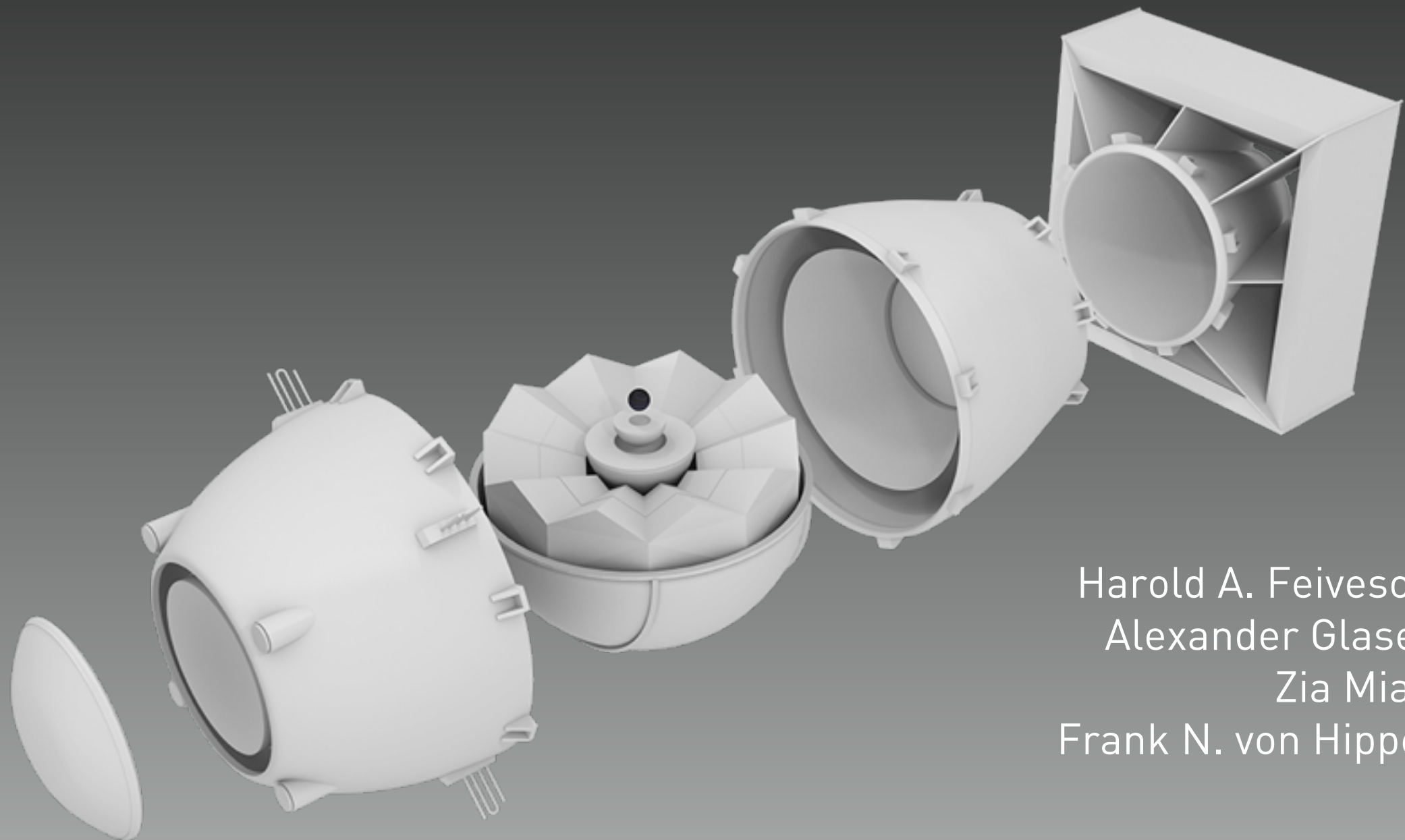


# UNMAKING THE BOMB

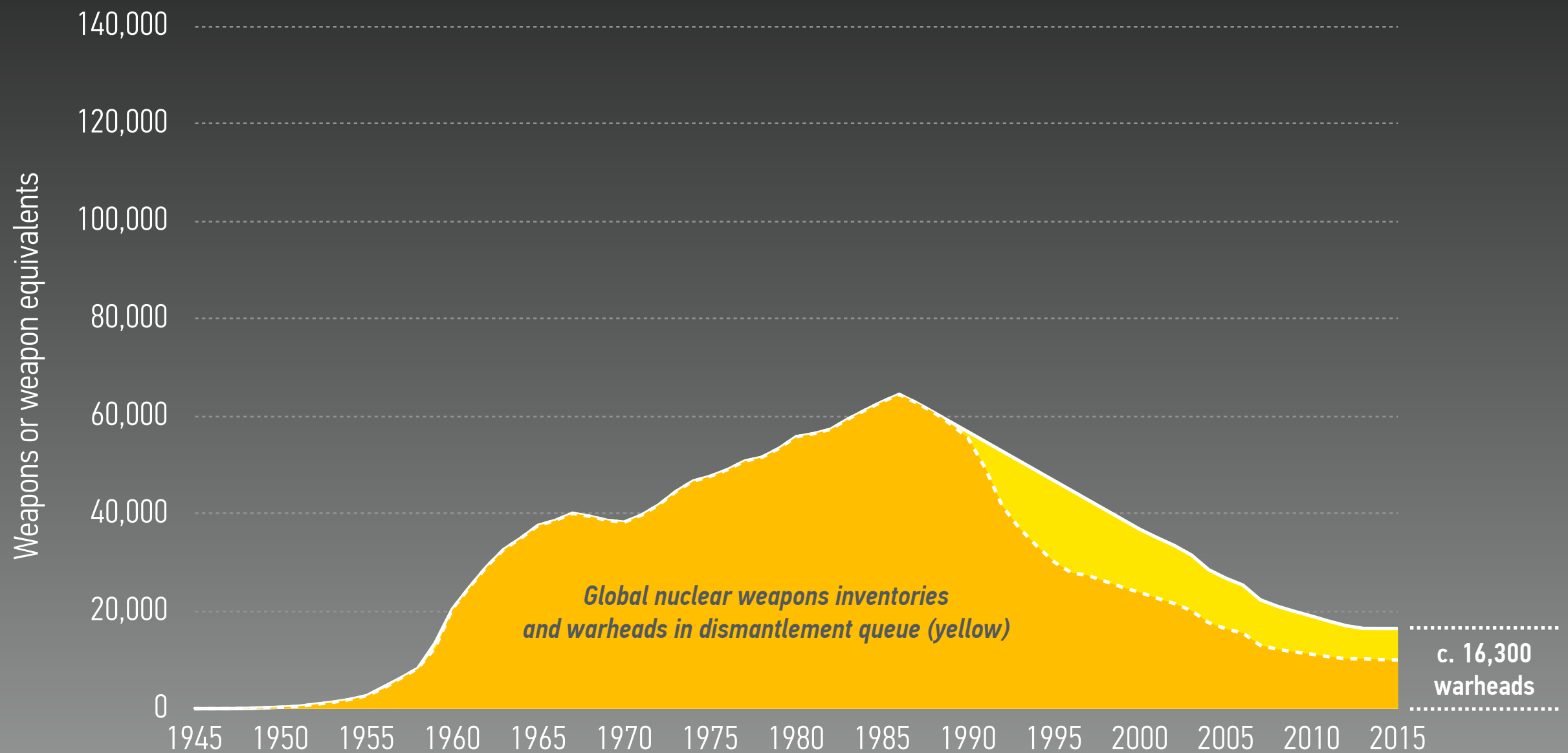
A FISSILE MATERIAL APPROACH TO NUCLEAR  
DISARMAMENT AND NONPROLIFERATION



Harold A. Feiveson  
Alexander Glaser  
Zia Mian  
Frank N. von Hippel

# NUCLEAR WEAPONS AND FISSILE MATERIALS

## GLOBAL INVENTORIES, 1945–2014

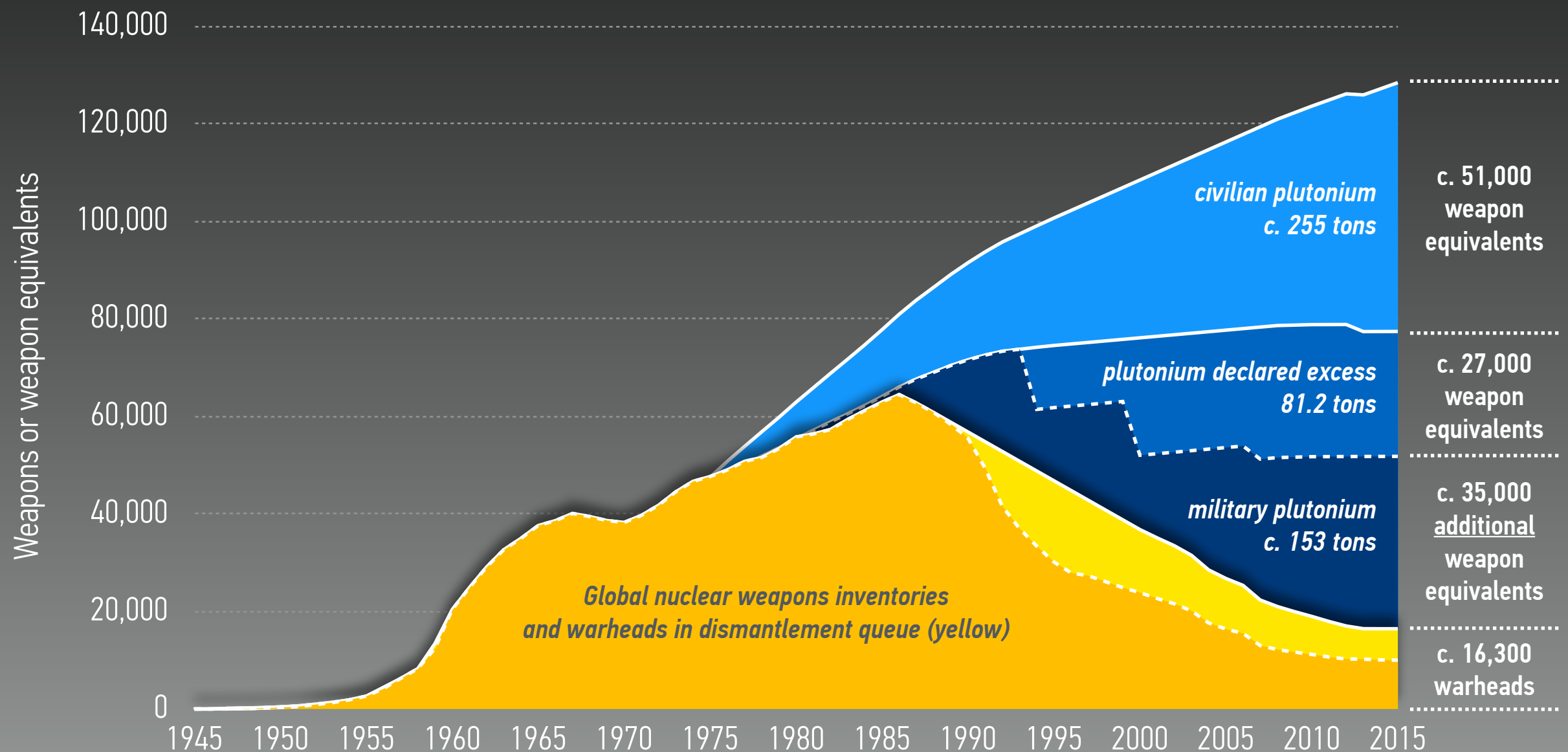


Hans M. Kristensen and Robert S. Norris, "Global Nuclear Weapons Inventories, 1945–2013," *Bulletin of the Atomic Scientists*, 69 (5), 2013, 75–81

# NUCLEAR WEAPONS AND FISSILE MATERIALS

## GLOBAL INVENTORIES, 1945–2014

### THE PLUTONIUM CASE



Hans M. Kristensen and Robert S. Norris, "Global Nuclear Weapons Inventories, 1945–2013," *Bulletin of the Atomic Scientists*, 69 (5), 2013, 75–81  
Fissile material estimates and weapon-equivalents are authors' estimates



INSIDE | Drone Proliferation Tests Arms Control

# Arms Control TODAY

THE SOURCE ON NONPROLIFERATION  
AND GLOBAL SECURITY

Volume 44  
Number 3  
APRIL 2014

## A Win-Win Solution for Iran's Arak Reactor

By Ali Ahmad, Frank von Hippel,  
Alexander Glaser, and Zia Mian

### IN THIS ISSUE

Advancing the  
Trade Treaty:  
Interview With  
ATT Negotiator  
Thomas C...

Rough Sea  
Issues for  
NPT Review  
By Gaukhar M...

### IN THE

States C  
Nuclear

U.S. Nu  
Spending

Missile  
Budget

Gottel  
Confir

Arms  
By U

Iran  
'Cor

Syr  
Re

UN  
N.

U.S. \$7.00  
Canada \$8.00



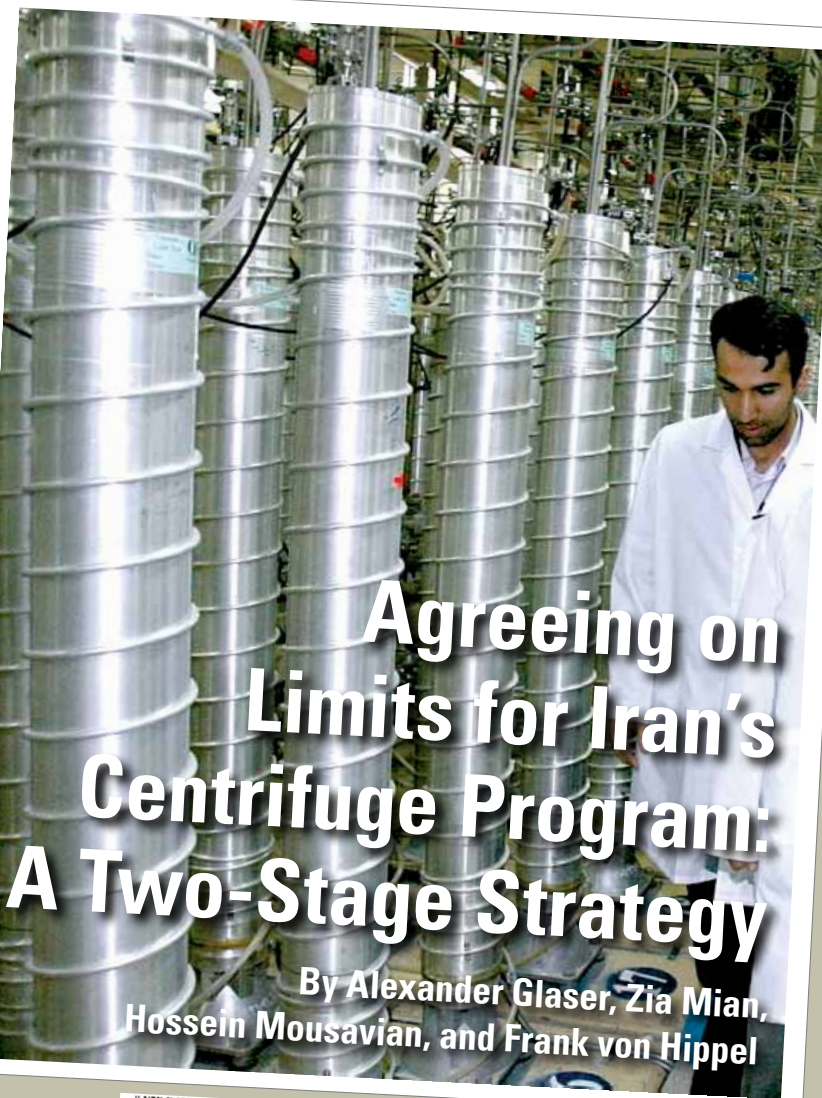
A Publication of the Arms Control Association  
[www.armscontrol.org](http://www.armscontrol.org)

INSIDE | Last Chemical Arms Materials Leave Syria

# Arms Control TODAY

THE SOURCE ON NONPROLIFERATION  
AND GLOBAL SECURITY

Volume 44  
Number 6  
JULY/AUGUST 2014



## Agreeing on Limits for Iran's Centrifuge Program: A Two-Stage Strategy

By Alexander Glaser, Zia Mian,  
Hossein Mousavian, and Frank von Hippel

### IN THIS ISSUE

Russian-U.S.  
Cooperative Threat  
Reduction Beyond  
Nunn-Lugar and Ukraine  
By Richard Weitz

Disarmer in Chief:  
An Interview With  
The UN's Angela Kane

Getting to Know  
Tun Channareth

### IN THE NEWS

Iran, P5+1 Make  
Progress on Nuclear Deal

U.S. Formally Ends  
Landmine Production

Fate of Space Code  
Remains Unclear

China Seen Nearing  
Sea-Based Deterrent

Troubled Missile  
System Hits Target

U.S. Sends Nuclear  
Bombers to Europe

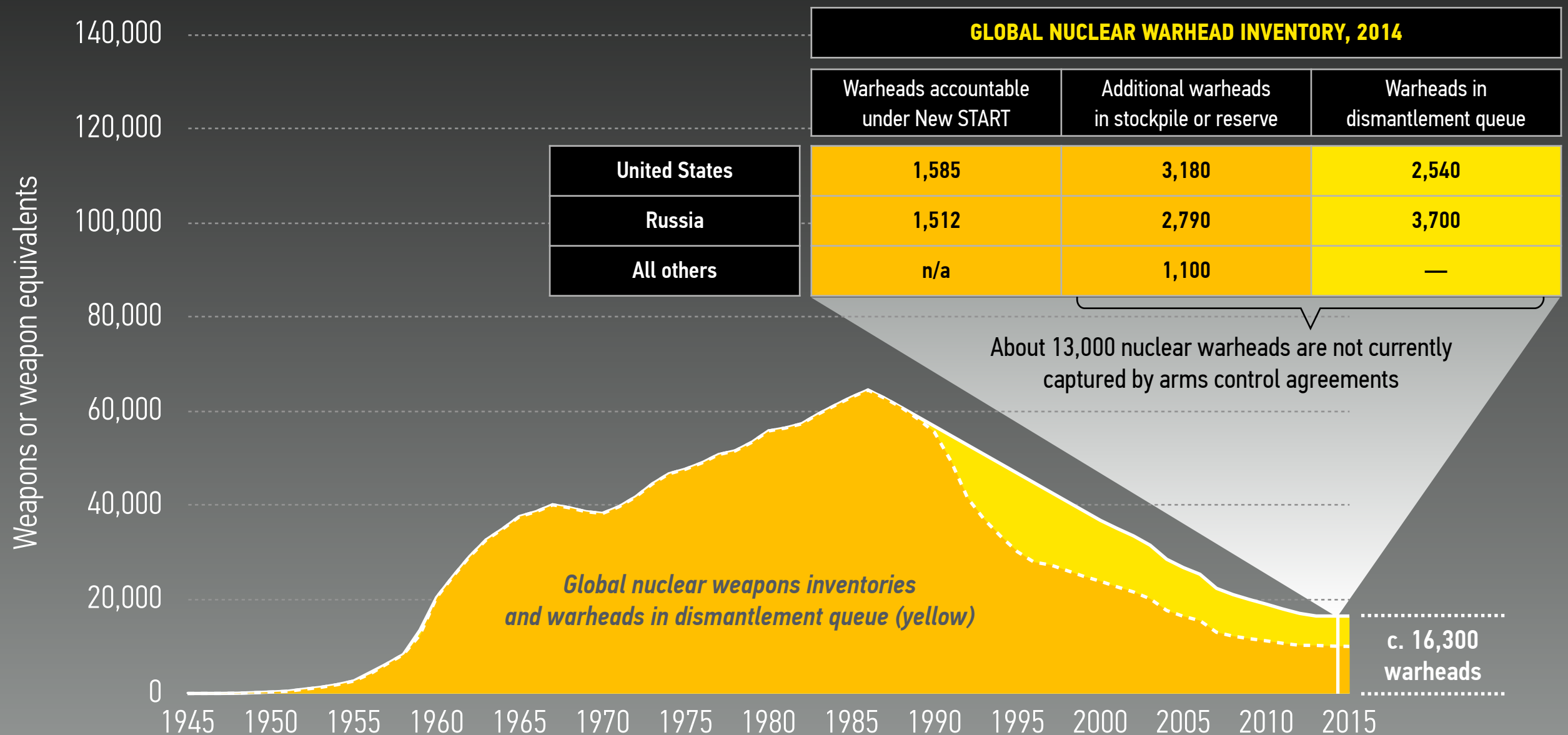
U.S. \$7.00  
Canada \$8.00



A Publication of the Arms Control Association  
[www.armscontrol.org](http://www.armscontrol.org)

# COUNTING WARHEADS

## (VERIFIED AND UNVERIFIED)



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

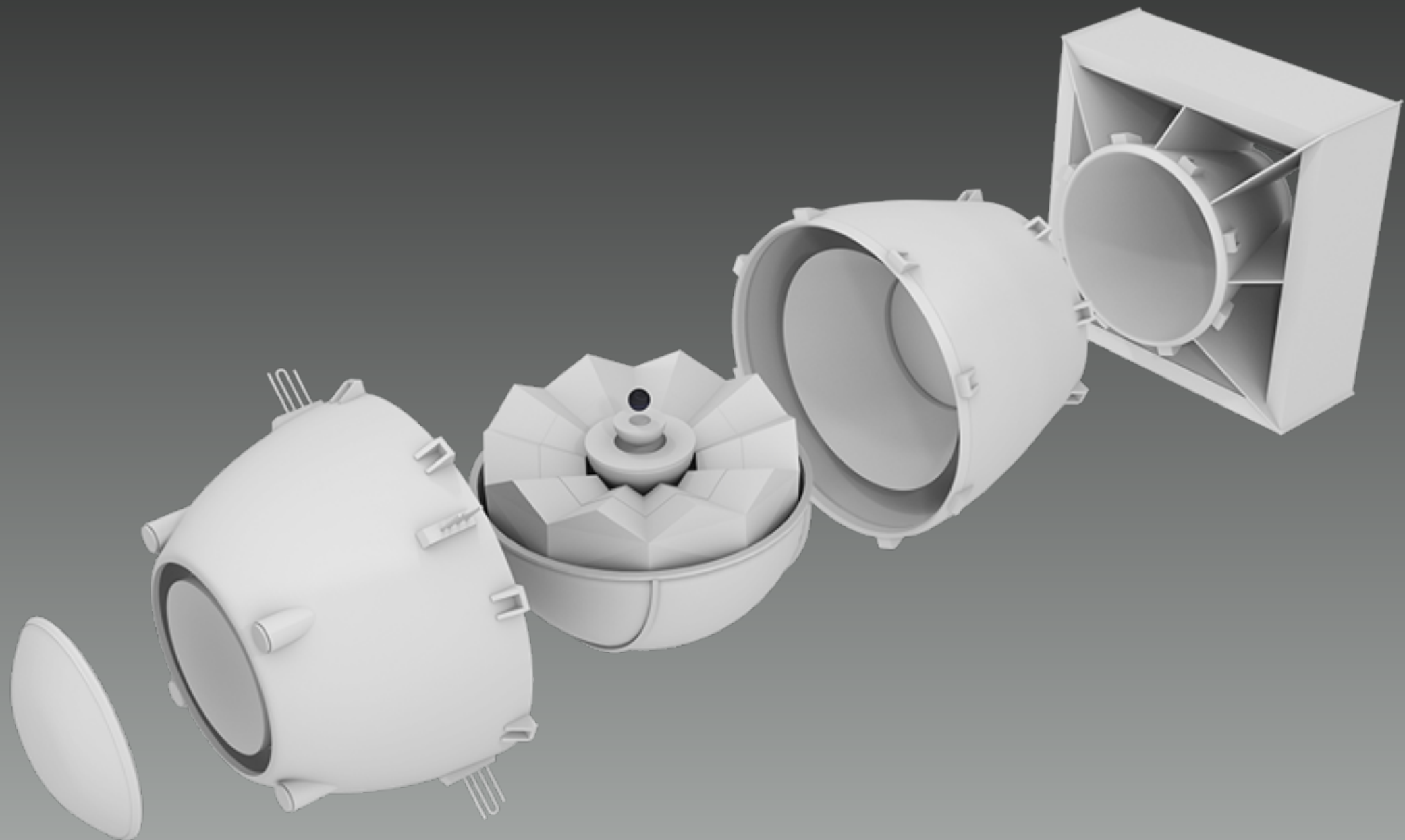
ARE CURRENTLY NON-DEPLOYED (i.e., IN RESERVE OR AWAITING DISMANTLEMENT)



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

# HOW TO DISMANTLE AN ATOMIC BOMB

(WITHOUT LEARNING ANYTHING ABOUT IT)





# 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  
*Source: U.S. DOE (for illustration only)*



Electronic equipment has been used to  
“filter” classified information  
but it is difficult to certify and authenticate



# PROOF AND EXPLANATION

7,779,194,804,244,557

IS NOT A PRIME NUMBER

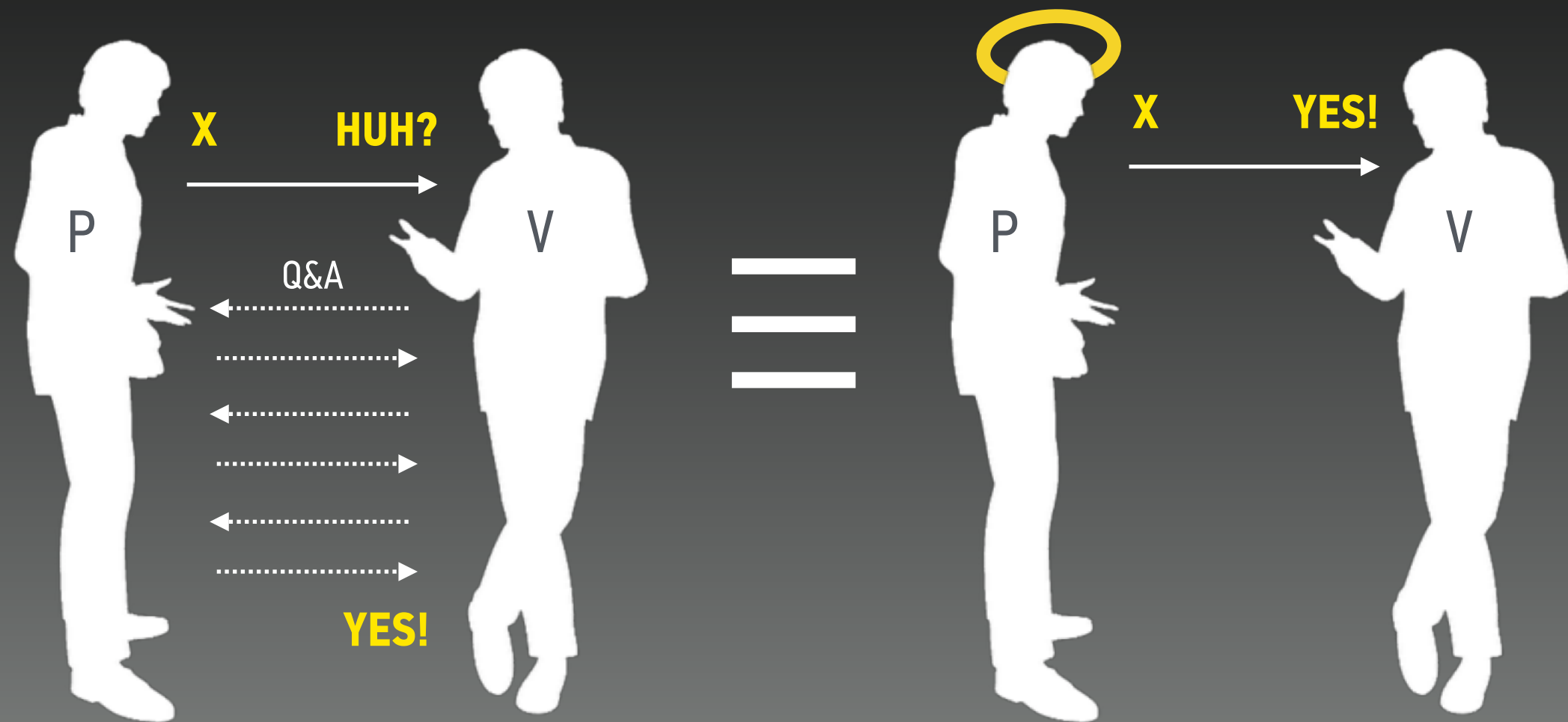
THE QUICK WAY TO PROVE IT

$$23,985,737 \times 324,325,861 = 7,779,194,804,244,557$$

THE THOUSAND DOLLAR QUESTION

Can one prove that a statement is true without revealing why it is true?

# ZERO-KNOWLEDGE INTERACTIVE PROOFS



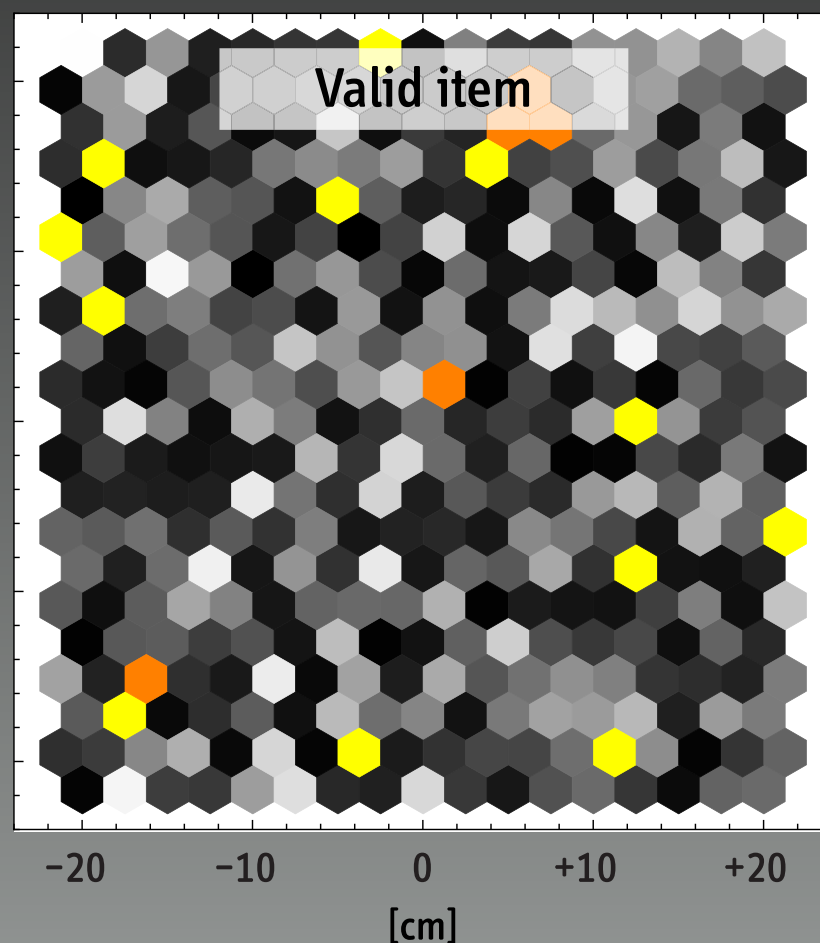
Zero-Knowledge Proofs: The prover (P) convinces the verifier (V) that s/he knows a secret without giving anything about the secret itself away

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 [sean.trank/flickr.com](https://www.flickr.com/photos/seantrank/)

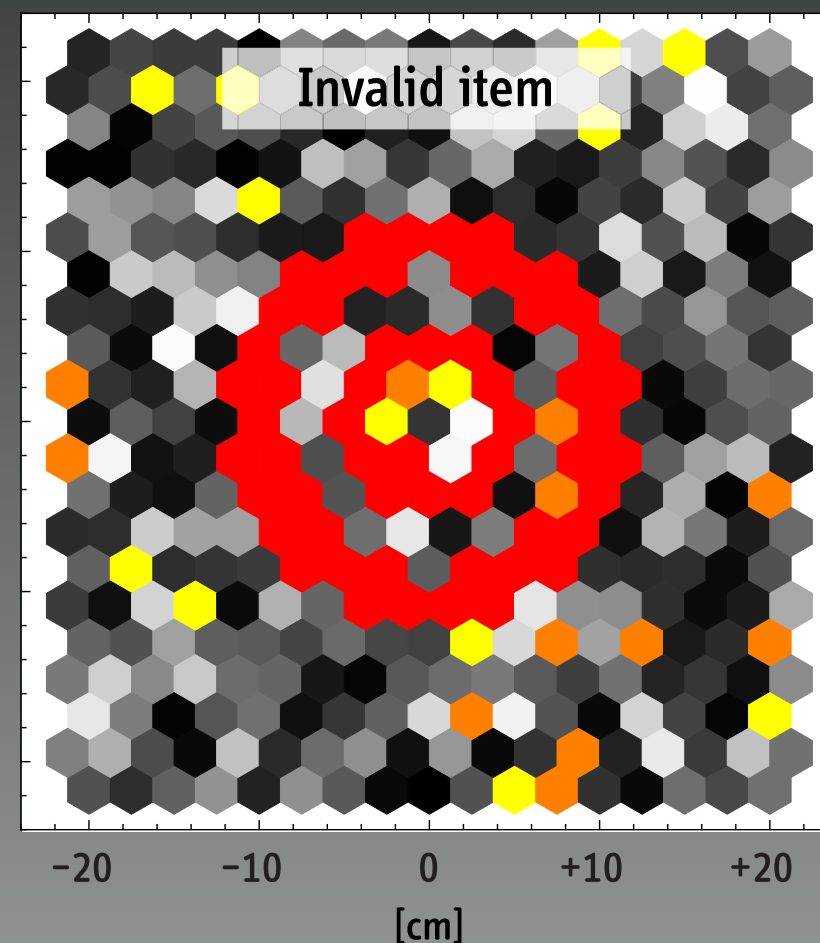
# ZERO-KNOWLEDGE WARHEAD VERIFICATION

(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



# SETTING THE AGENDA

## CONSORTIUM FOR VERIFICATION TECHNOLOGY

Five-year project, funded by U.S. DOE, 22 U.S. universities and national labs, led by U-MICH  
\$3.5 million for Princeton

Princeton leads the research thrust of the consortium on policy

