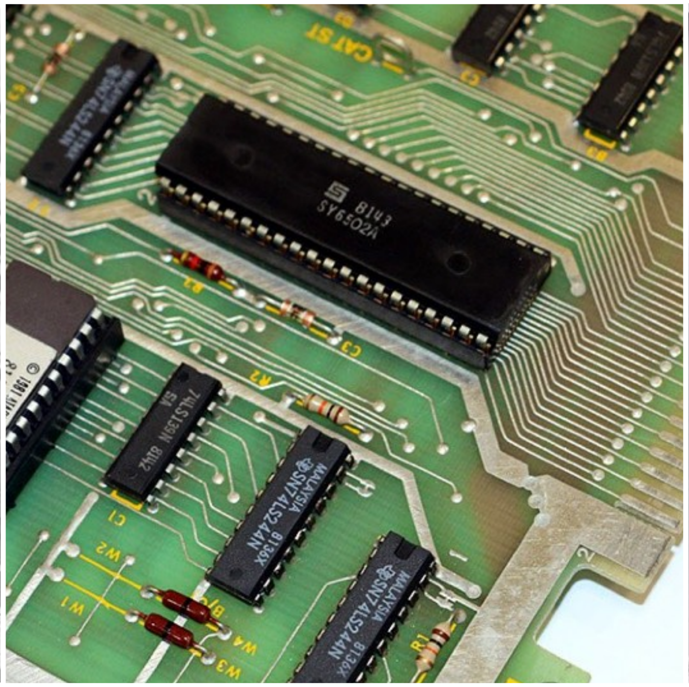


KEEPING SECRETS AT A DISTANCE

NEW APPROACHES TO NUCLEAR MONITORING & VERIFICATION

Alex Glaser

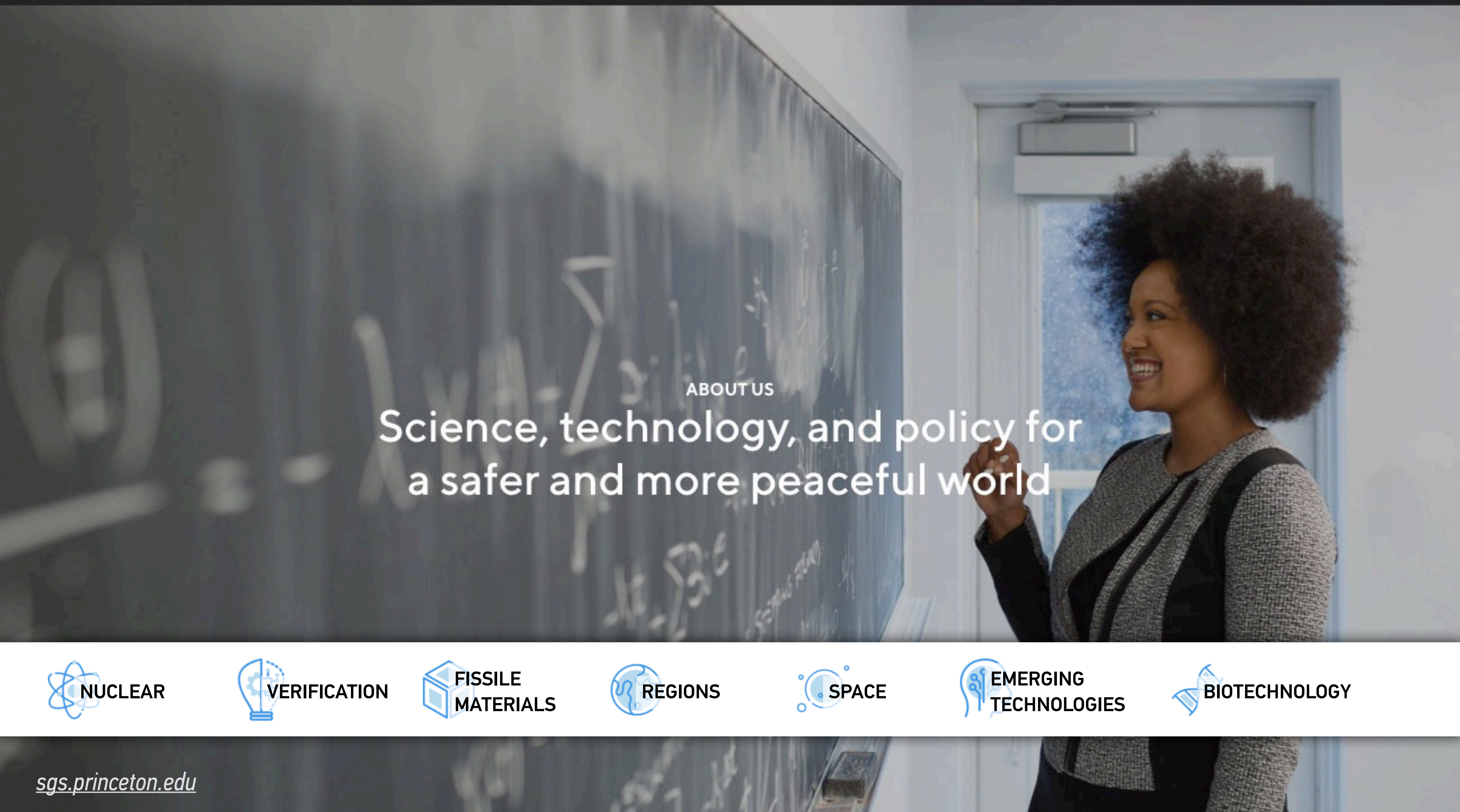
Program on Science and Global Security
Princeton University

Exzellenzcluster Cyber Security in the Age of Large-Scale Adversaries (CASA), Ruhr-Universität Bochum
Bochum, June 24, 2022

Revision 3b


Sara Al-Sayed
Robert Goldston
Sharon Weiner
Ernesto Mané
Laura Kahn
Frank von Hippel
Zia Mian
Ray Acheson
Igor Moric
Tamara Patton
Christopher Chyba
Geralyn McDermott
Jihye Jeon
Alex Glaser
Eric Lepowsky
Sébastien Philippe
Harold Feiveson
Hossein Mousavian
Ryo Morimoto
Anne Stickells
A. H. Nayyar
Stewart Prager
Nancy Burnett
Pavel Podvig
SCIENCE &
GLOBAL SECURITY
PRINCETON UNIVERSITY

SCIENCE &
GLOBAL SECURITY
PRINCETON UNIVERSITY

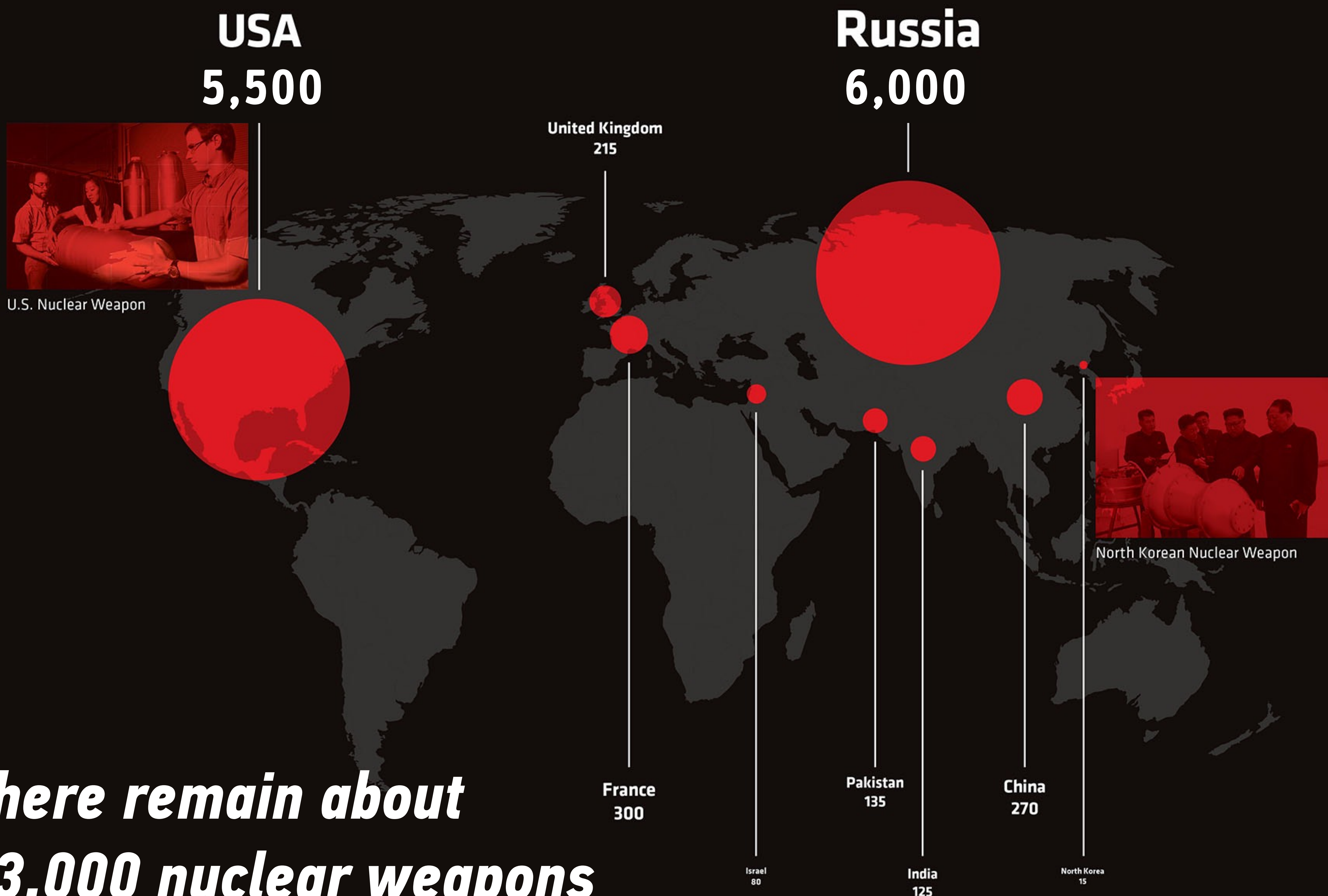


NUCLEAR | VERIFICATION | FISSILE MATERIALS | REGIONS | SPACE | EMERGING TECHNOLOGIES | BIOTECHNOLOGY

sgs.princeton.edu

BACKGROUND

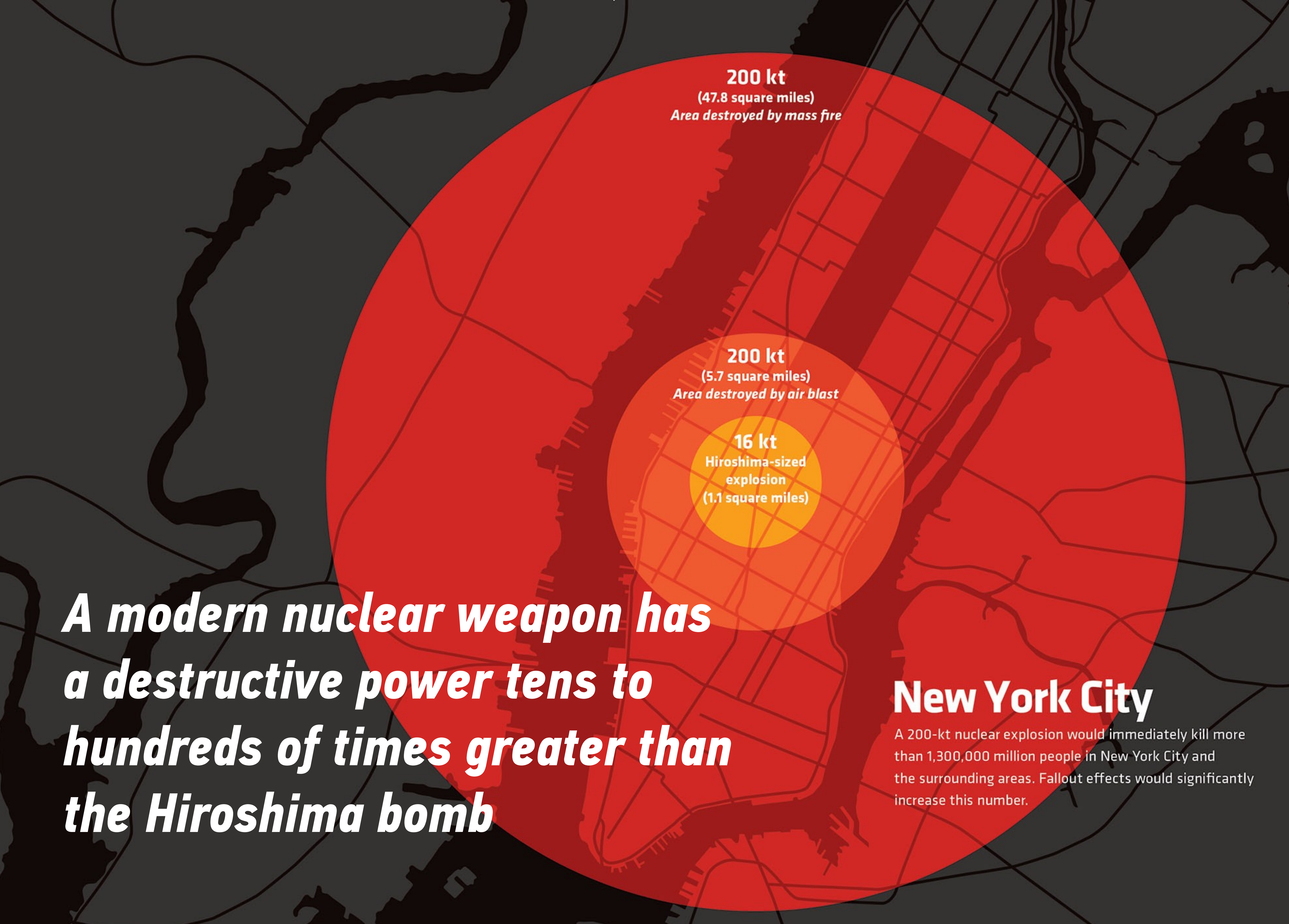
Nuclear weapons in 2022



There remain about 13,000 nuclear weapons in the world today

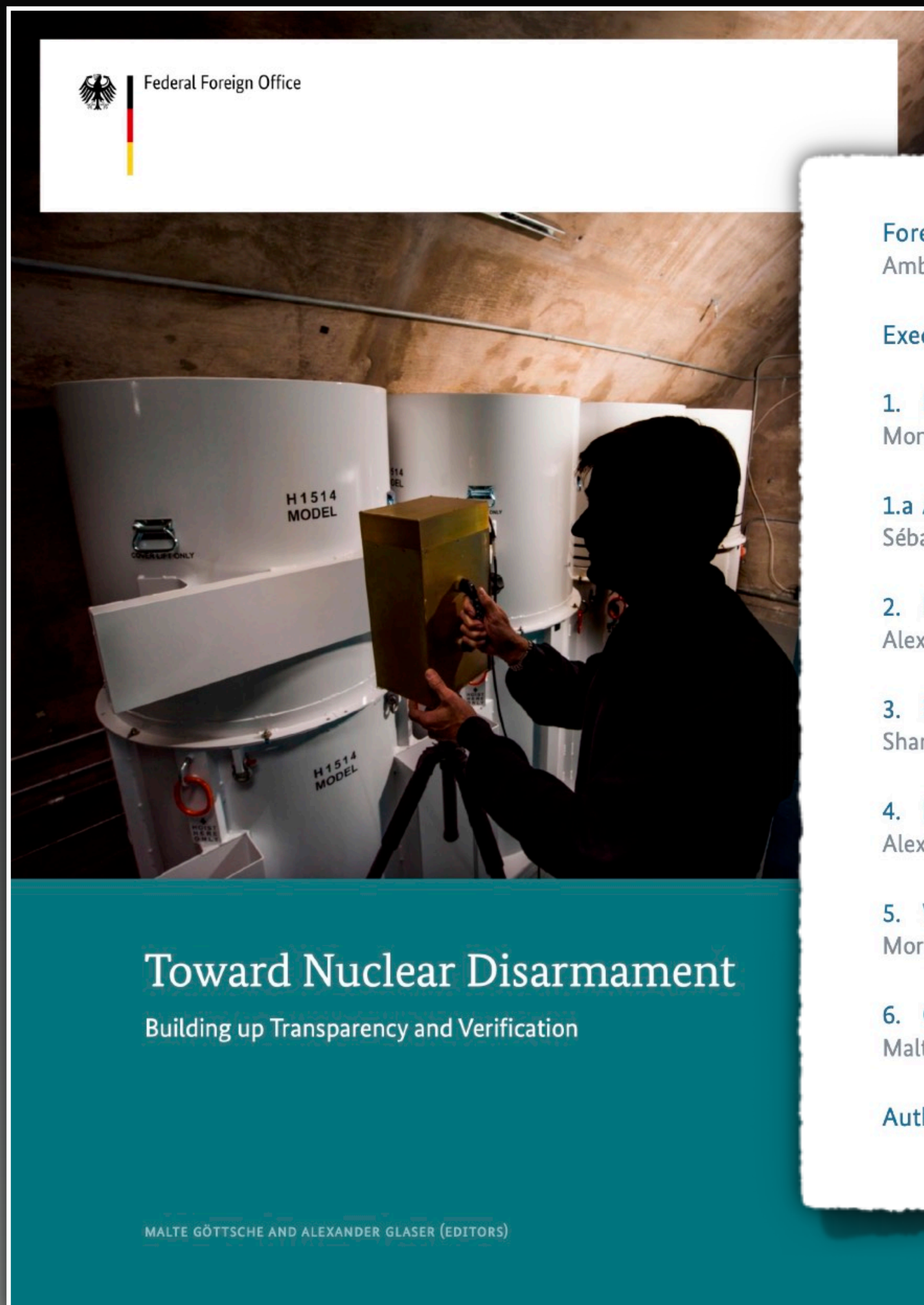
Based on Hans Kristensen and Robert Norris, Nuclear Notebook, Federation of American Scientists and thebulletin.org/nuclear-notebook/

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


PLAN A
www.youtube.com/watch?v=2jy3JU-ORpo
There never has been a moment's justification for having the capability to destroy humanity.
Daniel Ellsberg



Foreword — 4
Ambassador Rüdiger Bohn

Executive Summary — 8

1. Baseline Declarations — 14
Mona Dreicer

1.a Appendix: Secure Declarations — 26
Sébastien Philippe

2. Monitoring Regimes for All-Warhead Agreements — 34
Alexander Glaser

3. Fissile Material Stocks and Production — 54
Sharon Squassoni and Malte Göttsche

4. Nuclear Monitoring and Verification Without Onsite Access — 86
Alexander Glaser and Irmgard Niemeyer

5. Weapons Production and Research — 116
Moritz Kütt

6. Conclusion: Building up Transparency and Verification — 140
Malte Göttsche and Alexander Glaser

Authors — 150

M. Göttsche and A. Glaser (eds.), *Toward Nuclear Disarmament: Building Up Transparency and Verification*
German Federal Foreign Office, Berlin, May 2021, www.auswaertiges-amt.de/en/about-us/foreignservice/brochures

Germany is currently planning to acquire 35 F-35A; these aircraft are certified to carry and deliver U.S. B61 nuclear bombs

The upgraded B61 bomb (Mark 12) will replace all currently in Europe deployed U.S. nuclear weapons in 2022–2024

www.bmvg.de/de/tornado-nachfolger-beschaffung-neue-kampfflugzeuge-fuer-truppe
nsarchive.gwu.edu/briefing-book/nuclear-vault/2022-03-28/natos-european-nuclear-deterrent-b61-bomb

WHAT ARE THE technical CHALLENGES?

(How to enable reductions in the nuclear arsenals)

THERMONUCLEAR WARHEAD

ON AVERAGE, A MODERN NUCLEAR WARHEAD MAY CONTAIN 3–4 KG OF PLUTONIUM AND UP TO 25 KG OF HIGHLY ENRICHED URANIUM

Primary
Typically contains plutonium
(and/or highly enriched uranium)

Secondary
Typically contains highly enriched uranium
(and lithium-deuteride as fusion fuel)

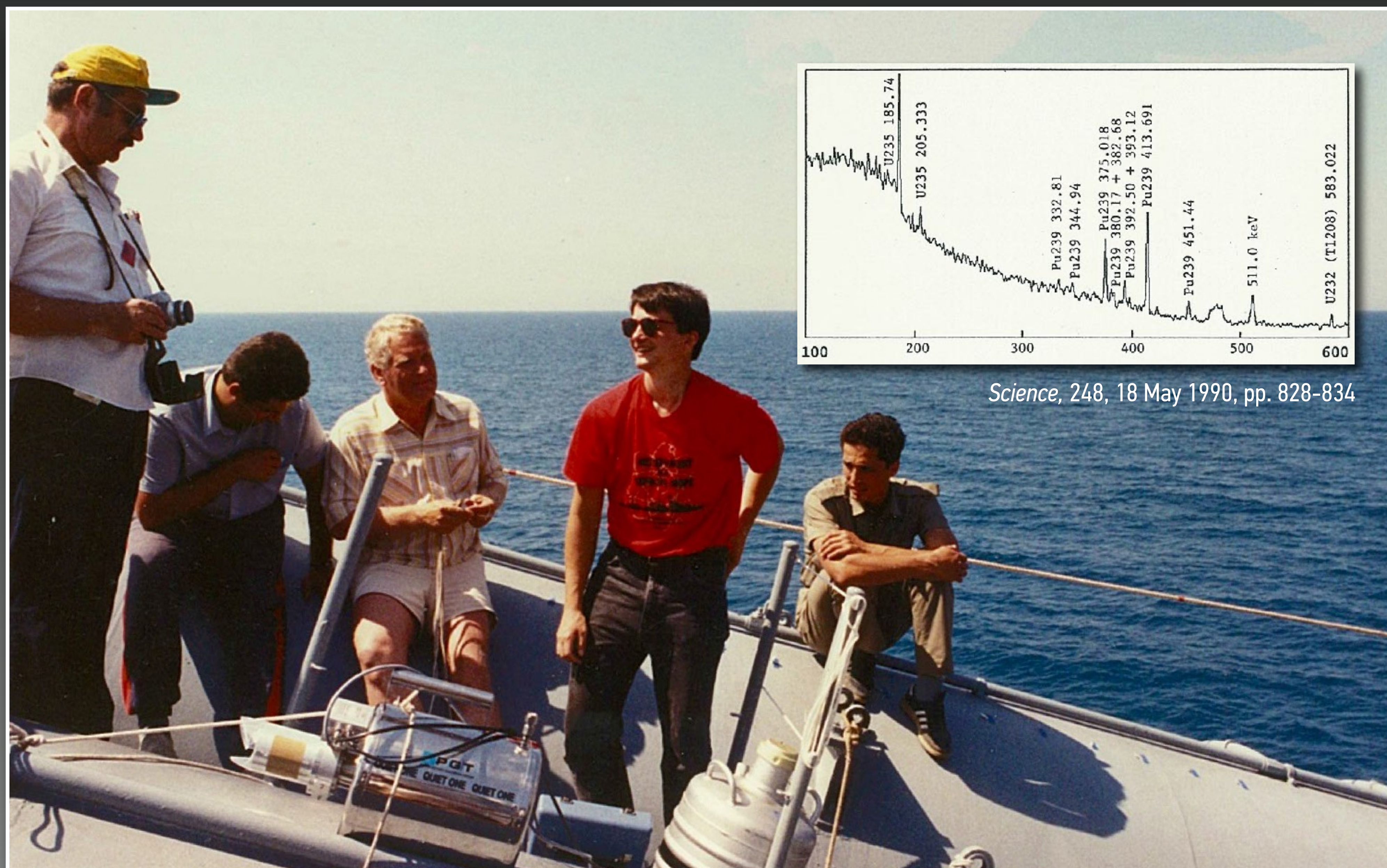
Source: fas.org; U.S. Department of Defense

“THE PEANUT”

September 2, 2017, Source: KCNA/EPA
North Korea tested a nuclear weapon with an estimated yield of 250 kt(TNT) on September 3, 2017

NUCLEAR WEAPONS HAVE UNIQUE RADIATION SIGNATURES

BUT THEY ARE SENSITIVE AND CANNOT BE REVEALED TO INSPECTORS



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

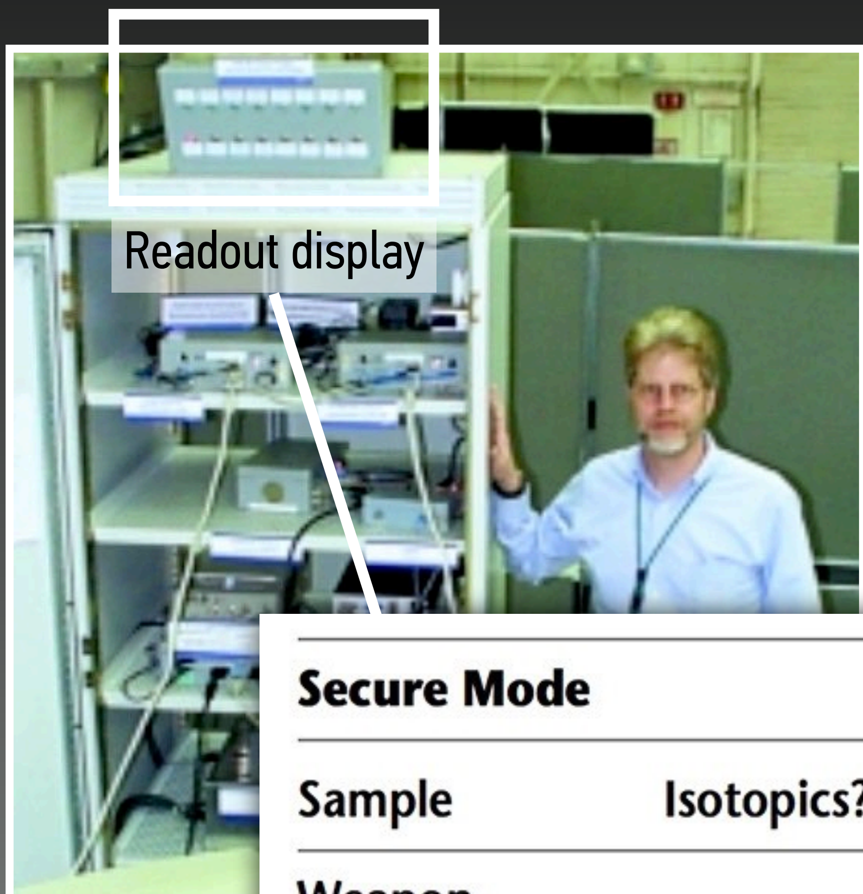
U.S. Scientists on the Soviet Cruiser "Slava" (later renamed "Moskva") in the Black Sea, 1989

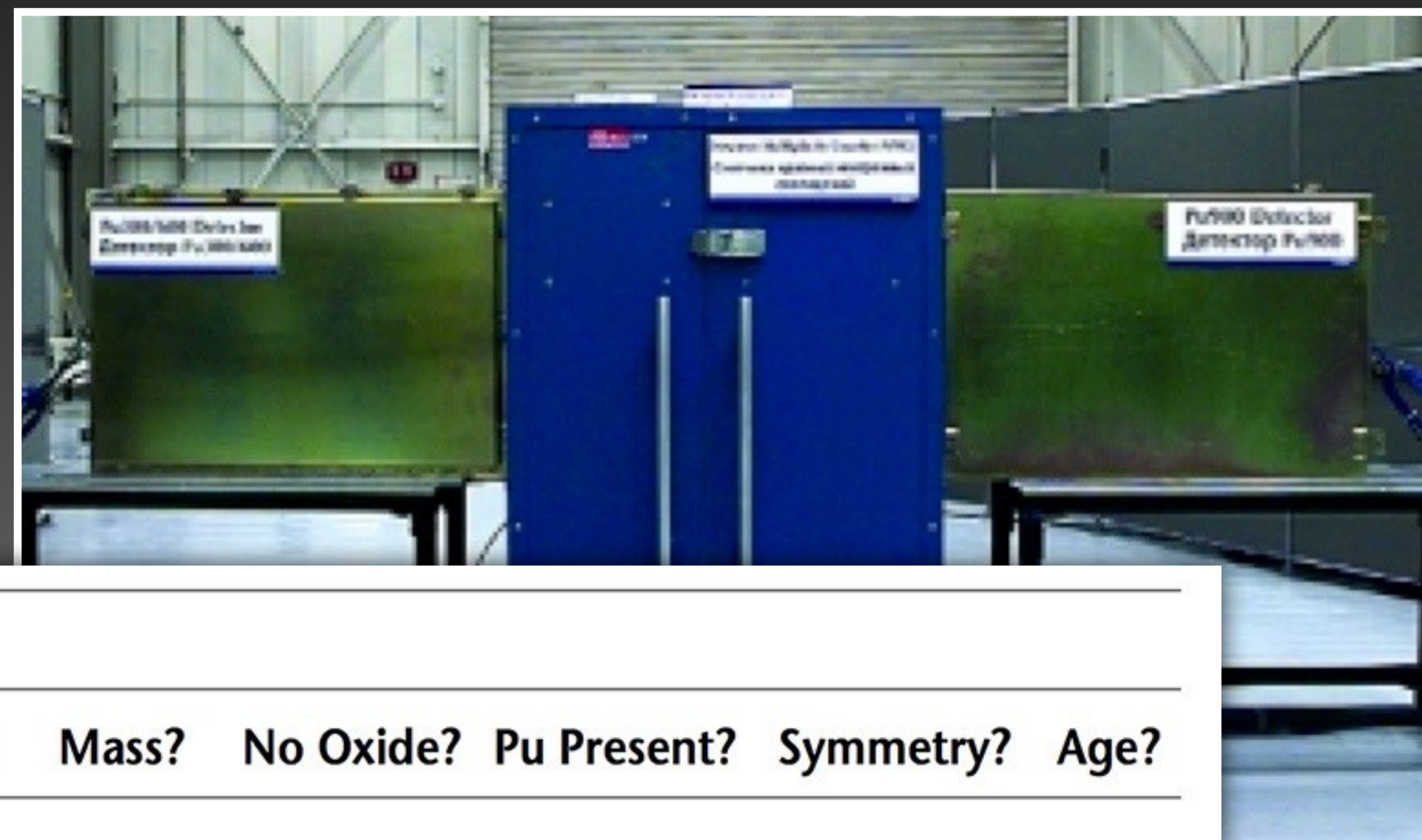
DEALING WITH SECRETS

(in nuclear arms control and disarmament)

EARLY INFORMATION BARRIERS

(RESEMBLED RUBE-GOLDBERG MACHINES)





Secure Mode

Sample	Isotopics?	Mass?	No Oxide?	Pu Present?	Symmetry?	Age?
Weapon component	● (green)	● (green)	● (green)	● (green)	● (green)	● (green)
Large oxide sample on its side	● (green)	● (green)	● (red)	● (green)	● (red)	● (green)

David Spears (ed.), *Technology R&D for Arms Control,* U.S. Department of Energy, Washington, DC, 2001
Fissile Material Transparency Technology Demonstration (FMTTD), Los Alamos, August 2000

"All I see is a green LED with a battery connected to it."

Russian nuclear weapons expert during technology demonstration at a U.S. national laboratory in the early 2000s

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)

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 radically different verification technologies and approaches; for example, avoid need for trusted hardware or seek 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) and Johannes Tobisch (middle)

"SOMETHING OLD"

Example 1: Zero-knowledge Verification

SUPERHEATED DROPLET DETECTORS MAY OFFER A WAY TO IMPLEMENT SECURE INSPECTIONS

BY AVOIDING DETECTOR-SIDE ELECTRONICS

Superheated C-318 fluorocarbon (C_4F_8) droplets suspended in aqueous gel

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

Sensitive to neutrons with $E_n > E_{min}$

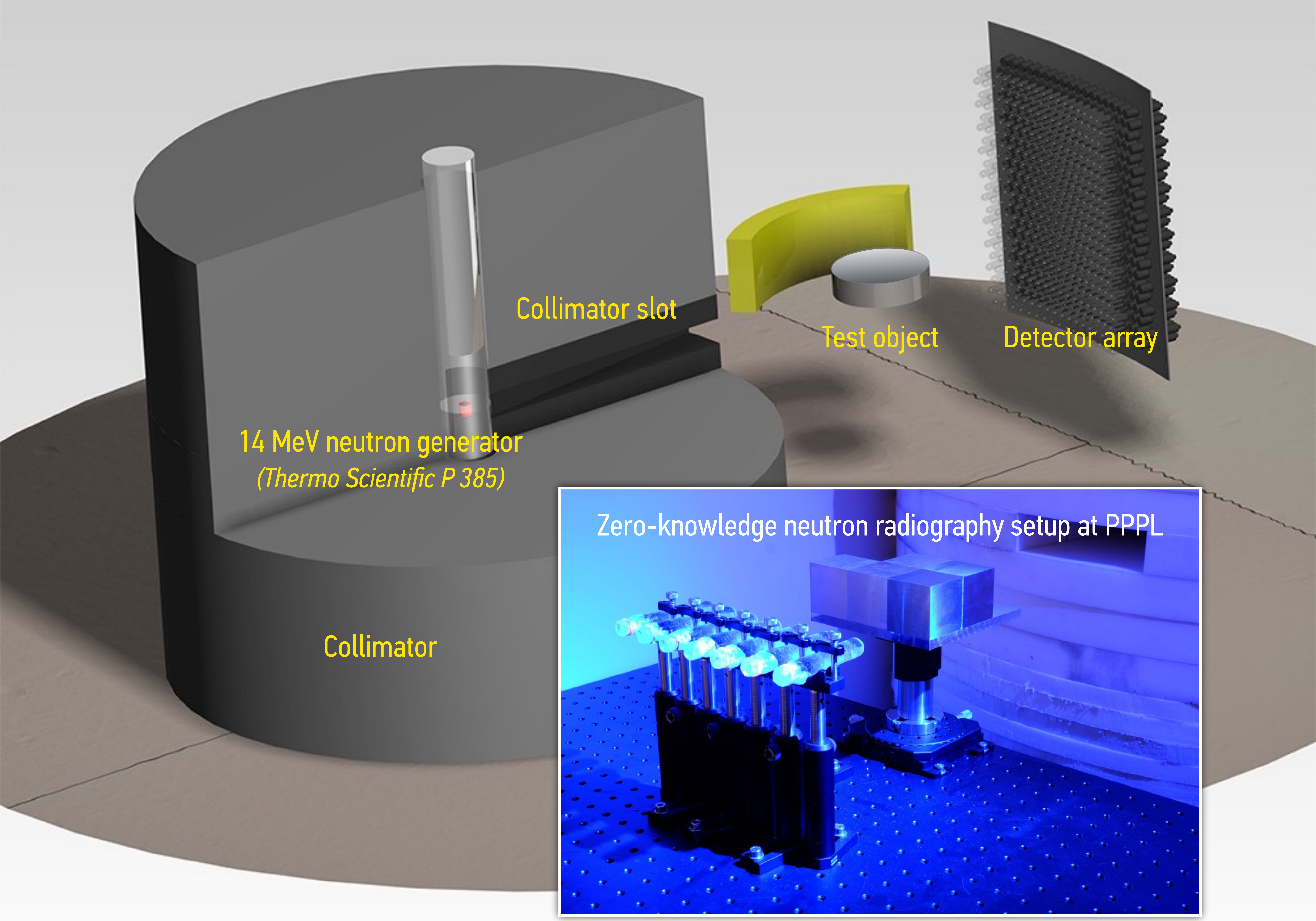
Designed to be insensitive to γ-radiation

Active volume .... : 6.0 cm^3

Droplet density .... : 3500 cm^{-3}

Droplet diameter ...... : ~100 μm

Absolute Efficiency ... : 4×10^{-4}

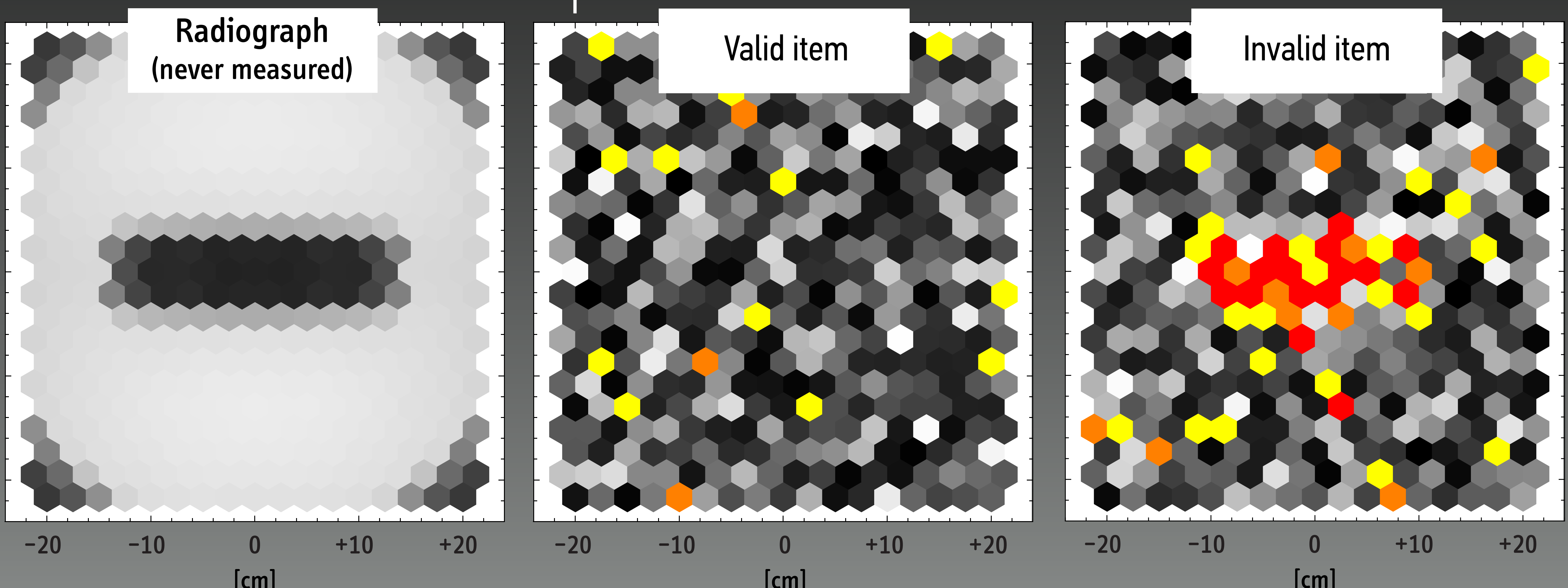


S. Philippe, R. J. Goldston, A. Glaser, F. d'Errico, *Nature Communications,* 7, September 2016, www.nature.com/articles/ncomms12890

ZERO-KNOWLEDGE NEUTRON RADIOGRAPHY

WITH PRELOADED, NON-ELECTRONIC (BUBBLE) DETECTORS

Detector array (each pixel corresponds to one bubble detector)



Small deviations from N_{MAX} Significant deviations from N_{MAX} (2.0, 2.5, 3.0 sigma)

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

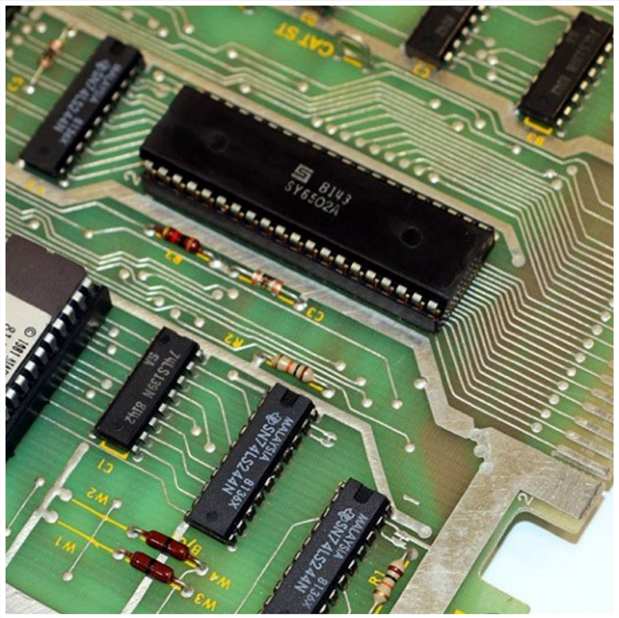
"SOMETHING really OLD"

Example 2: Vintage Verification

(skip)

VINTAGE VERIFICATION

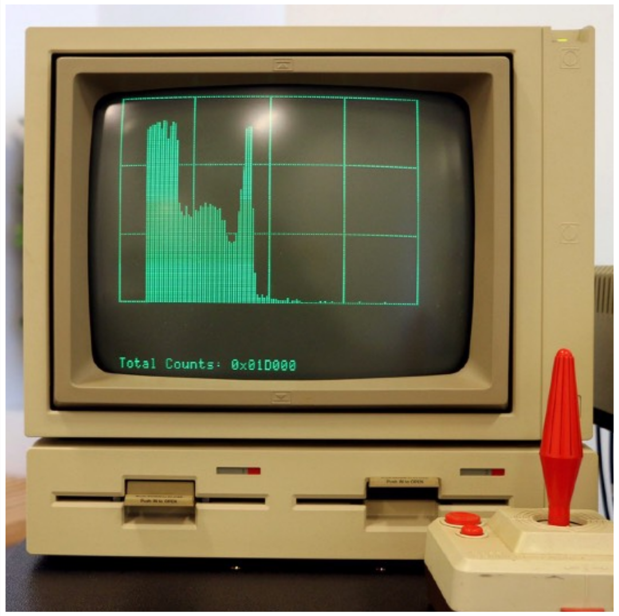
"TRUST THROUGH SIMPLICITY AND OBSOLESCENCE?"



IDEA

Use simple, quasi open-source hardware from 1970s

Hardware designed in the distant past may drastically reduce concerns about the existence of backdoors or hidden switches



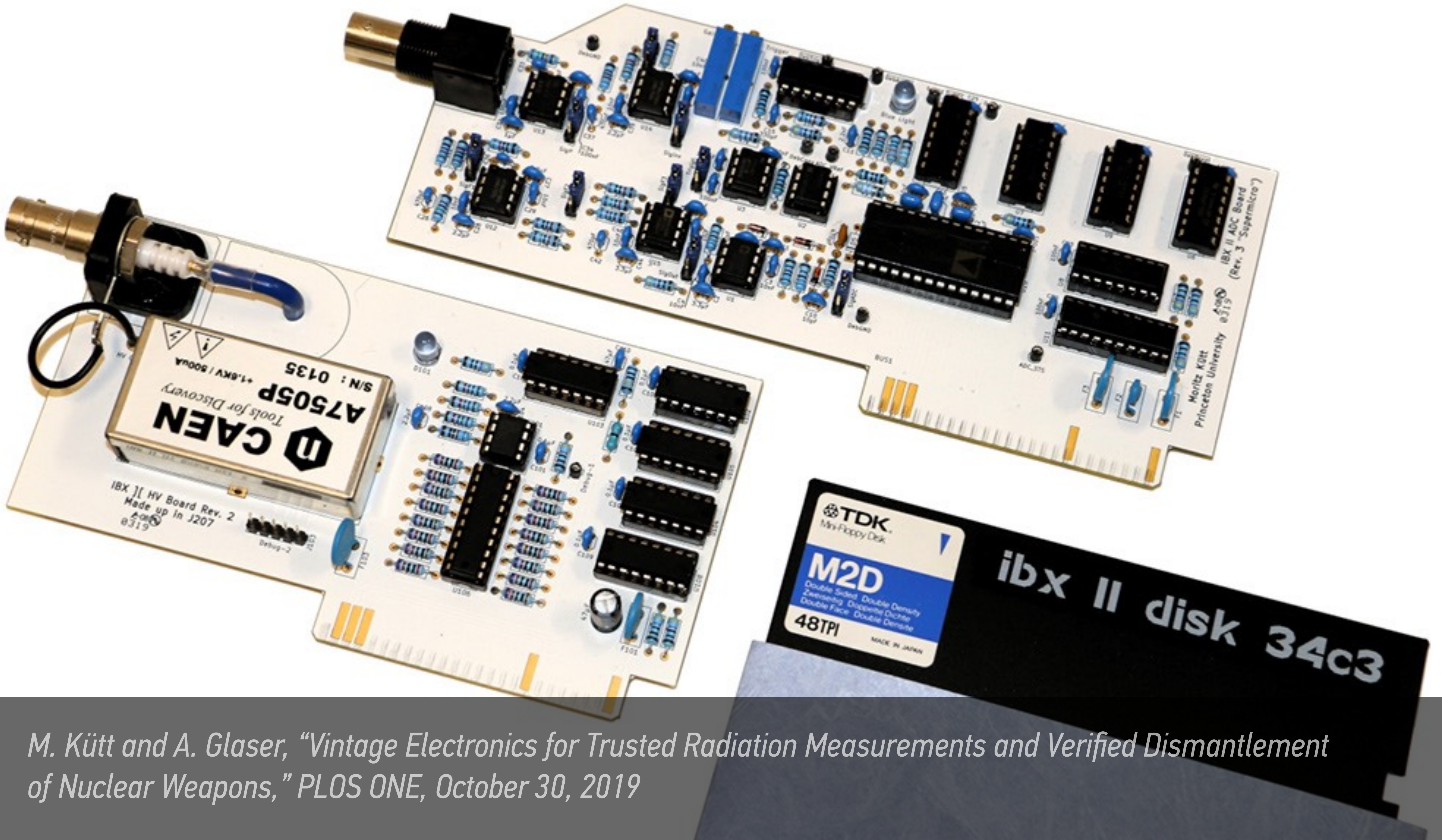
CHOOSING THE HARDWARE & ALGORITHM

MOS 6502 (8 µm technology, 3,500 transistors, 1 MHz) and an Apple IIe, combined with a low-resolution sodium-iodide detector

Template-matching approach using standard chi-squared test

Source: Author

“EXTENSION CARDS” FOR THE APPLE II



M. Kütt and A. Glaser, “Vintage Electronics for Trusted Radiation Measurements and Verified Dismantlement of Nuclear Weapons,” PLOS ONE, October 30, 2019


34th Chaos Communication Congress
December 27–30, 2017, Leipzig, Germany

SOMETHING NEW

Toward Secure Virtual Inspections

FROM ONSITE TO REMOTE INSPECTIONS

PROS & CONS OF ONSITE INSPECTIONS

Onsite inspections remain the "gold standard" for IAEA safeguards and nuclear arms-control verification

Inspections tend to be costly and are often considered intrusive, especially in the arms-control context

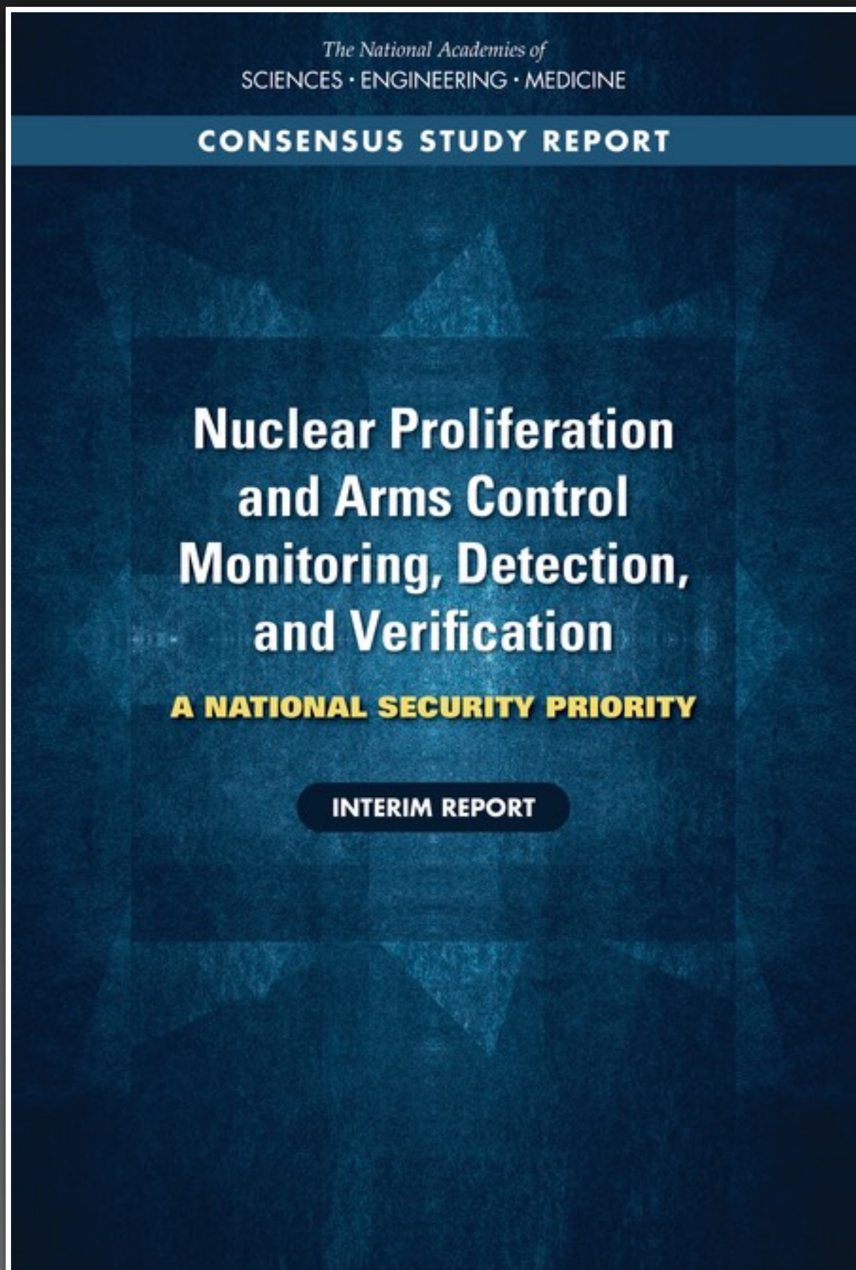
CAN WE (PHYSICALLY) "SEPARATE" HOST & INSPECTOR ?

Many concerns could be addressed and resolved if inspectors were not "physically" present onsite

The host performs the prescribed activities onsite, while the inspector follows, influences, or directs the activities remotely

Source: ukni.info (top) and microsoft.com (bottom)

FINDINGS FROM A 2021 NATIONAL ACADEMIES STUDY



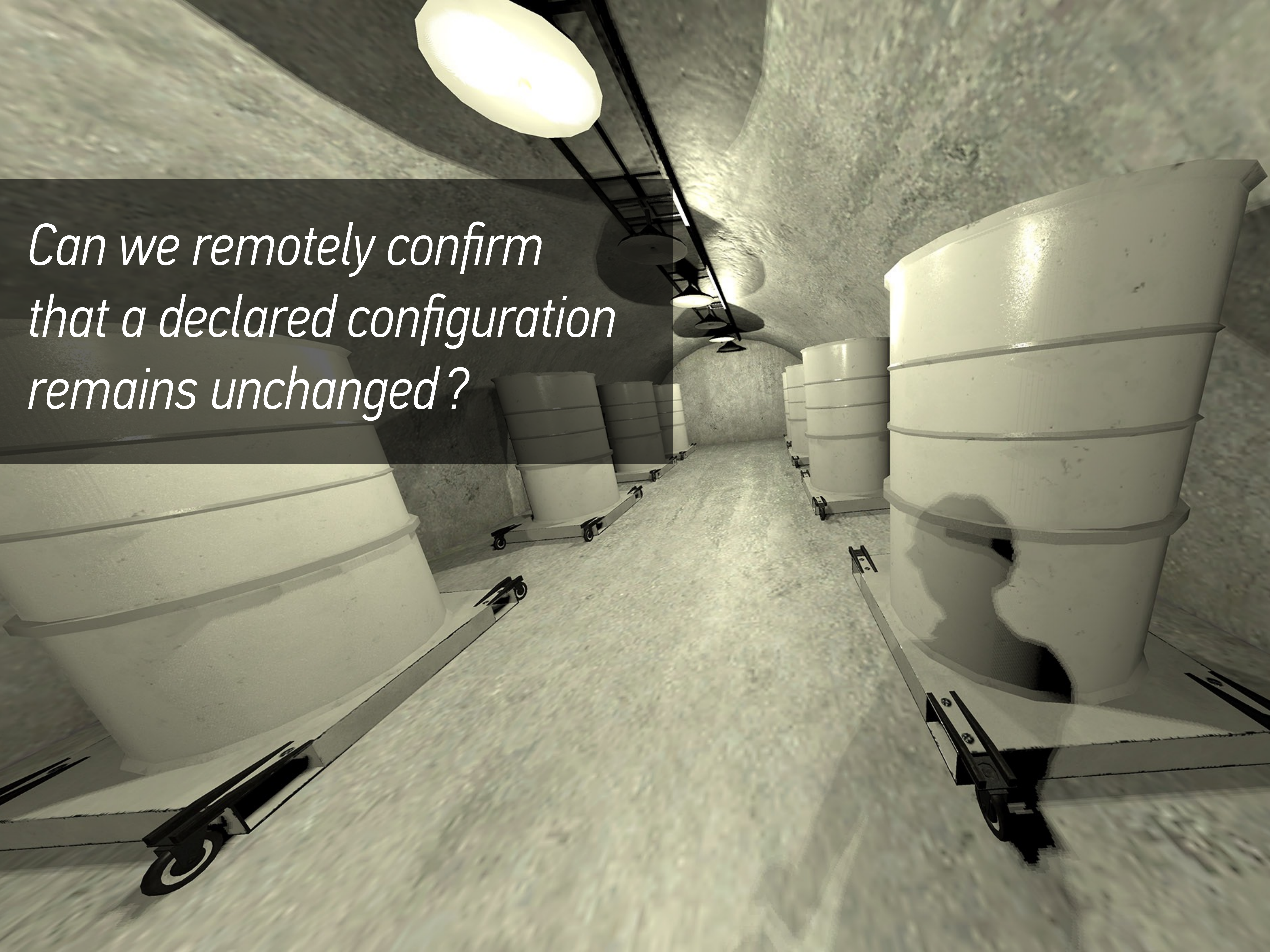
3.4 MDV FOR ARMS CONTROL

3.4.1 Capability Needs

…

Treaties that include weapons in storage or weapons designed for shorter-range delivery systems are anticipated to require new MDV techniques. As a minimum, ***such treaties would likely require access to storage areas either directly or remotely,*** *and confirmation of warhead count (either a baseline confirmation or through routine/challenge inspections).*

Jill Hruby, Corey Hinderstein, et al., Committee on the Review of Capabilities for Detection, Verification, and Monitoring of Nuclear Weapons and Fissile Material, National Academy of Sciences, Washington, DC, 2021, doi.org/10.17226/26088


Can we remotely confirm
that a declared configuration
remains unchanged?

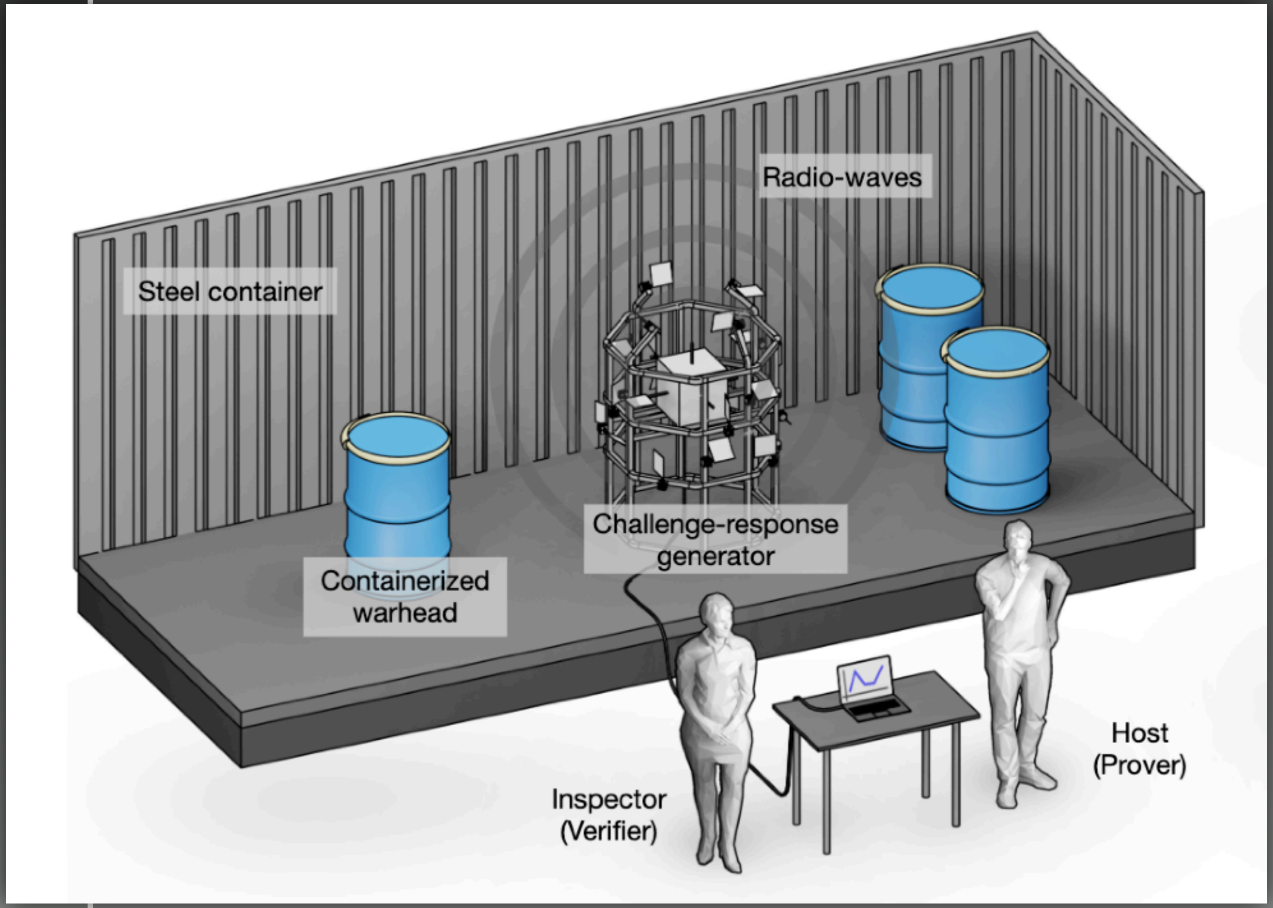
Art storage
Source: montel.com

Gold storage
Source: Federal Reserve Bank of New York

Experimental setup, Max Planck Institute for Security and Privacy (MPI-SP), Bochum, Germany
Source: Johannes Tobisch

SECURE VIRTUAL INSPECTIONS

WITHOUT TRUSTED HARDWARE



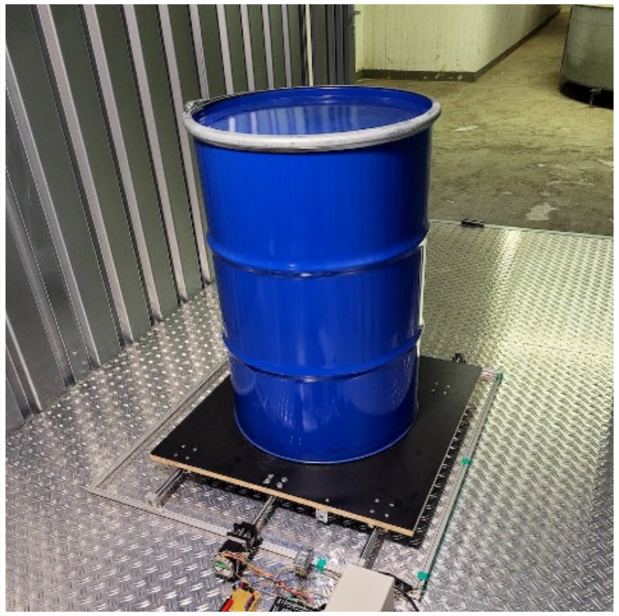
SETUP & INSPECTION PROTOCOL

- Room contains a "challenge-response generator" that emits and receives radio-wave signals
- Complex multi-path propagation provides a unique and reproducible fingerprint of the configuration
- During a setup phase, the inspector creates a private "dictionary" of challenge-response pairs
- From then on, the inspector queries the room remotely; correct answers can only be provided if the configuration remains unchanged

J. Tobisch, S. Philippe, B. Barak, G. Kaplun, C. Zenger, A. Glaser, C. Paar, and U. Rührmair, manuscript in preparation

SECURE VIRTUAL INSPECTIONS

FINDINGS & RESULTS



WHAT THE TECHNIQUE & PROTOCOL ACCOMPLISH

- Room can't be manipulated (without detection, ~ 3 mm displacements)
- Challenge space is large (~ 10^{22}) and can't be exhaustively measured
- All communication channels are public; no trusted hardware
- Only a single inspector visit is required during the initial setup phase

ROBUSTNESS AGAINST ATTACKS

- Room can't be simulated
- Room can't be cloned
- Machine-learning attacks (aimed at predicting challenge-response pairs) fail … and would require very large training sets

J. Tobisch, S. Philippe, B. Barak, G. Kaplun, C. Zenger, A. Glaser, C. Paar, and U. Rührmair, manuscript in preparation

(Photos: Johannes Tobisch)

SOMETHING NEW

Toward Virtual Inspections

(another example)


Can we remotely follow certain (allowed) activities that the host performs ?

VIDEO BROADCAST

KEY REQUIREMENTS

SECURITY & PRIVACY

How to follow relevant activities without also capturing additional information that is considered sensitive but irrelevant for the task at at hand?

DATA TRANSMISSION & INTEGRITY

How to transmit the footage to an offsite location, especially from the interior of a hardened and highly secured building? (Can it be done in real-time?)

LIVE VERIFY & LOCAL VERIFY (Johnston and Warner, 2010)

How to ensure that the footage is recorded in real-time? (How to preclude replay attacks?)
How to ensure that the data is transmitted from the correct location?

Source: IAEA (top and middle) and author (bottom)

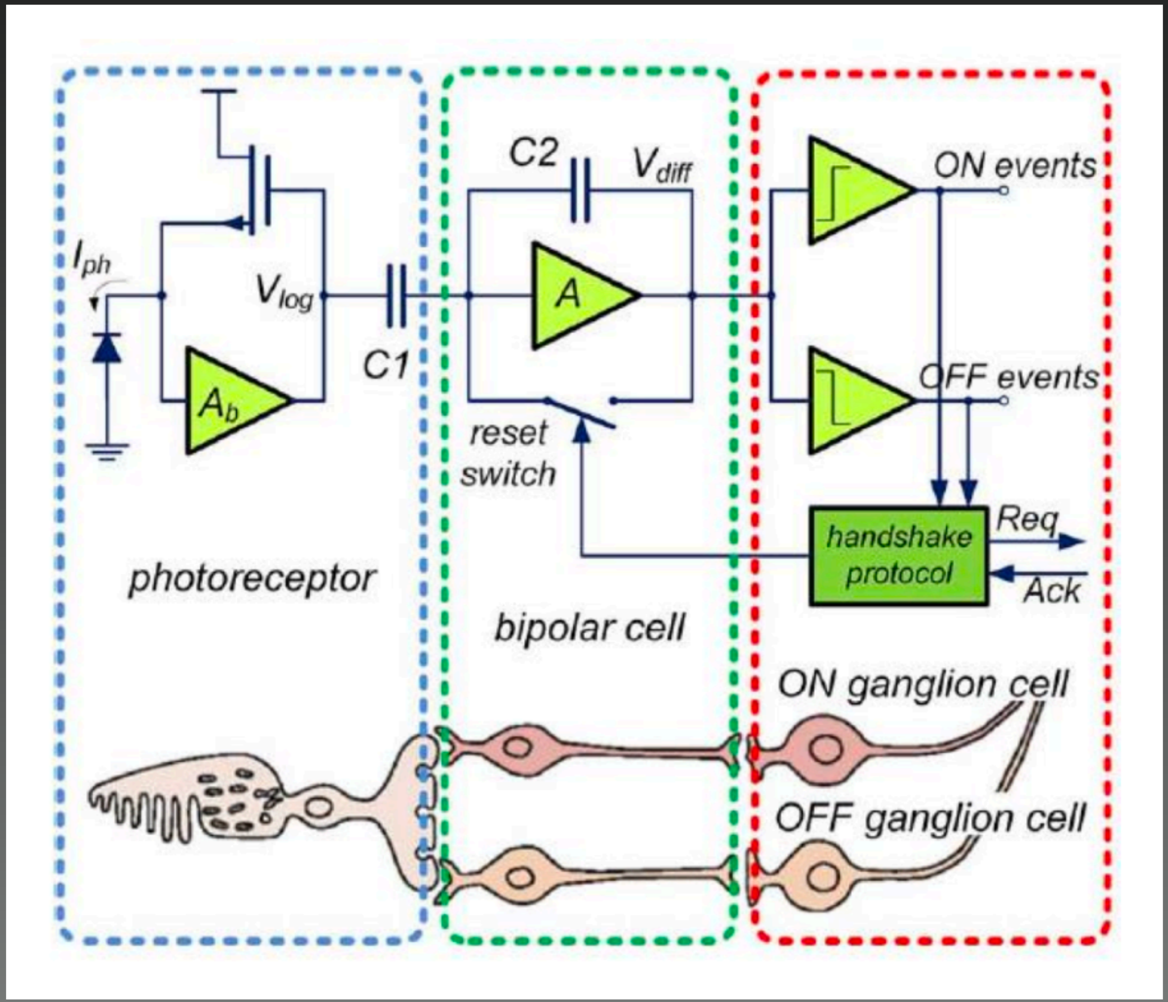
Recorded at TU Berlin, June 2022, courtesy of Guillermo Gallego

Recorded at TU Berlin, June 2022, courtesy of Guillermo Gallego

“SILICON RETINA”

Misha Mahowald (1963–1996)

For a documentary on Mahowald's work, see *www.dailymotion.com/video/x28ktma*



Dynamic Vision Sensor

Source: Posch et al., 2014

Misha Mahowald, *VLSI Analogs of Neuronal Visual Processing: A Synthesis of Form and Function*
PhD Thesis, California Institute of Technology, May 1992, www.ini.uzh.ch/~amw/publicat/mishathesis.pdf

Guillermo Gallego et al., “Event-based Vision: A Survey,” I*EEE Transactions on Pattern Analysis and Machine Intelligence,* July 2020

EVENT-BASED VISION

iniVation DAVIS346

FEATURES

- Extremely low bandwidth, no redundant data
- Very low power consumption (~ 100 mW)
- Asynchronous, fast data acquisition (μs-scale)
- High-dynamic range (> 120 dB)
- Sensitive to relative changes, not absolute values

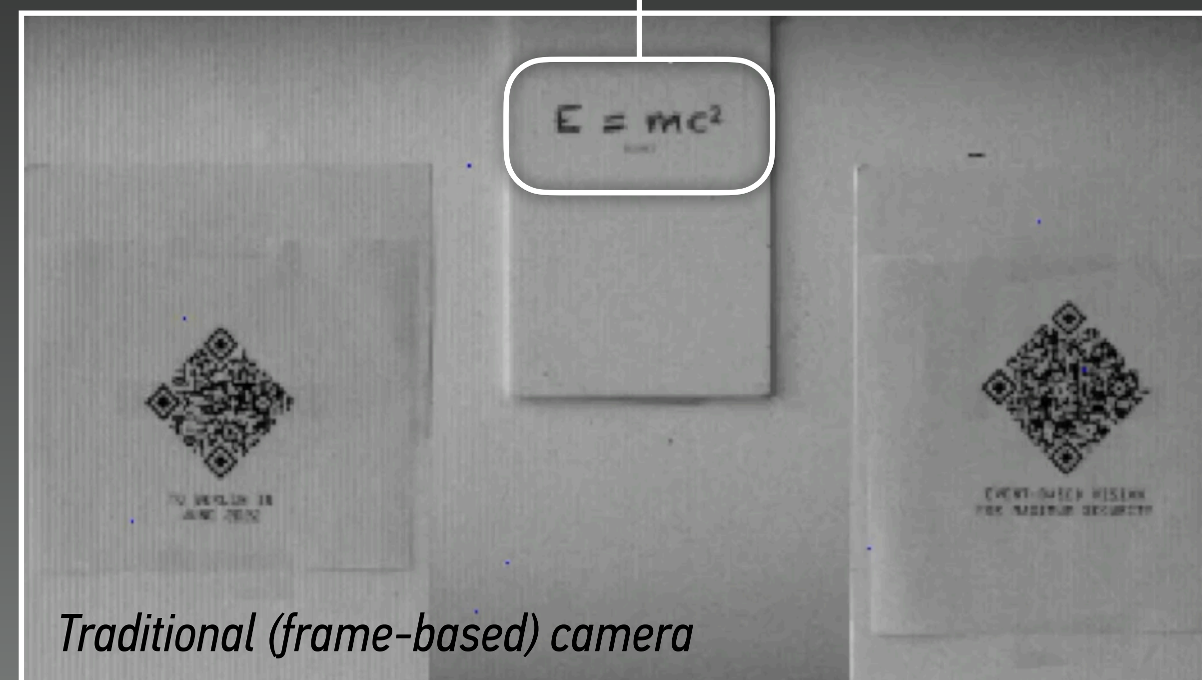
- Commercially available since early 2010s
- Resolution: originally ~ 320 x 240 pixels
  Currently moving to megapixel designs

“NOTHING TO SEE HERE”

EVENT-BASED VISION FOR INTRINSIC INFORMATION SECURITY

Event-based camera

“Secret” information visible at inspected site



Traditional (frame-based) camera

Recorded at TU Berlin, June 2022, courtesy of Guillermo Gallego

EVENT-BASED VISION

CHALLENGES & OPPORTUNITIES FOR SECURE REMOTE MONITORING

OPPORTUNITIES

Remote monitoring of specific activities in sensitive facilities

for example, to read unique identifiers, to confirm integrity of tags and seals, and perhaps even to follow some radiation measurements

CHALLENGES

Can one design CONOPS that can take full advantage of the features?
(i.e., preclude subliminal or accidental release of information)

Note: Most R&D efforts are aimed at image reconstruction (from sparse event data) leveraging advanced machine-learning techniques

Source: IAEA (top) and UZH Robotics and Perception Group (bottom, www.youtube.com/watch?v=eomALySSGVU)

CALL TO ACTION

(IN LIEU OF CONCLUSIONS)

PERSISTENT AND EMERGING VERIFICATION CHALLENGES

25 years of research and development have not produced the technologies needed to verify future arms-control agreements

Virtual inspection techniques could play an increasingly important role in future arms-control verification and safeguards

BRINGING COMMUNITIES TOGETHER & THINKING OUTSIDE THE BOX

Advanced concepts from the (hardware & software) security community could help address important challenges in nuclear security

Unique circumstances: hardware cost is irrelevant; only few units are needed
An opportunity for "exotic" approaches to state-of-the-art security?

Source: Sandia National Laboratories (top) and Wikipedia/Tobias Klenze (30c3 audience, bottom)


SCIENCE &
GLOBAL SECURITY
PRINCETON UNIVERSITY