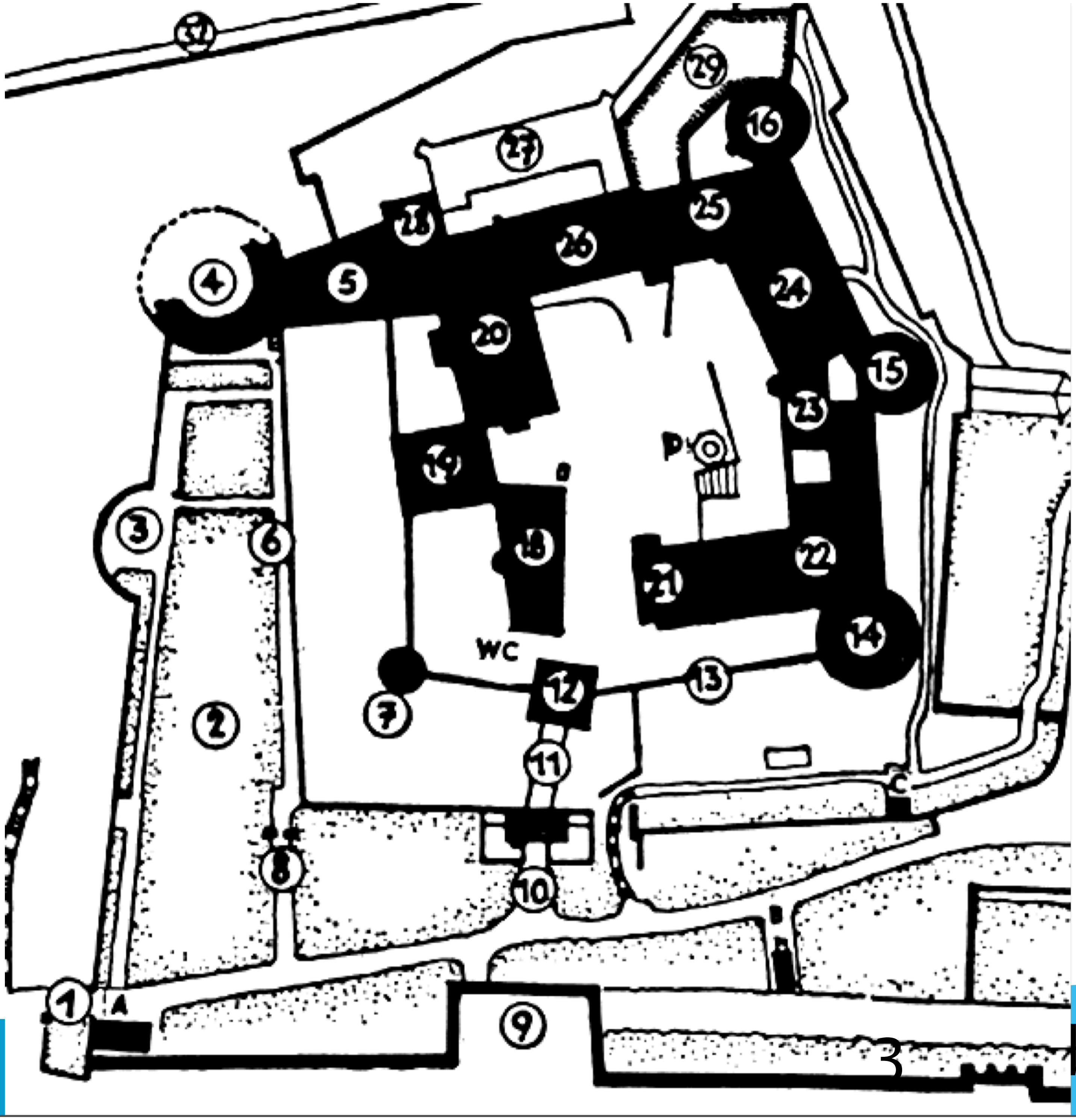
Firewalls and Perimeter Defense

Bill Cheswick
AT&T Shannon Labs
ches@research.att.com
http://www.cheswick.com/ches/talks/

Perimeter Defenses allow one to focus defensive expertise and efforts on a small area

Heidelberg Castle



Heidelberg Castle:

Heidelberg Castle:

- 1622: Tilly captured the castle after a two-month siege

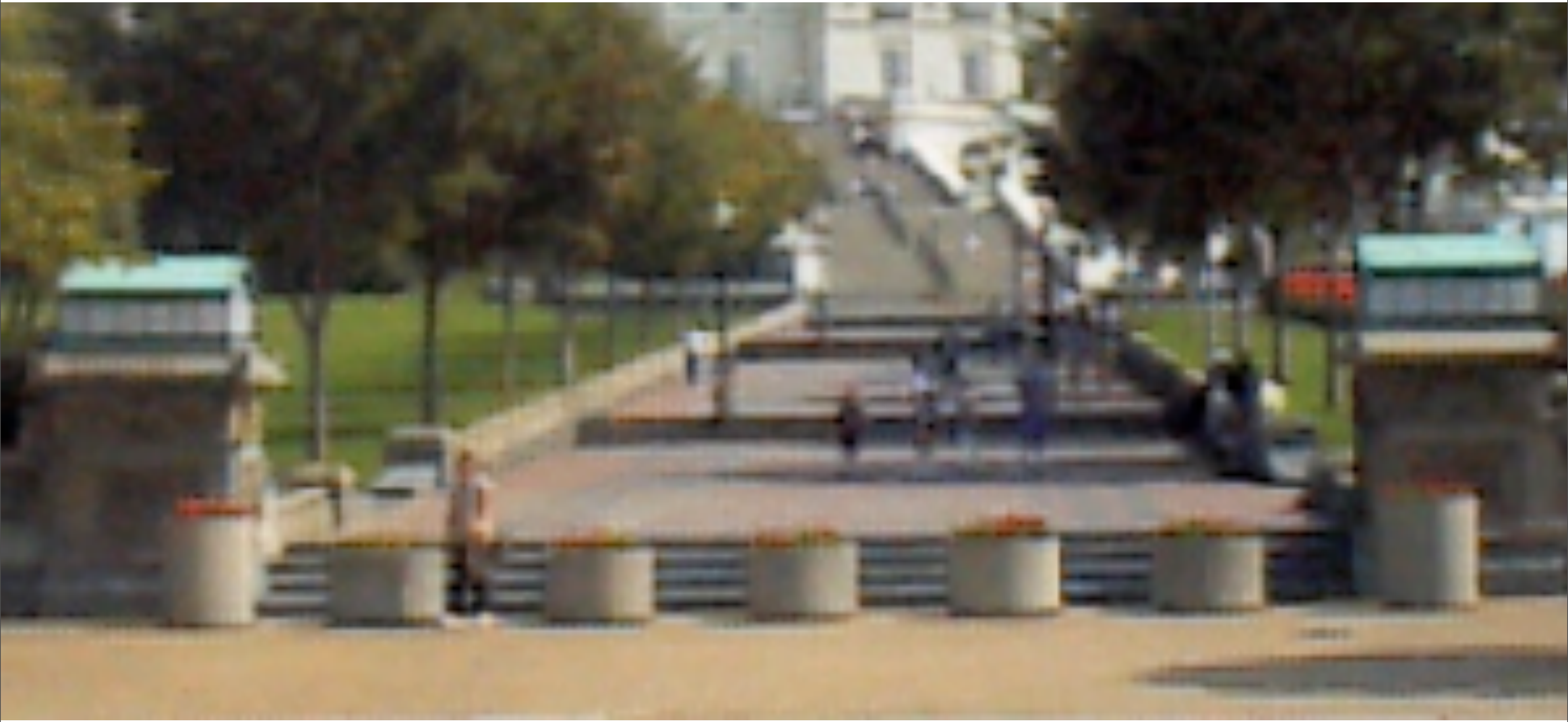
Heidelberg Castle:

- 1622: Tilly captured the castle after a two–month siege
- 1689: Captured by 30,000 French in a few hours
  - insufficient number of defenders

Scotland Yard

Edinburgh castle

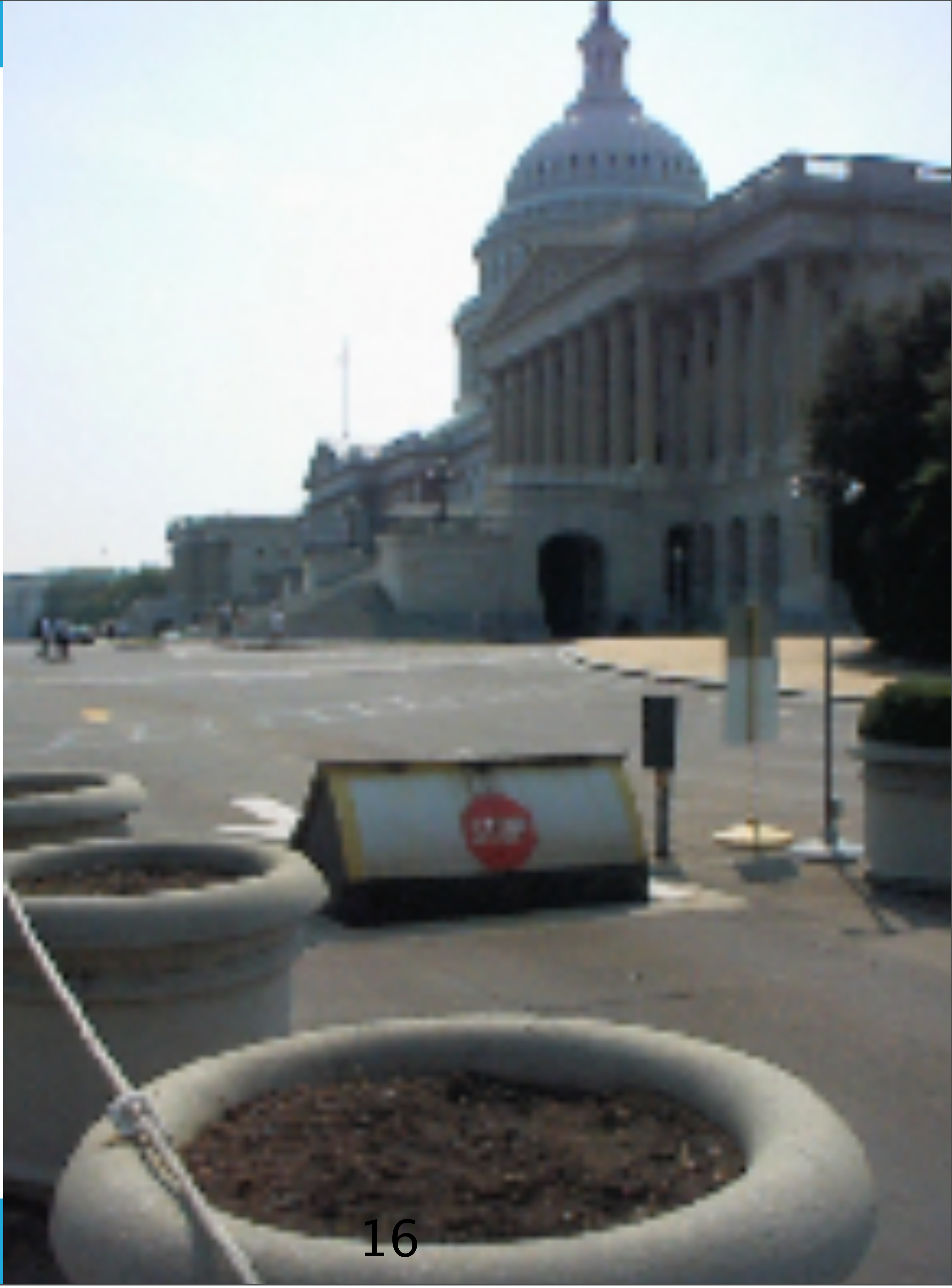
Flower pots



- Security doesn’t have to be ugly

15

Delta barriers



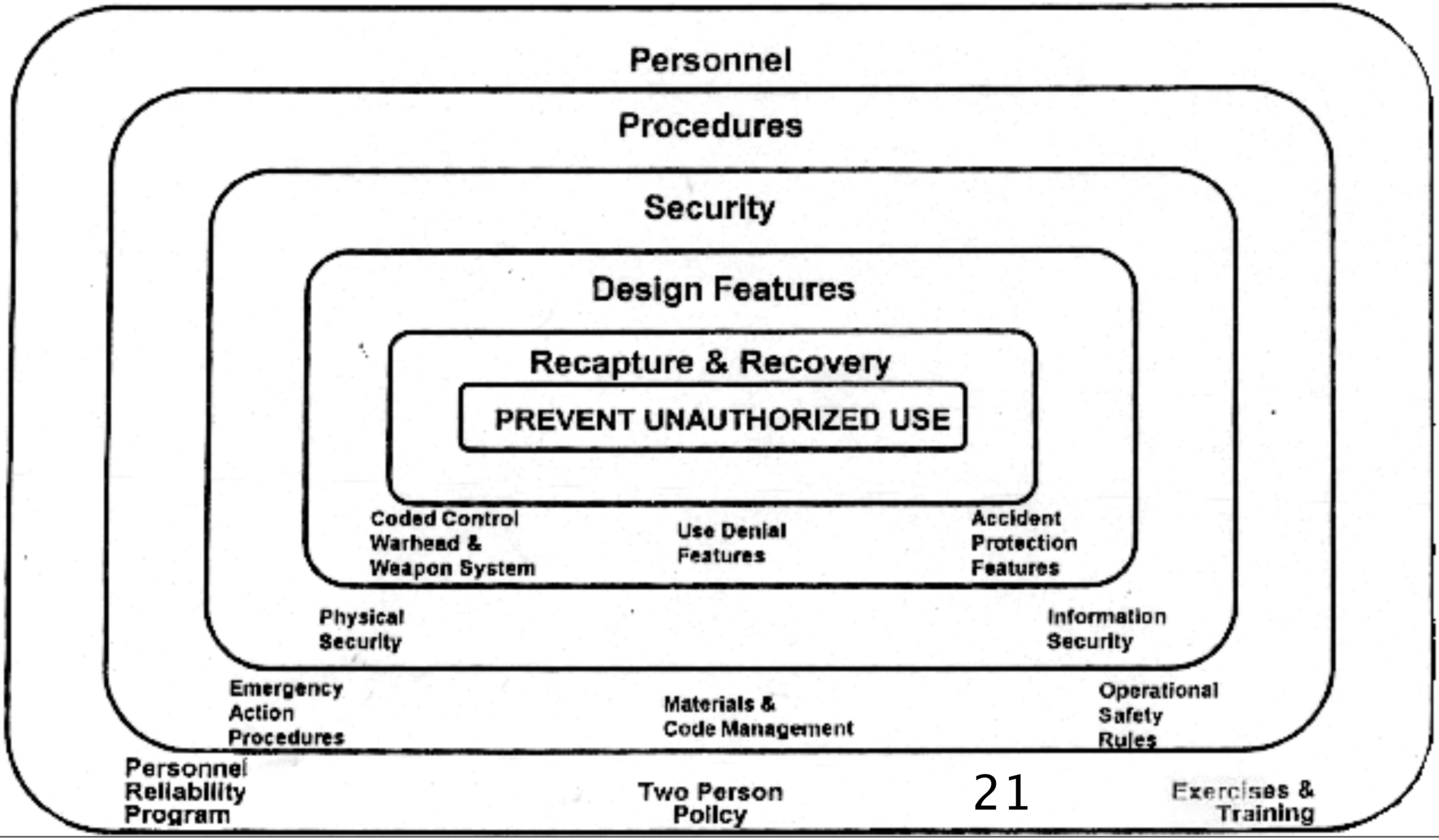
17

ut 71

We Use Layers to Achieve Higher Security

Layered Positive Measures to Assure Against Unauthorized Use

The Adversary: Humans or Accidents



Personnel

Procedures

Security

Design Features

Recapture & Recovery

PREVENT UNAUTHORIZED USE

Coded Control Warhead & Weapon System

Use Denial Features

Accident Protection Features

Physical Security

Information Security

Emergency Action Procedures

Materials & Code Management

Operational Safety Rules

Personnel Reliability Program

Two Person Policy

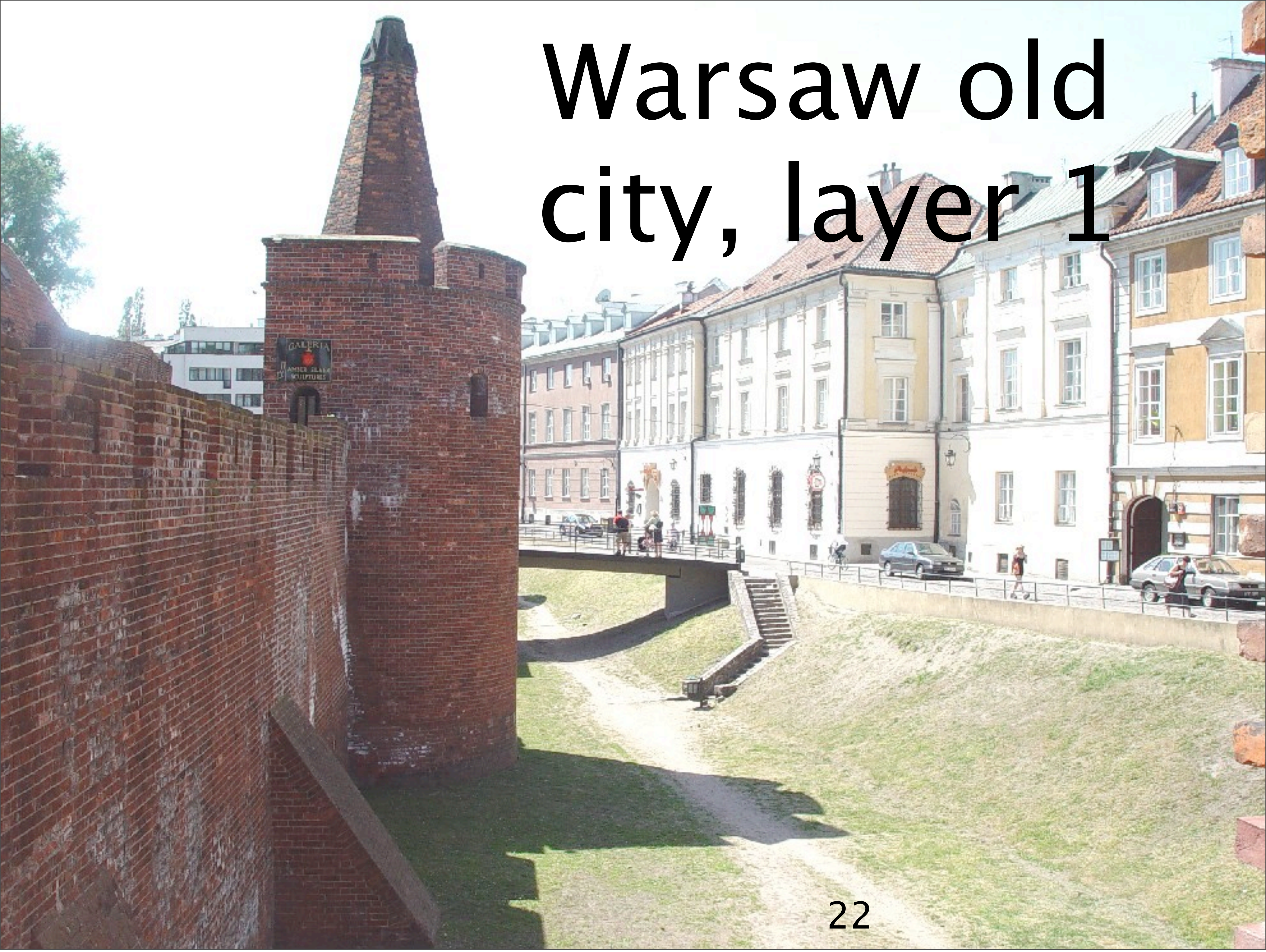
Exercises & Training

~~SECRET~~

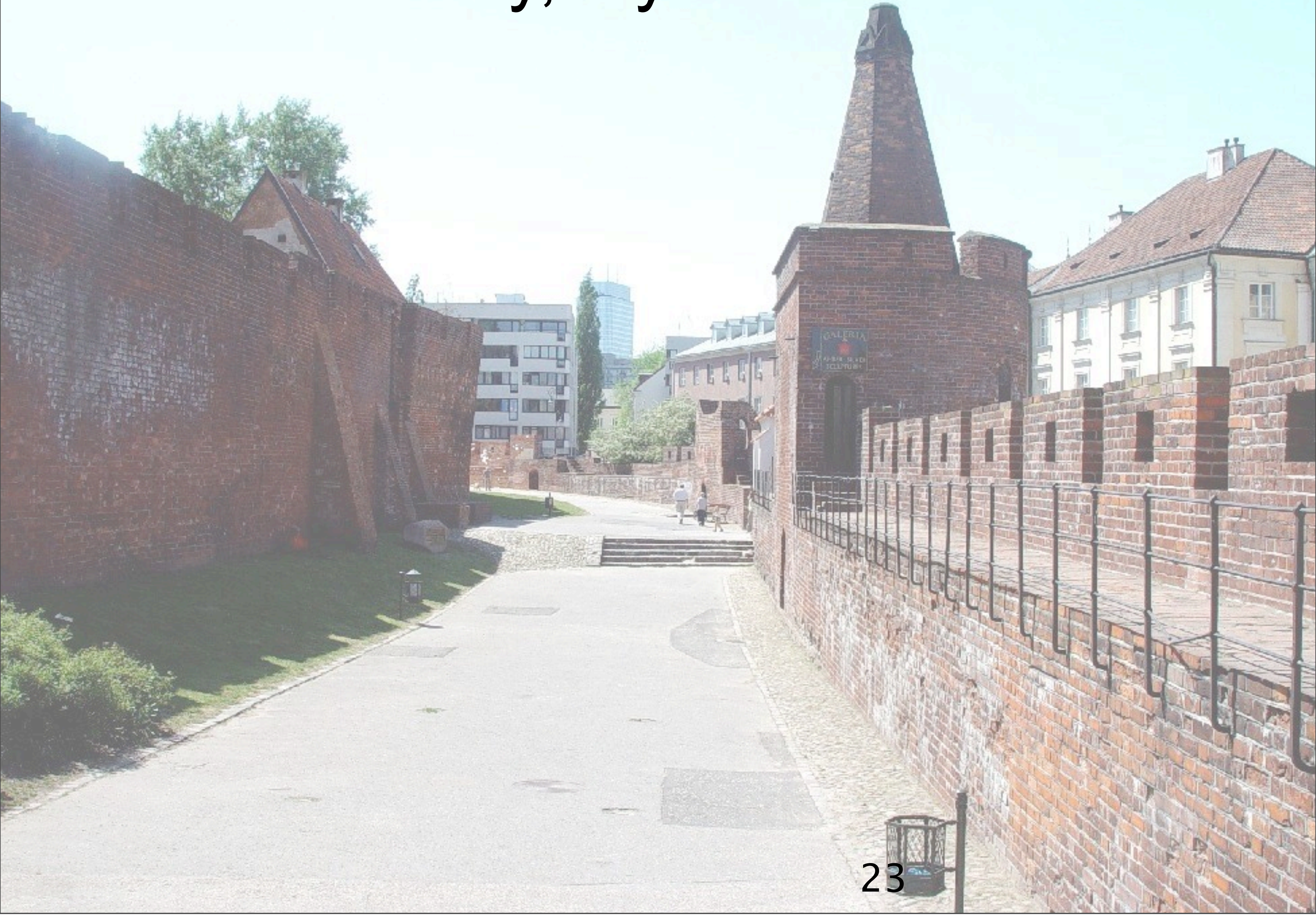
UNCLASSIFIED

UNCLASSIFIED

Warsaw old city, layer 1



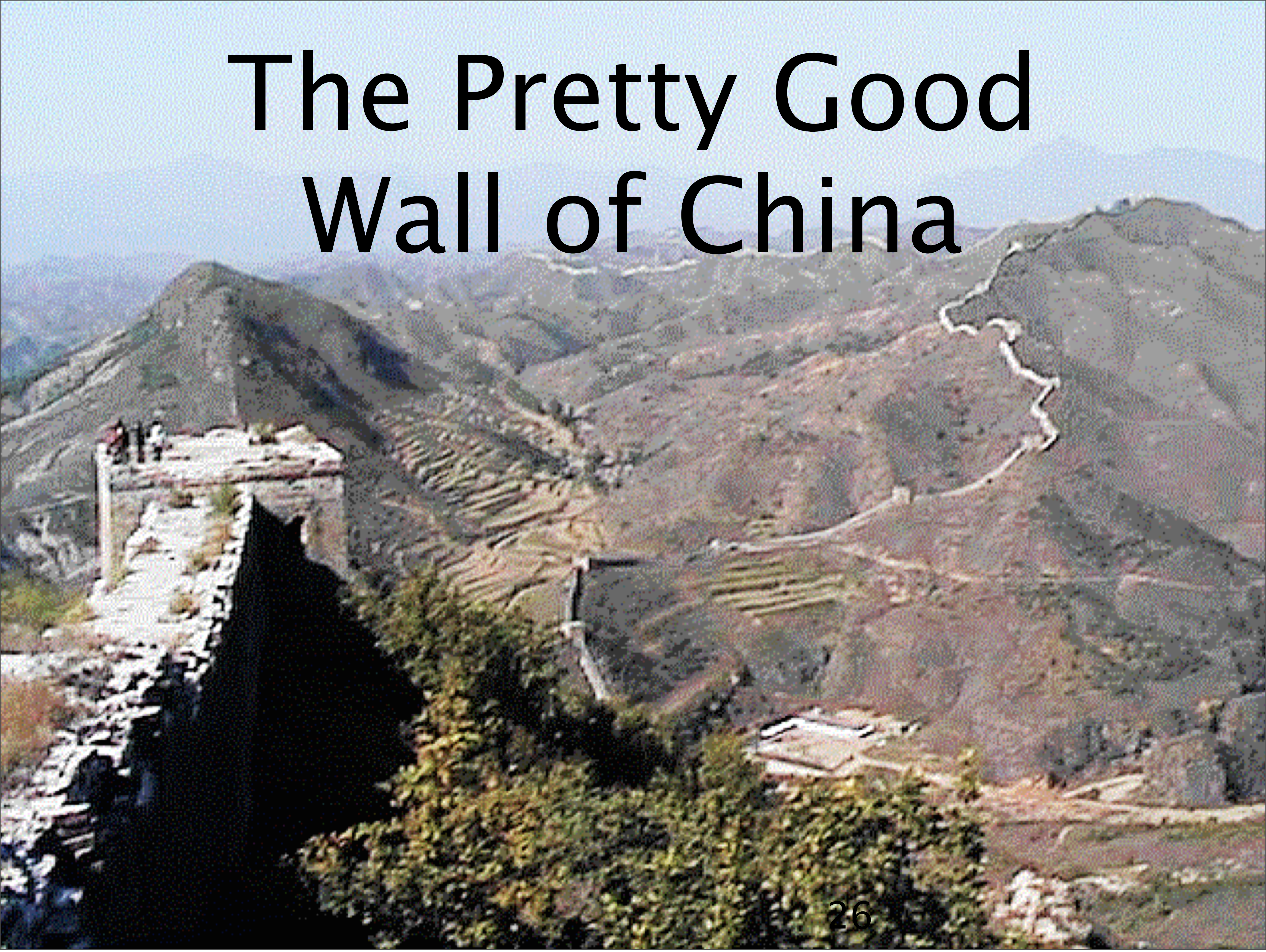
Warsaw old city, layer 2



Intimidation is a layer

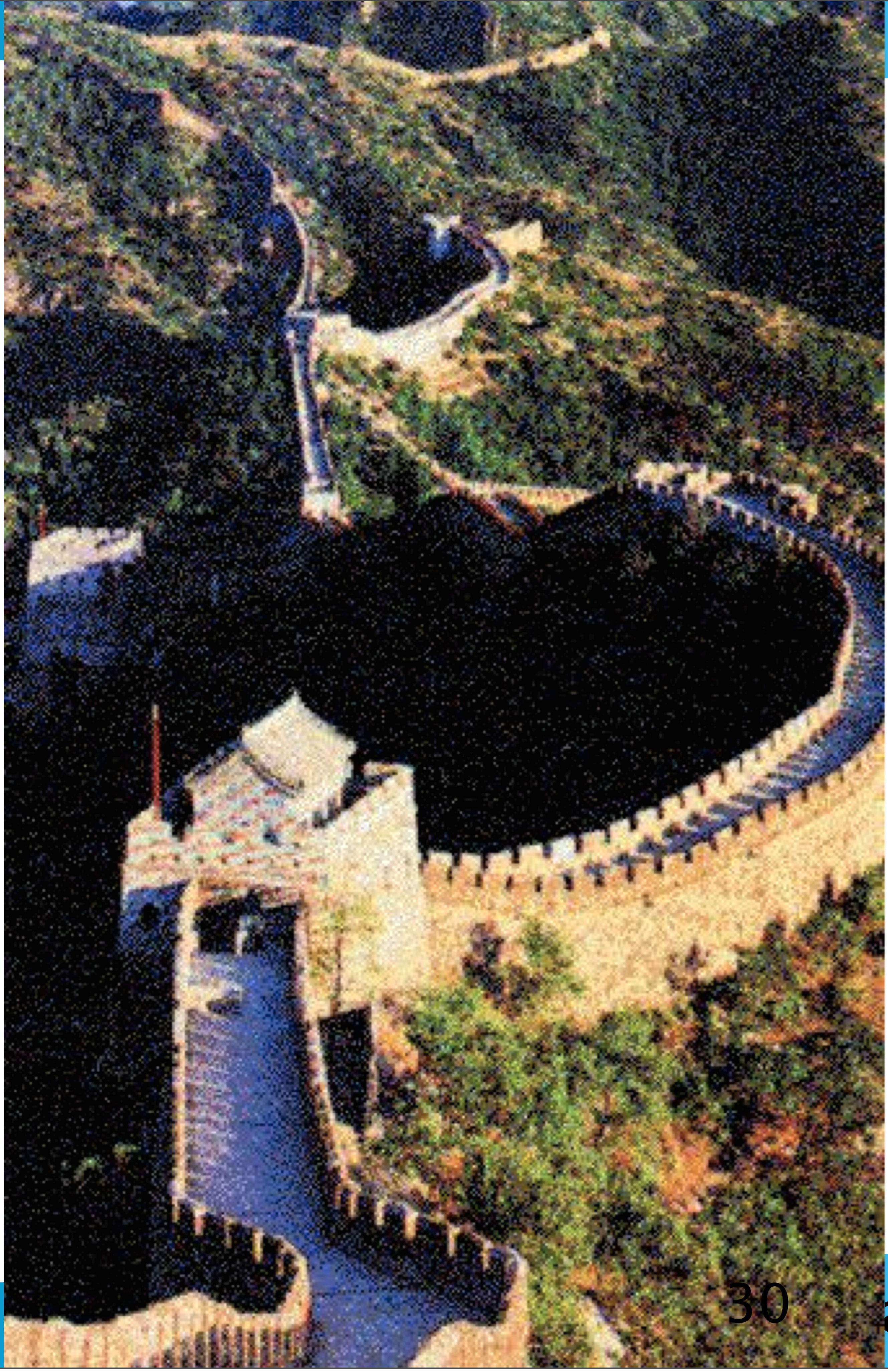
Perimeter Defenses don’t scale

The Pretty Good Wall of China



The Great Wall

- Built to keep out the barbarians of the north
  - and their economy
- Formed from shorter segments
- Ghengis Khan walked past the wall, unopposed, and into Beijing
  - A wall is a single layer

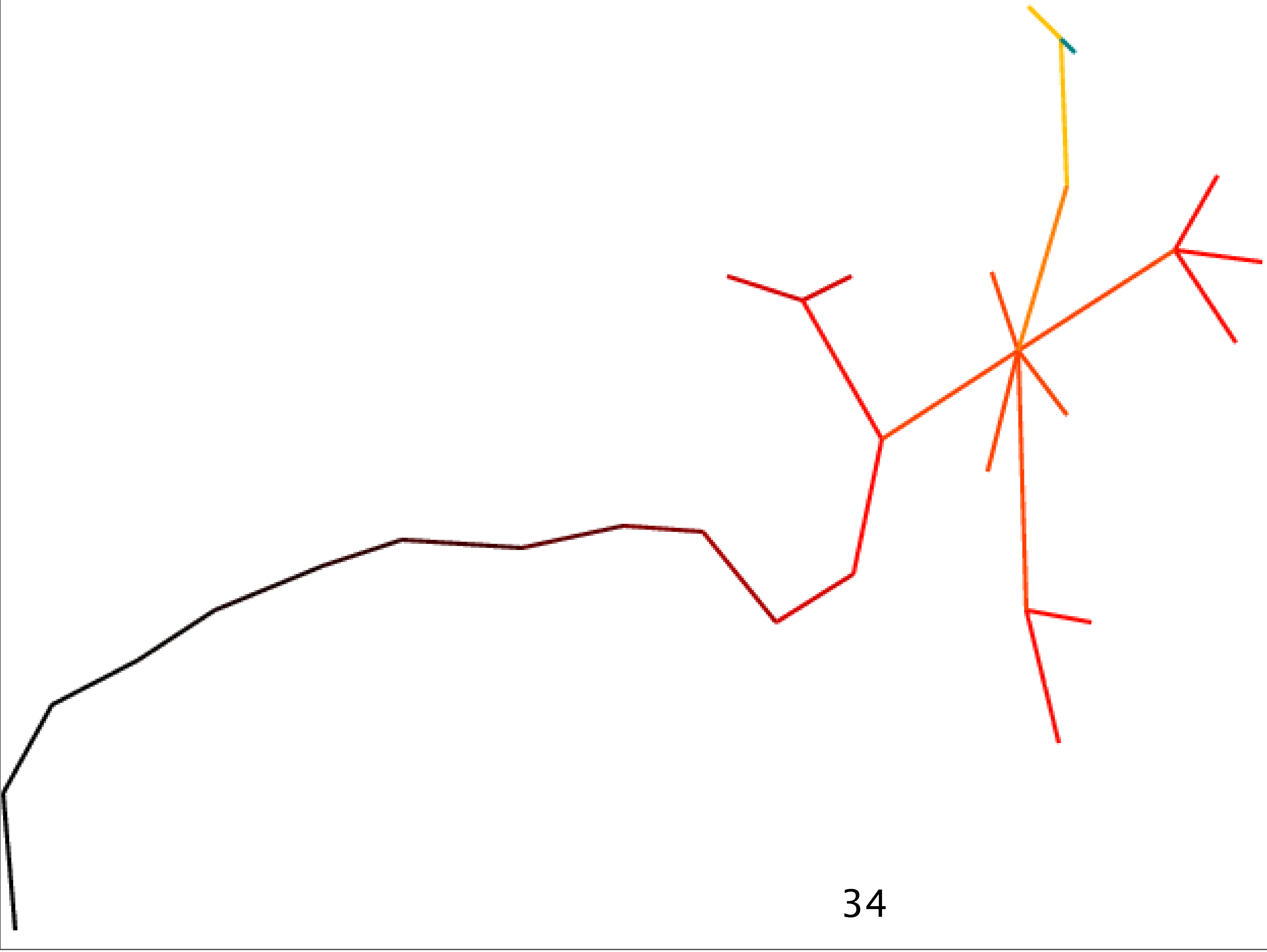


about 71

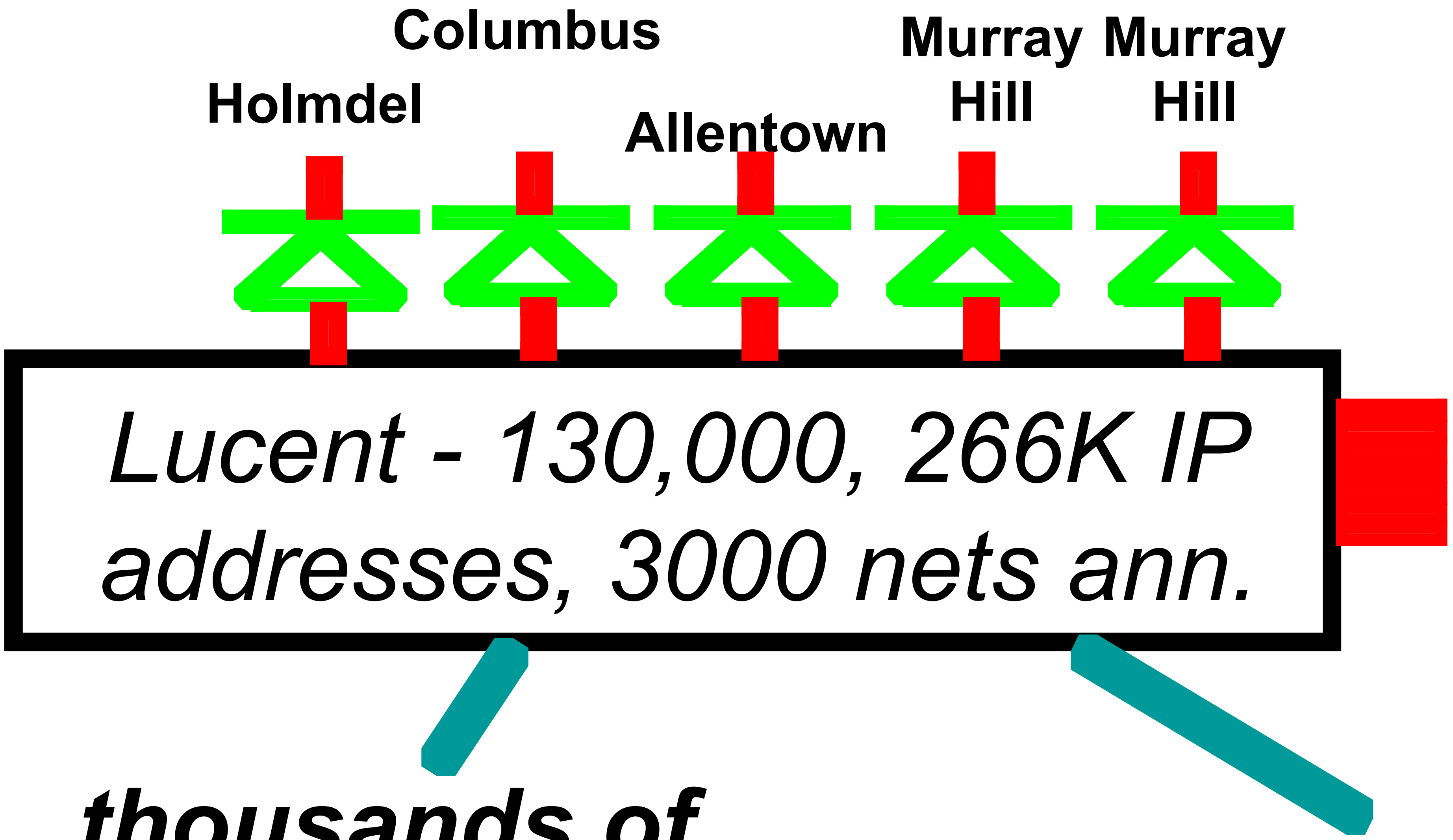
Parliament: entrance

Parliament: exit

Intranets



The Internet



Columbus

Holmdel

Allentown

Murray Hill

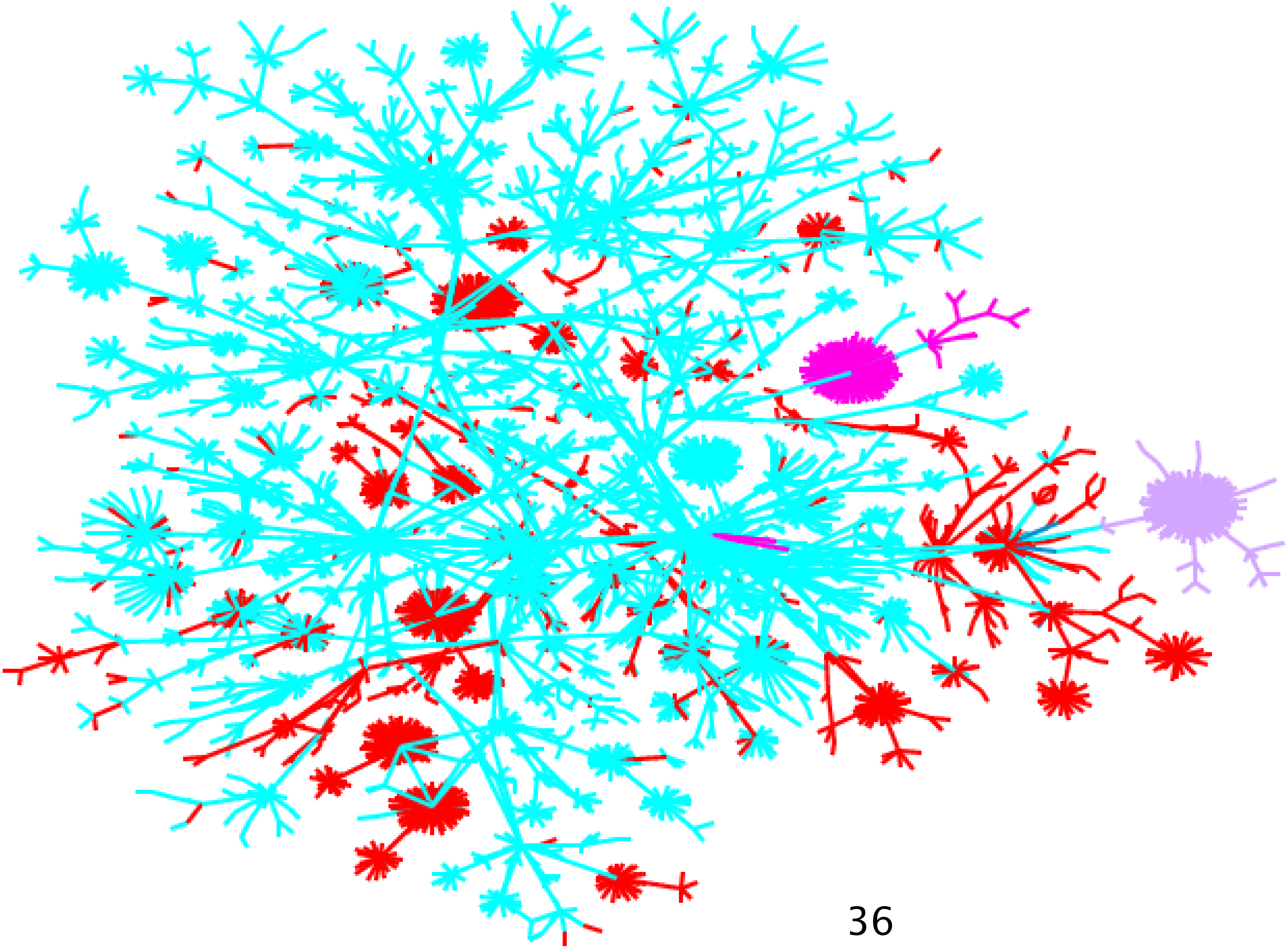
Murray Hill

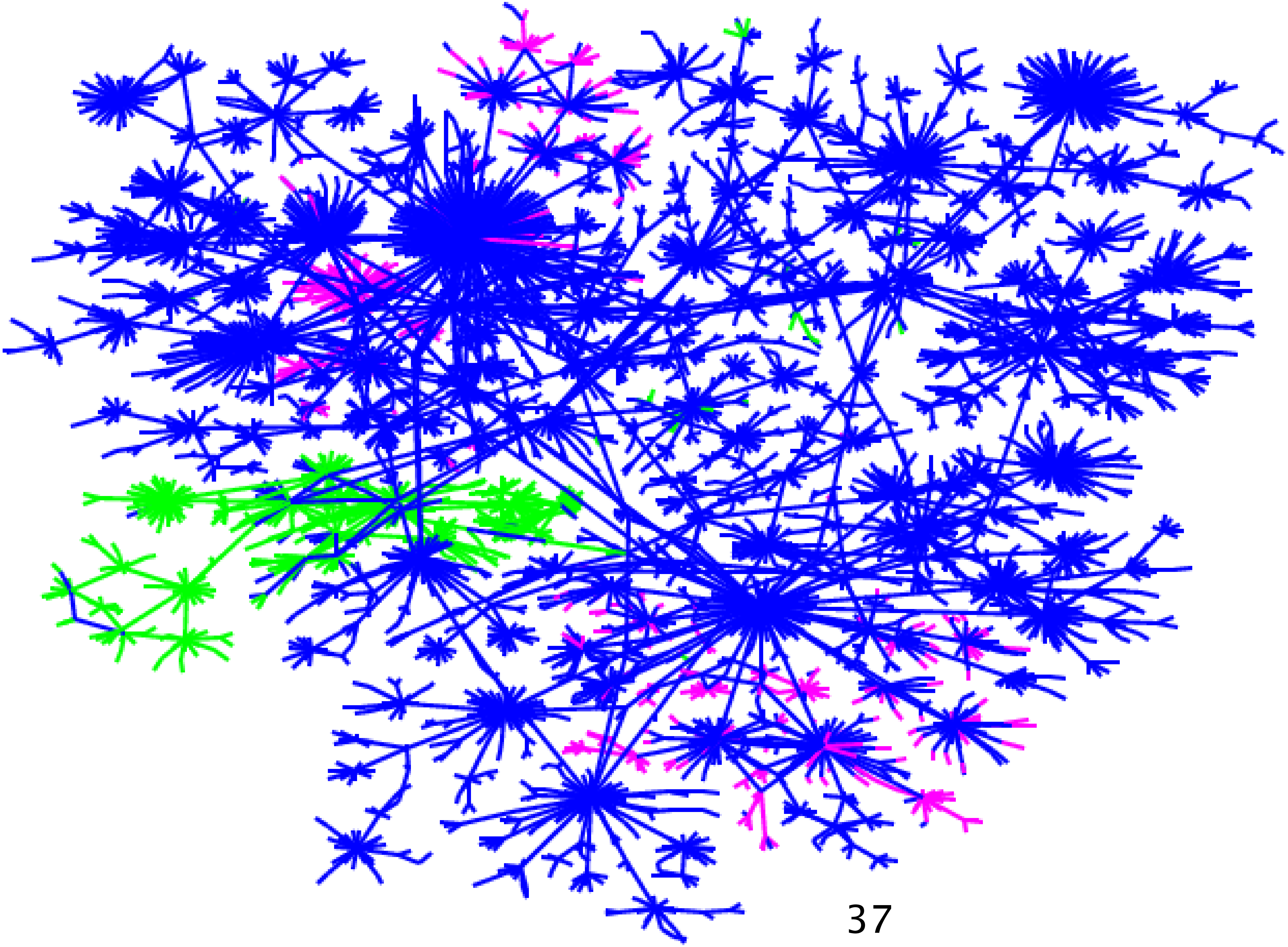
Lucent - 130,000, 266K IP addresses, 3000 nets ann.

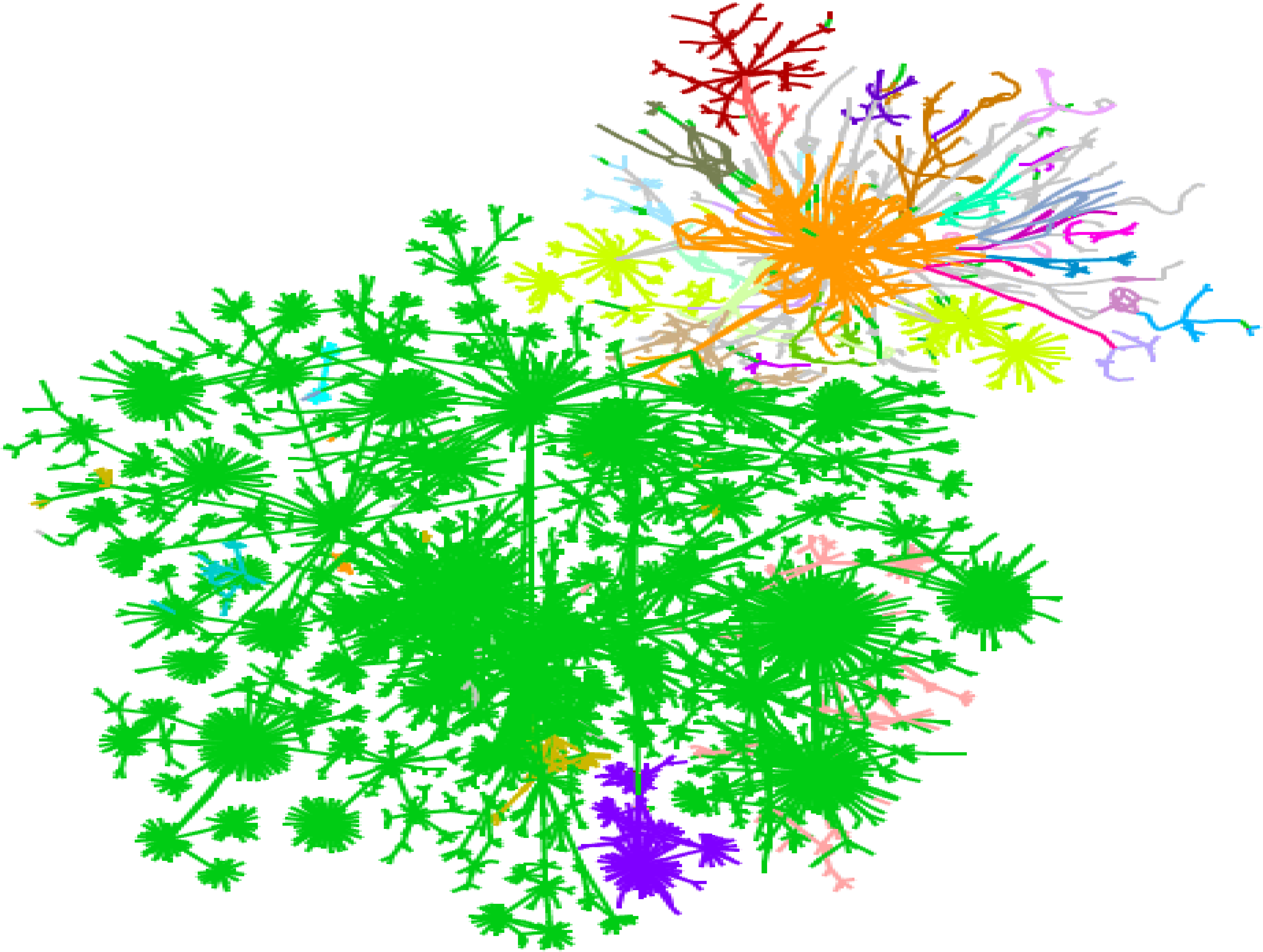
SLIP
PPP
ISDN
X.25
cable
...

thousands of telecommuters

~200 business partners







Anything large enough to be called an intranet is probably out of control

A simile for the ages?

“All of [the gateway’s] protection has, by design, left the internal AT&T machines untested---a sort of crunchy shell around a soft, chewy center.”

Fun intranet facts

- The largest is probably NIPRNET, ~2 million hosts
- A high tech company has about two active IP addresses per employee
- Low tech is around one per employee
- Small ones are enclaves.

Perimeter Defenses

- For wusses with hosts that can’t hack it on the real Internet
- A gateway fascist decides which traffic is good and bad
- Cheaper than deploying firewalls in every host
- But we do that, too

Problems with PDs

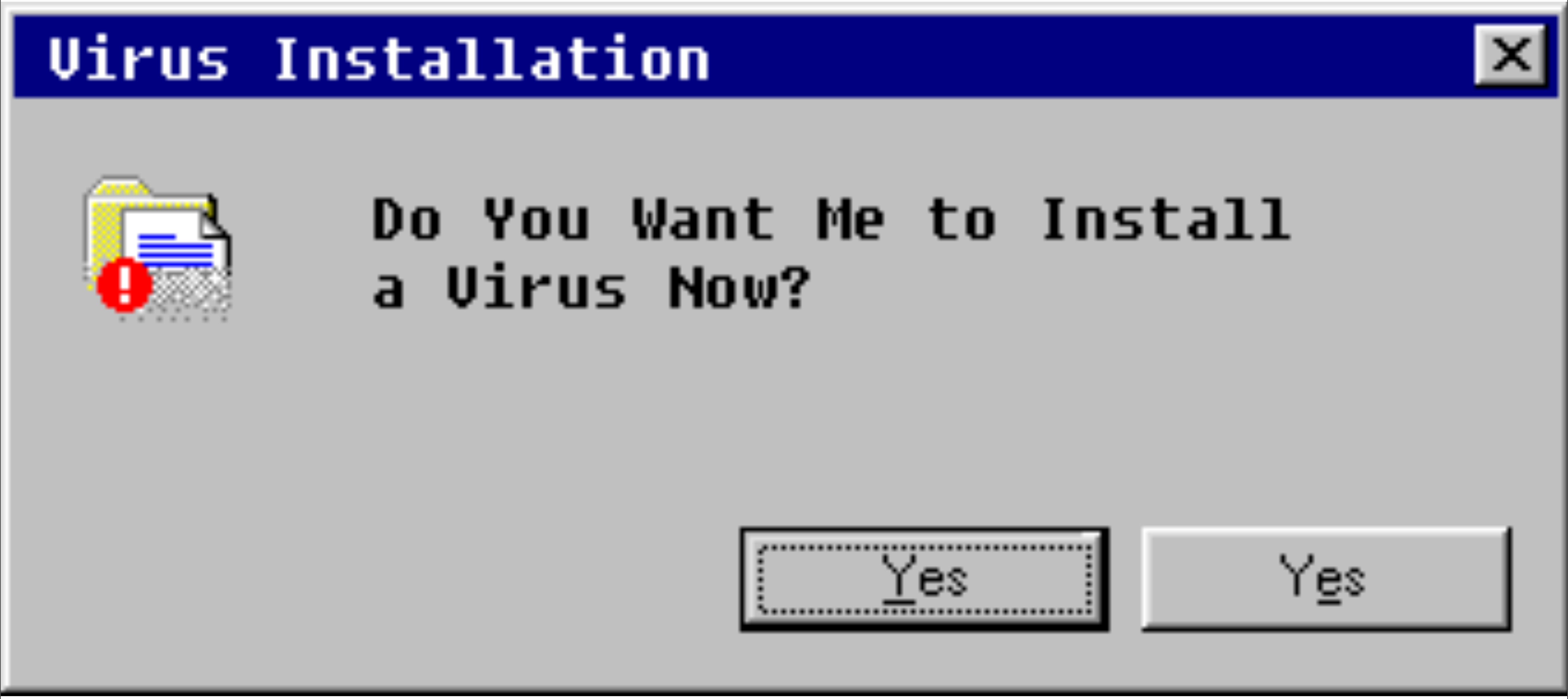
- They are hard to do
- They look easy to do
- They provide a false sense of security
- They don't scale
- Everybody scales them

How Does Trouble Arrive?

- Dangerous services are attacked from the outside
- We import trouble, like Buffy's vampires

Attack from the outside

- Network services may have exploitable security holes
- Best answer: remove services
- PD answer: get out of the game



Virus Installation

Do You Want Me to Install a Virus Now?

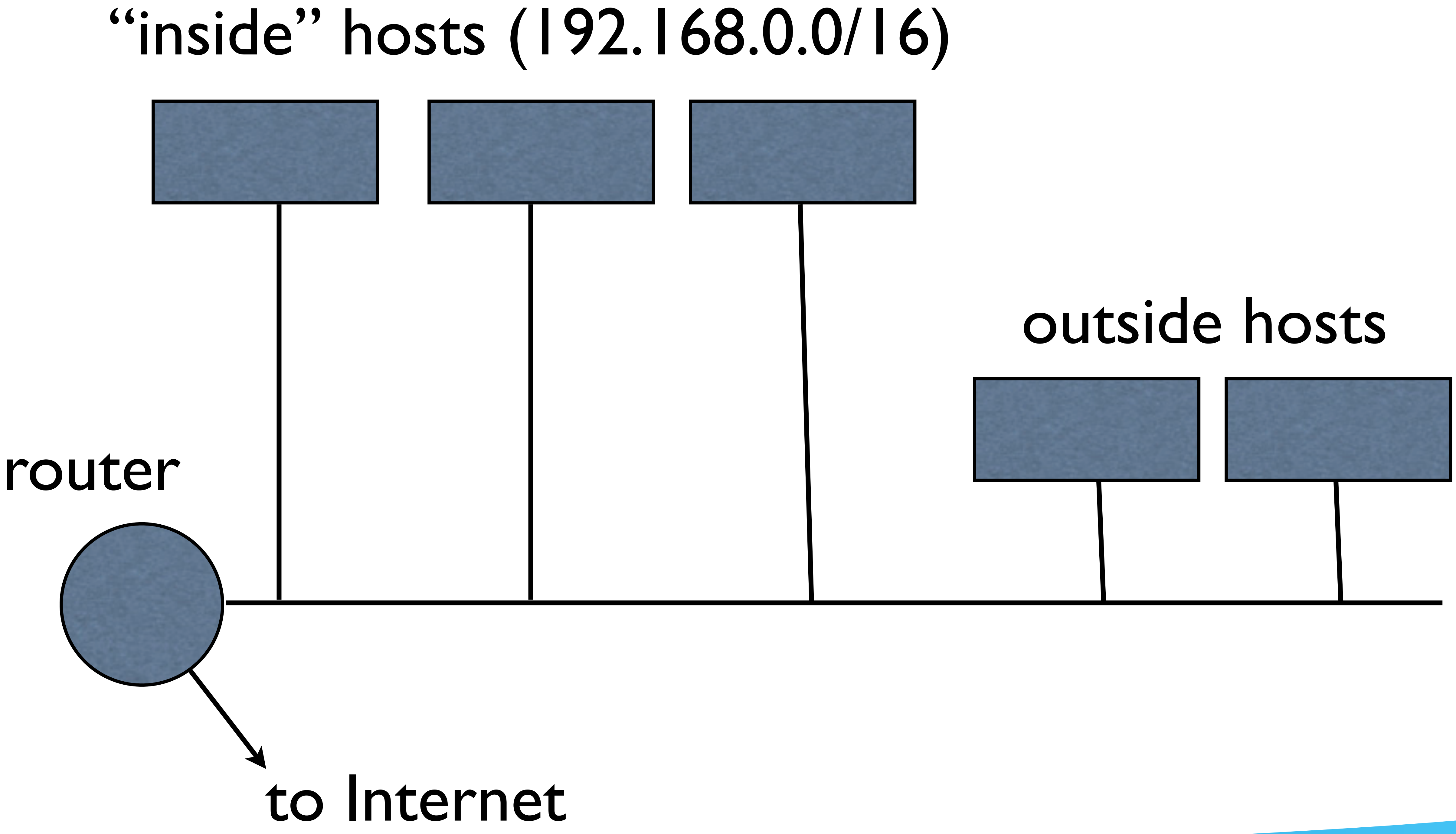
“Best block is not be there”

–– Mr. Miyagi, Karate Kid

Getting out of the game

- Firewalls block the bad stuff, and let in the good stuff
- Routing and addressing tricks also get you out of the game
  - RFC 1918 addresses
  - IPv6 FD address range

Unreachable...

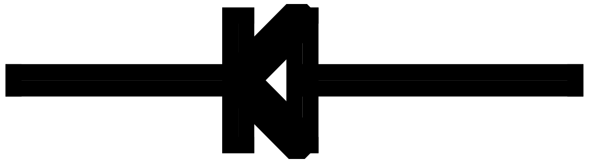


Key Points to hiding networks

- Indirectly-connected hosts can be scanned by intermediaries
  - if they are compromised or
  - if spoofed packets are possible
- Important: block spoofed packets

Internet Firewalls

Original firewall



Firewalls tend to be directional

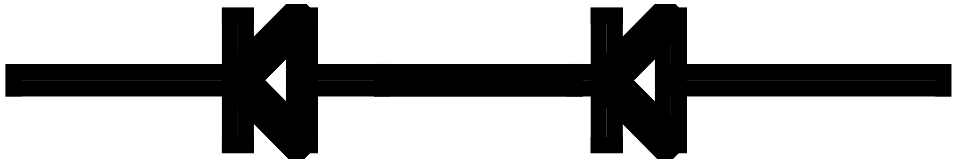
- “inside” and “outside”
- the weakest part: thinking of “the inside” as being secure. It mostly isn’t.

Behind firewalls

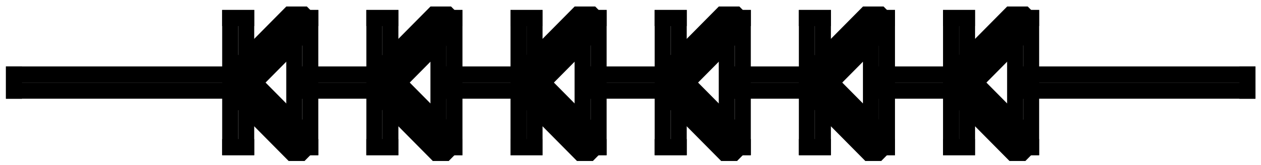
- Standard servers are too dangerous to expose to outside access
- TCP/IP packets are too dangerous
  - No IP connectivity to outside

at&t

My (Safer!) Firewall



Referee’s suggestion



Two benefits

- Avoids Denial of Service Attacks (DOS) attacks on important hosts
  - This is a network-level, not host-level problem
- Walled garden makes intruders easy to spot, by definition

Firewalls

- Generally centralized defense against attacks
- Cheaper to focus your smarts in one location
- Host-based firewalls blend into host-based security

Levels of firewalls

- Packet: usually "packet filter"
- Circuit: c.f. socks
- Application level
- Deep packet inspection: packet–level analysis of deeper data

Packet filters

- Generally fast and cheap
- Generally stupid: use tricks to enhance
    - stateful: keep track of sessions

Circuit level

- “Computer acting as a wire”
- Specific TCP connections copied by a relay program
- Not used much any more, but can be a convenient tool

Application level

- Understands the service it is filtering
- mailer receives and scans email before forwarding

Benefits of DPI

- Relatively cheap and easy to do
- Can be done at network speeds
- Note: not new technology

Problems with DPI

- It is impossible to do correctly, so
  - good enough has to be good enough
- Why? Doing it right requires packet normalization.

Packet Normalization Problems

- Fragmented packets
- TCP overlap interpretation
- Packet distance hacks
- See Vern Paxson’s work for gory details

General Filtering Rules

- Block everything by default
- Allow safe stuff through
- Outgoing is generally okay
- UDP is generally not okay
  - but what about DNS, voice?

NAT is a close match for these

- RFC1918 addressing inside
- Outgoing stuff only
- Cheap from Costco, etc.
- You can patch your Windows system in relative safety

Invited Attacks

- Much harder to filter with firewalls
- Sandboxing seems to be the most promising technology
- It is getting harder to cruise the web safely, even at “safe” sites. (Thank advertising)

Internet Skinny Dipping

Alternative to Firewalls and Perimeter Defenses

Strong Host Security

- It can be done
- Many services are too dangerous to run
- Requires some user forebearance
- Can defend nicely against insider attacks

Inviting trouble in

- browsers, etc. are full-featured
- full-featured is a technical term for "full of security bugs"
- This is an open security problem: better OSes, sandboxing, VMs, etc.
- iPhone might be leading this!

Summary – perimeters

- Does not scale
- Medium-level defense at best
- No protection from insider attacks

Summary – firewalls

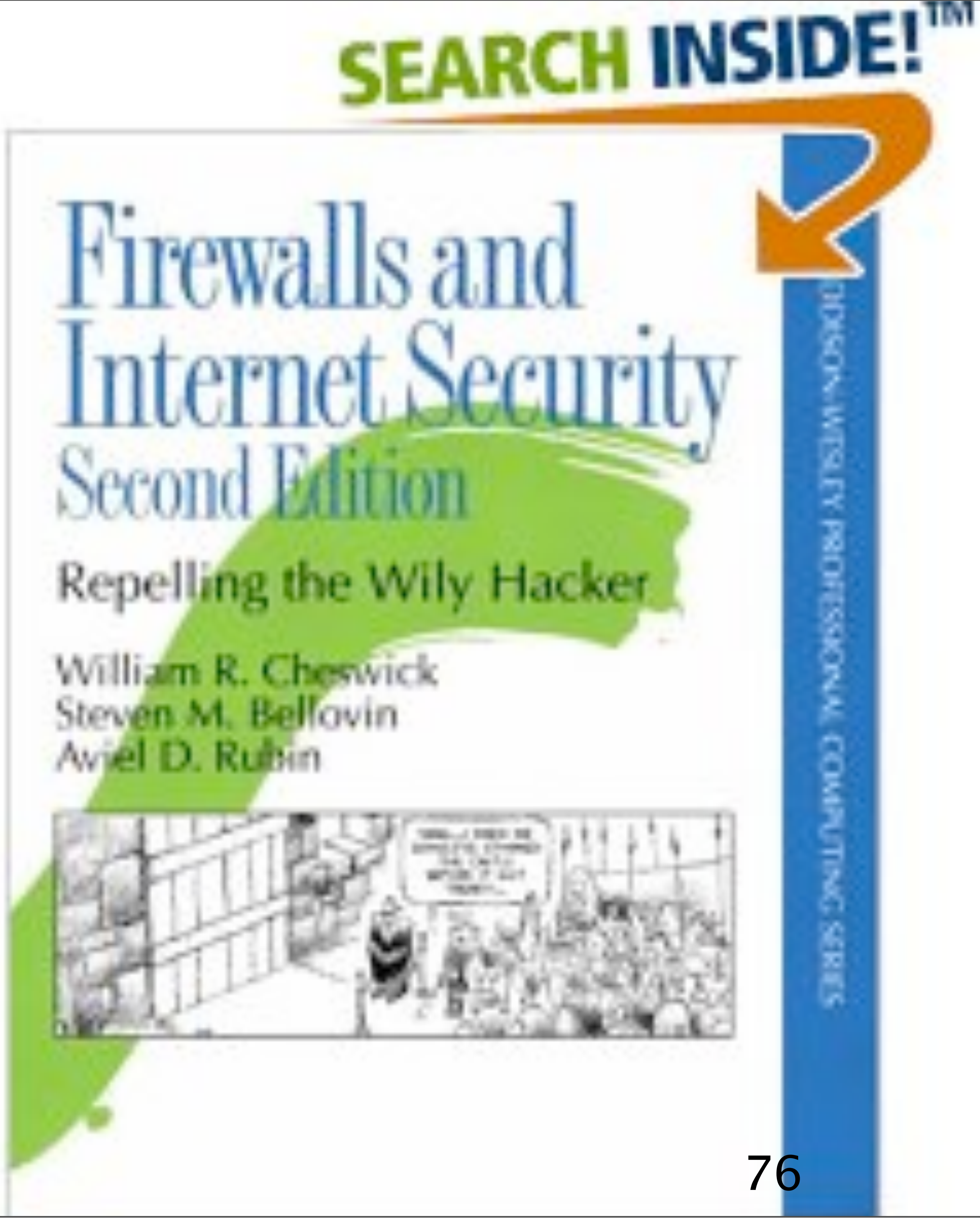
- Useful medium-level defense
- Little protection from invited trouble
- One of many tools

Many Bad Things are Out There

- We are losing the virus detection war
- Supply chain attacks are coming
- The bad guys only have to find one weakness
- Patch analysis reveals weaknesses

Firewalls and Perimeter Defense

Bill Cheswick
AT&T Shannon Labs
ches@research.att.com
http://www.cheswick.com/ches/talks/



SEARCH INSIDE!™

Firewalls and Internet Security

Second Edition

Repelling the Wily Hacker

William R. Cheswick
Steven M. Bellovin
Aviel D. Rubin

DDISON-WESLEY PROFESSIONAL COMPUTING SERIES