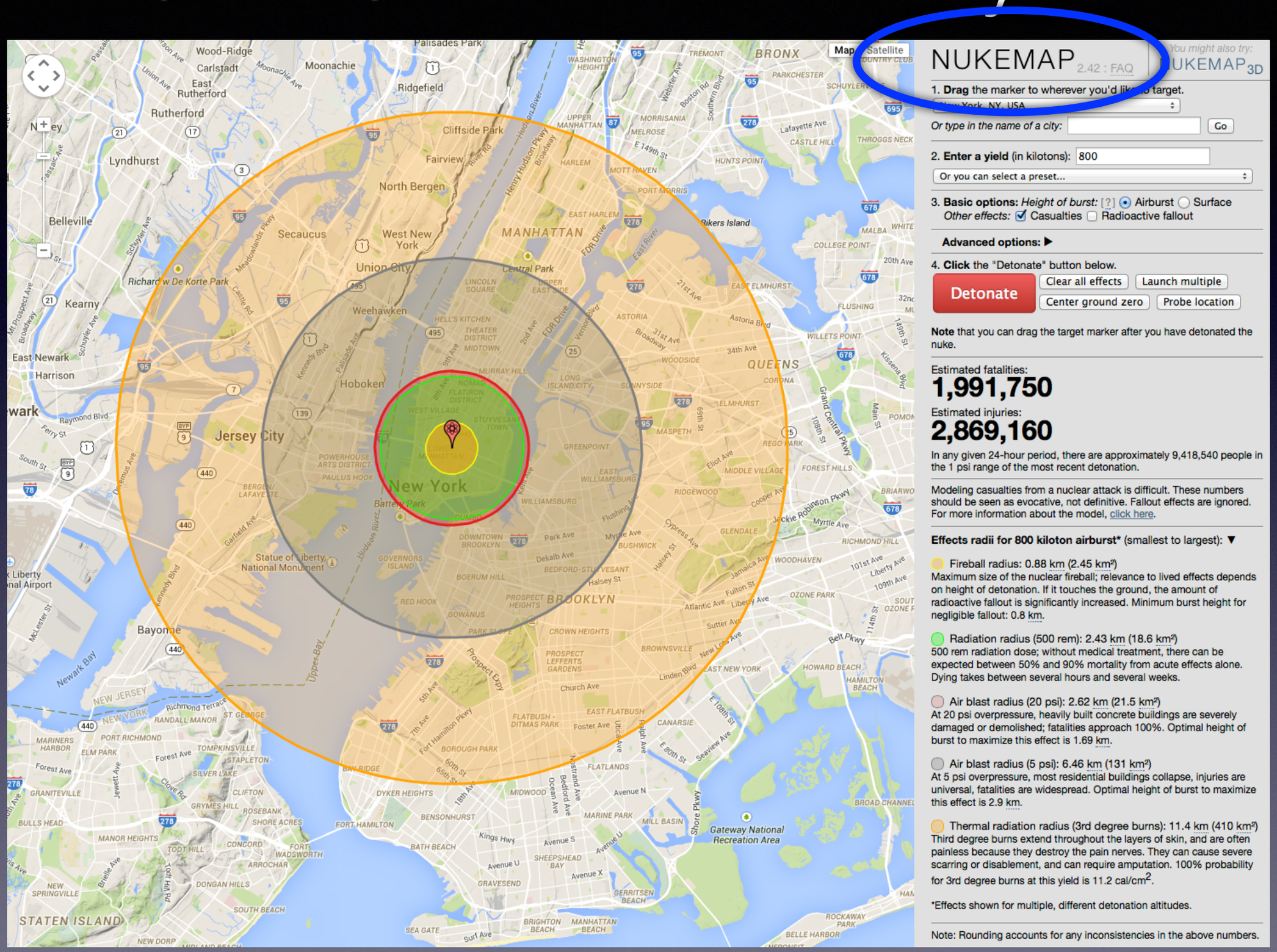
4,300 Ready to Go
5,800 in Storage

Status of World Nuclear Forces 2014*

Country	Operational Strategic	Operational Nonstrategic	Reserve/ Nondeployed	Military Stockpile	Total Inventory
Russia	1,800[a]	0[b]	2,500[c]	4,300	8,000[d]
United States	1,920[e]	184[f]	2,661[g]	4,765[h]	7,315[i]
France	290	n.a.	?[j]	300	300
China	0[j]	?[k]	250	250	250[k]
United Kingdom	160[l]	n.a.	65	225	225[l]
Israel	0	n.a.	80	80	80[m]
Pakistan	0	n.a.	100-120	100-120	100-120[n]
India	0	n.a.	90-110	90-110	90-110[o]
North Korea	0	n.a.	<10	<10	<10[p]
Total:[q]	**~4,100**	**~180**	**~5,800**	**~10,100**	**~16,300**

Federation of American Scientists

Just One is Too Many - I



5 million people

Just One is Too Many - II

No survivors. Within tens of minutes, everything within approximately five to seven miles of Midtown Manhattan would be engulfed by a gigantic firestorm. The fire zone would cover a total area of 90 to 152 square miles (230 to 389 square kilometers). The firestorm would rage for three to six hours. Air temperatures in the fire zone would likely average 400 to 500 degrees Fahrenheit (200 to 260 Celsius).

After the fire burned out, the street pavement would be so hot that even tracked vehicles could not pass over it for days. Buried, unburned material from collapsed buildings throughout the fire zone could burst into flames when exposed to air—months after the firestorm had ended.

Those who tried to escape through the streets would have been incinerated by the hurricane-force winds filled with firebrands and flames. Even those able to find shelter in the lower-level sub-basements of massive buildings would likely suffocate from fire-generated gases or be cooked alive as their shelters heated to oven-like conditions.

Bulletin of the Atomic Scientists

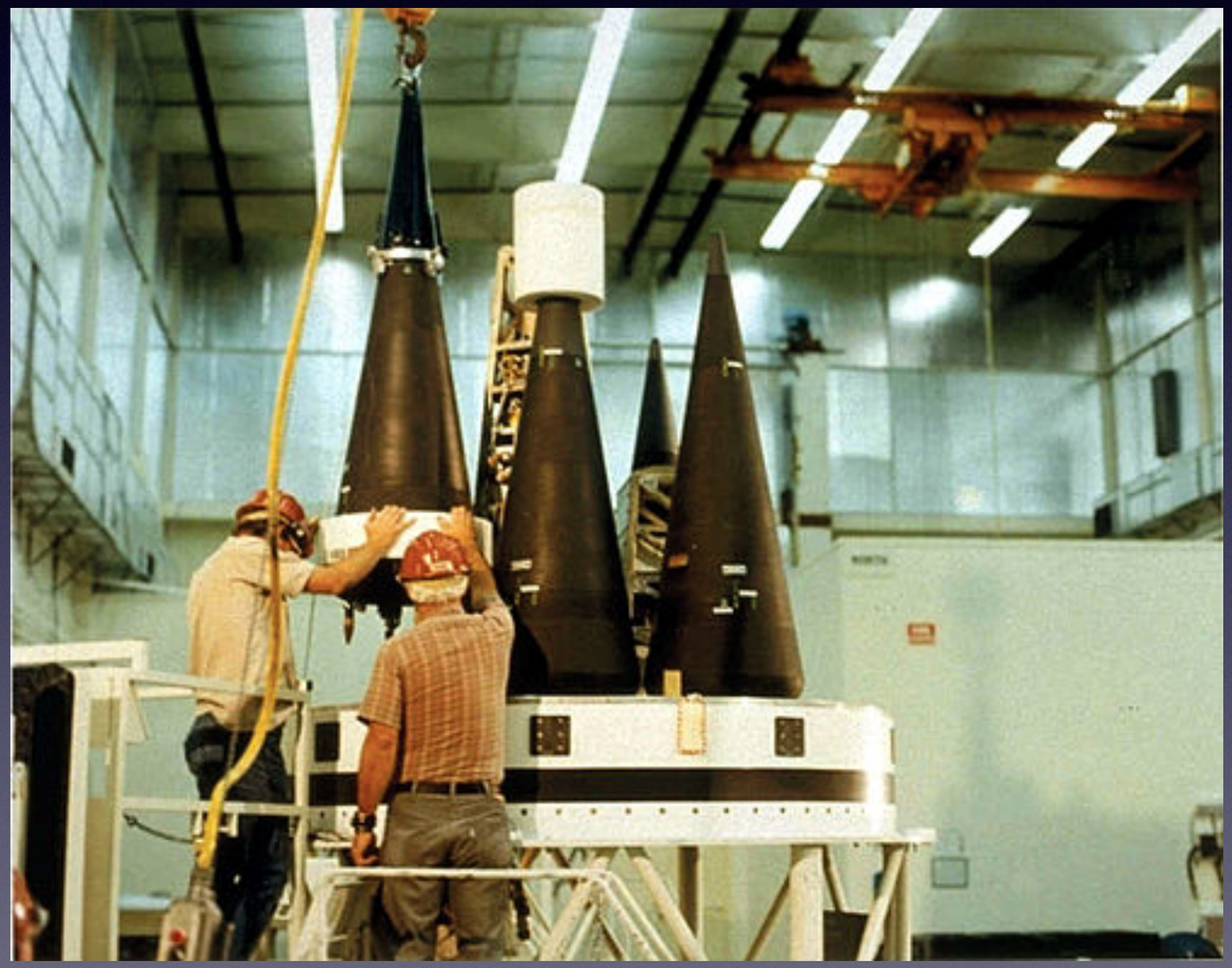
In Past Treaties We Have Counted only Delivery Vehicles

Bombers

Submarines

Missiles

Multiple Independently Targetable Re-entry Vehicles



The most destabilizing idea ever.

A first-strike weapon.

US is eliminating them.
Russia is building more.

How do you count their warheads without learning what's inside?

Confirm that the claimed non-warheads make no radiation.
Count the rest as real.

The Paradox of the Next Phase of Arms Control

To get to low numbers we need to verify the dismantlement of real warheads – including from storage.

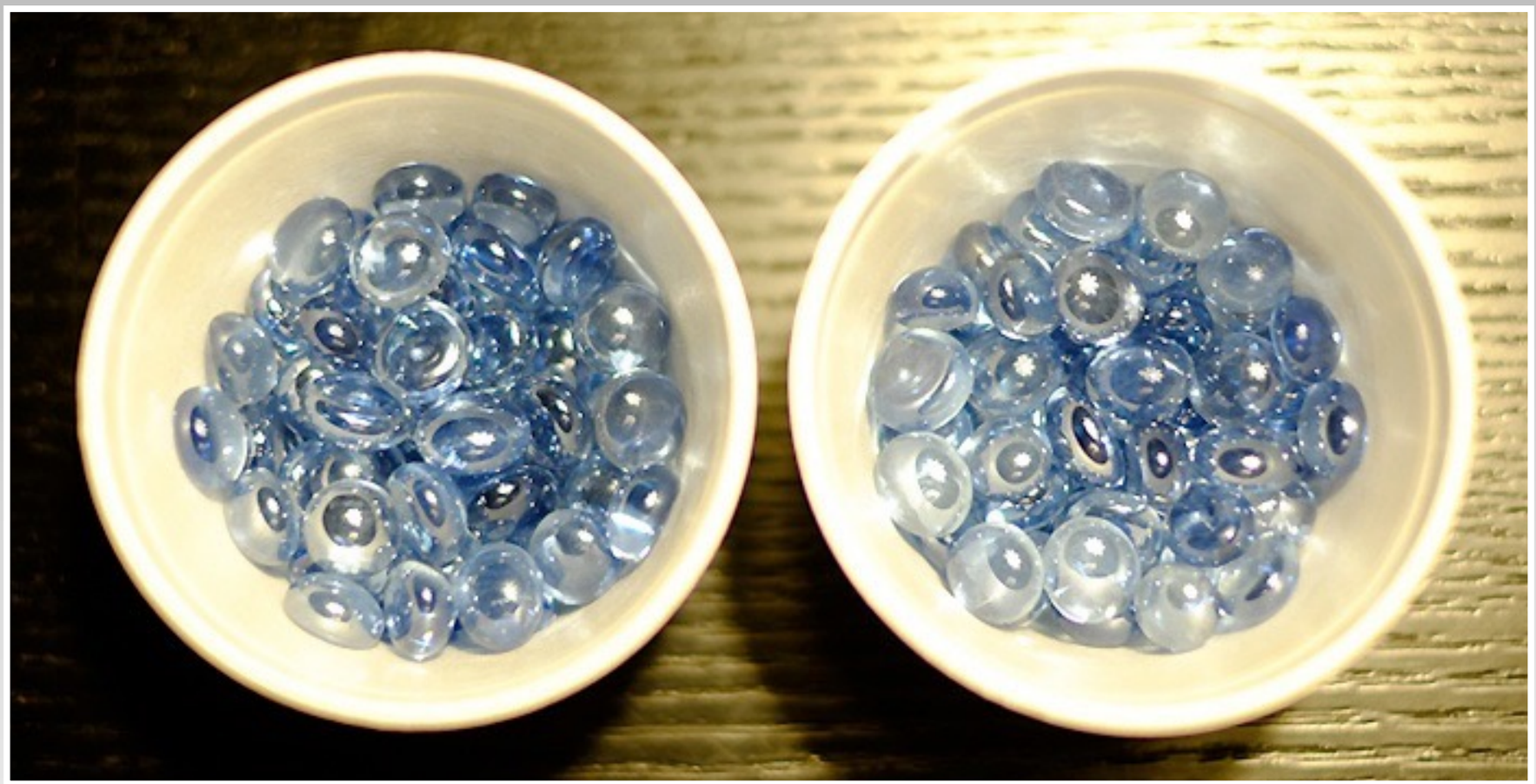
But the U.S. and Russia do not want to reveal their weapon designs to each other.

And no one wants to reveal weapons designs to non-weapons states. Arms control should not cause nuclear proliferation.

So how do you prove a warhead is real without learning anything at all about it?

Filled with Rocks?

“Number of Marbles in a Cup”



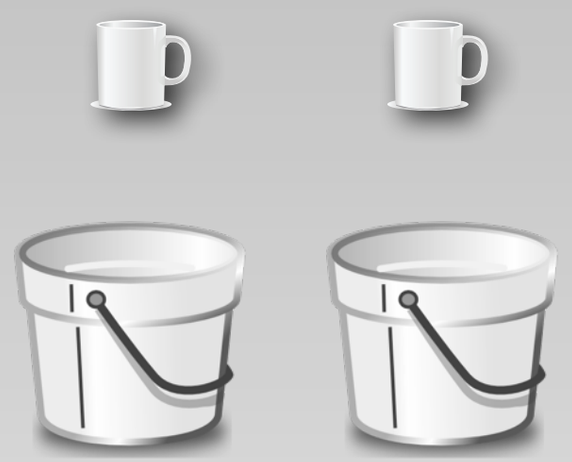
Alice has two small cups each containing the same number of marbles. She wants to prove to Bob that both cups contain the same number of marbles without revealing to him what this number is.

So, what does she do?

“Number of Marbles in a Cup”

1

Alice claims that two cups contain the same number of marbles



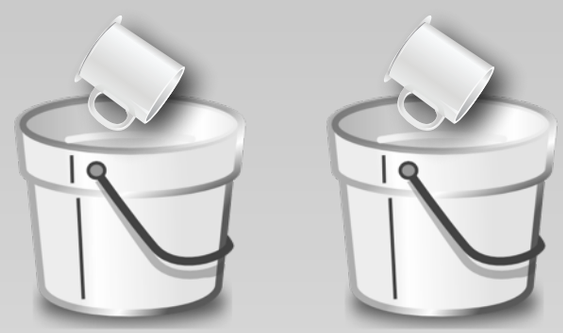
She then also offers two buckets of marbles

She claims these buckets also contain an identical number of marbles

2

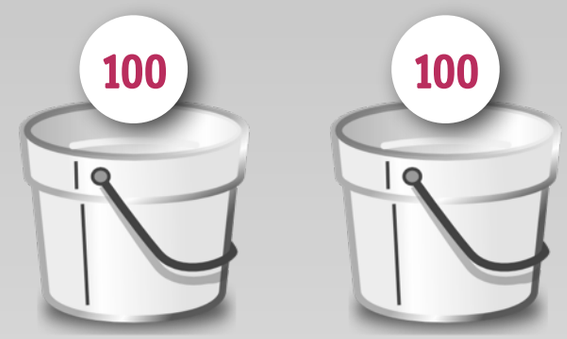
Bob chooses randomly into which bucket which cup is poured

(L,L) and (R,R) or (L,R) and (R,L)



3

Bob now counts the marbles in each bucket and should find the same number in both



50% confidence after 1st game

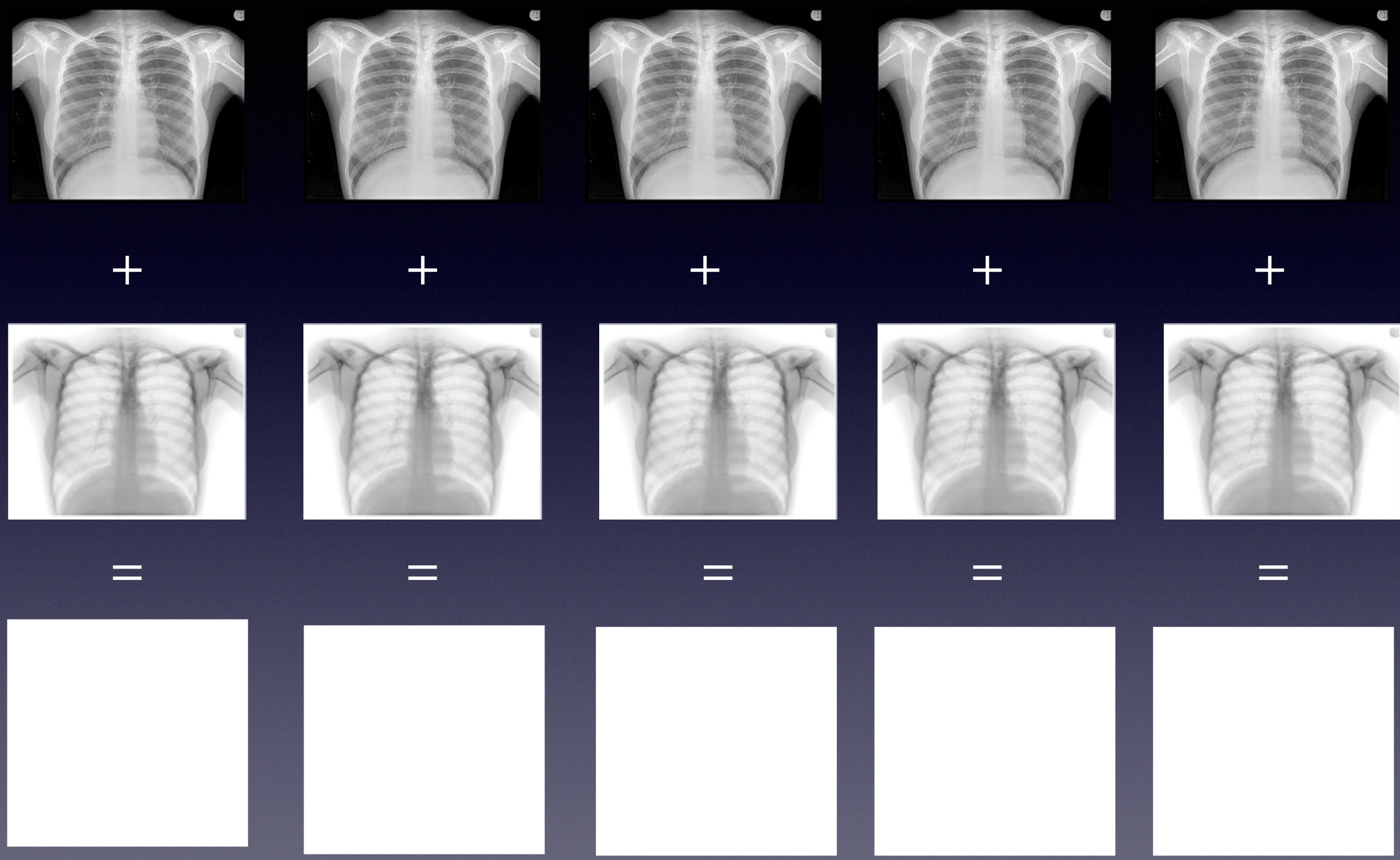
75% confidence after 2nd game

95% confidence after 5th game

X- Rays are a Great Way to Learn What's Inside People

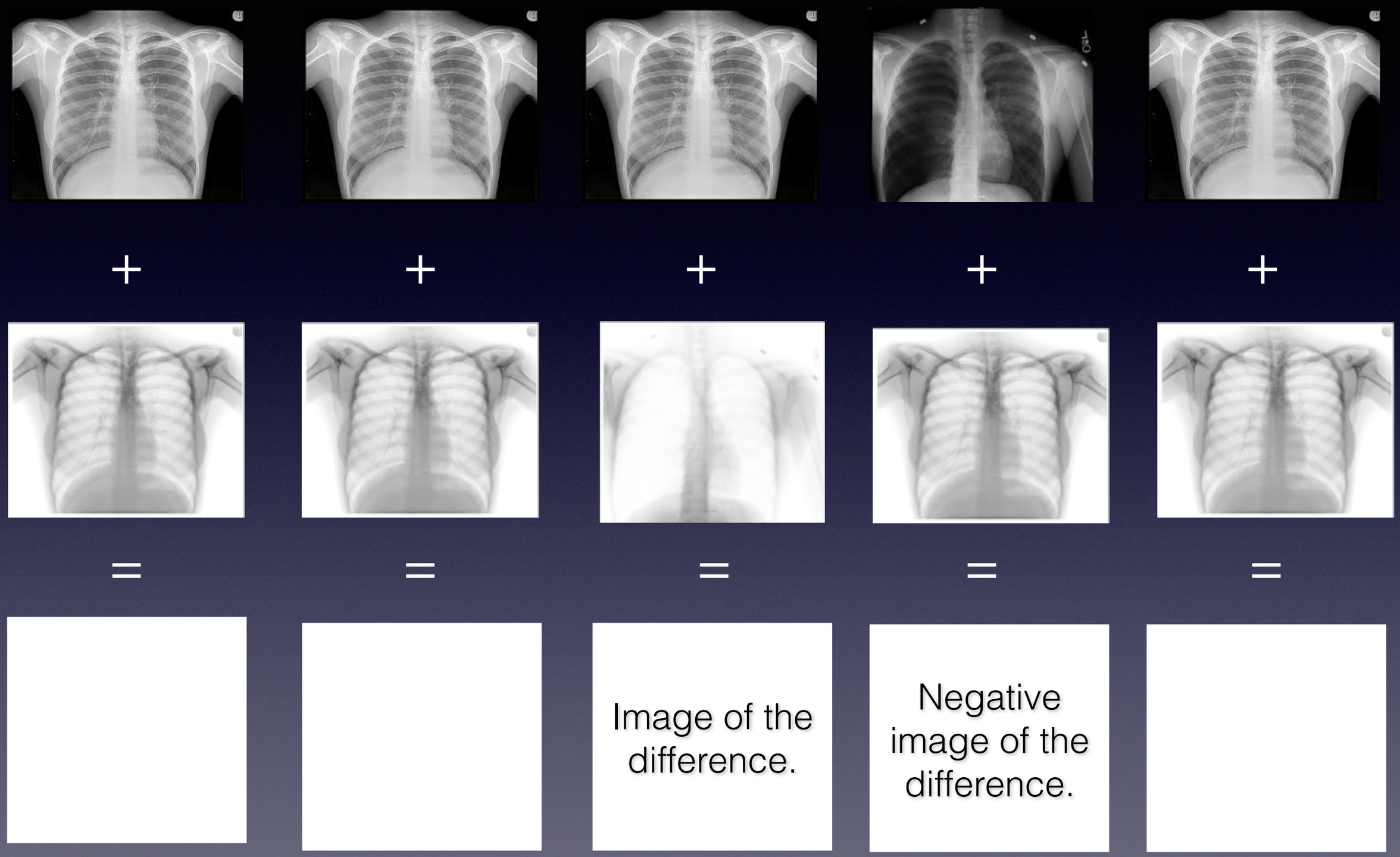
How can I use X-rays to prove that
these are 5 identical twins –
but not learn how many ribs they have?

Use Alice & Bob's Approach



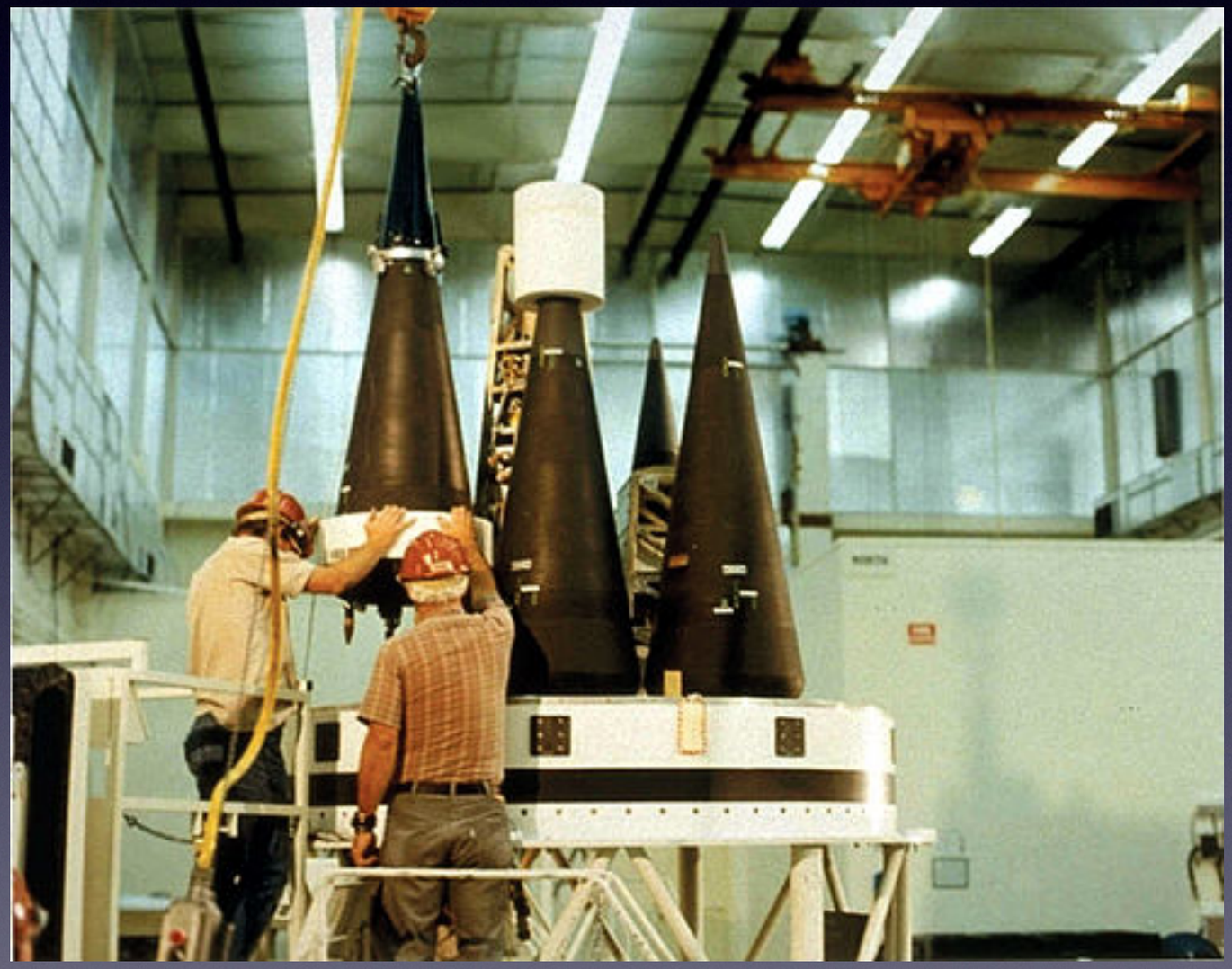
It doesn't matter how Bob pairs the images.
Bob sees all white & Alice gives away no information.

Suppose Alice Tries to Cheat



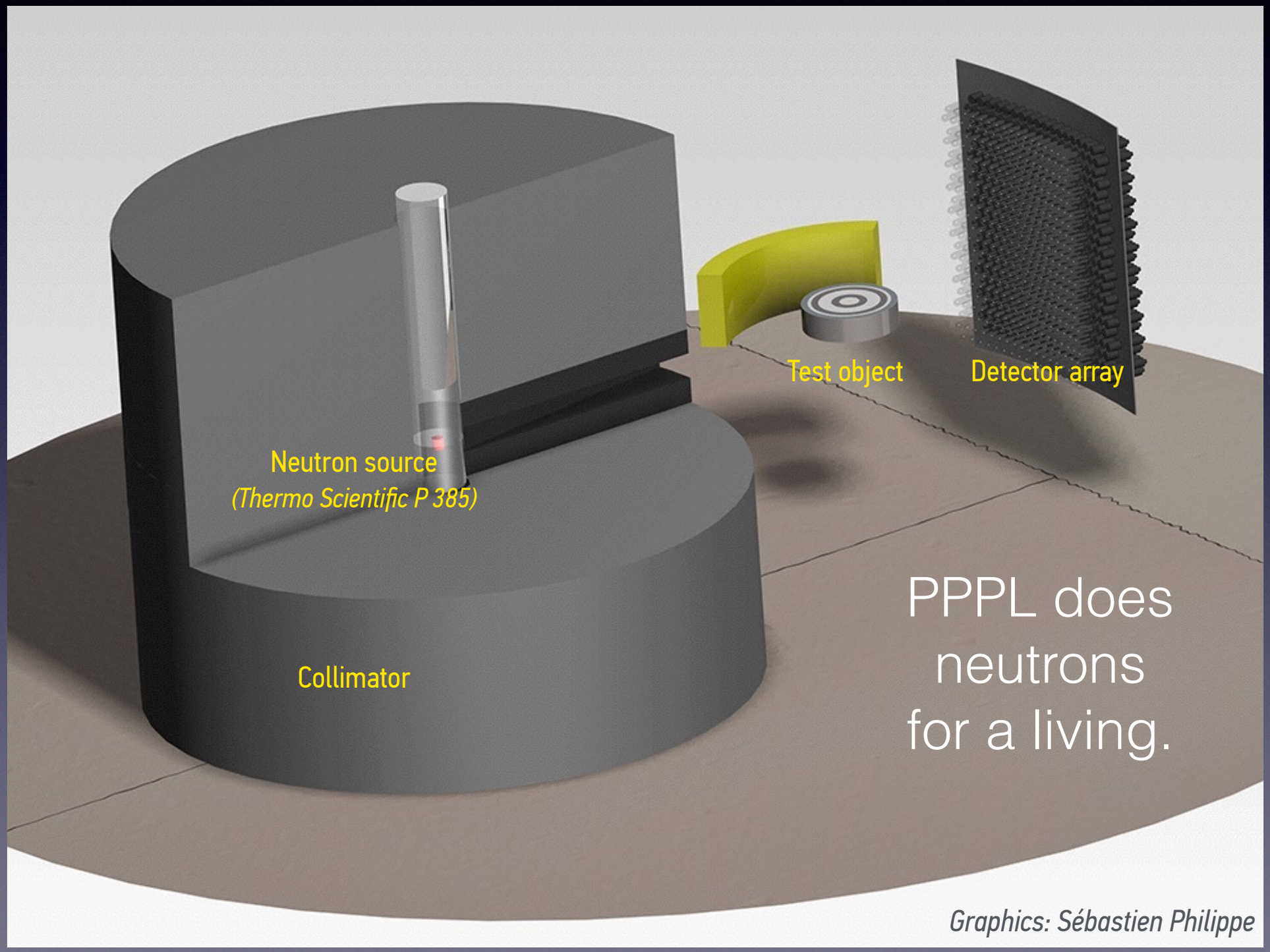
Alice is likely to get caught if she cheats.
And she risks giving away the number of ribs!

For Arms Control we would Test Weapons from Storage against Deployed Weapons



Inspector selects warheads randomly from active delivery systems.

Neutron Radiography is Better for Weapons than X-Rays



We need Pre-loadable Non-Electronic Neutron Detectors

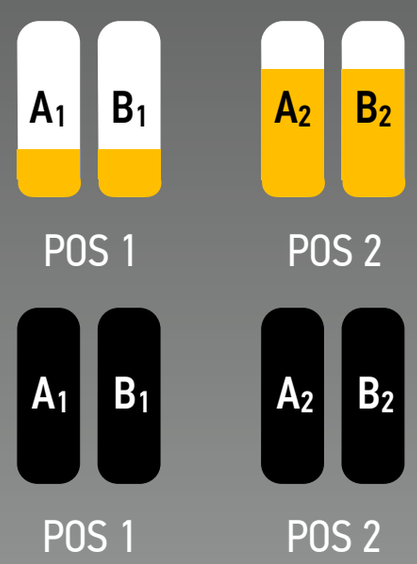
Why preloadable? Why non-electronic?

"Bubble Detectors"
from Yale University
fill the bill.

Zero Knowledge Protocol for Warhead Verification

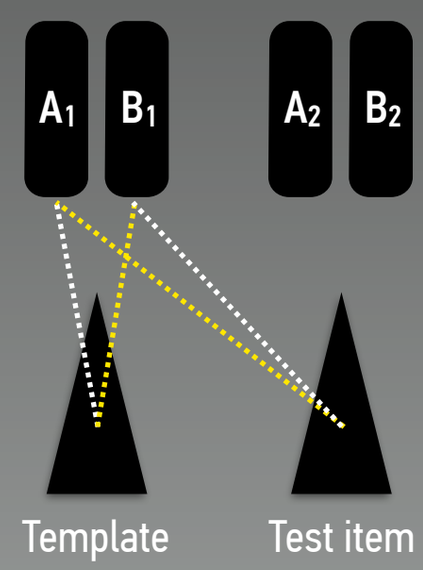
1

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



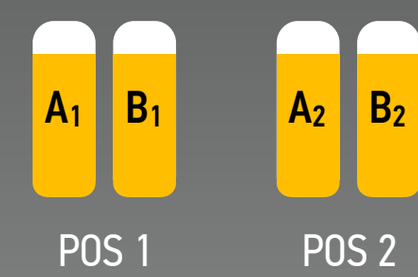
2

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



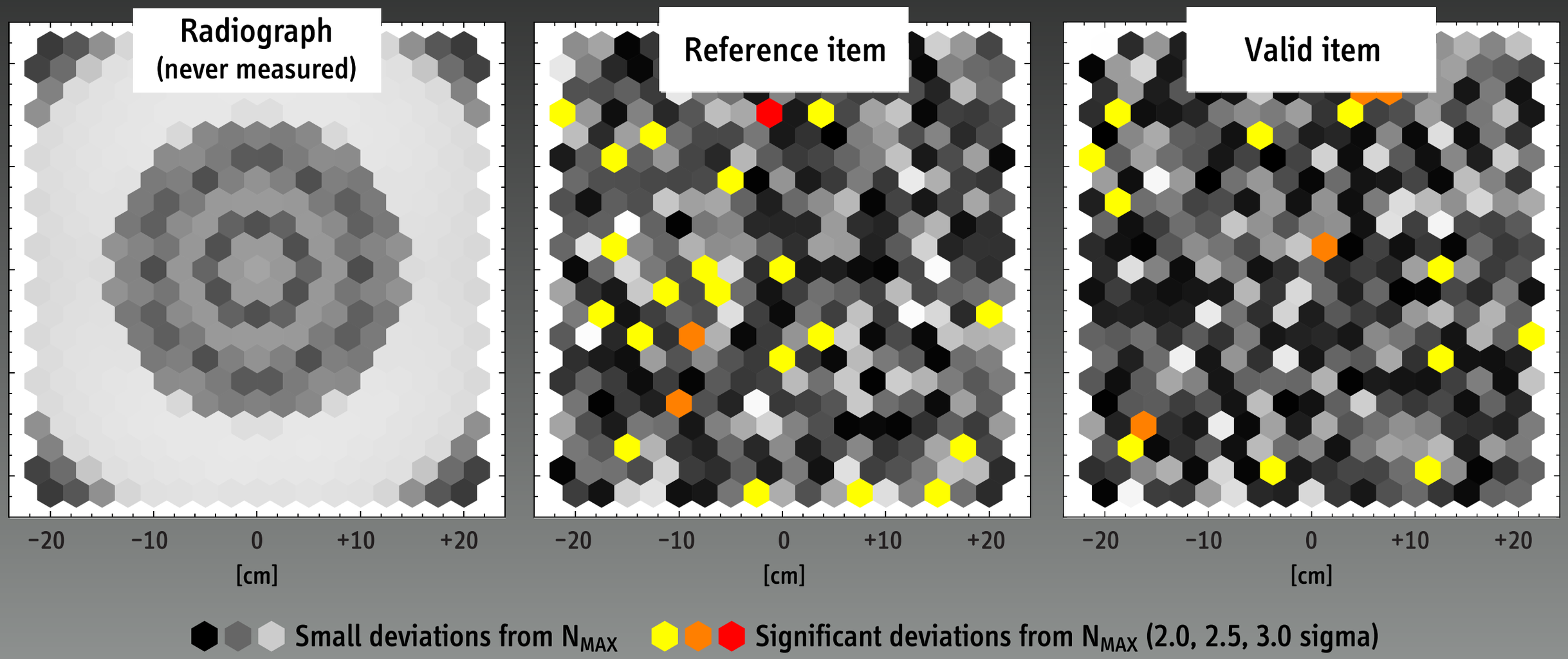
50% confidence after 1st round

...

95% confidence after 5th round

ZERO-KNOWLEDGE VERIFICATION

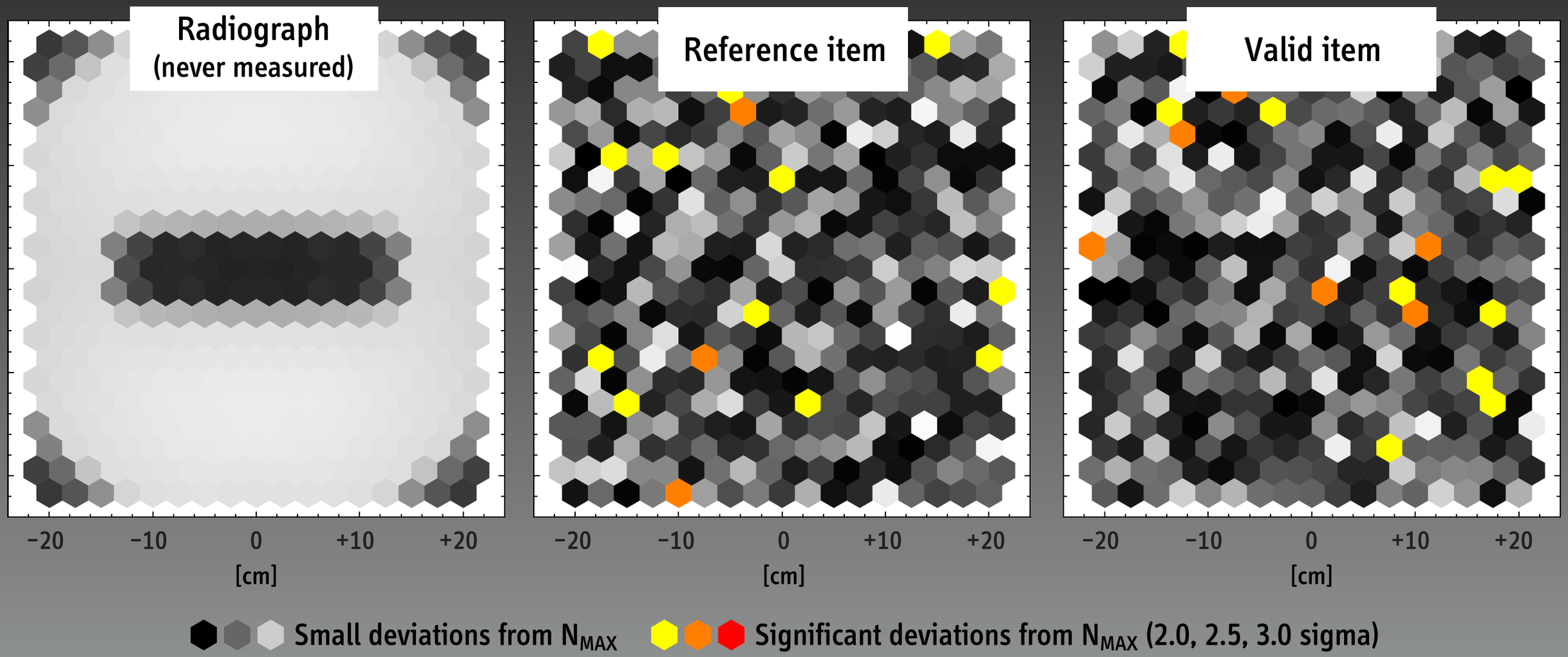
AUTHENTICATING WARHEADS WITHOUT MEASURING CLASSIFIED INFORMATION



Even the noise carries no information!

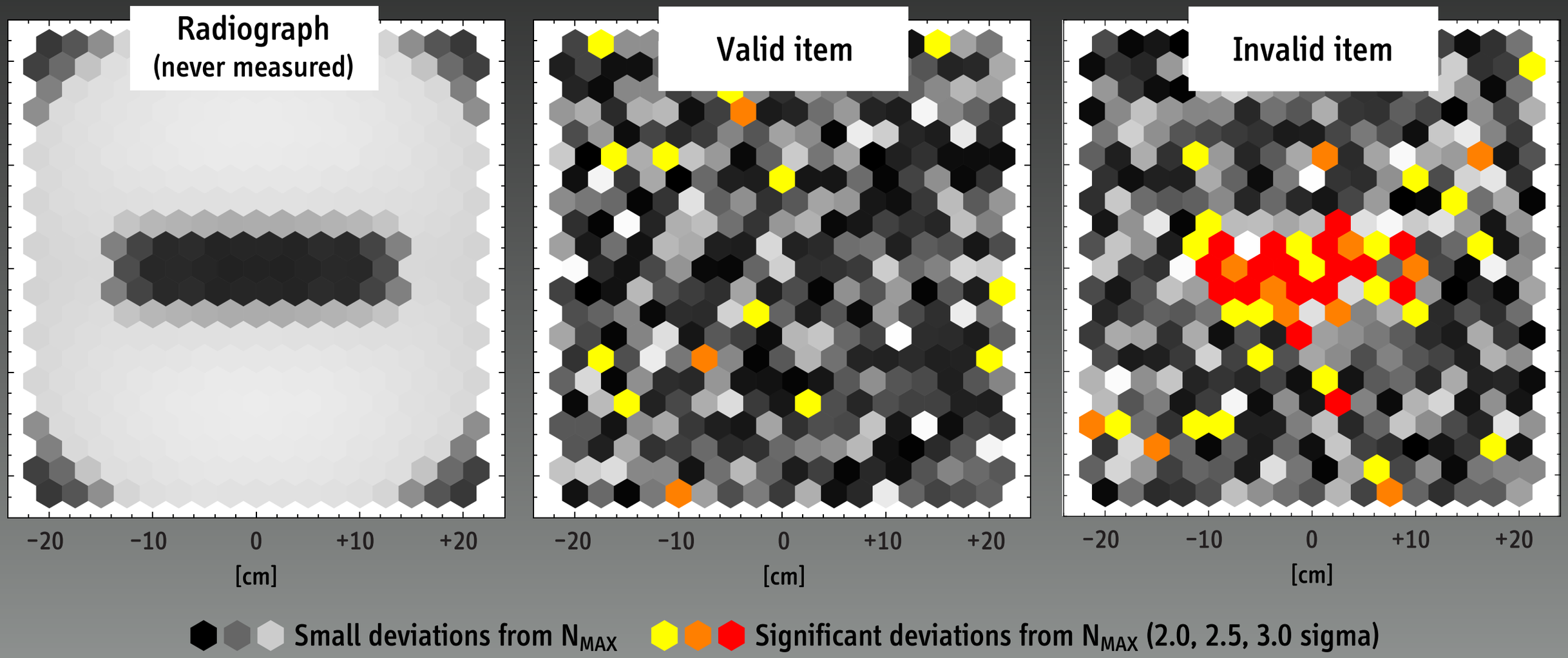
ZERO-KNOWLEDGE VERIFICATION

AUTHENTICATING WARHEADS WITHOUT MEASURING CLASSIFIED INFORMATION



ZERO-KNOWLEDGE VERIFICATION

AUTHENTICATING WARHEADS WITHOUT MEASURING CLASSIFIED INFORMATION

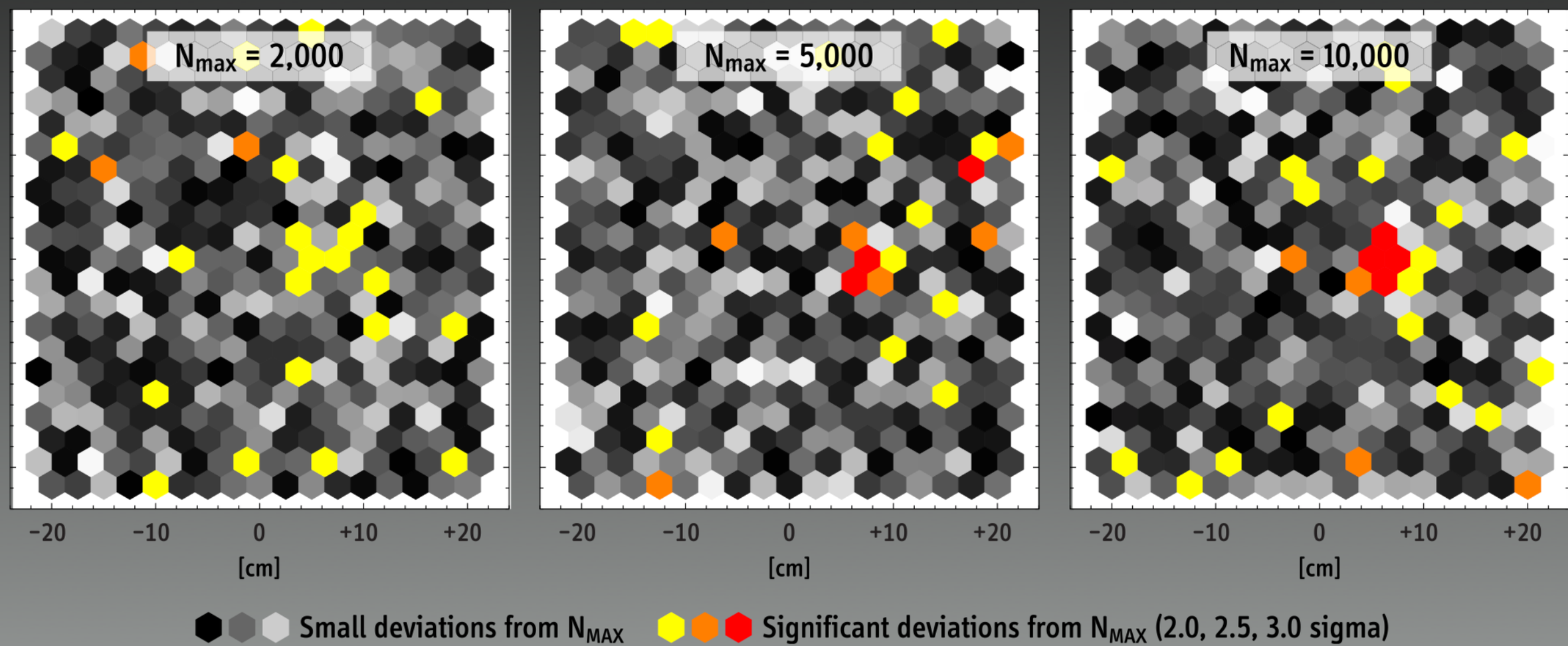


Simulated data from MCNP5 calculations, neutron energies > 10 MeV, N(max) = 5,000; invalid item: lead for tungsten

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

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

Path Forward

Demonstrate first ZKP differential radiographic measurement.

Confirm that bubbles don't "age". (Why?)
(Or select other non-electronic detectors)

Demonstrate highly reproducible irradiations. (Why?)

Demonstrate high sensitivity to small differences.

Test how much information can leak due to real-world effects, e.g., misalignments. (Other issues?)

Try it out on real U.S. warheads!

Convince the Russians, French, British and Chinese that this was their idea – by encouraging them to improve it.