Nuclear Disarmament - Hacks for a world free of nuclear weapons?

Moritz Kütt

moritz@nuclearfreesoftware.org

MRMCD, September 2014

How to build a nuclear weapon?

~~How to build a nuclear weapon?~~

What do we need to know to disarm a nuclear weapon?

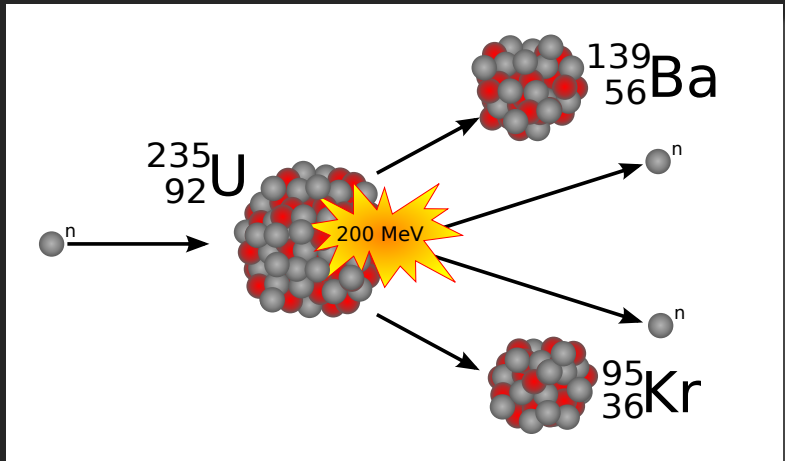
Basic principle

Energy produced by reactions of atomic nucleus.

- Proton
- Neutron

Elements	Depend on proton number
Isotopes	Different neutron numbers for particular proton number

Fission of heavy elements produces large amount of energy (200 MeV):



C-oxidation: several eV

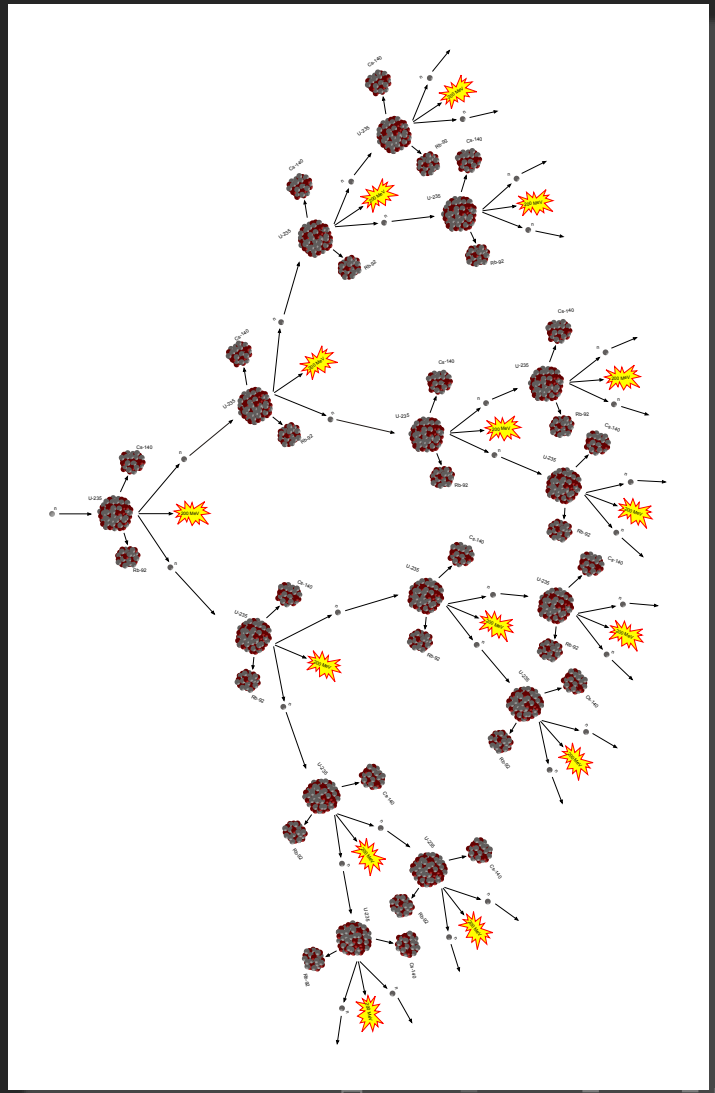
Nuclear Chain Reaction

Initial fission leading to exponential growth of fissions.

Critical Mass

Minimal amount of material needed for which chain reaction is possible.

Smaller amount: more neutrons lost by absorption / escape.



Fissile Material

for weapon purposes do not occur naturally

Highly Enriched Uranium

Protons: 92
Neutrons: 235/238

Natural uranium: 0.7% U-235
For weapons: $>$ 90% U-235 needed

U-235 fraction can be increased by enrichment.

Highly Enriched Uranium = HEU

Plutonium

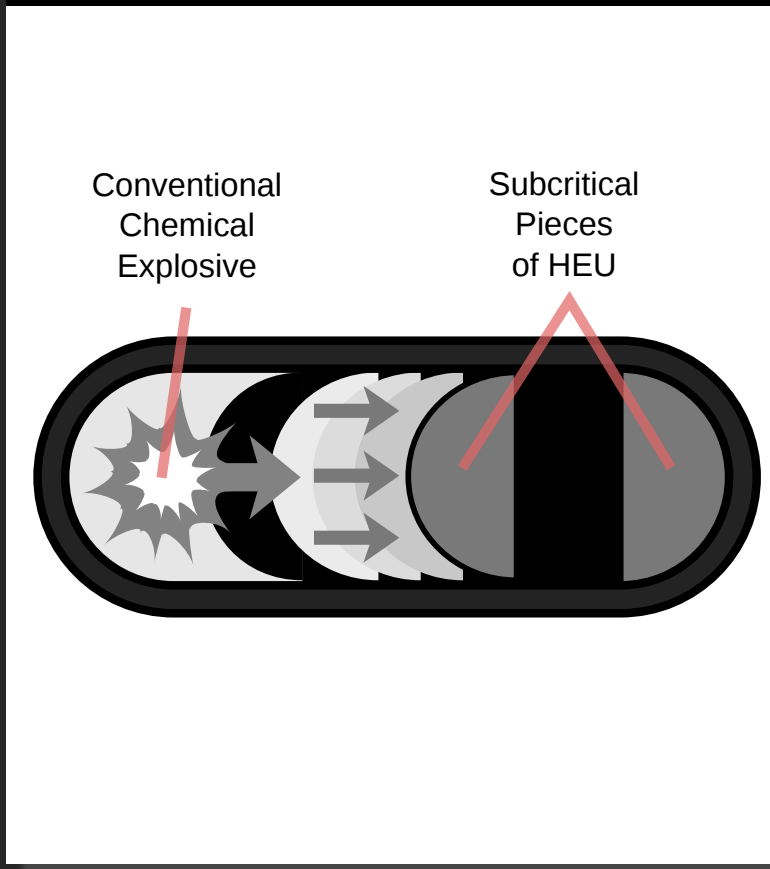
Protons: 94
Neutrons: 239 (240/241/...)

Plutonium produced in any nuclear reactor.

It needs to be separated from spent fuel by reprocessing.

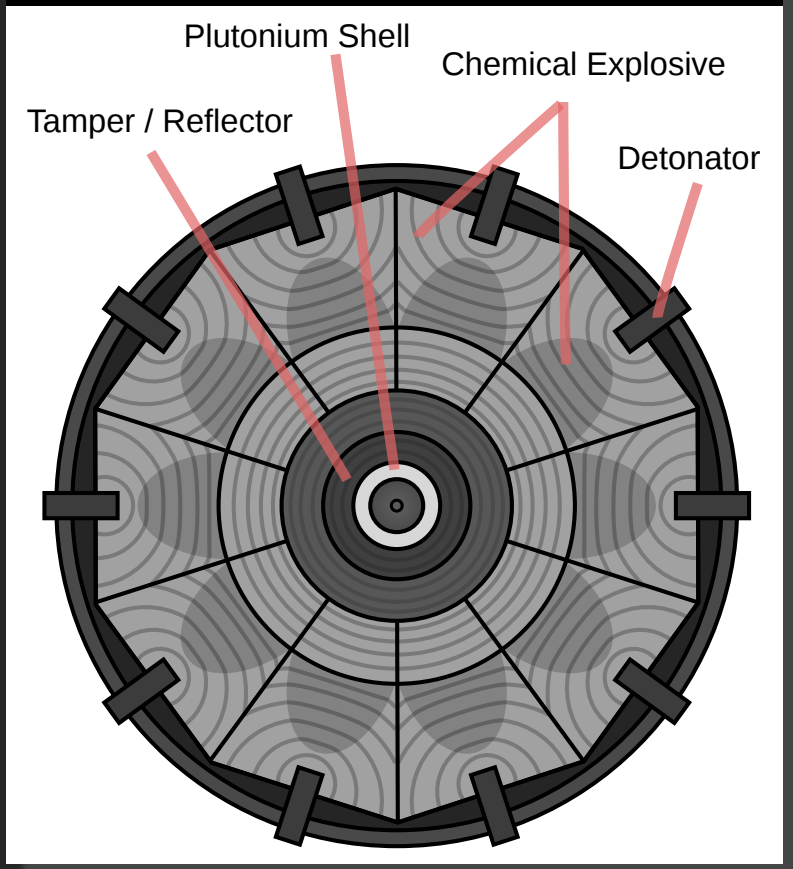
Weapon Principles

Gun Type



Public Domain - Wikimedia Commons (Modified)

Implosion



Public Domain - Wikimedia Commons (Modified)

Massive Explosive Power

Approx. 2000 nuclear weapons were exploded during nuclear testing.

Total yield (explosive power) of all tested weapons:
510 million tons TNT equivalent

R.S. Norris and W.M. Arkin, NRDC Nuclear Notebook - Known Nuclear Tests Worldwide, 1945–1998, *Bulletin of the Atomic Scientists*, 1998, 1, 2003

Massive Explosive Power

Approx. 2000 nuclear weapons were exploded during nuclear testing.

Total yield (explosive power) of all tested weapons:
510 million tons TNT equivalent

R.S. Norris and W.M. Arkin, NRDC Nuclear Notebook - Known Nuclear Tests Worldwide, 1945–1998, *Bulletin of the Atomic Scientists*, 1998, 1, 2003

Can you imagine
510.000.000.000 kg
of TNT?

Massive Explosive Power

Approx. 2000 nuclear weapons were exploded during nuclear testing.

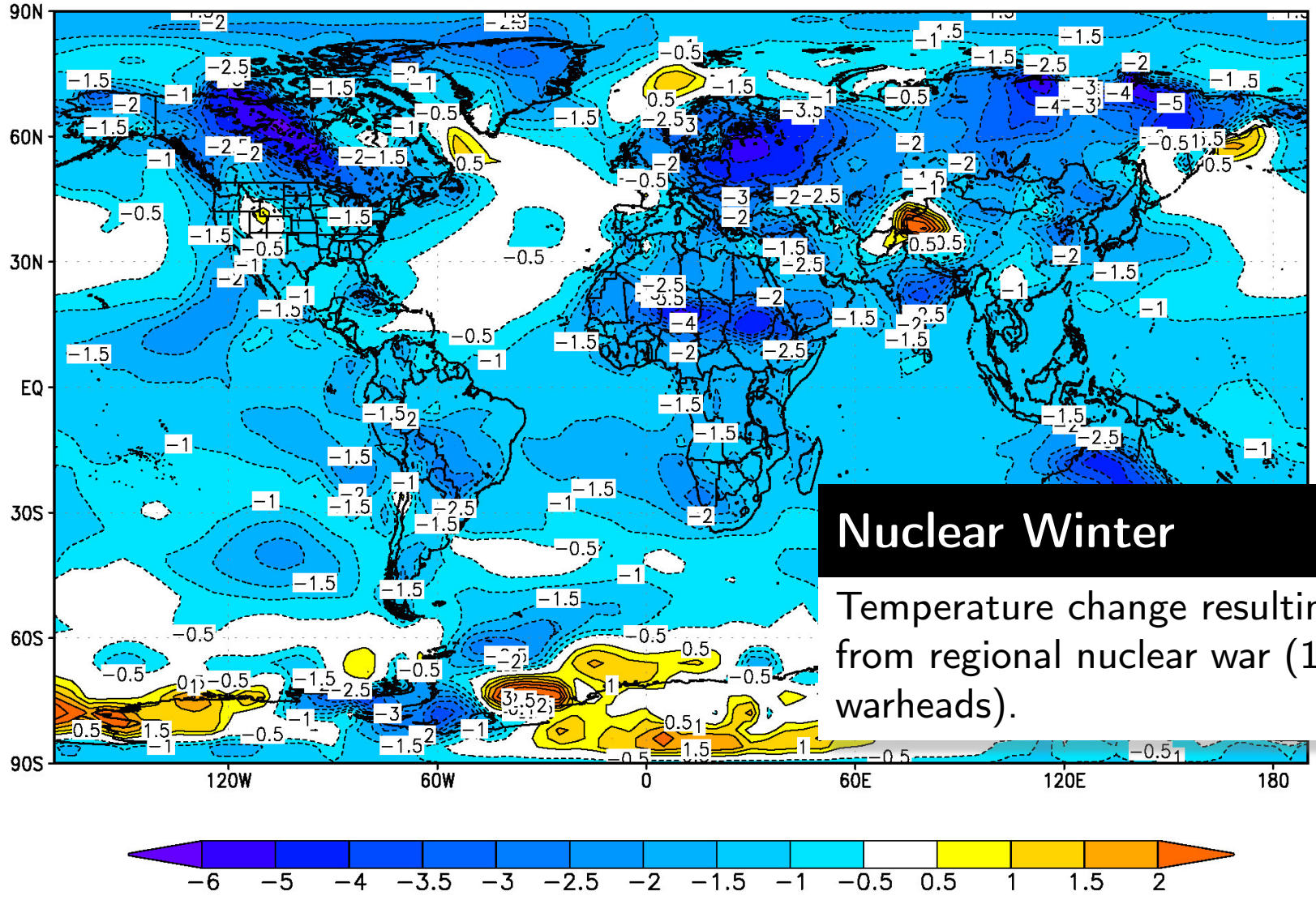
Total yield (explosive power) of all tested weapons:
510 million tons TNT equivalent

R.S. Norris and W.M. Arkin, NRDC Nuclear Notebook - Known Nuclear Tests Worldwide, 1945–1998, *Bulletin of the Atomic Scientists*, 1998, 1, 2003

Can you imagine
510.000.000.000 kg
of TNT?

1.000 kg did this...

CC-BY-SA Sajak



Nuclear Winter

Temperature change resulting from regional nuclear war (100 warheads).

Global Warhead stockpiles

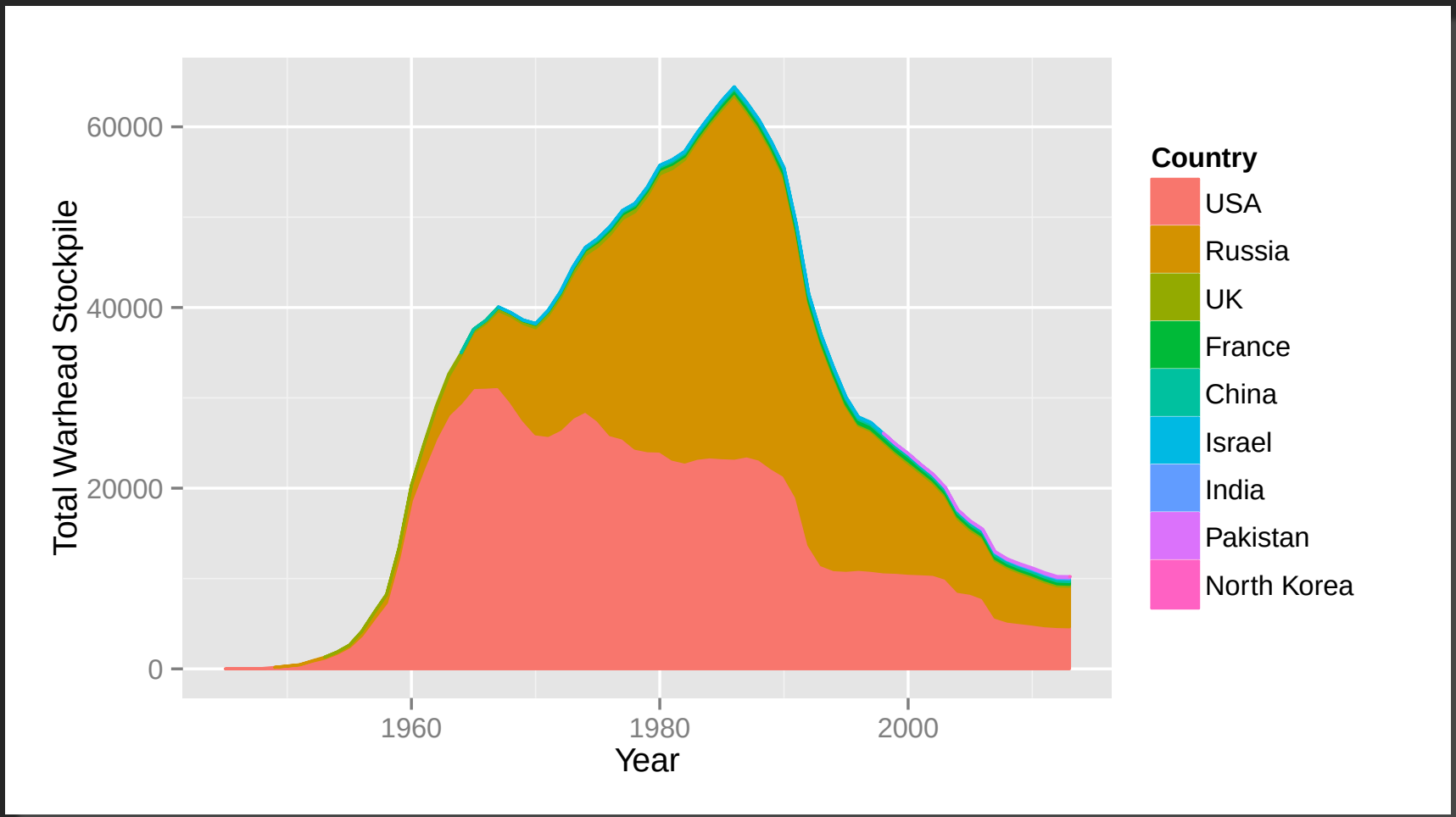


Image created with data from: Kristensen, H. M. and Norris, R. S. Global nuclear weapons inventories, 1945-2013 Bulletin of the Atomic Scientists, SAGE Publications, 2013, 69, 75–81

Germany

Nuclear Weapons in Germany?

Germany

Nuclear Weapons in Germany?

U.S. nuclear weapons stationed as part of "NATO nuclear sharing"

approx. 20 stored at Büchel

CC-BY-SA Stahlkocher

B61 warheads

Public Domain, U.S. DoD

Present Arms Control

Non-Proliferation Treaty

Entered into force in 1970
Defines Nuclear Weapon States and Non-Nuclear Weapon States
Prohibits development of nuclear weapons for latter.

Partial Test Ban Treaty:
Bans nuclear weapon testing in atmosphere, under water and on surface.

Several other smaller treaties exist, often only bilateral between Russia and the United States.

Future Regulation

Comprehensive Test Ban Treaty (CTBT)

Banning all testing, including underground testing.
International Monitoring System already in place and working (e.g. North Korea).

Fissile Material Cut-off treaty

Ban production of weapon-usable fissile material.

Disarmament Treaty

Not yet discussed!
Nuclear Weapons Convention / Ban-Treaty / . . . ?

Independent of political solutions:

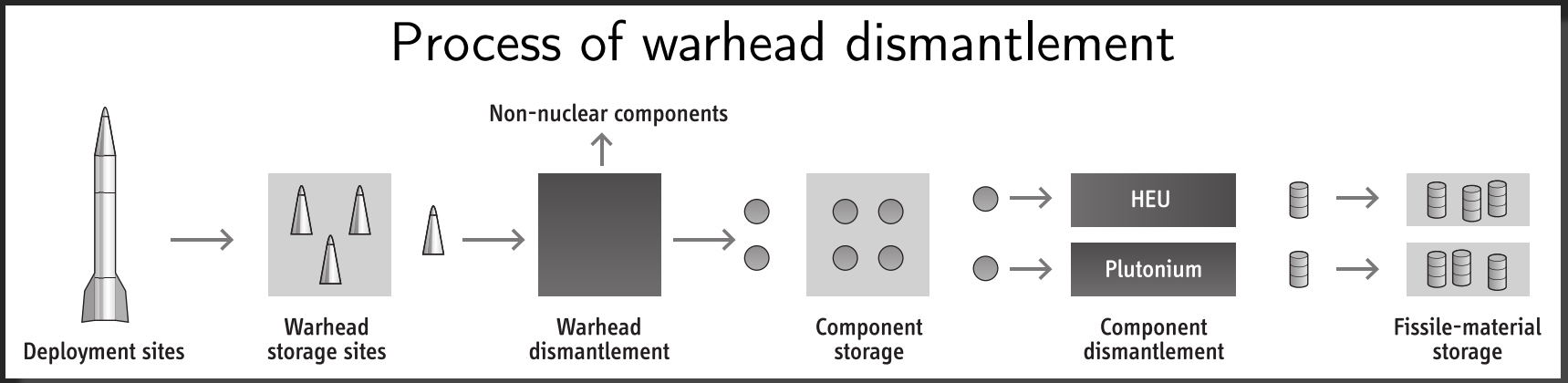
There are
many technical problems and challenges
without a solution.

Independent of political solutions:

There are
many technical problems and challenges
without a solution.

Complicated task - Help from every community needed!

Disarmament Verification



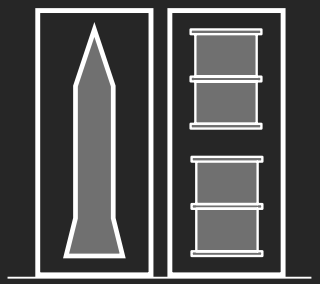
Verification

Carried out to have high confidence in number / location of dismantled warheads.

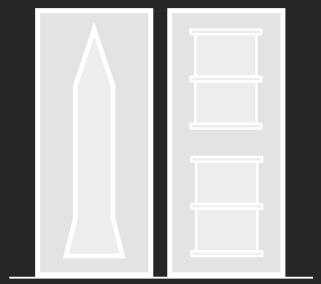
Should include participation of non-nuclear weapon states.

Verification Goal

Is there a bomb in the box?



Host Party (Host) owns weapon ready for dismantlement, or spoof.



Inspecting Party (Inspector) needs to verify weapon / spoof without opening the box.

Two Approaches:

Template Approach

Items are compared to "Golden Sample", which identity is proved by other means.

Attribute Approach

Items are checked for particular attributes (e.g. presence/mass of fissile material).

Further Complication

Adherance to existing regulation in the Non-Proliferation Treaty required:

> *Article I*
> *Each nuclear-weapon State Party to the Treaty undertakes [. . .] not in any way to assist, encourage, or induce any non-nuclear-weapon State to manufacture or otherwise acquire nuclear weapons or other nuclear explosive devices, or control over such weapons or explosive devices.*

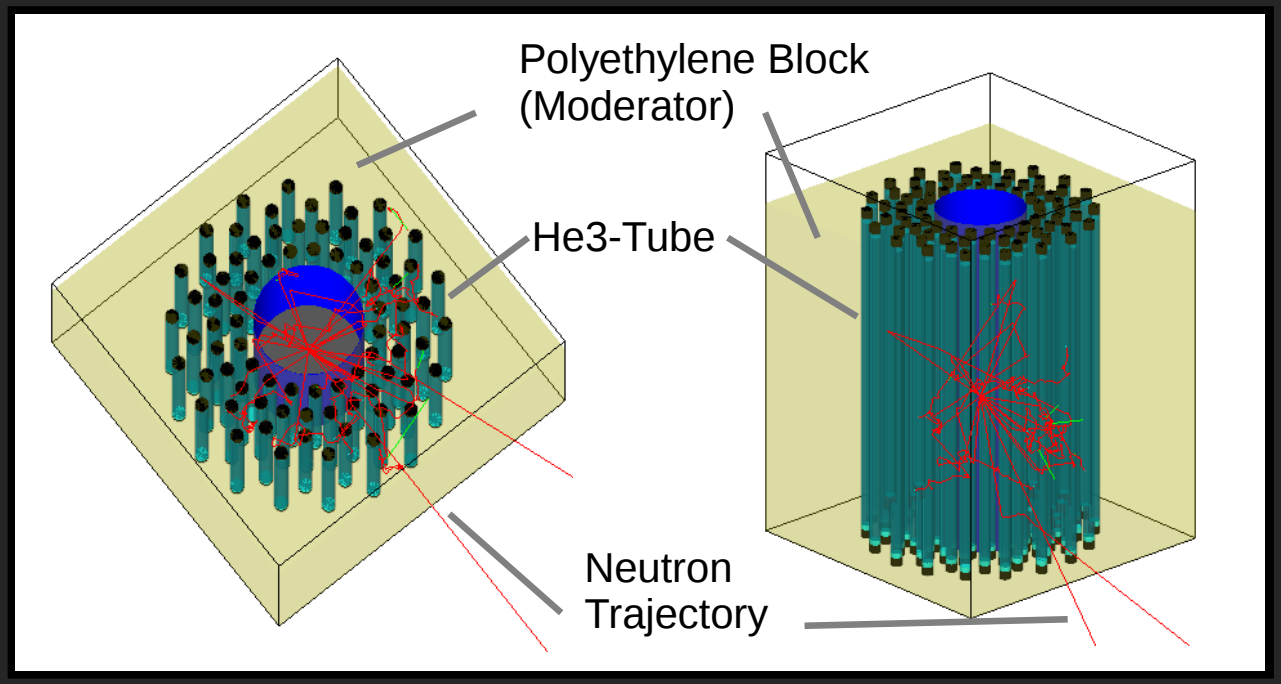
In addition, states claim information sensitivity / classification because of national security interests.

Hack 1: Free Software

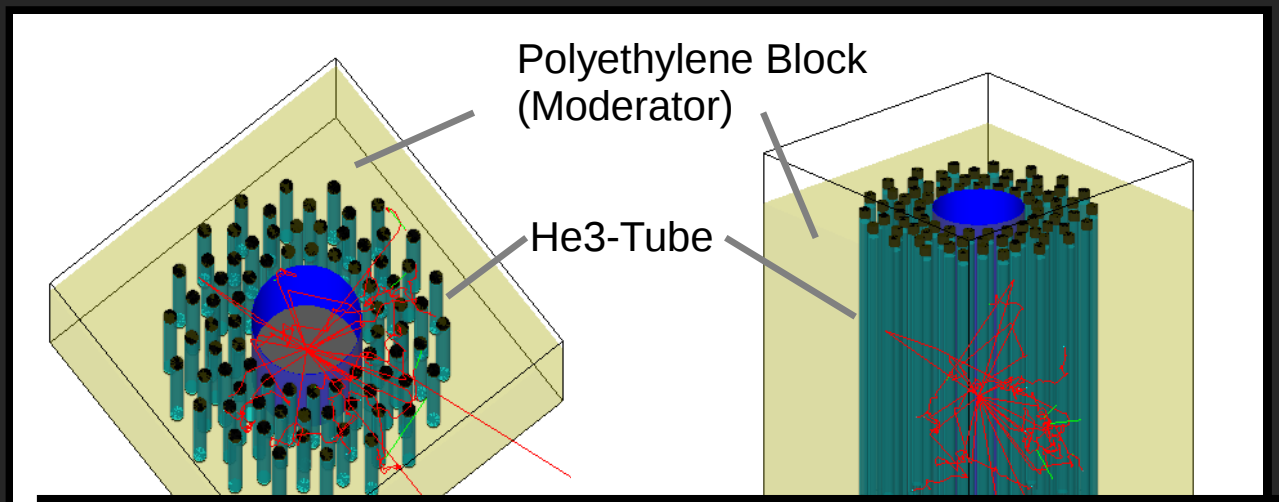
Software is used
to develop new measurement technologies
and during implementation of disarmament verification

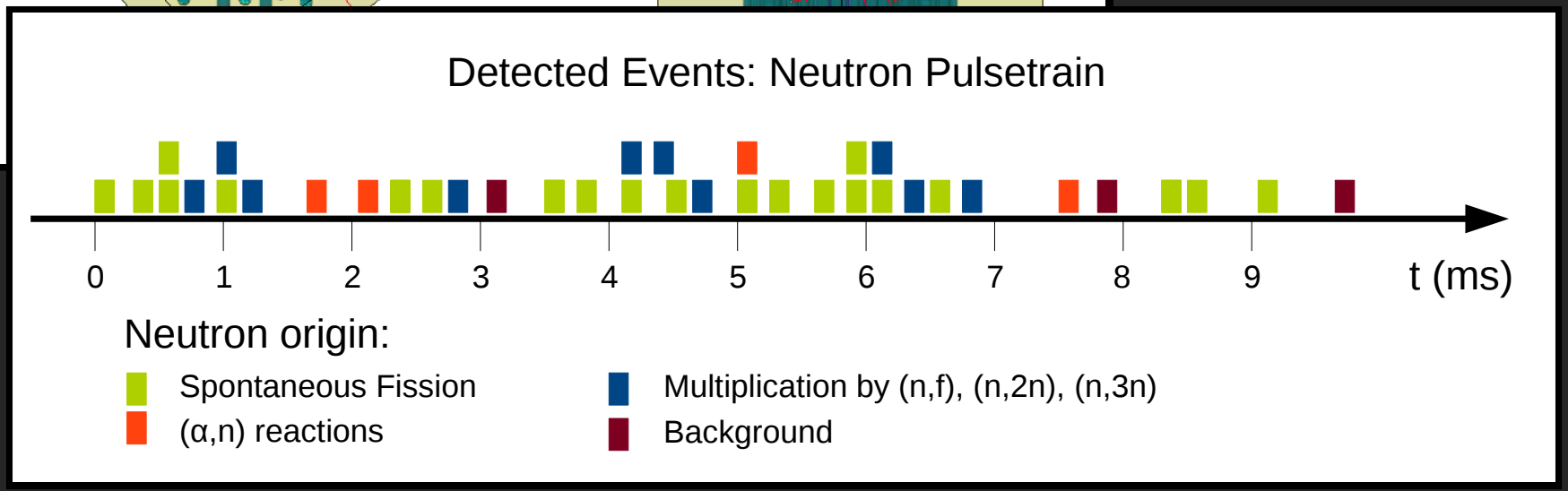
(also needs hardware and institutional arrangements...)

Neutron Multiplicity Measurements

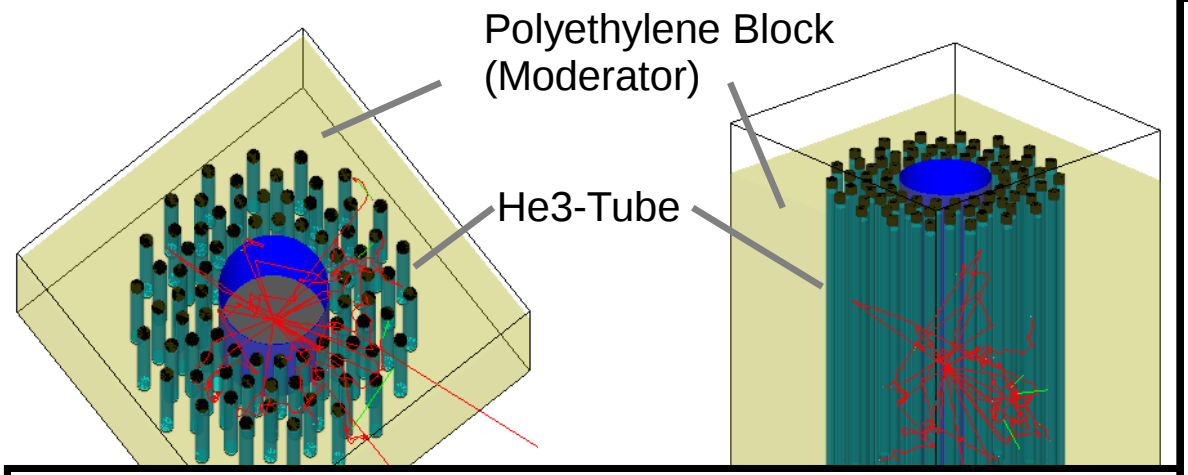


Neutron Multiplicity Measurements



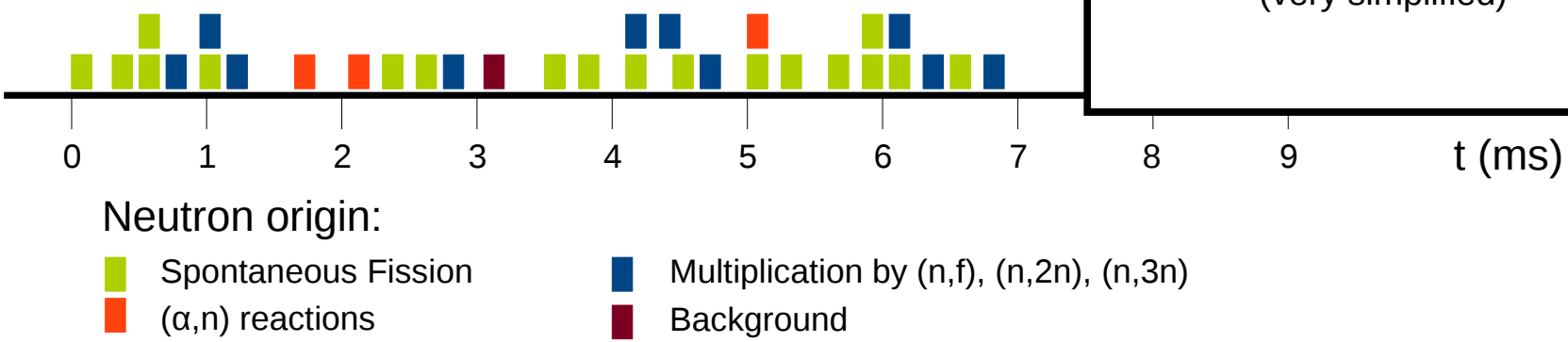


Neutron Multiplicity Measurements



$$\frac{\text{Spontaneous Fission Rate}}{\text{Fission Rate per Mass}} \cdot \frac{1}{\text{Pu240 Mass fraction}} = \text{Plutonium Mass}$$

(very simplified)



Problem

Currently used software often suffers from

Difficulties for software verification (no source code access)

Limited application and development (“expert communties”)

Limited access (export controls)

(High) financial requirements

Problem

Currently used software often suffers from

Difficulties for software verification (no source code access)

Limited application and development (“expert communties”)

Limited access (export controls)

(High) financial requirements

How to establish trust. . .

if software is used as tools for decision making?

if states rely on results of software?

Free Software criteria for software in Nuclear Arms Control!

Three Criteria derived from Free Software / Open Source

(1) No restrictions for access to program.
(2) Distribution of program must include full source code.
(3) Modifications of the program are allowed to anybody.

Public Domain CC-BY-SA NicoBZH

CC-BY Open Source Initiative CC-BY-SA Manon Anne Ress

Prevent Backdoors/Cheating

Kerckhoffs' principle (cryptography)

> *Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi;*
>
> *(It must not require secrecy, and can without concerns fall into enemy hands.)*
>
> — *Auguste Kerckhoffs, La cryptographie militaire 1883, IX, 5-38, 161-191*

"Verification of the Verification"

Inspected & Inspecting Party can review functionality of Open Source Software

Increase Participation

Three groups

Verification Experts	Nuclear Technical community
Other Experts	Academia, technical communities, not related to Arms Control
Society	Public, laypersons

Open Source

- enables connection between communities
- verification supported beyond arms control community
- to involve of society, Crowd-Sourcing / Societal Verification

Work on this issue is part of my PhD project.

www.nuclearfreesoftware.org

M. Kütt, A. Glaser and M. Englert. "Open Source meets Nuclear Arms Control", In: Proceedings of 55th Annual INMM Meeting, Atlanta, GA, 21-24 July 2014.

M. Kütt and M. Englert. "Increased transparency in simulations of measurements for nuclear disarmament verification", In: F. Sevini (Ed.). 35th ESARDA Symposium proceedings, Bruges, 27-30 May 2013.

Work on this issue is part of my PhD project.

www.nuclearfreesoftware.org

M. Kütt, A. Glaser and M. Englert. "Open Source meets Nuclear Arms Control", In: Proceedings of 55th Annual INMM Meeting, Atlanta, GA, 21-24 July 2014.

M. Kütt and M. Englert. "Increased transparency in simulations of measurements for nuclear disarmament verification", In: F. Sevini (Ed.). 35th ESARDA Symposium proceedings, Bruges, 27-30 May 2013.

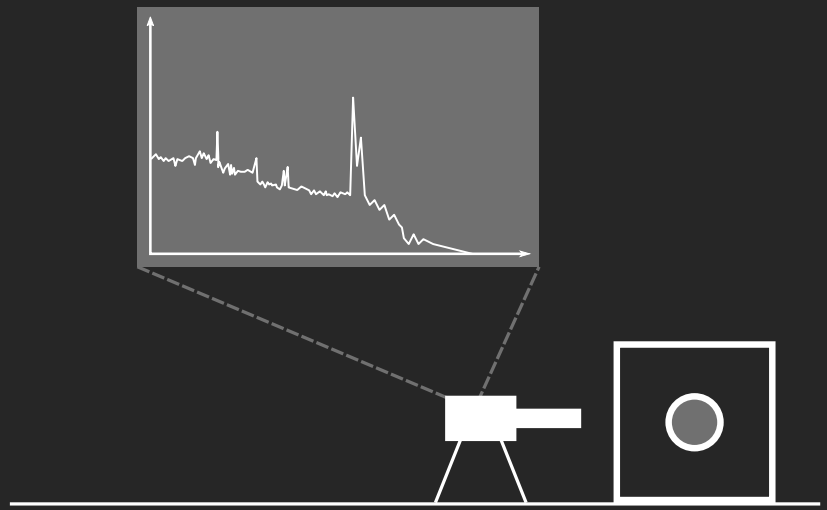
Can you imagine to help?

Hack 2: Information Barrier

Information Barrier

Measurement of classified/sensitive physical quantity (e.g. attribute)

Public Domain - U.S. DoE NNSA

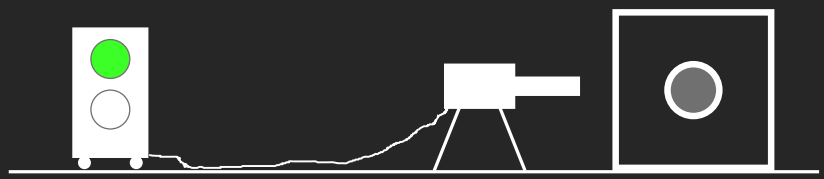


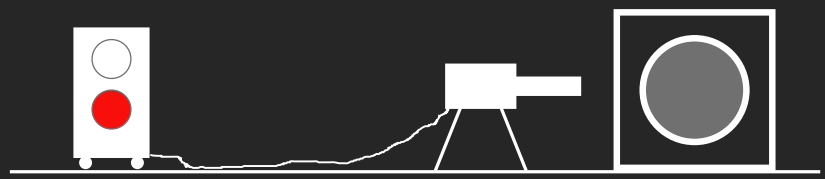
Information Barrier

Classified information transformed into unclassified information:

Information barrier shows simple information to inspector

But should be able to detect cheating





Typically based on jointly developed hardware/software.

Development Examples

Trilateral Initiative (90s)

Russia, USA and International Atomic Energy Agency.
Research mechnologies / methods to verify fissile material coming from nuclear weapons.

UK-Norway-Initiative (2010-2015)

Exercise for verified warhead dismantlement.
Research: Social issues (inspector / host), development of information barrier.

Challenges

Hardware Verification
(e.g. Hardware Trojans?)

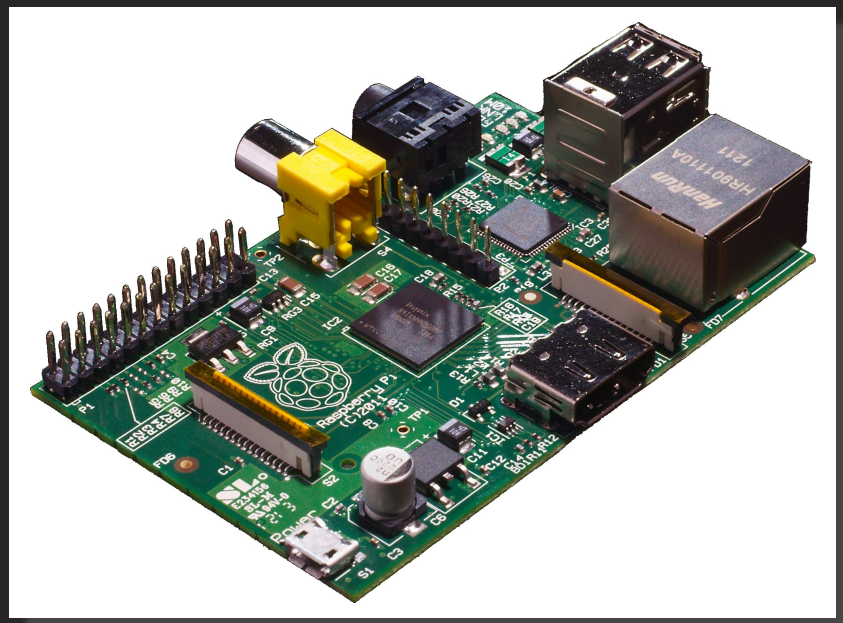
Software Verification
(Backdoor / Cheating)

Challenges

Hardware Verification
(e.g. Hardware Trojans?)

Software Verification
(Backdoor / Cheating)

Could you trust this system?



Challenges

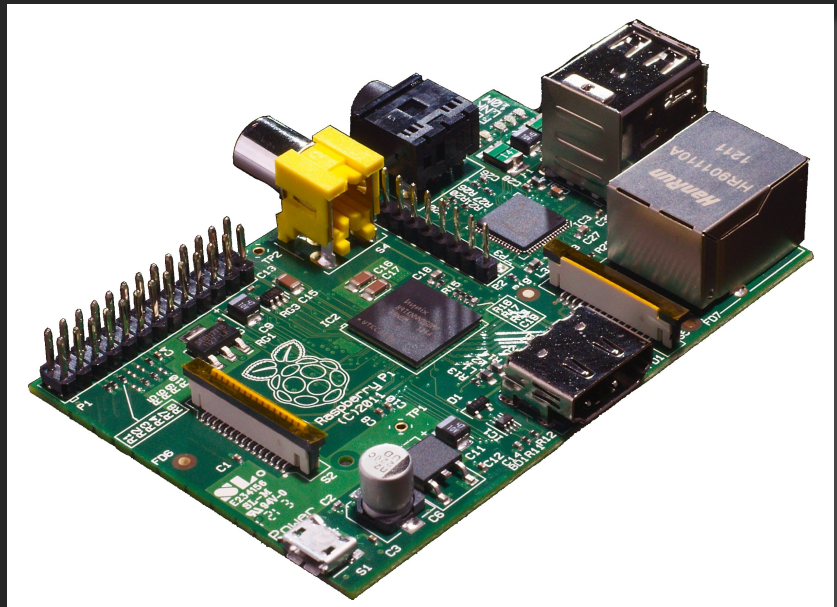
Hardware Verification
(e.g. Hardware Trojans?)

Software Verification
(Backdoor / Cheating)

Host Provided Hardware
"Warhead" Certified

Quality / Validity
of Measurements

Could you trust this system?



Current Research

J. Fuller. "The functional Requirements and Design Basis for Information Barriers", Report PNNL-13285, Pacific Northwestern National Laboratory, 1999.

K. Allen et al. "UK-Norway Initiative (UKNI) approach for the development of a Gamma Ray Attribute Measurement System with an integrated Information Barrier", In: F. Sevini (Ed.), proceedings of 35th ESARDA Symposium proceedings, Bruges, 27-30 May 2013.

M. Göttsche and G. Kirchner. "Measurement Techniques for Warhead Authentication with Attributes: Advantages and Limitations," *Science & Global Security*, 22, no. 2, 2014.

(more . . .)

Current Research

J. Fuller. "The functional Requirements and Design Basis for Information Barriers", Report PNNL-13285, Pacific Northwestern National Laboratory, 1999.

K. Allen et al. "UK-Norway Initiative (UKNI) approach for the development of a Gamma Ray Attribute Measurement System with an integrated Information Barrier", In: F. Sevini (Ed.), proceedings of 35th ESARDA Symposium proceedings, Bruges, 27-30 May 2013.

M. Göttsche and G. Kirchner. "Measurement Techniques for Warhead Authentication with Attributes: Advantages and Limitations," *Science & Global Security*, 22, no. 2, 2014.

(more . . .)

Can you imagine to help?

Hack 3: Zero-Knowledge Protocol

Basics

Cryptographic protocol

- proof a particular fact
- sound & complete
- without revealing more knowledge

Required: Interaction between parties.

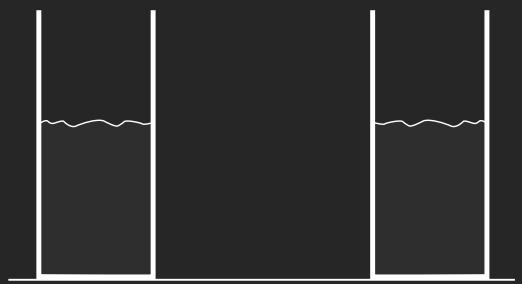
Distinguishing Drinks

Can Bob distinguish two drinks?

Drinks look equal

(e.g. Coca Cola / Fritz Cola, French Wine / Californian Wine)

Bob tastes each drink and places them in Alice's right and left hand.



Distinguishing Drinks

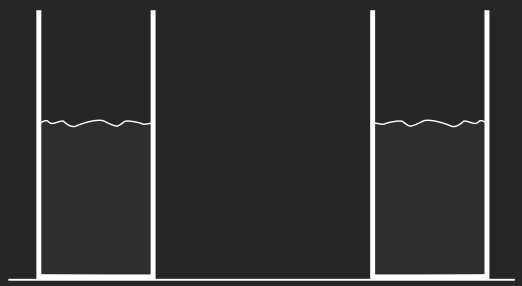
Can Bob distinguish two drinks?

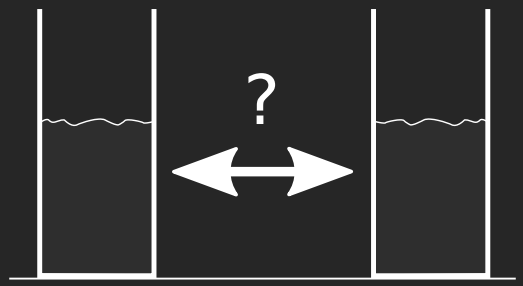
Drinks look equal

(e.g. Coca Cola / Fritz Cola, French Wine / Californian Wine)

Bob tastes each drink and places them in Alice's right and left hand.

Alice chooses to switch or not switch the cups (secretly).





Distinguishing Drinks

Can Bob distinguish two drinks?

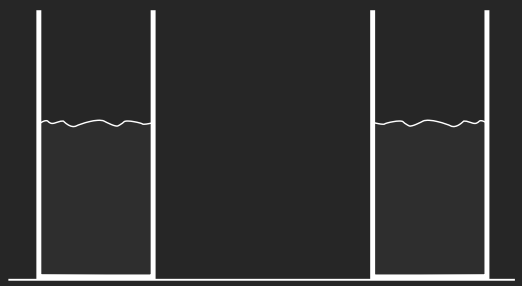
Drinks look equal

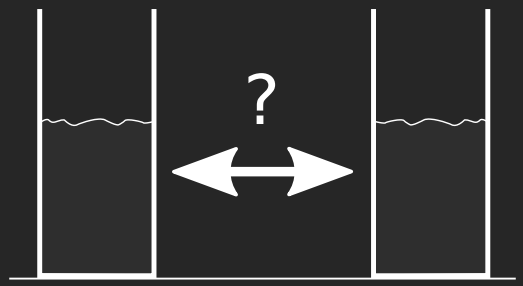
(e.g. Coca Cola / Fritz Cola, French Wine / Californian Wine)

Bob tastes each drink and places them in Alice's right and left hand.

Alice chooses to switch or not switch the cups (secretly).

Bob tastes again and tells Alice if she switched.





Repeating the game: More confidence in Bob's capabilities.

Nuclear Disarmament

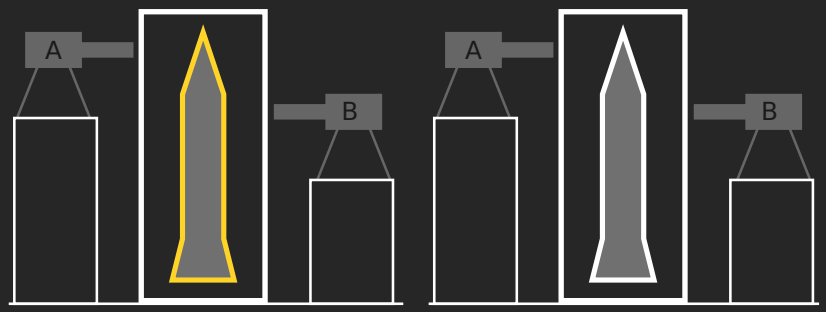
Could be used for the Template approach.

Idea (Glaser et al. 2014)

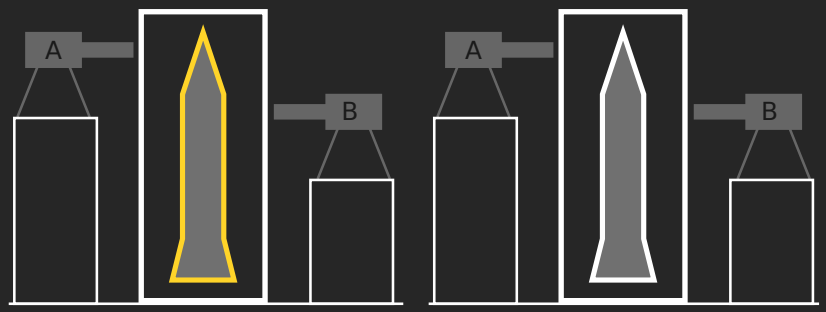
Proof that templates are equal without revealing anything else

- measurement: neutron radiograph
- preload detector with negative image
- preload to match predefined result
- inspector chooses placement of detector on template and item

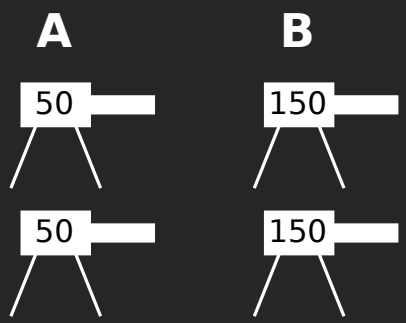
More practical. . .



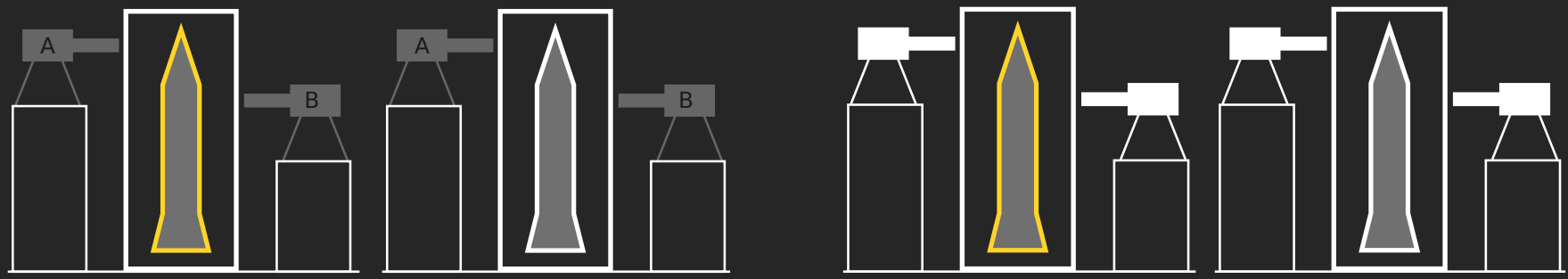
More practical. . .



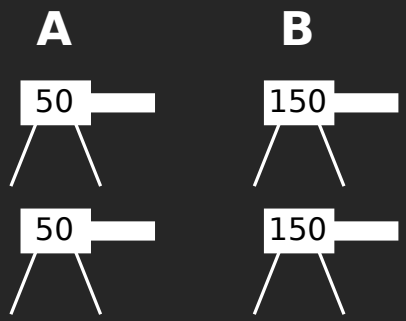
Parties agree on total count (e.g. 200). Host preloads detectors with "negative image".



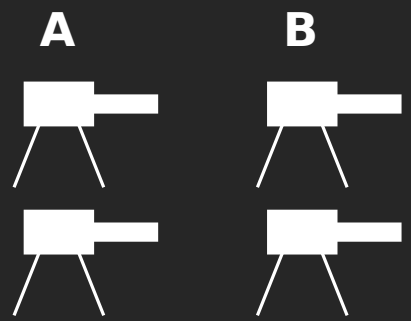
More practical. . .



Parties agree on total count (e.g. 200). Host preloads detectors with "negative image".

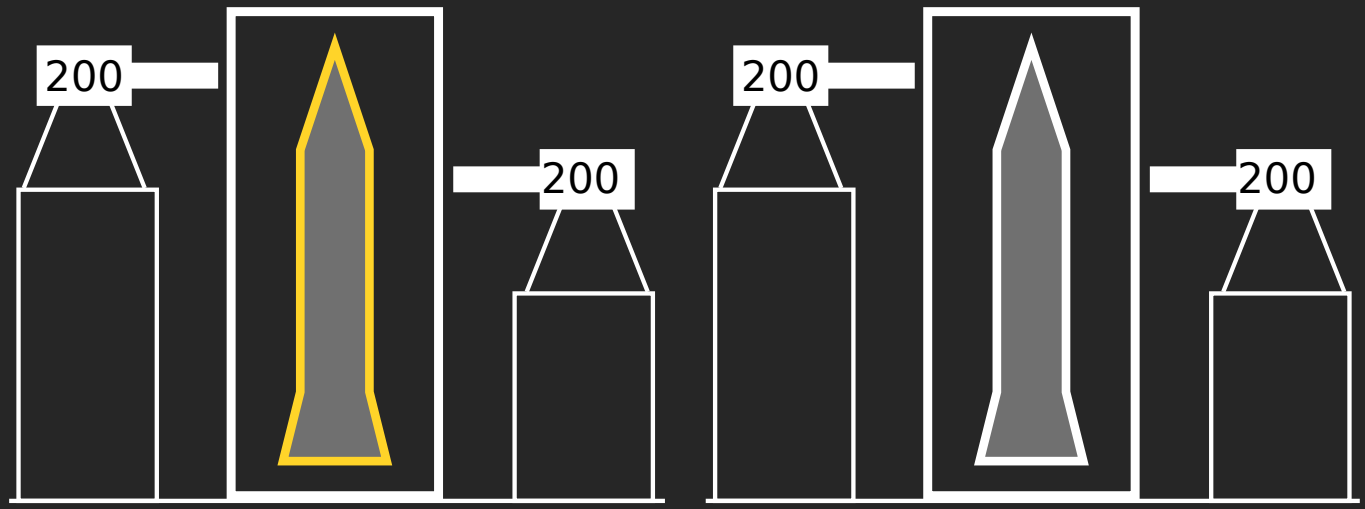


Inspector does not know preload and places detectors randomly (but A to A / B to B).



Result

After measurement, result is revealed to both inspector and host:



Detectors

Detectors could be Non-Electronic Devices

Public Domain - NASA

Current Research

A. Glaser, B. Barak and R. J. Goldston, "A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol", Proceedings of 53rd Annual INMM Meeting, Institute of Nuclear Materials Management, Orlando, Florida, July 15–19, 2012.

A. Glaser, B. Barak and R. J. Goldston. "A zero-knowledge protocol for nuclear warhead verification", *Nature*, 2014, 510, 497-502.

Current Research

A. Glaser, B. Barak and R. J. Goldston, "A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol", Proceedings of 53rd Annual INMM Meeting, Institute of Nuclear Materials Management, Orlando, Florida, July 15–19, 2012.

A. Glaser, B. Barak and R. J. Goldston. "A zero-knowledge protocol for nuclear warhead verification", *Nature*, 2014, 510, 497-502.

Can you imagine to help?

Summary

Nuclear Disarmament has relation to computers & technology.

Summary

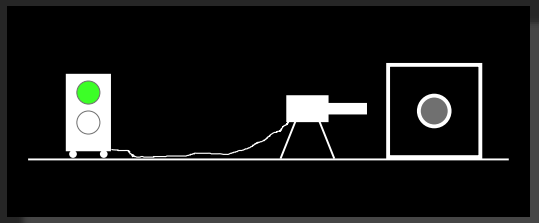
Nuclear Disarmament has relation to computers & technology.

```
while(totalnukes > 0) {
   for(i=1; i<=9; i++) {
      weaponstate[i]->disarm();
   }
}
```

Summary

Nuclear Disarmament has relation to computers & technology.

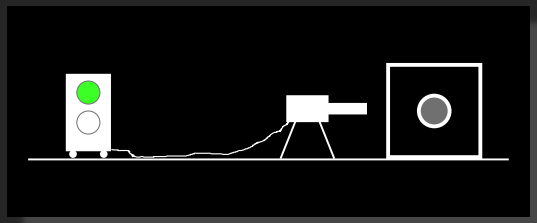
```
while(totalnukes > 0) {
    for(i=1; i<=9; i++) {
        weaponstate[i]->disarm();
    }
}
```

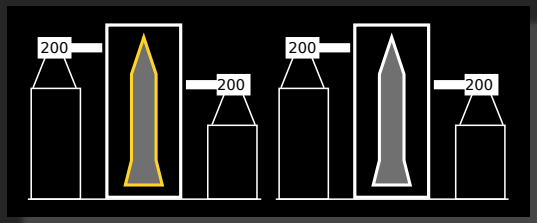


Summary

Nuclear Disarmament has relation to computers & technology.

```
while(totalnukes > 0) {
    for(i=1; i<=9; i++) {
        weaponstate[i]->disarm();
    }
}
```

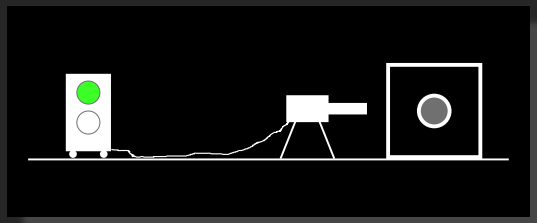


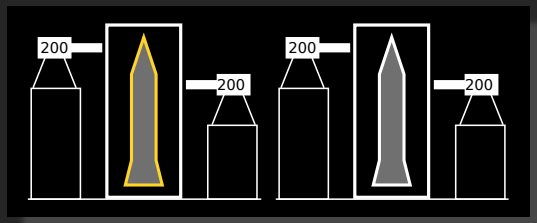


Summary

Nuclear Disarmament has relation to computers & technology.

```
while(totalnukes > 0) {
    for(i=1; i<=9; i++) {
        weaponstate[i]->disarm();
    }
}
```





Not the only tasks

- Virtual Reality for Training / Testing
- Large Sensor Networks
- Whistleblowing
- ...

Thanks for listening!

Contact: moritz@nuclearfreesoftware.org

(and other: ZNF Hamburg, FIfF, local groups...)

Image References 1

In order of appearance, own work not listed

CC-BY-SA Nanking2012 (Arak reactor): Creative Commons-Attribution-Share Alike, Nanking 2012, http://commons.wikimedia.org/wiki/File:Arak_Heavy_Water4.JPG, downloaded 2014-07-16

CC-BY-SA Stefan-XP / Wikimedia Commons (Nuclear Fission): http://commons.wikimedia.org/wiki/File:Kernspaltung.svg, downloaded 2014-08-29

CC-BY-SA Wikimedia Commons (Nuclear chain reaction): http://commons.wikimedia.org/wiki/File:Kettenreaktion.svg, downloaded 2014-08-29

Public Domain / Wikimedia Commons - modified (Gun-type weapon): http://en.wikipedia.org/wiki/File:Fission_bomb_assembly_methods.svg, downloaded 2014-08-18

Public Domain / Wikimedia Commons - modified (Implosion type weapon): http://en.wikipedia.org/wiki/File:Implosion_nuclear_weapon_design_-_shock_waves.svg, downloaded 2014-08-29

CC-BY-SA Sajak (AfE Tower Blasting), Sven-Sebastian Sajak, http://upload.wikimedia.org/wikipedia/commons/2/23/140202_Afe-Tower_Blasting.jpg, downloaded 2014-08-25

CC-BY-SA Robock et. al 2007 (Nuclear Winter), Robock, A.; Oman, L.; Stenchikov, G. L.; Toon, O. B.; Bardeen, C. and Turco, R. P. Climatic consequences of regional nuclear conflicts - Figure 5 Atmospheric Chemistry and Physics, 2007, 7, 2003-2012. (http://www.atmos-chem-phys.net/7/2003/2007/, downloaded 2014-08-28).

CC-BY-SA Stahlkocher (Airbase Büchel), http://commons.wikimedia.org/wiki/File:B%C3%BCchel_Fliegerhorst.jpg, downloaded 2014-09-01.

Public Domain, U.S. DoD (B61 bombs), United States Department of Defense (SSGT Phil Schmitten), http://de.wikipedia.org/wiki/Datei:B-61_bomb_rack.jpg, downloaded 2014-08-22.

CC-BY-NC IPFM, Global Fissile Material Report 2009, International Panel on Fissile Materials, Princeton, 2009, p. 67.

Image References 2

Public Domain - FSF (Free Software Foundation Logo), http://commons.wikimedia.org/wiki/File:Free_Software_Foundation_logo_and_wordmark.svg, **downloaded 2014-07-07**.

CC-BY-SA NicoBZH (portrait of Richard Stallman), **NicoBZH from Saint Etienne - Loire**, **France**, http://commons.wikimedia.org/wiki/File:NicoBZH_-_Richard_Stallman_%28by-sa%29_%285%29.jpg, **downloaded 2014-07-07**.

CC-BY Open Source Initiative (OSI Logo), http://commons.wikimedia.org/wiki/File:Opensource.svg, **downloaded 2014-07-07**.

CC-BY-SA Manon Anne Ress (portrait of Bruce Perens): http://commons.wikimedia.org/wiki/File:Bruce_perens_13jan09_tacd_MAR_1557x1188.JPG, **downloaded 2014-07-07**.

Public Domain - U.S. DoE NNSA (Warhead Measurement Campaing), **U.S. Department of Energy - National Nuclear Security Administration**, http://nnsa.energy.gov/sites/default/files/imagecache/feature_photo_689w_249h/nnsa/09-13-featurephoto/2013-09-30%20na22%203%20topline.PNG, **downloaded 2014-09-01**.

CC-BY-SA Cowjuice - Wikimedia Commons (Raspberry Pi), http://commons.wikimedia.org/wiki/File:Raspberry_Pi_Photo.jpg, **downloaded 2014-09-01**.

Public Domain - NASA (Bubble Detectors), http://www.nasa.gov/images/content/715781main_vial_XL.jpg, **downloaded 2014-08-29**.

Effects of a nuclear explosion

Thermal radiation

"Spontaneous" ignition of items, firestorm, burns.

Blast / pressure wave

Destruction of buildings and debris production.
Similar to conventional weapons, but more intense.

Radiation (direct / indirect)

Direct radiation from neutron / gamma emitted in reaction.
Indirect radiation (later) from activated debris.

Effects of nuclear weapons

Footage:
US test series: Upshot-Knothole
March 17, 1953
Explosion Annie (on tower)

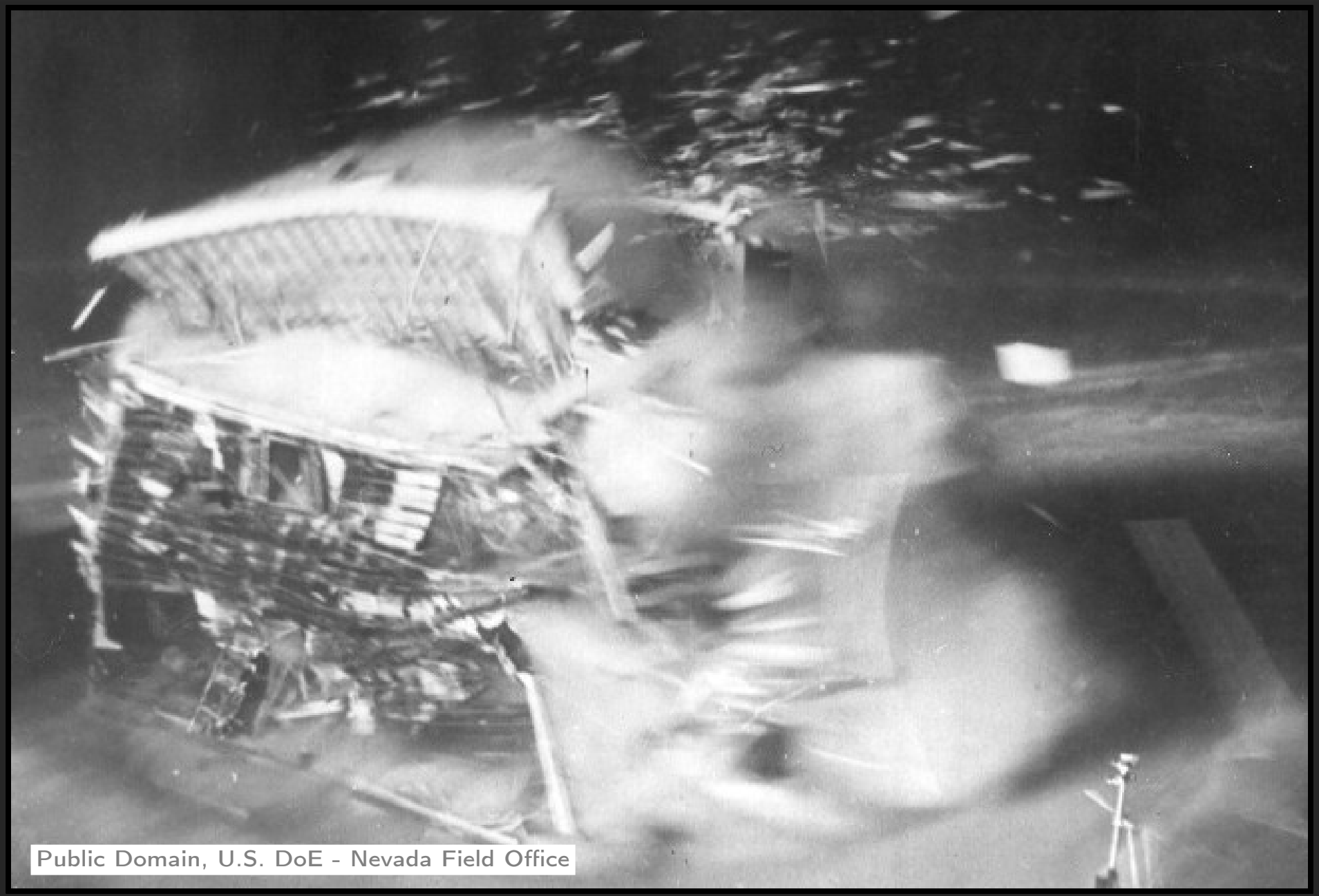

Public Domain, U.S. DoE - Nevada Field Office


Public Domain, U.S. DoE - Nevada Field Office

Public Domain, U.S. DoE - Nevada Field Office

Public Domain, U.S. DoE - Nevada Field Office

Public Domain, U.S. DoE - Nevada Field Office


Public Domain, U.S. DoE - Nevada Field Office


Public Domain, U.S. DoE - Nevada Field Office

Public Domain, U.S. DoE - Nevada Field Office

Examples for Software Use

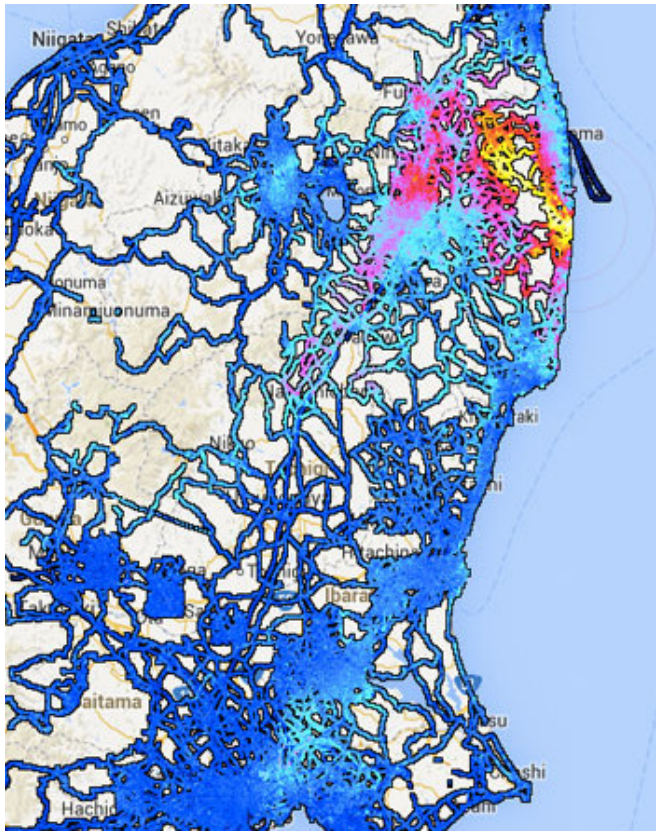
	Non-Proliferation / Safeguards	**Fissile Material Cutoff Treaty**	**Nuclear Disarmament Agreement**
Particle Transport (Stochastic/ Deterministic)	Development of NDA methods for fresh/spent fuel analysis	Development of NDA methods for material analysis	Development of NDA methods for warhead authentication
Depletion Calculations	Proliferation potential of reactors	Estimate past/current fissile material production capabilities	Fission product tagging for warhead identification
Spectrum Analysis	Identify items (spent/fresh fuel), determine material compositions	Identify items (spent/fresh fuel), determine material compositions	Identify items (warheads) and respective material compositions

(Extensive table in M. Kütt, A. Glaser, M. Englert: Open Source meets Nuclear Arms Control, in proceedings of 55th Annual INMM Meeting, Atlanta, GA, 21-24 July 2014)

Safecast

bGeigie nano

CC-BY Safecast



Measurements in Japan

CC-BY Safecast

Appendix Image References

Public Domain - U.S. DoE Nevada Field Office (Test Upshot-Knothole),
http://www.nv.doe.gov/library/photos/upshot.aspx, **downloaded 2013-08-10**.

CC-BY Safecast (bGeigie nano): **Creative Commons-Attribution**, **Safecast Project**,
http://blog.safecast.org/wp-content/uploads/2013/03/IMG_0009.jpeg, **downloaded 2014-07-25**.

CC-BY Safecast (Japan Map): **Creative Commons-Attribution**, **Safecast Project**,
http://blog.safecast.org/wp-content/uploads/2014/05/980x480.jpg, **downloaded 2014-07-25 (cutout)**.