Onion and Swiss Cheese Security Revisited

Jerry Kott, OSCP

image-ware.com/static/esug2019.pdf

Why Revisit?

Security is an Infinite Game

Quizz: what is CIA?

Quizz: what is CIA?

Confidentiality

Integrity

Availability

Three pillars of Information Security

Confidentiality

Integrity

Availability

Big Picture: 1980s

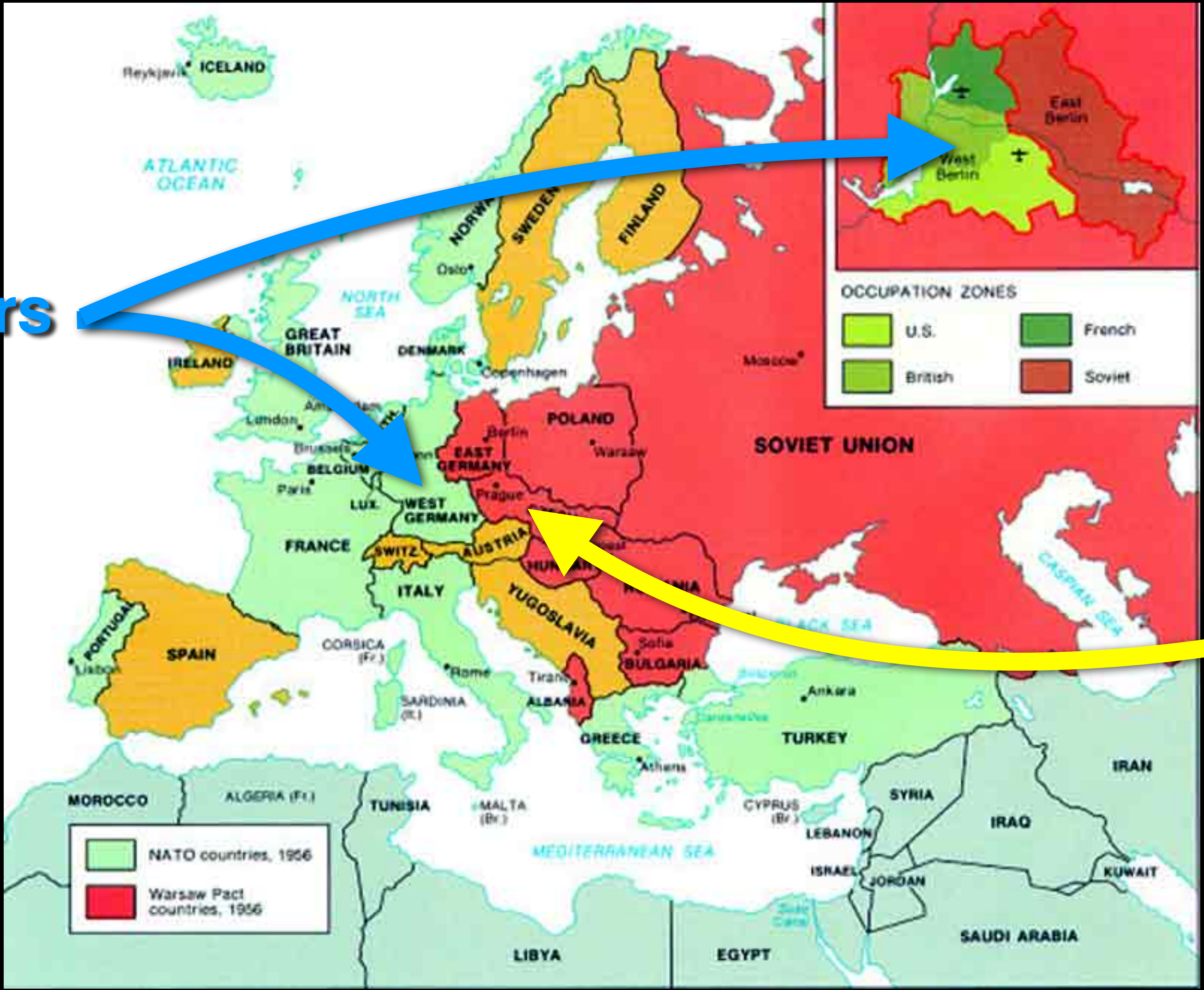


image-ware.com

Big Picture: 1980s

1981

image-ware.com

Big Picture: 1980s

1983

Big Picture: 1980s

1985

Big Picture: 1980s

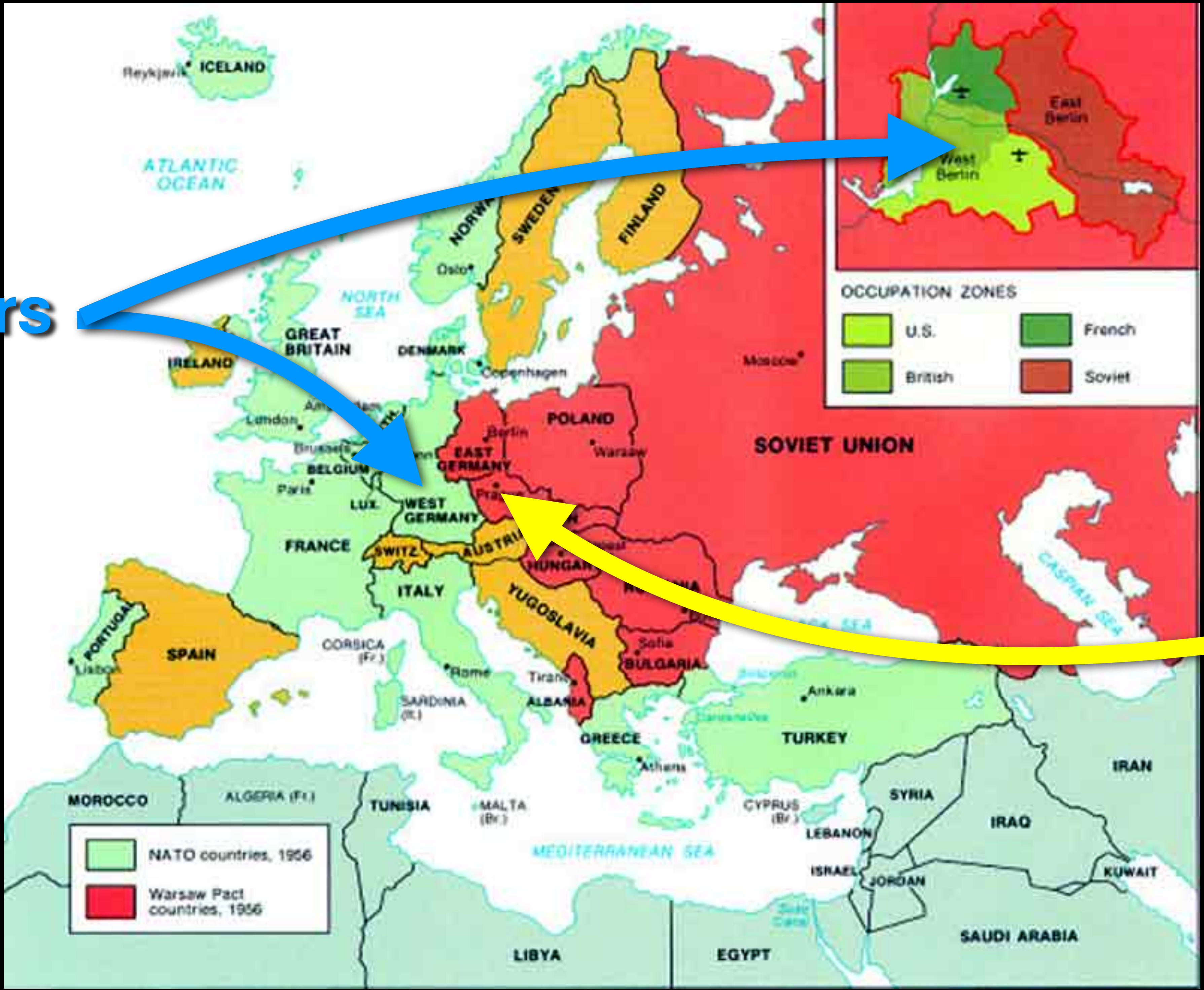


image-ware.com

Big Picture: 1980s

1986

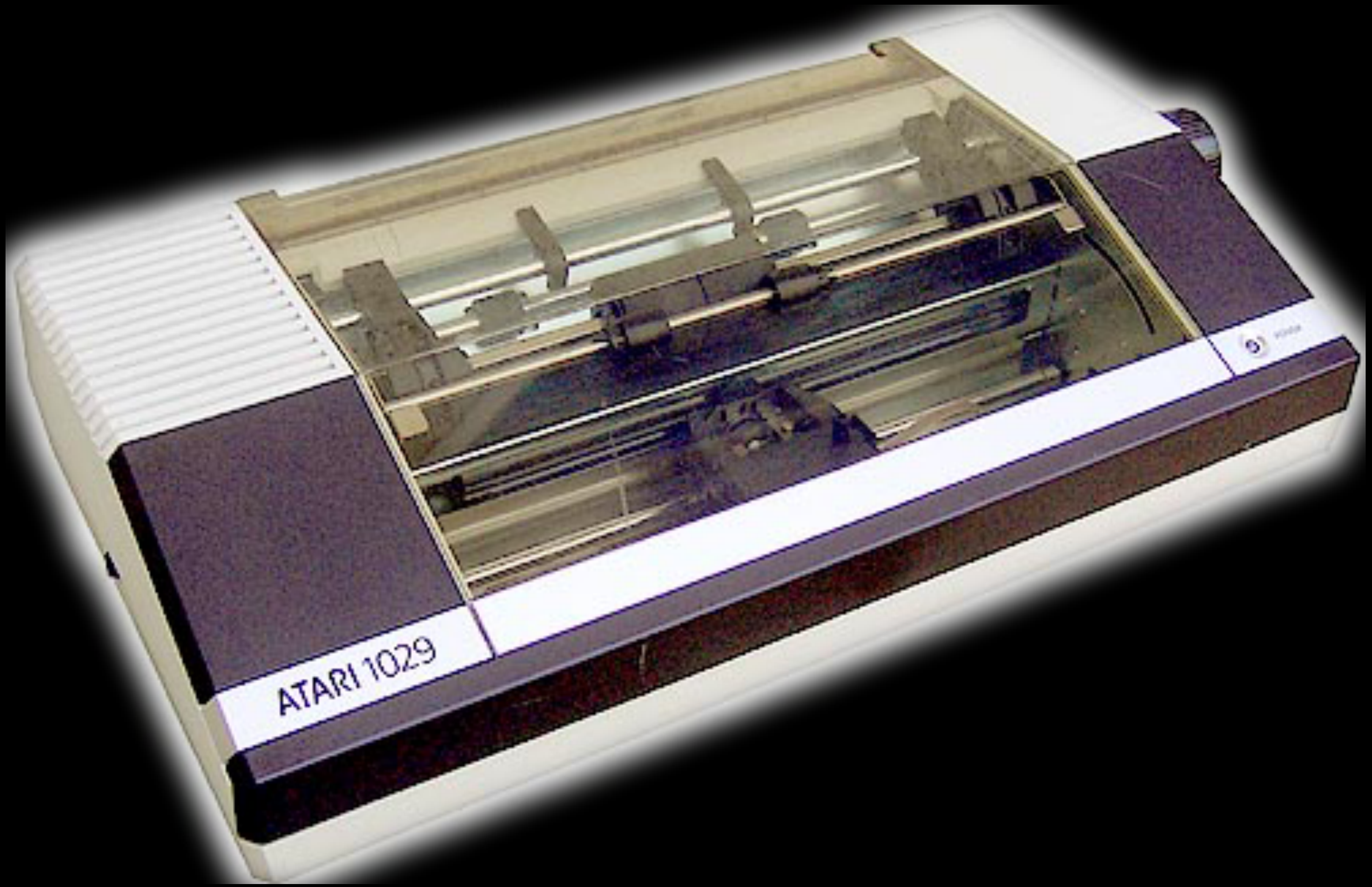
image-ware.com

Big Picture: 1980s

1986

Big Picture: 1980s

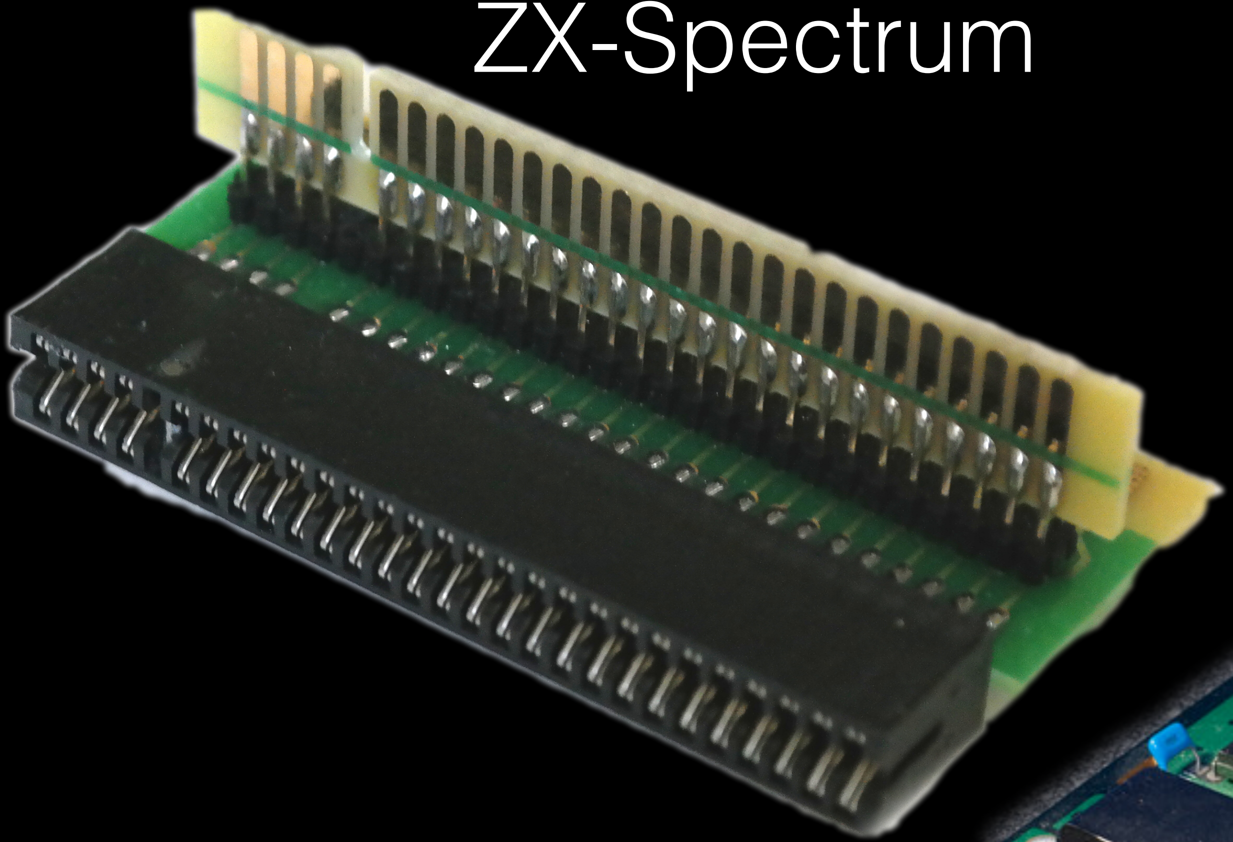
1987



Big Picture: 1980s

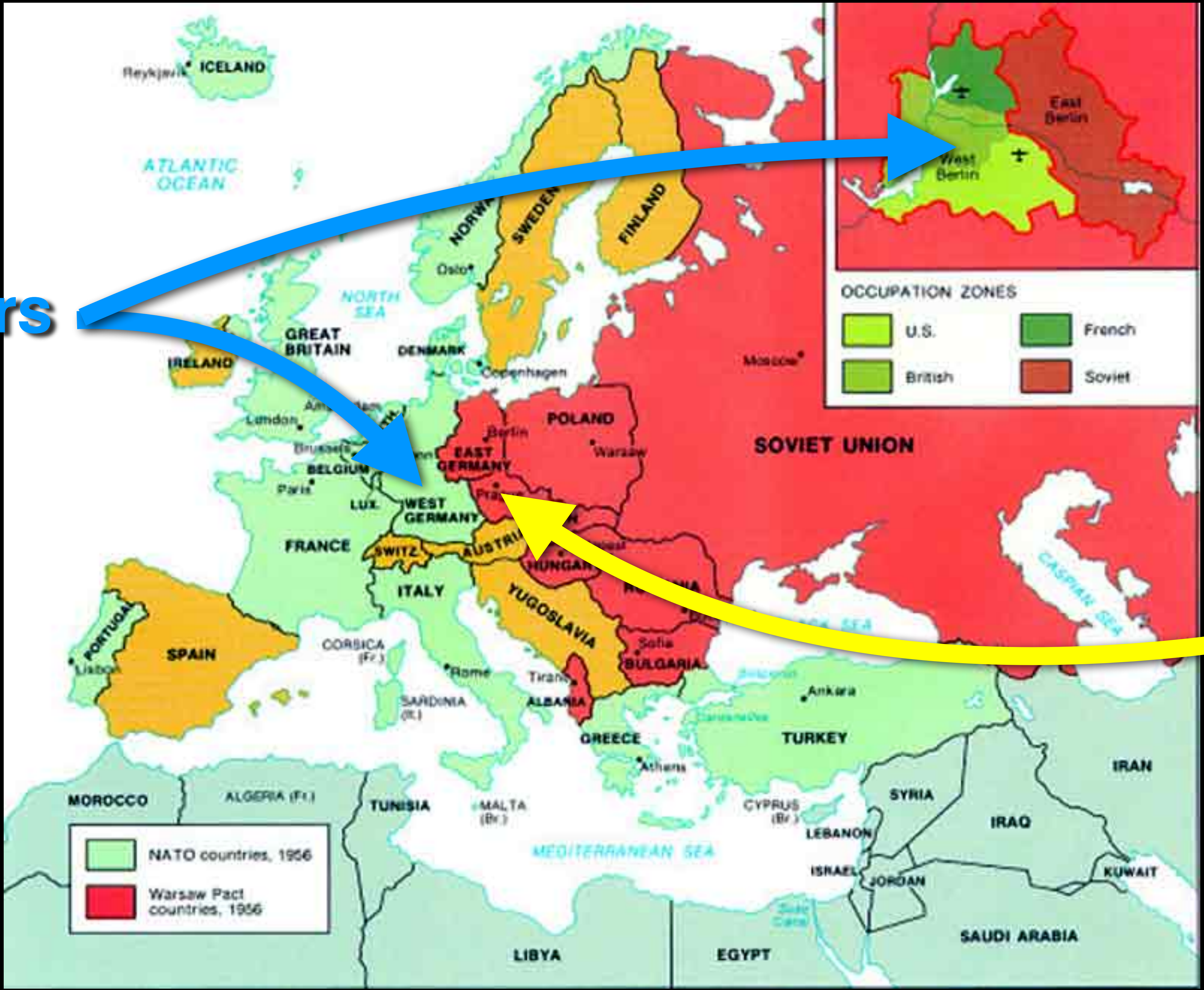
ZX-Spectrum

1987



Atari

Take it back to the store



Take it back to the store

or…

- Learn Z-80 Assembler
- Solder some components together
- Reverse Engineer
- Roll your own driver

1988 - still

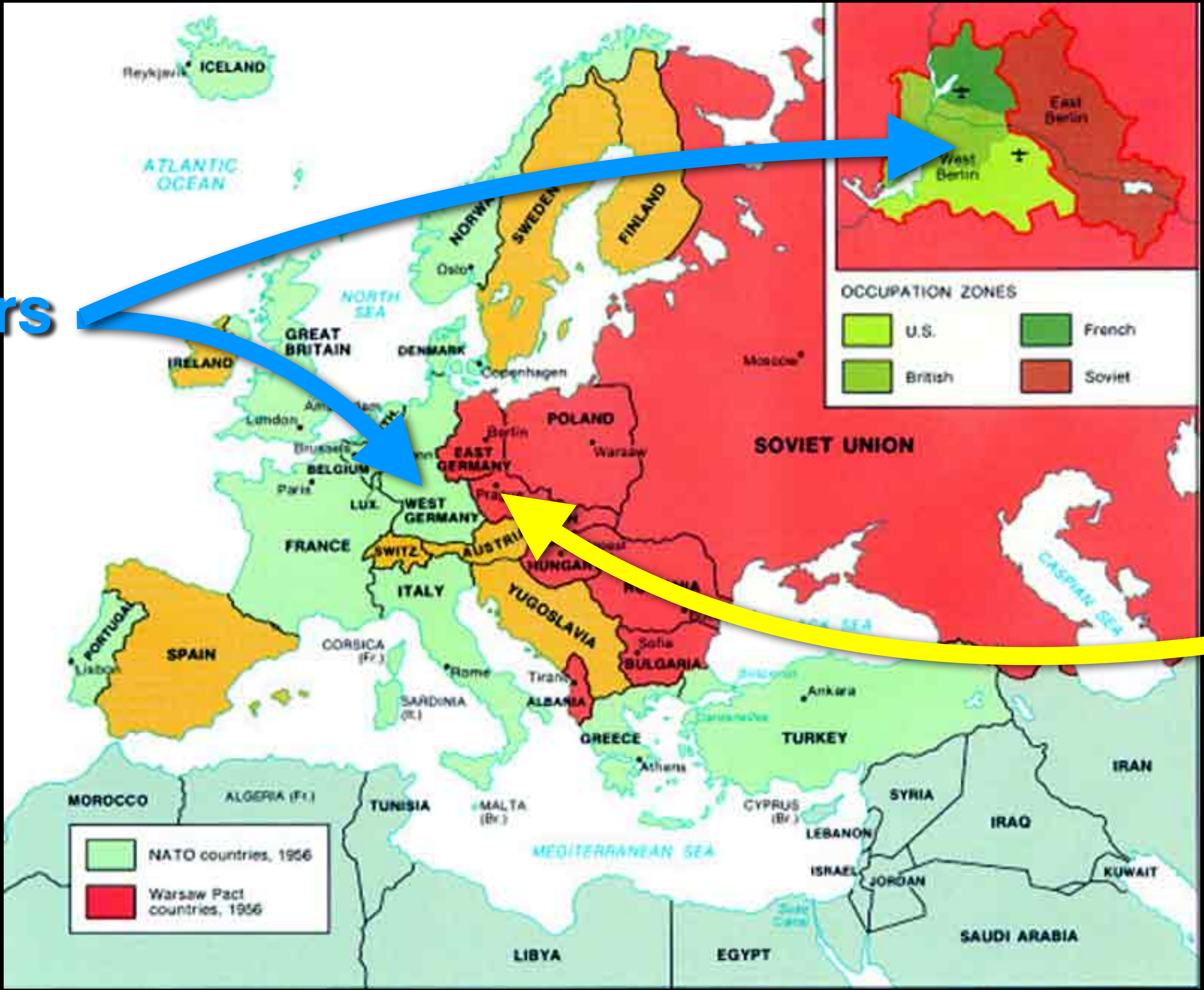


image-ware.com

1988

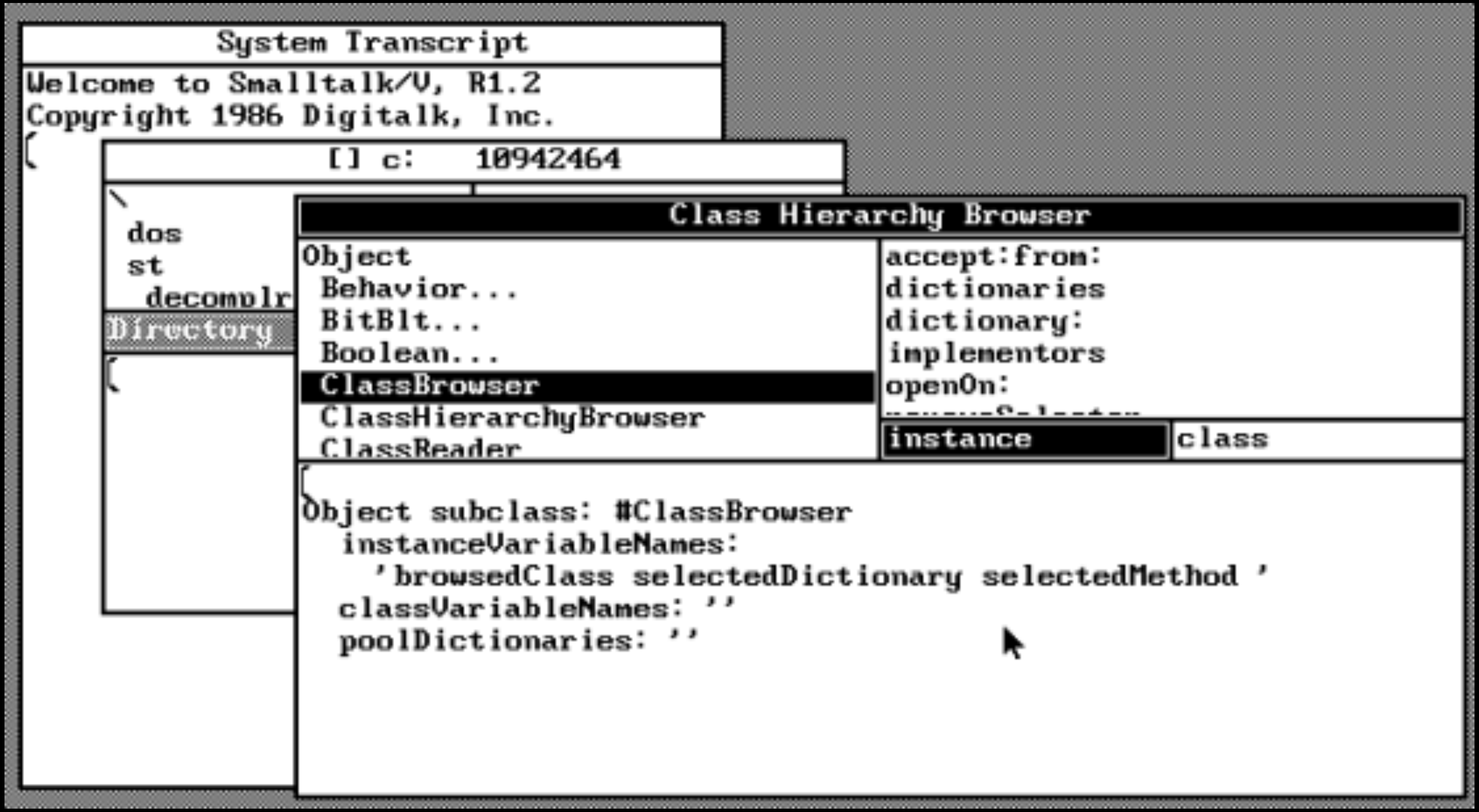
ACHTUNG!
SIE VERLASSEN
JETZT
WEST BERLIN

YOU ARE LEAVING
THE AMERICAN SECTOR
ВЫ ВЫЕЗЖАЕТЕ ИЗ
АМЕРИКАНСКОГО СЕКТОРА
VOUS SORTEZ
DU SECTEUR AMÉRICAIN
SIE VERLASSEN DEN AMERIKANISCHEN SEKTOR
US ARMY
Zimmerstraße

1988

- My first **real** computer
  - PC-compatible
  - 256 K RAM
  - Dual floppy disk
  - 20 MB HDD
  - Woo-hoo!

1988



```
System Transcript
Welcome to Smalltalk/V, R1.2
Copyright 1986 Digitalk, Inc.

[] c:   10942464
\
 dos
 st
  decomplr
Directory

Class Hierarchy Browser
Object
 Behavior...
 BitBlt...
 Boolean...
 ClassBrowser
 ClassHierarchyBrowser
 ClassReader

accept:from:
dictionaries
dictionary:
implementors
openOn:

instance    class

Object subclass: #ClassBrowser
  instanceVariableNames:
    'browsedClass selectedDictionary selectedMethod '
  classVariableNames: ''
  poolDictionaries: ''
```

image-ware.com

Life Is Great !

Meanwhile…

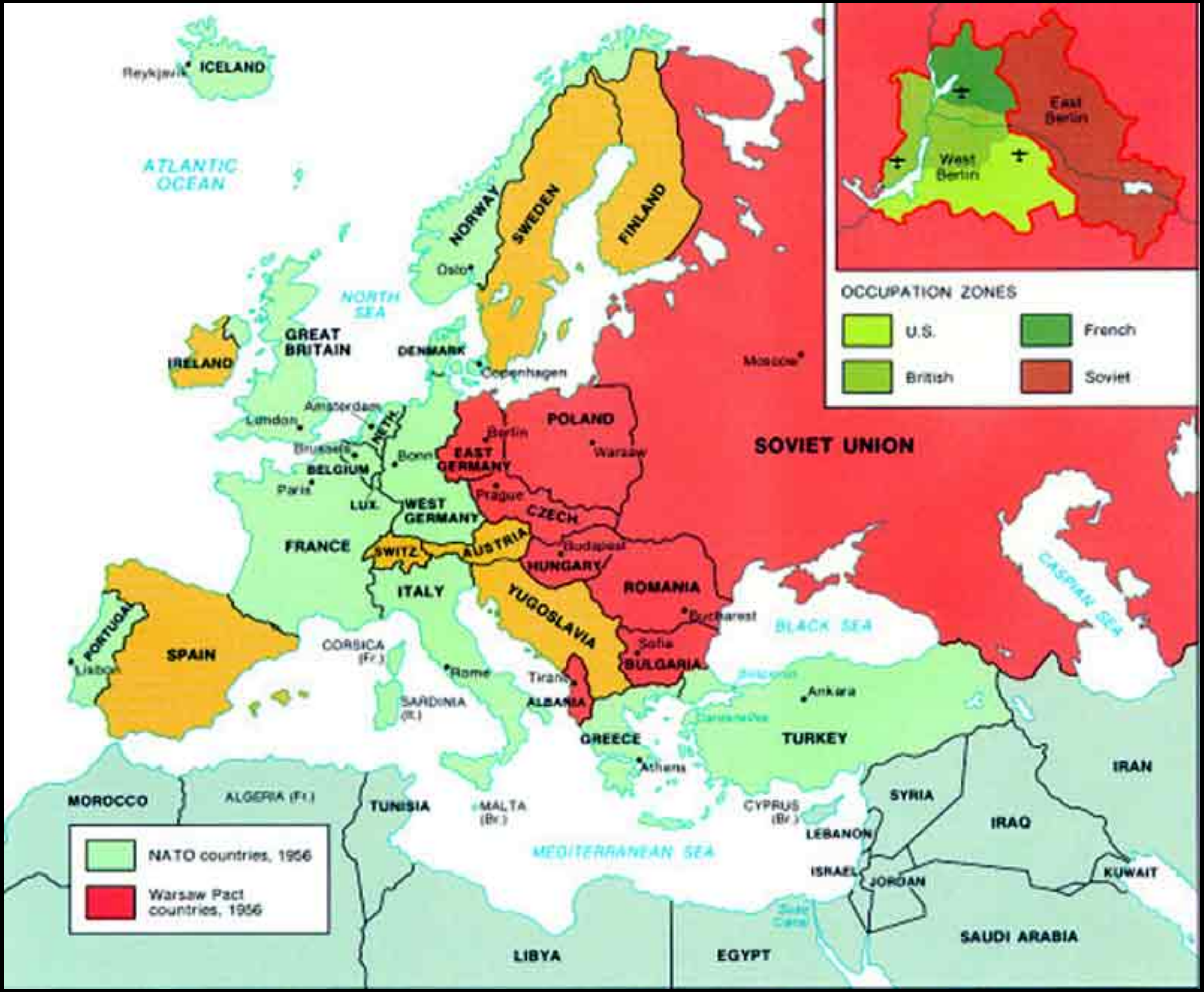


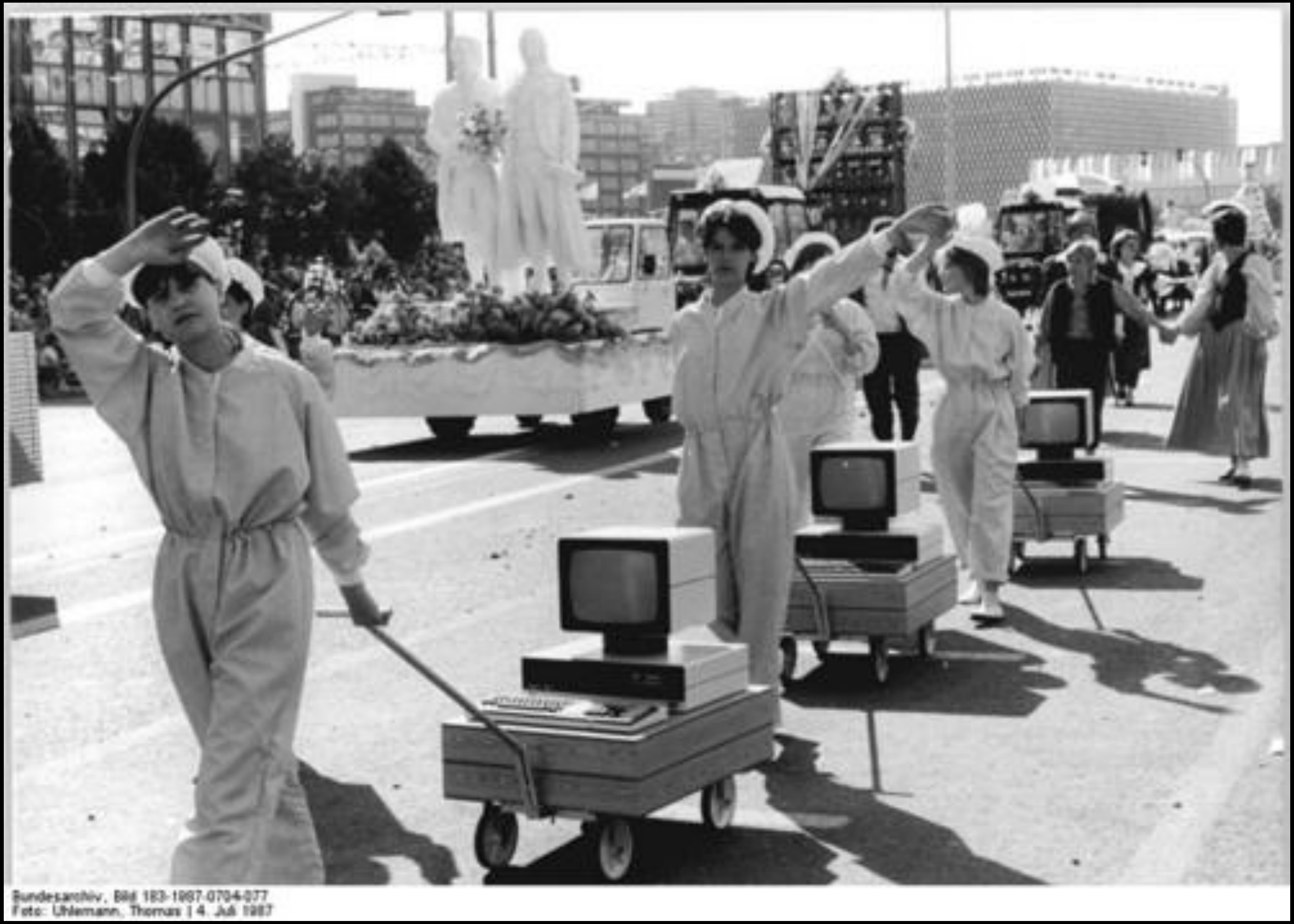
image-ware.com

East Germany, 1987

East Germany, 1987

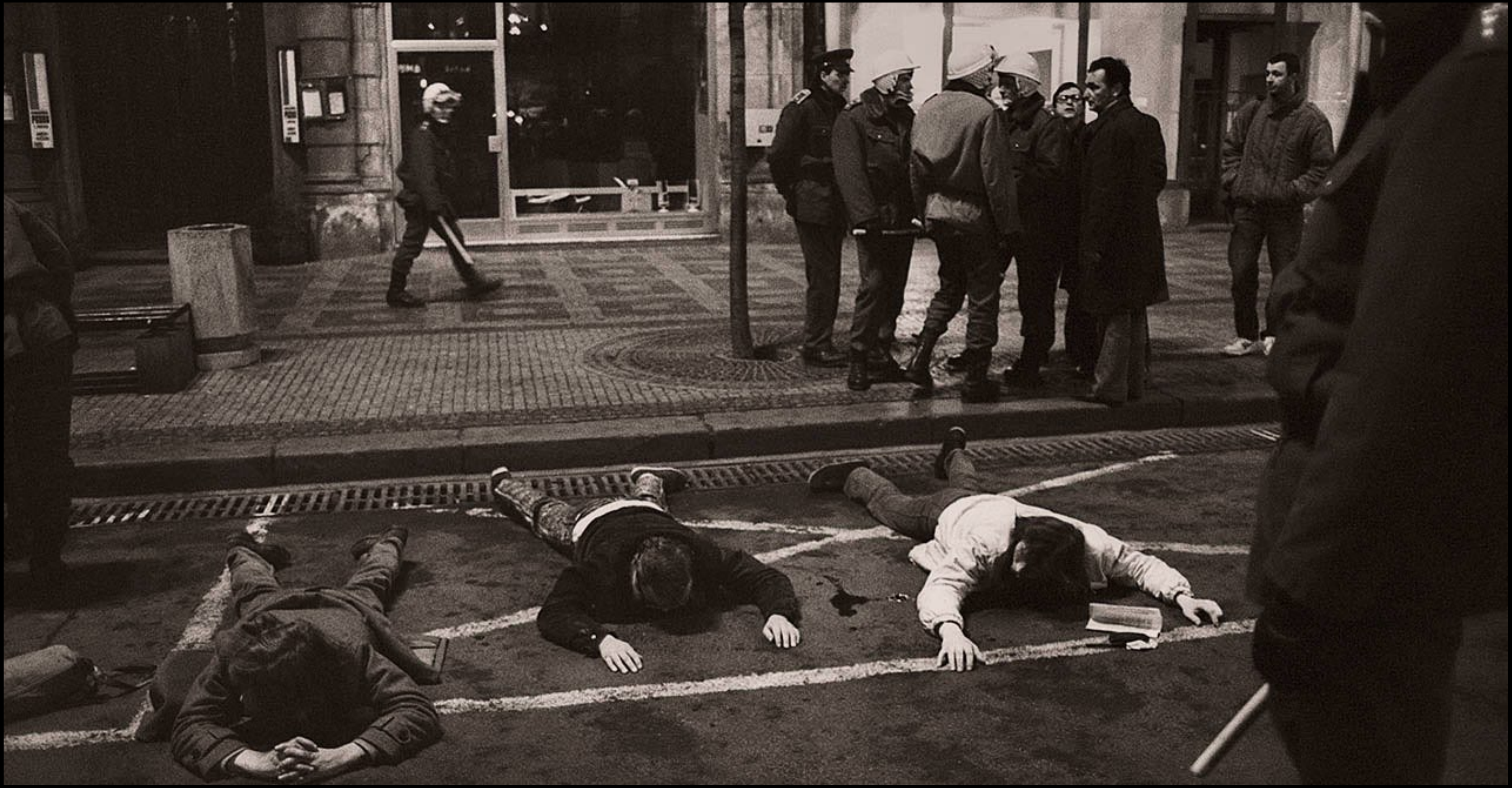
Honecker: Mauer bleibt noch 100 Jahre
Freitag, 20. Januar 1989 · 50 Pf
Skandal
DIE GEGENWART gehört dem KAMPF
WIR LEBEN

East Germany, 1987

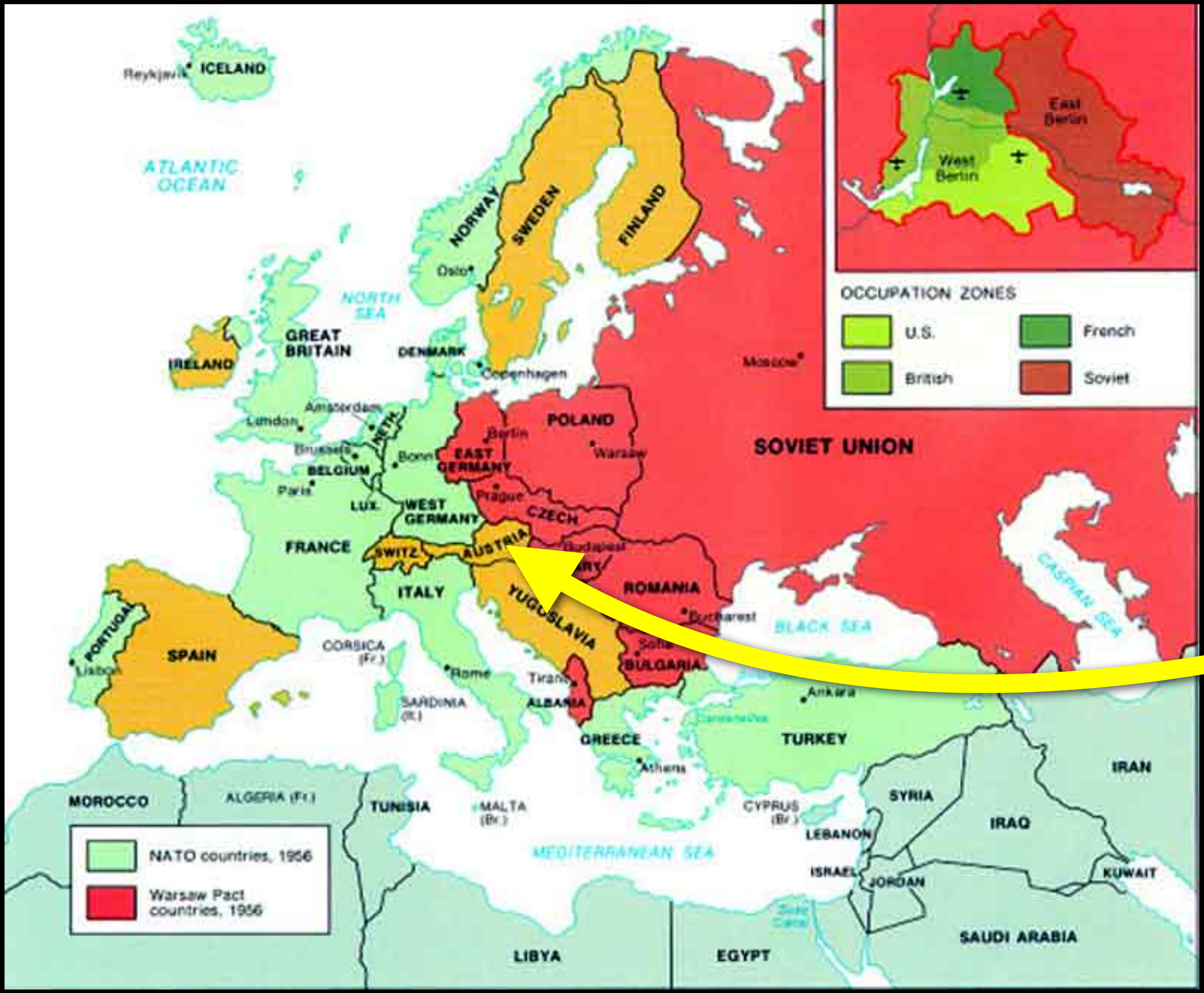

Bundesarchiv, Bild 183-1987-0704-077
Foto: Uhlemann, Thomas | 4. Juli 1987

Czechoslovakia, 1988

Czechoslovakia January 1989



Summer 1989

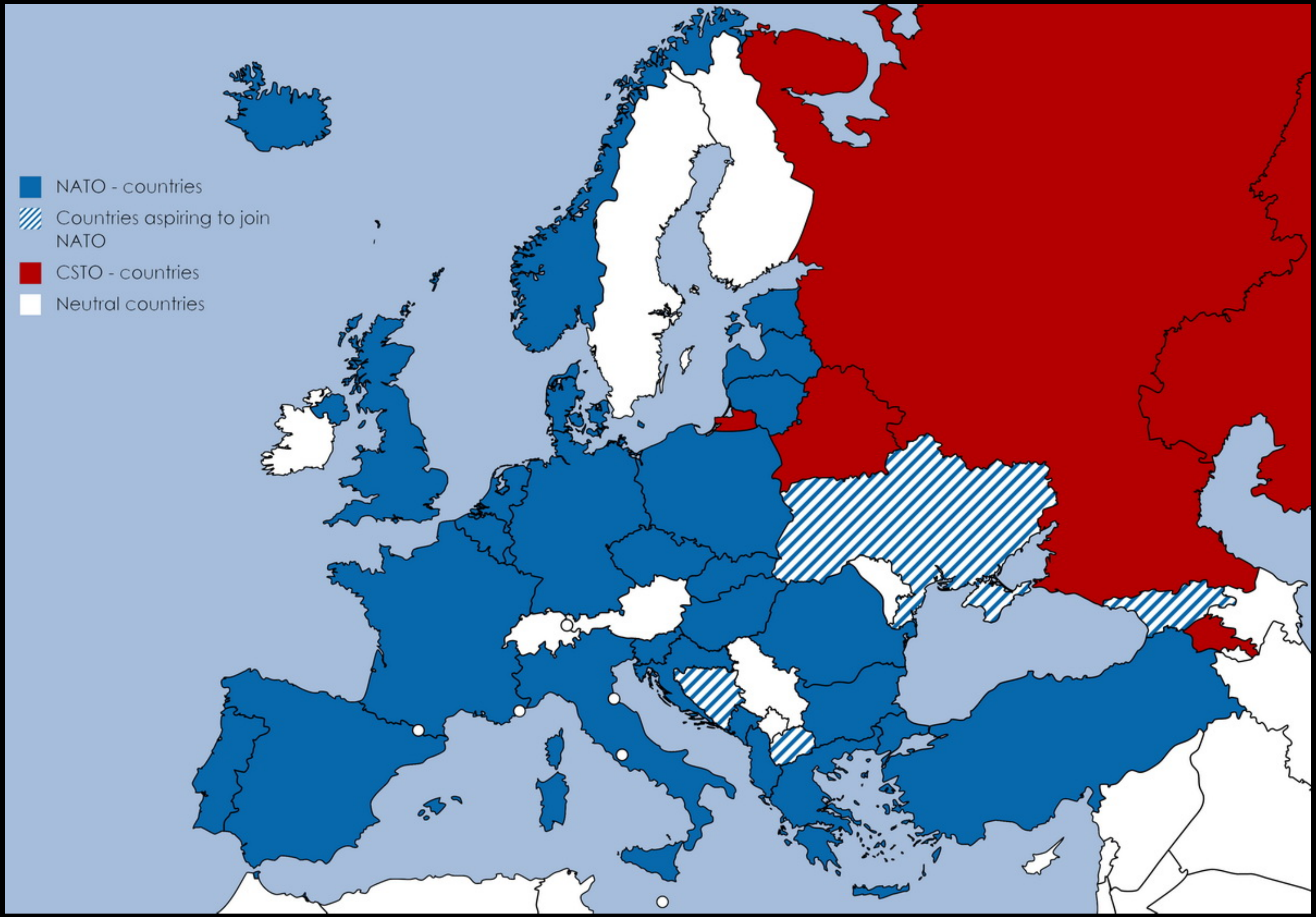


ICELAND
Reykjavik
ATLANTIC OCEAN
NORWAY
SWEDEN
FINLAND
Oslo
NORTH SEA
GREAT BRITAIN
IRELAND
DENMARK
Copenhagen
Moscow
SOVIET UNION
POLAND
Warsaw
Berlin
EAST GERMANY
WEST GERMANY
Bonn
Amsterdam
London
NETH.
Brussels
BELGIUM
Paris
LUX.
FRANCE
SWITZ.
AUSTRIA
Prague
CZECH
Budapest
ROMANIA
Bucharest
BLACK SEA
CASPIAN SEA
YUGOSLAVIA
BULGARIA
Sofia
ITALY
Rome
CORSICA (Fr.)
SARDINIA (It.)
SPAIN
PORTUGAL
Lisbon
Tirana
ALBANIA
GREECE
Athens
TURKEY
Ankara
IRAN
MOROCCO
ALGERIA (Fr.)
TUNISIA
MALTA (Br.)
CYPRUS (Br.)
SYRIA
IRAQ
LEBANON
ISRAEL
JORDAN
KUWAIT
SAUDI ARABIA
LIBYA
EGYPT
MEDITERRANEAN SEA
East Berlin
West Berlin
OCCUPATION ZONES
U.S.
French
British
Soviet
NATO countries, 1956
Warsaw Pact countries, 1956
Me

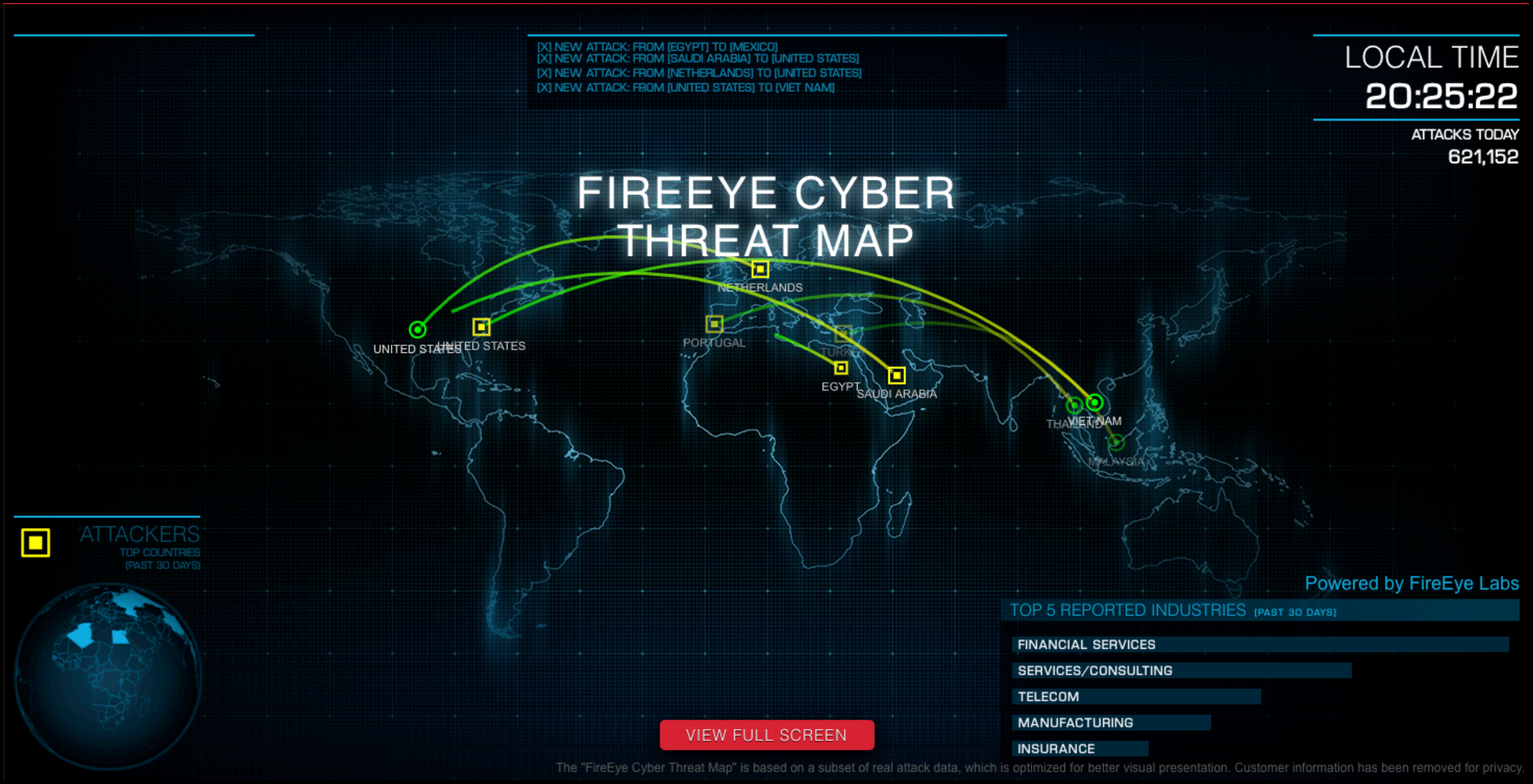
November 1989

- Berlin Wall Falls
- Velvet Revolution in Czechoslovakia
- Soviet communism collapses in Eastern Europe

FF >> 30 years


NATO - countries
Countries aspiring to join NATO
CSTO - countries
Neutral countries

FF >> 30 years


[X] NEW ATTACK: FROM [EGYPT] TO [MEXICO]
[X] NEW ATTACK: FROM [SAUDI ARABIA] TO [UNITED STATES]
[X] NEW ATTACK: FROM [NETHERLANDS] TO [UNITED STATES]
[X] NEW ATTACK: FROM [UNITED STATES] TO [VIET NAM]

LOCAL TIME 20:25:22

ATTACKS TODAY 621,152

TOP 5 REPORTED INDUSTRIES [PAST 30 DAYS]

- FINANCIAL SERVICES
- SERVICES/CONSULTING
- TELECOM
- MANUFACTURING
- INSURANCE

The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy.

https://www.fireeye.com/cyber-map/threat-map.html

The Points…

- Geopolitics tends to shape careers (more so in authoritarian states)
- Motivation matters
- Hackers go where the action is (HW, SW, data)
- Always look at things from the ‘other side’

The Points…

- Even the most powerful systems are vulnerable on multiple fronts - a large attack surface
- Reality doesn't care about what you think or wish
- Denial of a problem won't make it go away
- "*I don't know*" - admission of own ignorance leads to a path of discovery

Hacker’s best friends

- google.com
- kali.org
- exploitdb.com
- shodan.io

Hacker's best friends

- Imagination
- Creativity
- Perseverance
- Ignorance
- Gullibility

The metaphors

- Onion
  - Layers of security
  - The best stuff is at the centre

- Swiss Cheese
  - Holes (bubbles) are vulnerabilities
  - Breaches happen when cheese is sliced and holes are aligned to allow penetration of multiple layers

The metaphors

- Onion
  - Layers of security
  - The best stuff is at the centre

- Swiss Cheese
  - Holes (bubbles) are vulnerabilities
  - Breaches happen when cheese is sliced and holes are aligned to allow penetration of multiple layers

The metaphors

- Approximations
- Very useful
- Not quite accurate

To Understand Security

- Understand **Risk**
  (*Probability* that a *Threat* will exploit a *Vulnerability* to cause harm to an *Asset*)
- Understand **Behaviour** of
  - Threats (hackers, malware, nature)
  - Assets (employees, systems, applications)

To Understand Behaviour

- Study and analyze the **PAST**
- Observe the **PRESENT**
- **Imagine** the **FUTURE**

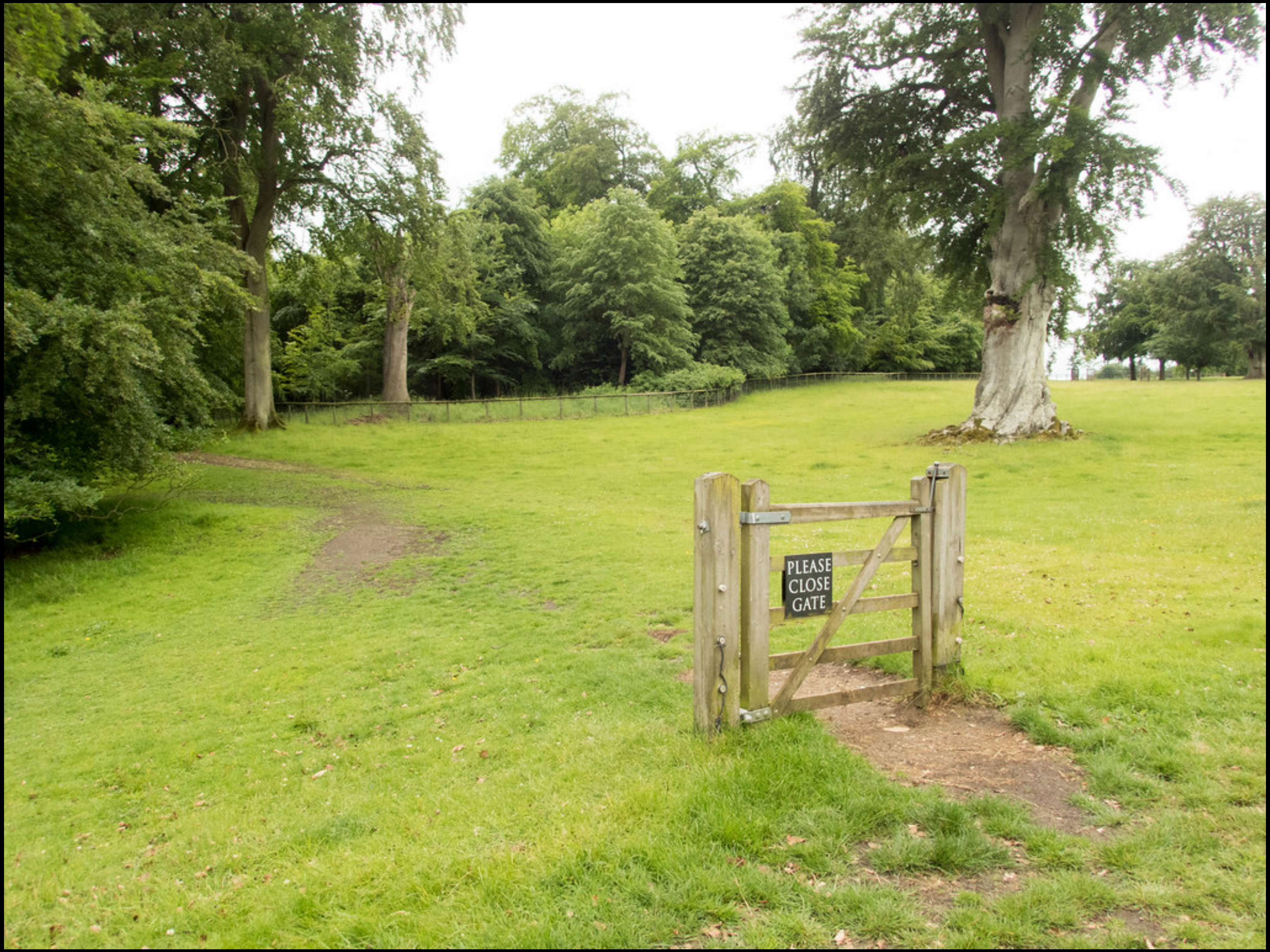
Imagining Behaviour

Failure of Imagination

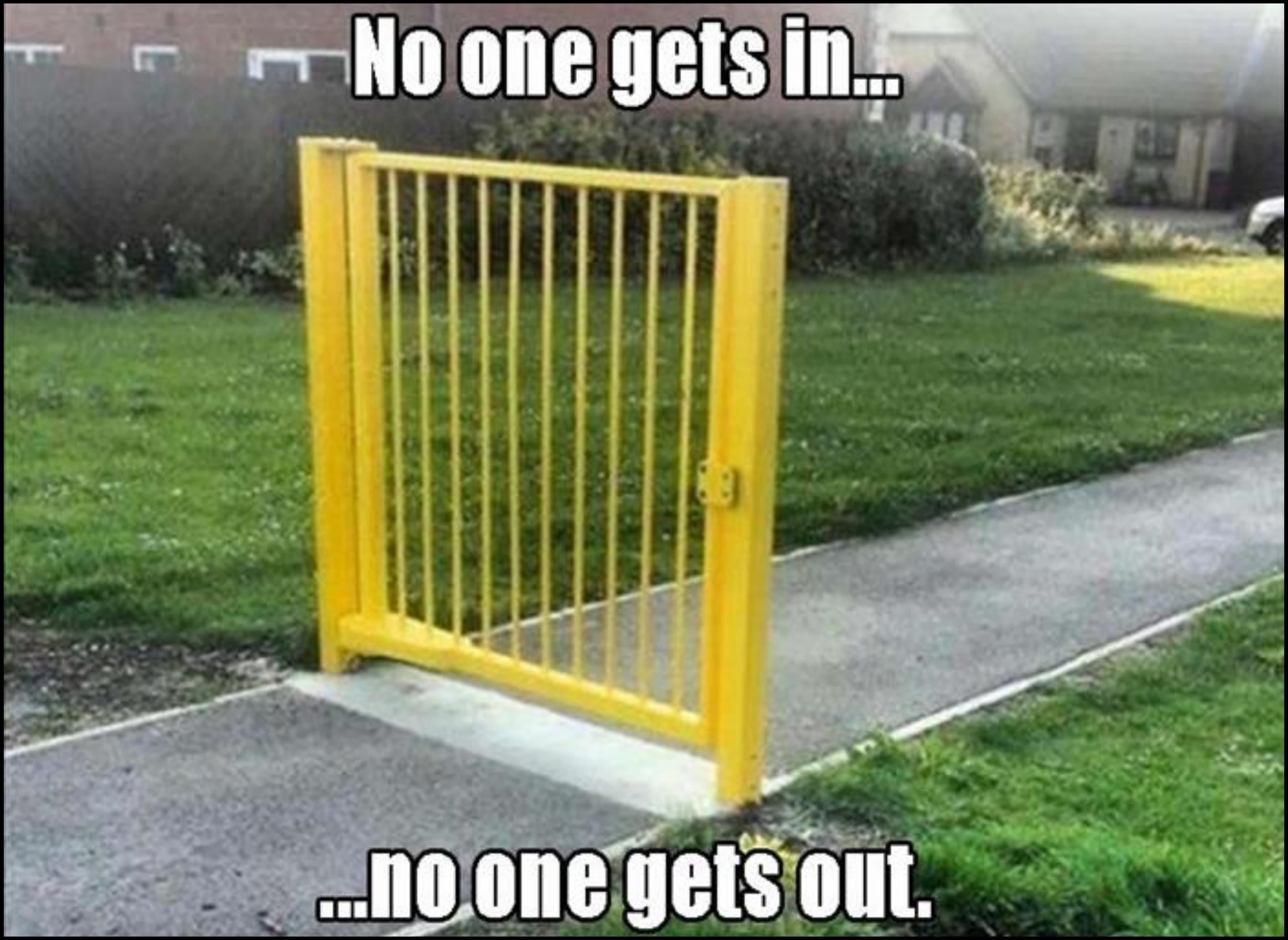
Failure of Imagination

- The expectation that current and future opportunities and risks will resemble the past.
- Major failures of risk management and strategy based on static, unimaginative and reactive thinking.
- "*This would never happen here*"
- "*It looked like such a clever idea at the time*"
- "*I have nothing to hide*"

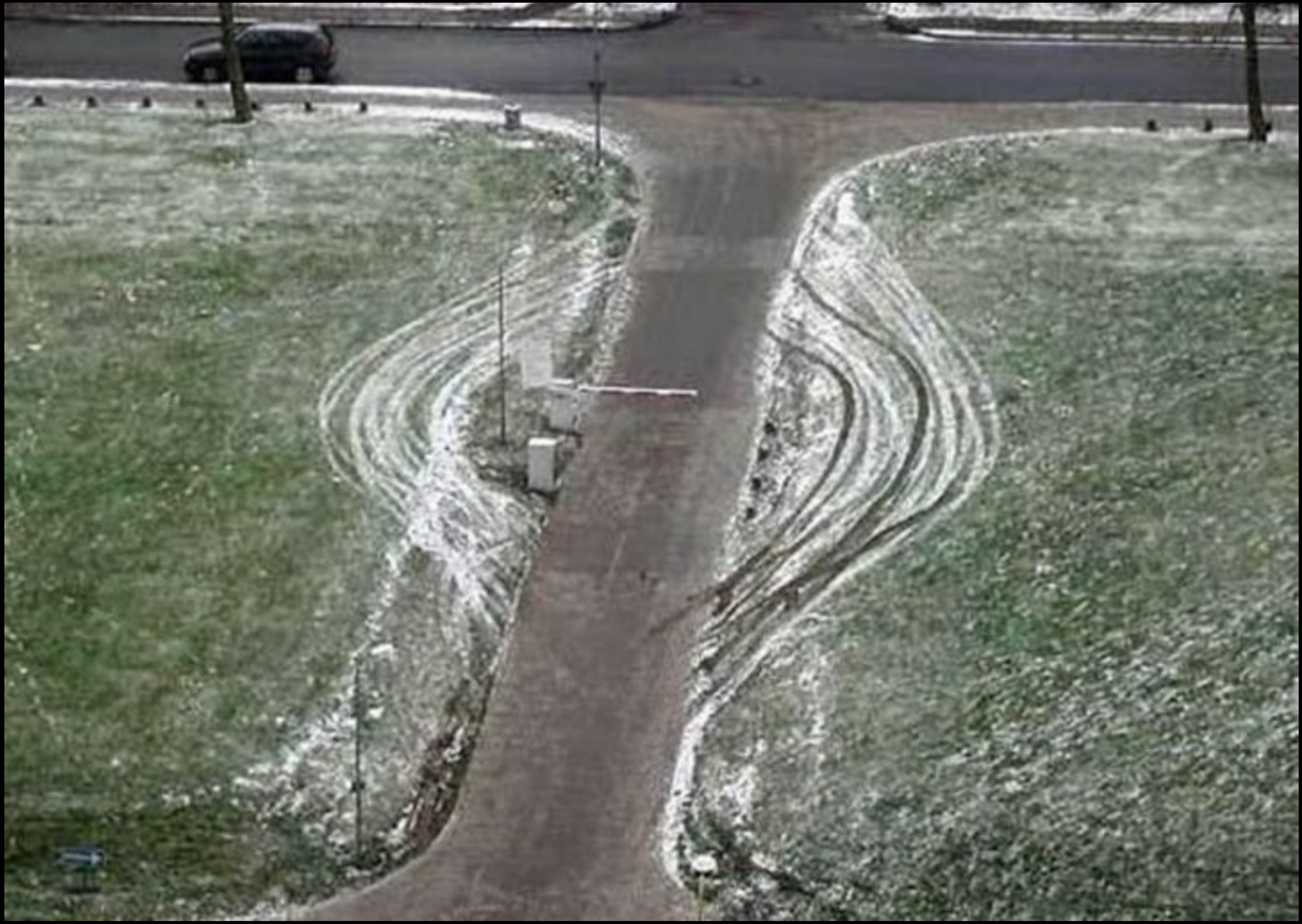
Failure of Imagination



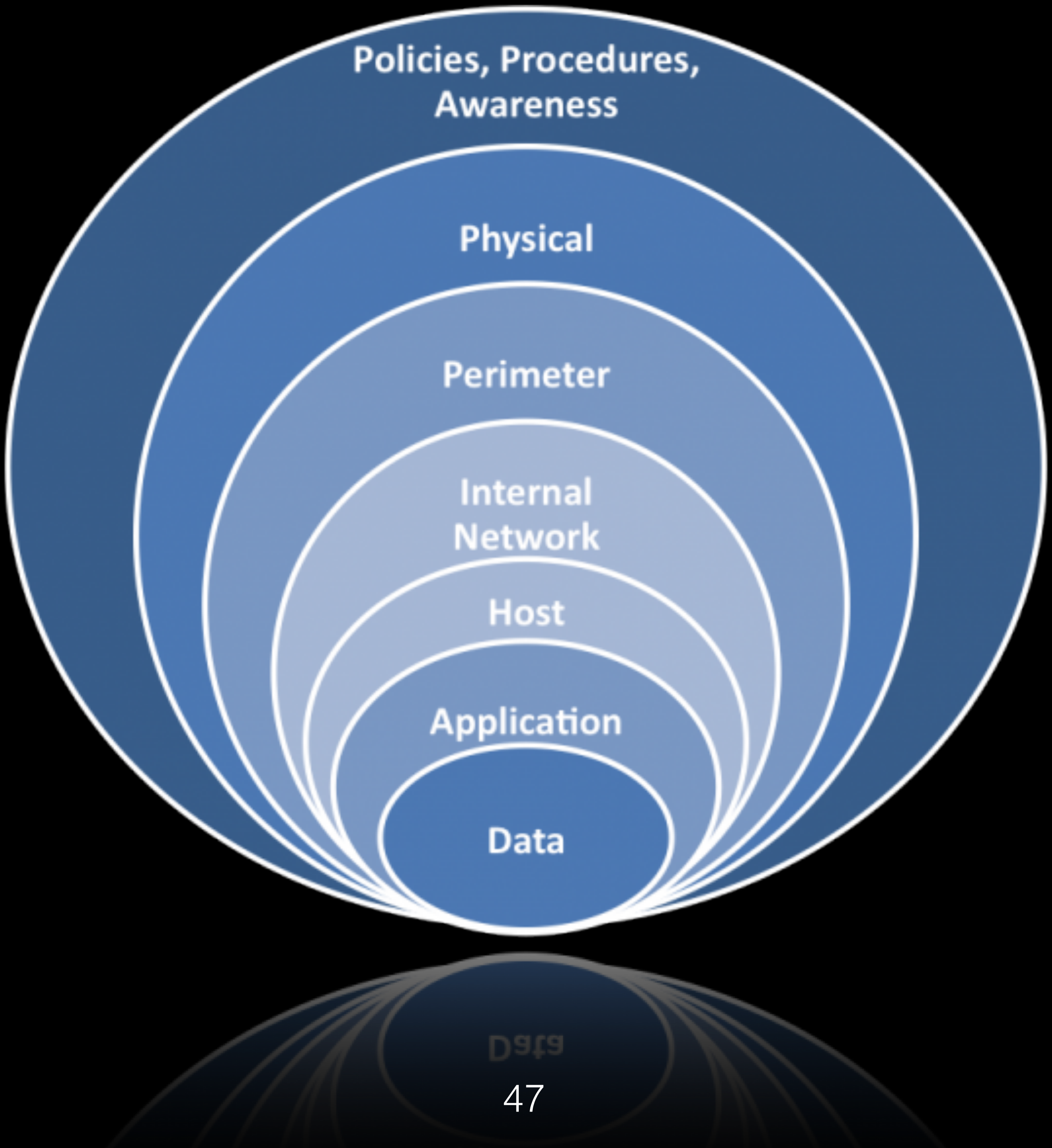
Failure of Imagination



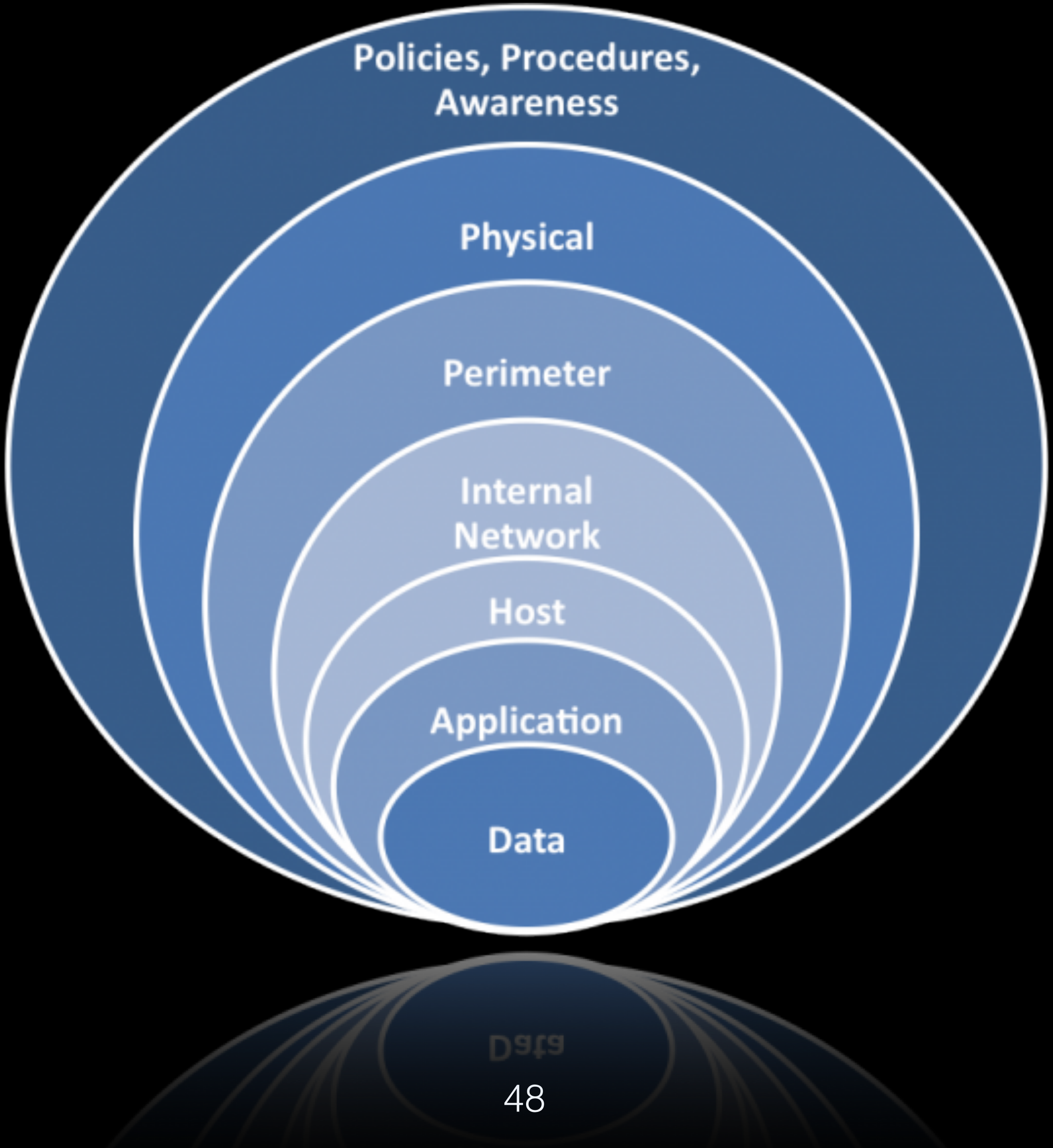
Failure of Imagination



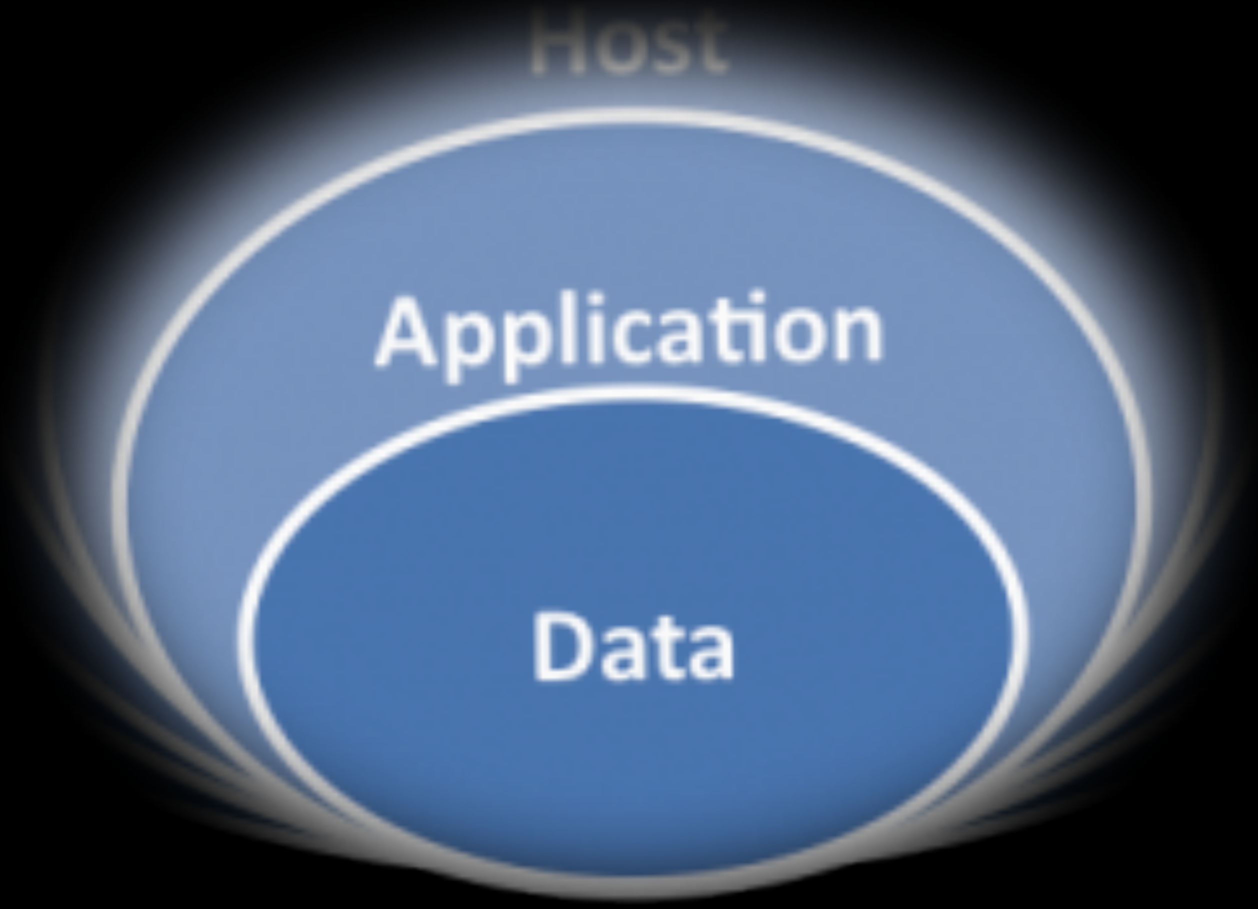
Defense In Depth



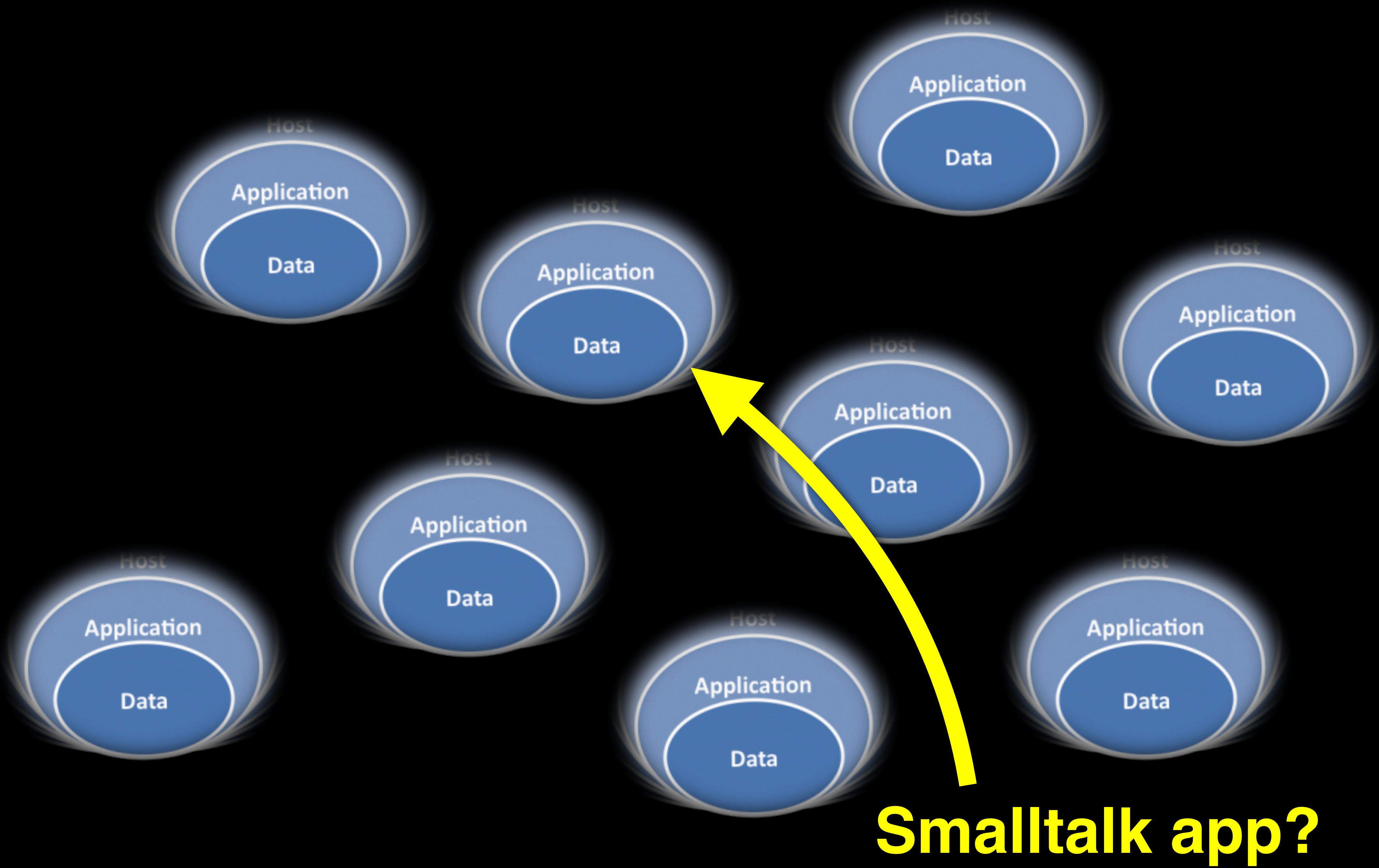
Assume **BREACH**



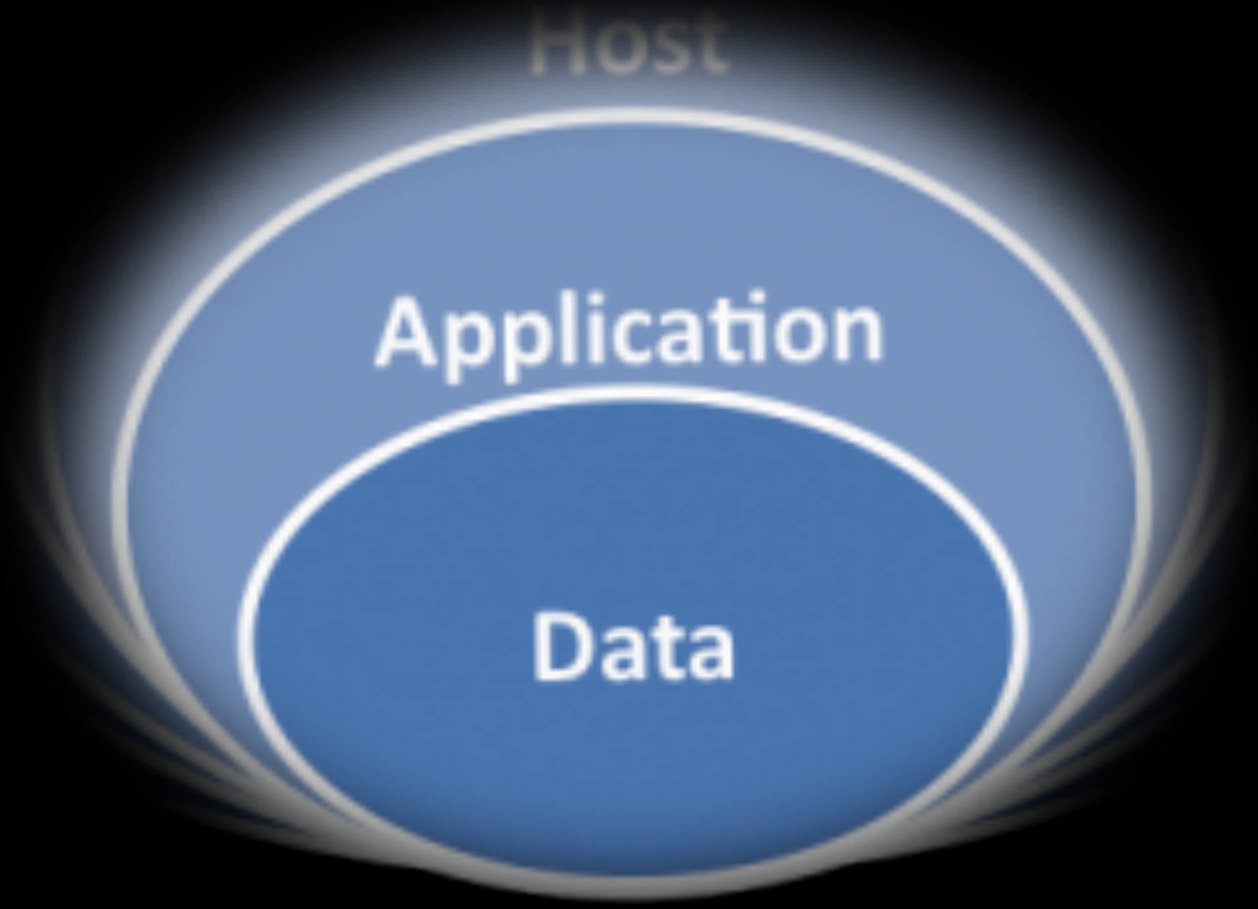
Assume **BREACH**



Assume **BREACH**



Smalltalk comes in…



Imaginary Scenario

- Smalltalk based web application
- Front-end web server (Apache, reverse proxy)
- Seaside app at the back-end
- GemStone database
- Store code repository

Imaginary Scenario

- Web server is misconfigured
- Vulnerable to path traversal
  root-path/../../something-interesting-here
- Allows arbitrary file upload
  a .PHP web shell or a reverse shell launcher
- Both are common vulnerabilities usually outside of a Smalltalk app developers scope or control.
- Assume **BREACH**

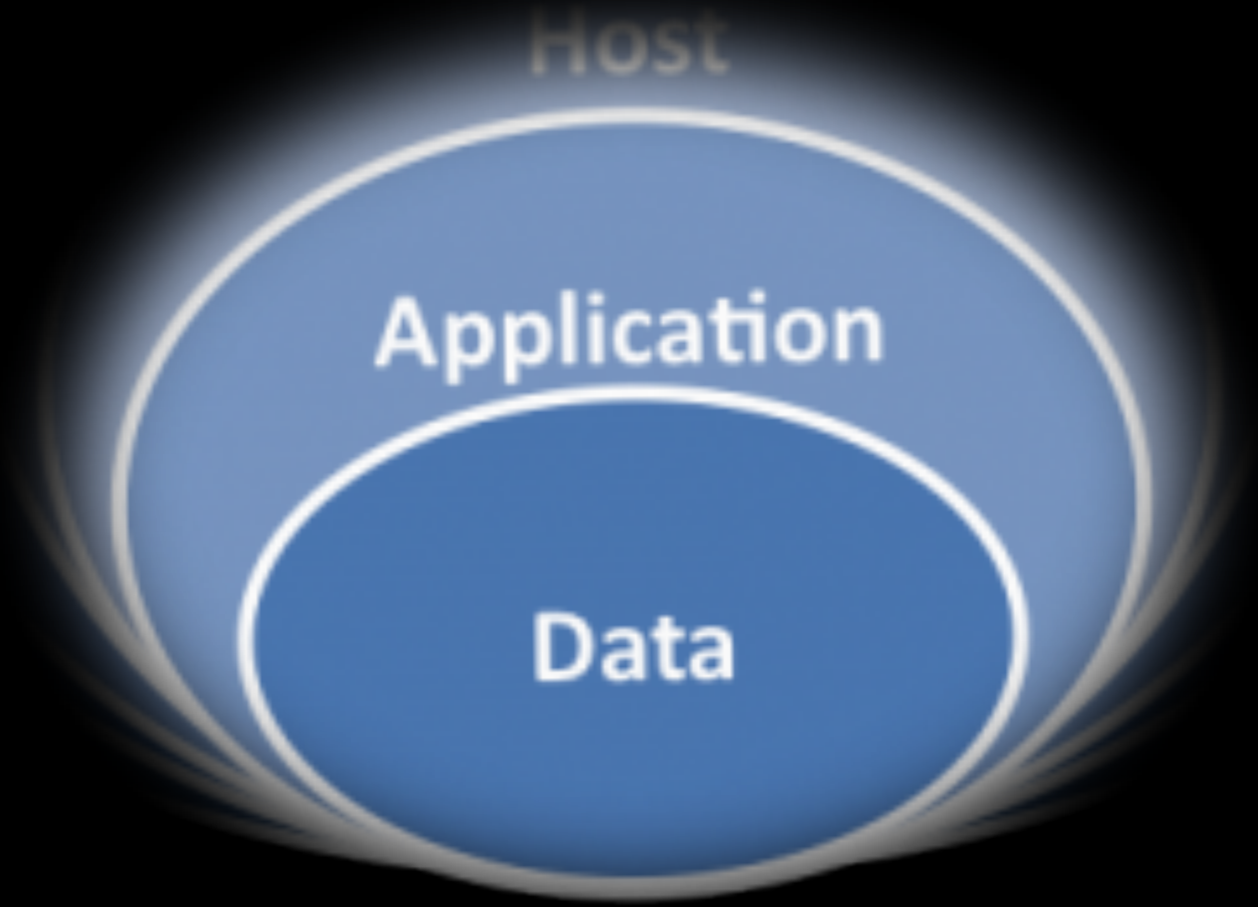
Assume BREACH…

- A host is compromised.
- The famous *reverse shell* - a remote access to the target host command line.
- Let's assume this has happened.
- What will an attacker do? (**behaviour**)

Assume BREACH…

- An attacker will look for:
  - OS & User information (‘uname -a’, ‘id’, ‘whoami’)
  - Network information (‘ifconfig’, ‘ipconfig’)
  - Running processes (‘ps -ef’, ‘tasklist’)
  - Open network connections and listeners (‘netstat’)
  - Ways to move to other systems - lateral move
  - FILES - Smalltalk images?

Targeting a Smalltalk application



Targeting a Smalltalk application

- The image file (*.im, *.image, *.dbf)

★ **Application**

  - Domain behaviour
  - UI behaviour
  - Communications (TCP/IP, file I/O)
  - Smalltalk IDE tools (compiler, workspace, etc…)

★ **Data**

  - Transient: objects created and GC’d
  - Persistent: passwords, DB & repository credentials, Seaside config. etc…

Other Smalltalk Artifacts

- Changes file (.cha, .changes)
- Source files (.st, .pst, .sources)
- Configuration files (.ini, .xml, .conf)
- Log files
- Binary object storage (BOSS files etc)

Imaginary Scenario
(continued)

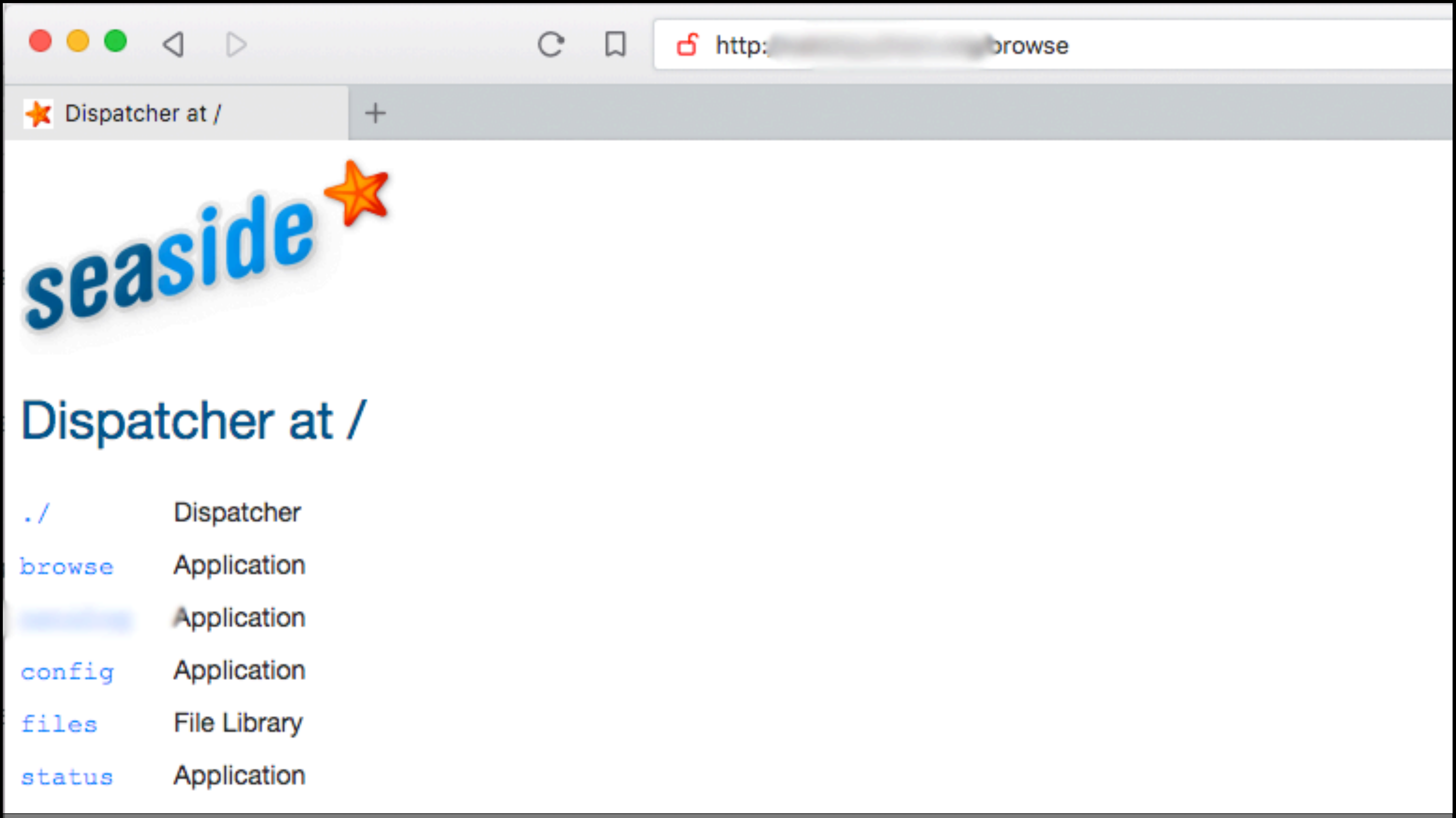
- OS: linux
- whoami: www-data
- pwd: /var/www/html
- ps: process info show paths of running Smalltalk images
- netstat:
  - listening ports: 80, 5900, 7777, 8080
  - connections to other hosts on ports 5432, 10377
- file enumeration: *.st scripts with hard-coded credentials

Imaginary Scenario
(continued)

- OS: Windows 7
- whoami: IUSR
- tasklist: processes show paths of running Smalltalk images
- netstat:
  - listening ports: 3389, 7777
  - connection to another host on port 4800

Imaginary Scenario
(continued)

- Plethora of information
- Expanding the reach (learn about other hosts in the network)
- Opportunities for lateral movement
- Are any of these files / applications vulnerable?
- Can I download them, modify & upload to gain more access (typically: YES)

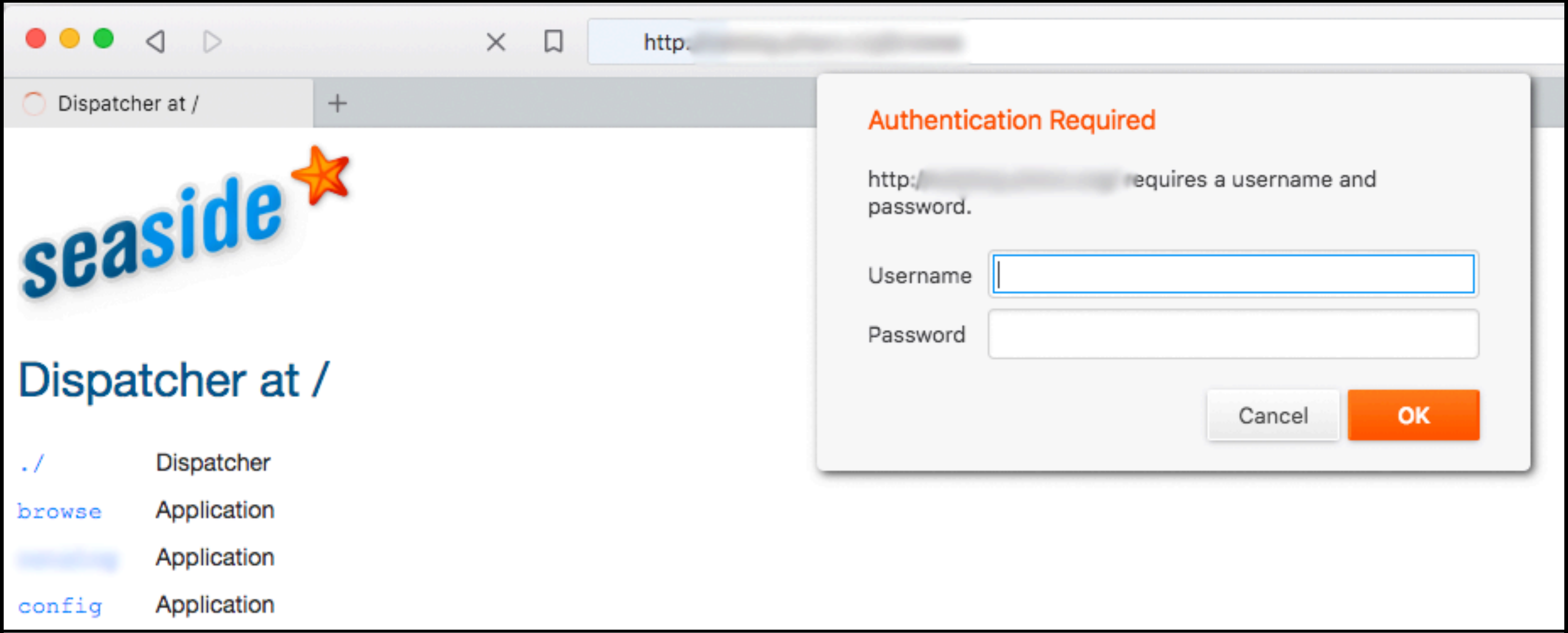

http: browse

Dispatcher at /

Dispatcher at /

./	Dispatcher
browse	Application
	Application
config	Application
files	File Library
status	Application

image-ware.com



Dispatcher at /

Authentication Required

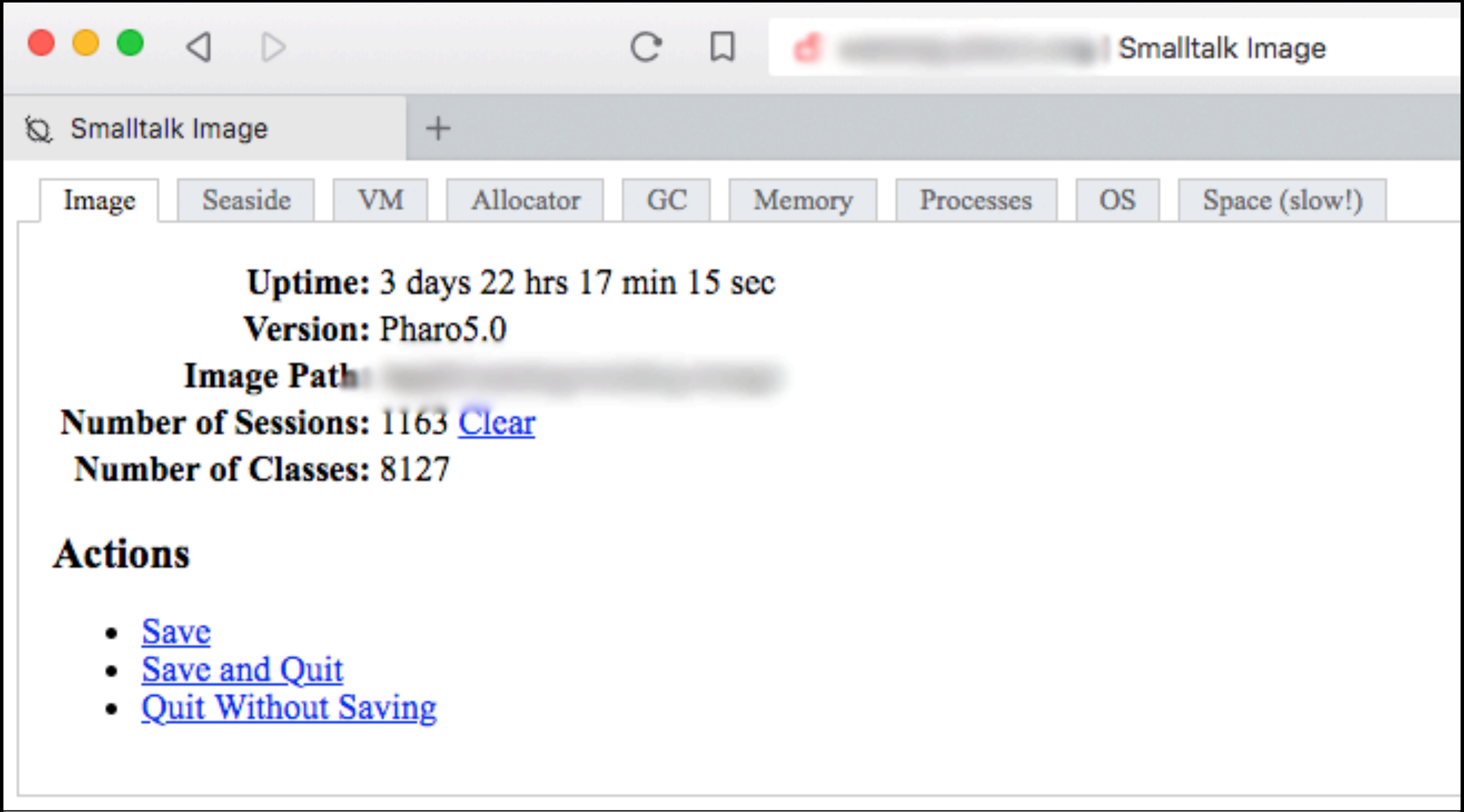
http:/ [illegible] requires a username and password.

Username

Password

Dispatcher at /

./	Dispatcher
browse	Application
[illegible]	Application
config	Application



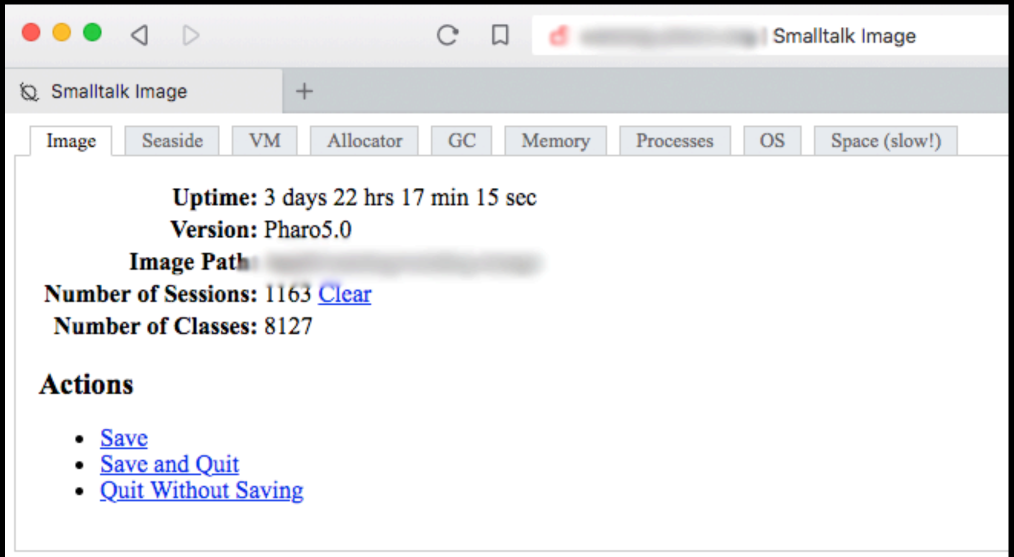
Uptime: 3 days 22 hrs 17 min 15 sec
Version: Pharo5.0
Image Path:
Number of Sessions: 1163 Clear
Number of Classes: 8127

Actions

- Save
- Save and Quit
- Quit Without Saving

Breach of:

- **Confidentiality**
  - Reveal internal directory structure
  - Save a running image with credentials in it
- **Integrity**
  - Saving the image can change the state of the application
- **Availability**
  - Clear sessions
  - Save and Quit, Quit Without Saving



Uptime: 3 days 22 hrs 17 min 15 sec
Version: Pharo5.0
Image Path: [redacted]
Number of Sessions: 1163 Clear
Number of Classes: 8127

Actions

- Save
- Save and Quit
- Quit Without Saving

Don’t

- Hard-code credentials in scripts

- Use default credentials
  admin:123456, DataCurator:swordfish

- Store login credentials in the image
  instvars, Seaside sessions, configuration objects

- Think that just because your application doesn’t do anything ‘important’, it would be of no interest to a malicious actor

Do

- Assume BREACH. Imagine ‘WWJD’ (What Would Jerry Do)
- Protect sensitive files (read-only by the account permitted to access)
- Wipe credentials, private keys, etc… from memory after use
  ```
  aPassword become: String new
  ```
- Have an Incident Response Plan - what will you do when (not if) you get hacked
- Perform regular Vulnerability Assessment and Penetration Tests
- Engage a certified Penetration Tester who also understands Smalltalk ;-)

Questions?

esug2019@image-ware.com

image-ware.com/static/esug2019.pdf