

Cybercrime, Cyberterrorism, and Cyberwar

Hostilities

Juan Tapiador

uc3m



In the beginning was the
command-line Internet

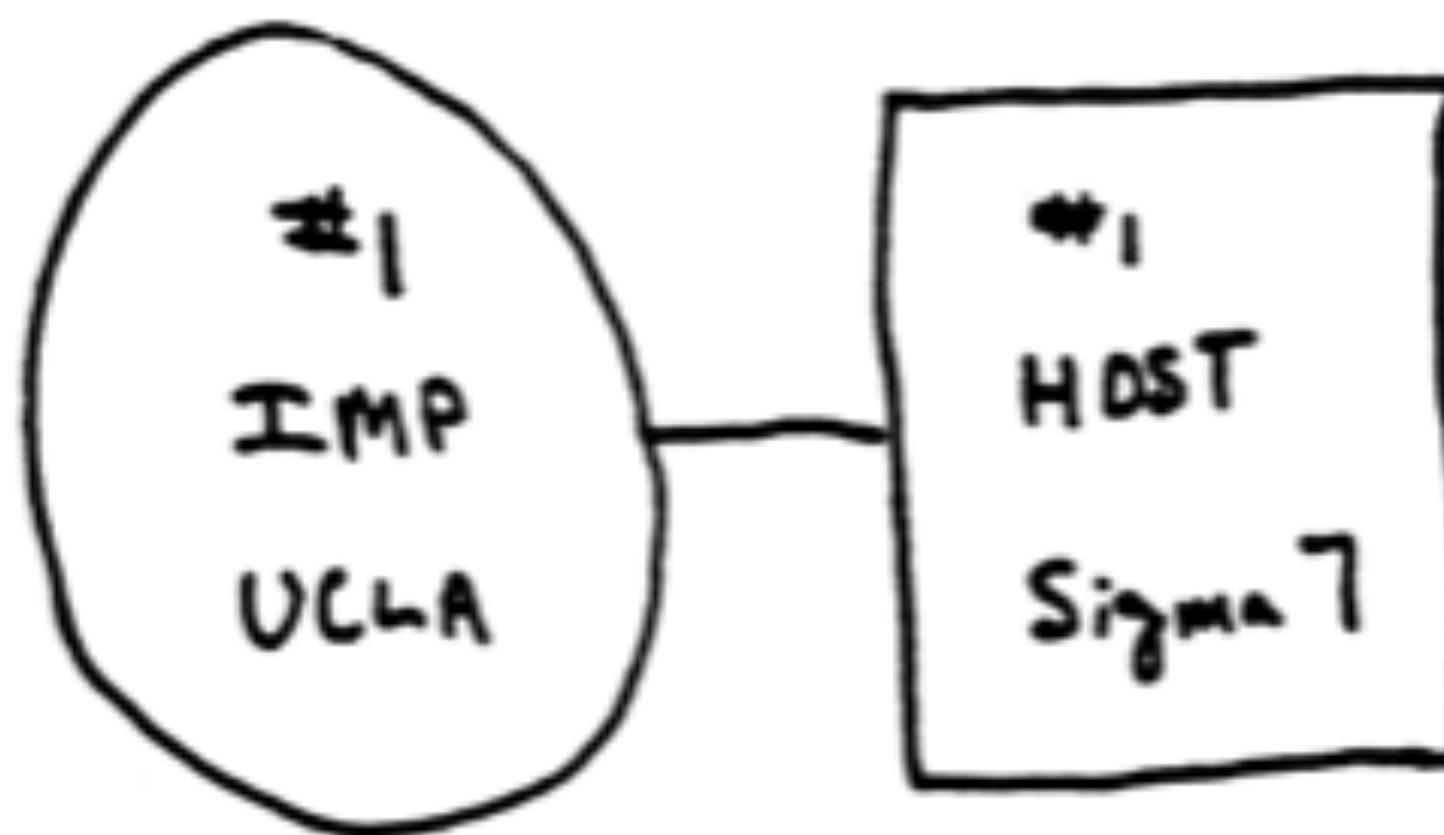
A drama in two parts



"It seems reasonable to envision, for a time 10 or 15 years hence, a '**thinking center**' that will incorporate the **functions of present-day libraries** together with anticipated advances in information storage and retrieval [...] The picture readily enlarges itself into a **network of such centers**, connected to one another by **wide-band communication lines** and to individual users by **leased-wire services**. In such a system, the speed of the computers would be balanced, and the cost of the gigantic memories and the sophisticated programs would be divided by the number of users."

J.C.R. Licklider, "Man-Computer Symbiosis", 1960

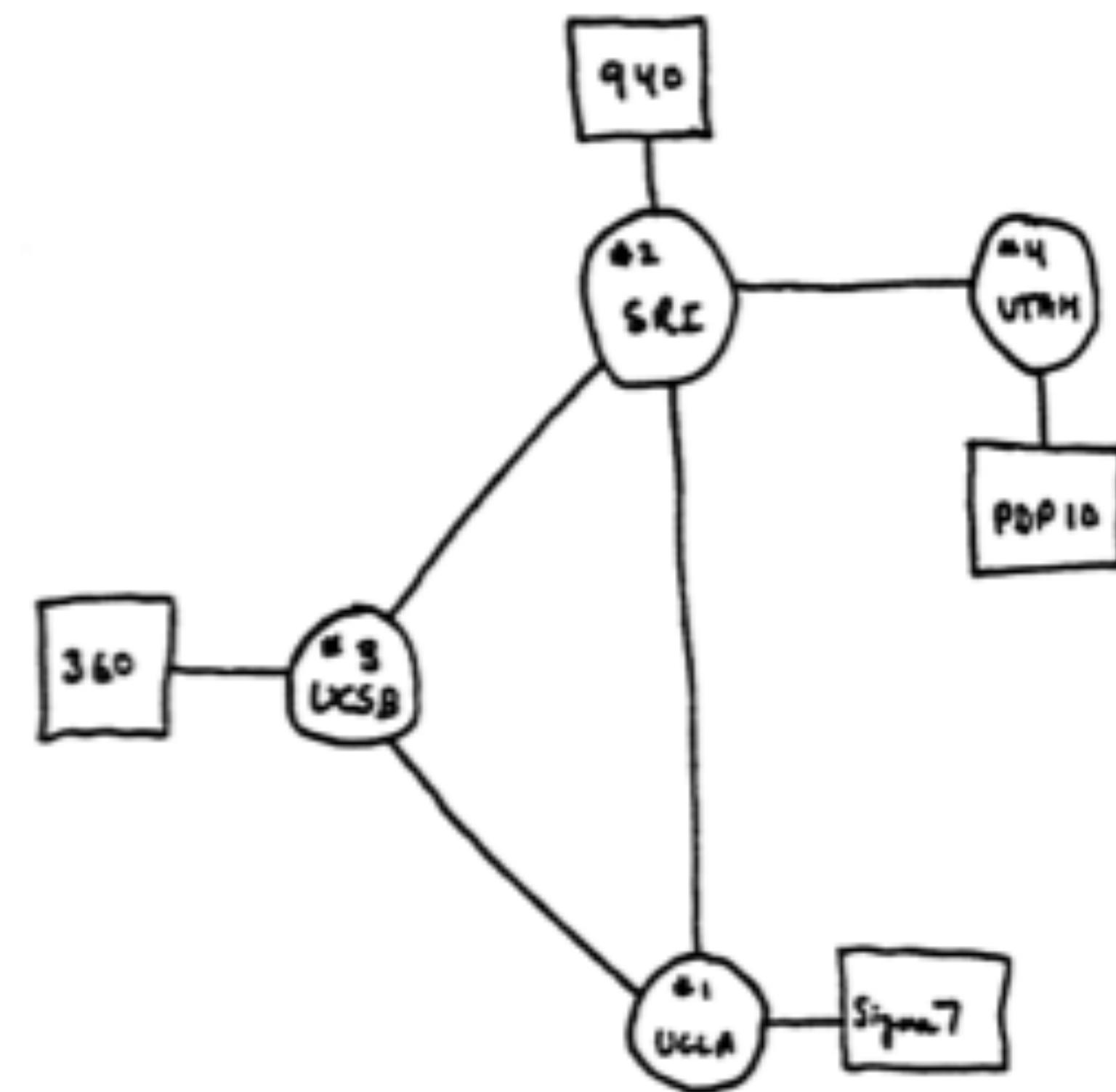
1969



THE ARPA NETWORK

SEPT 1969

1 NODE

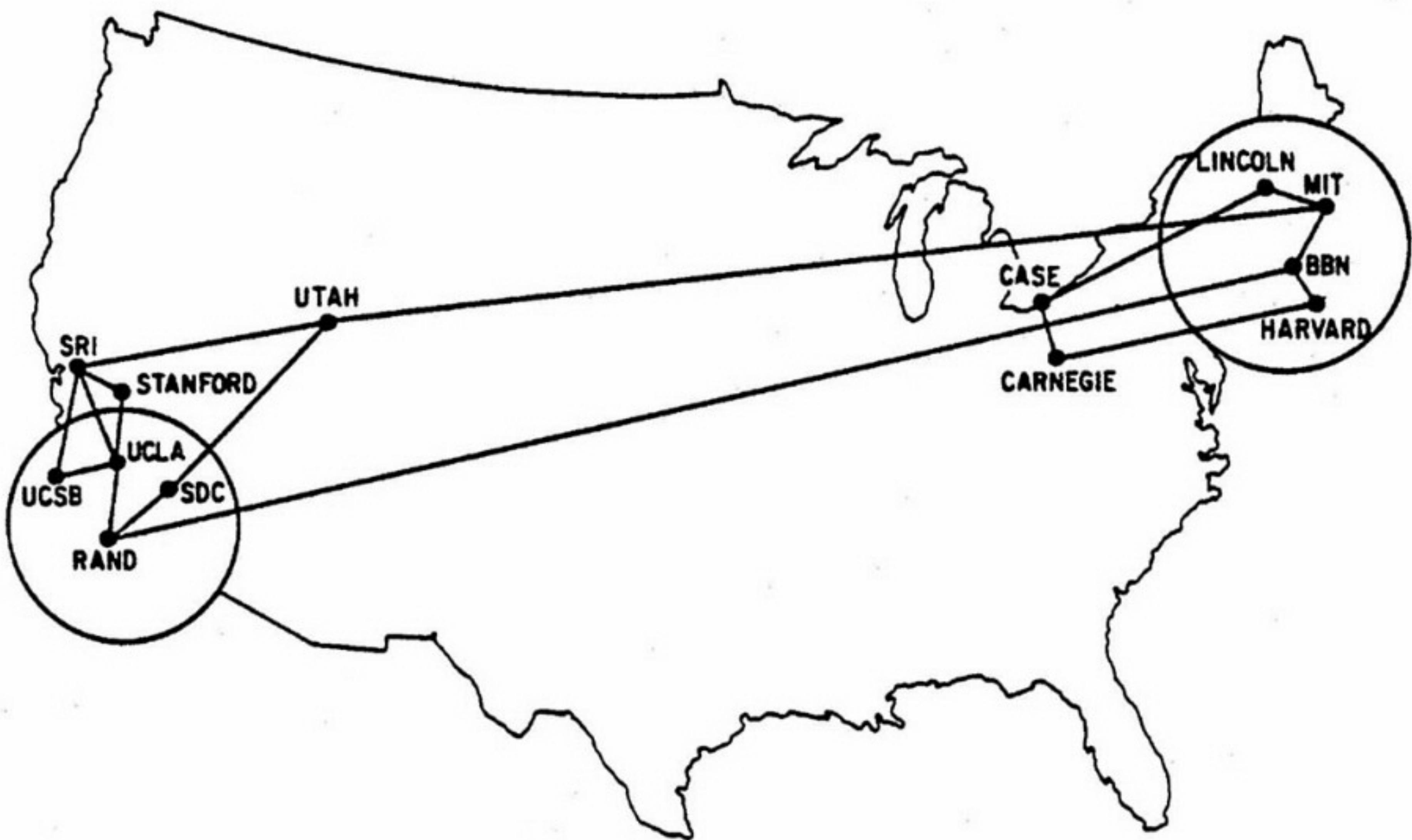


THE ARPA NETWORK

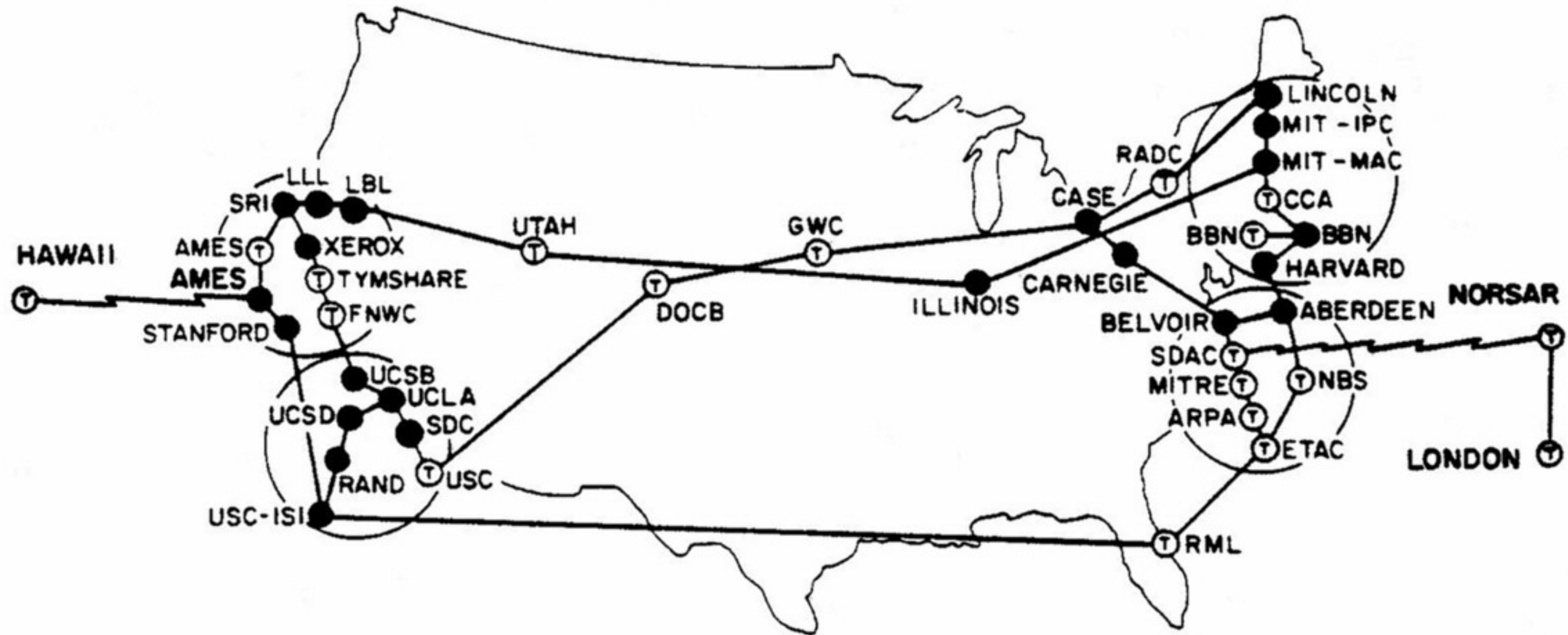
DEC 1969

4 NODES

1970

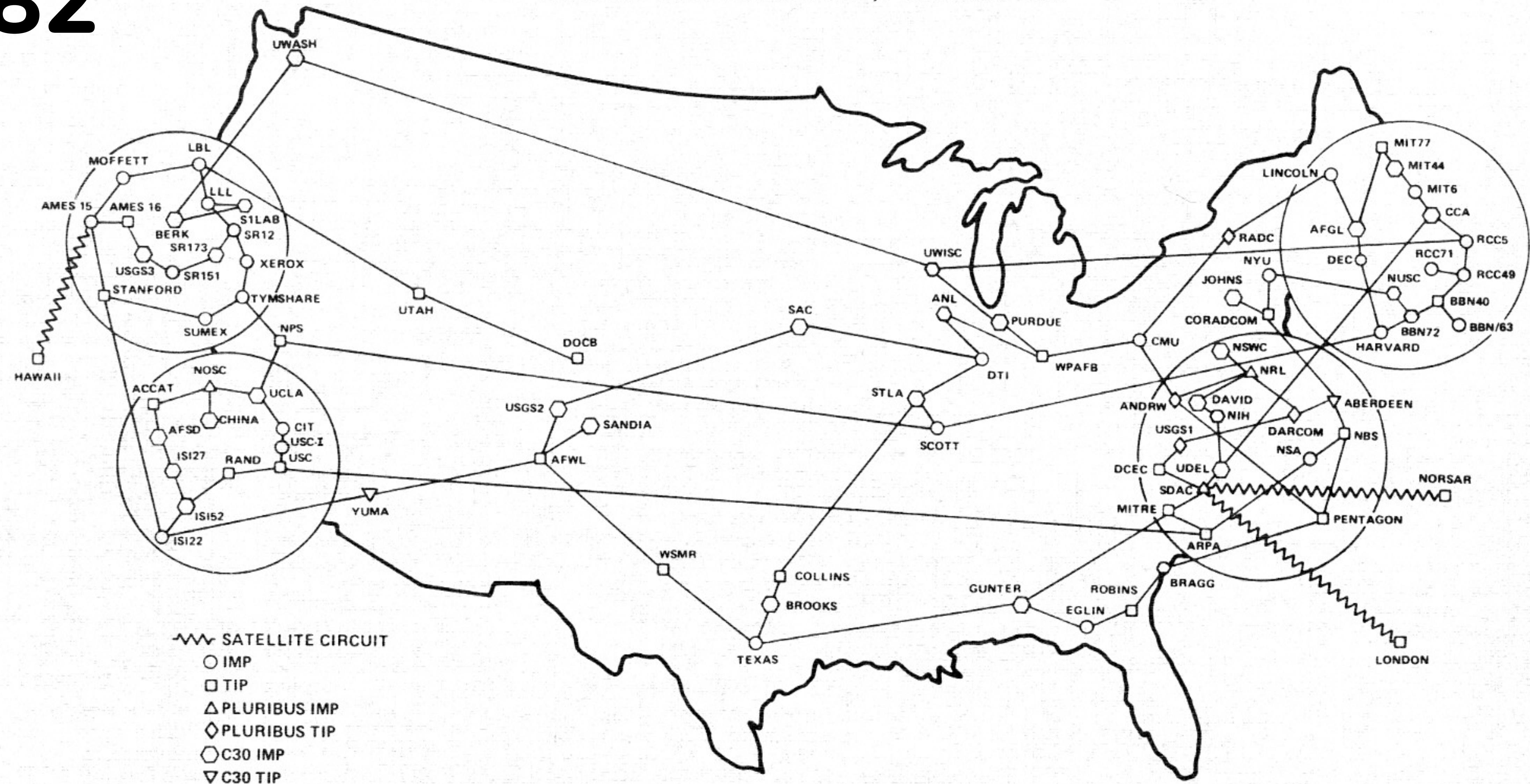


1973



1982

ARPANET GEOGRAPHIC MAP, FEBRUARY 1982

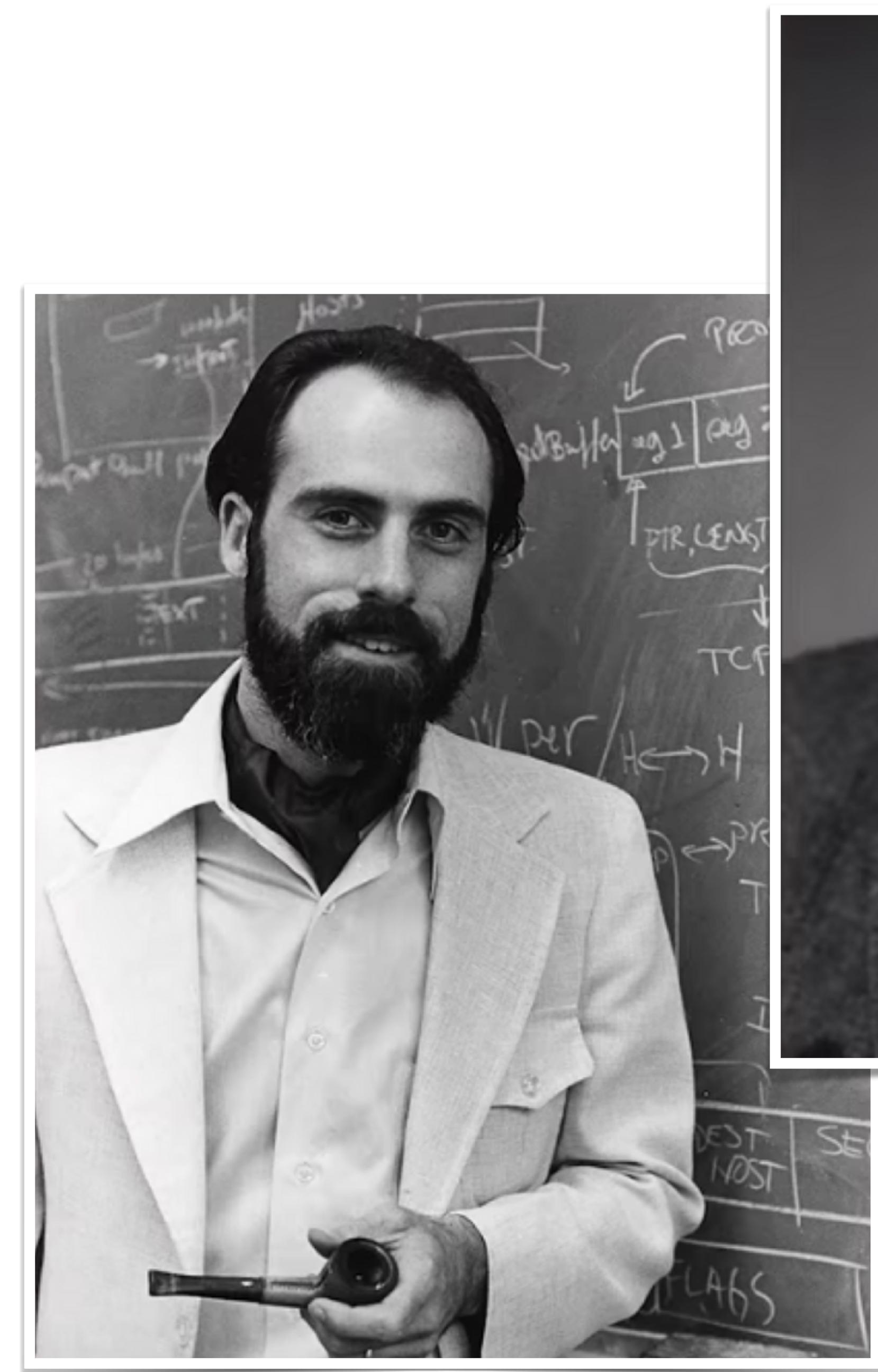


(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

1983

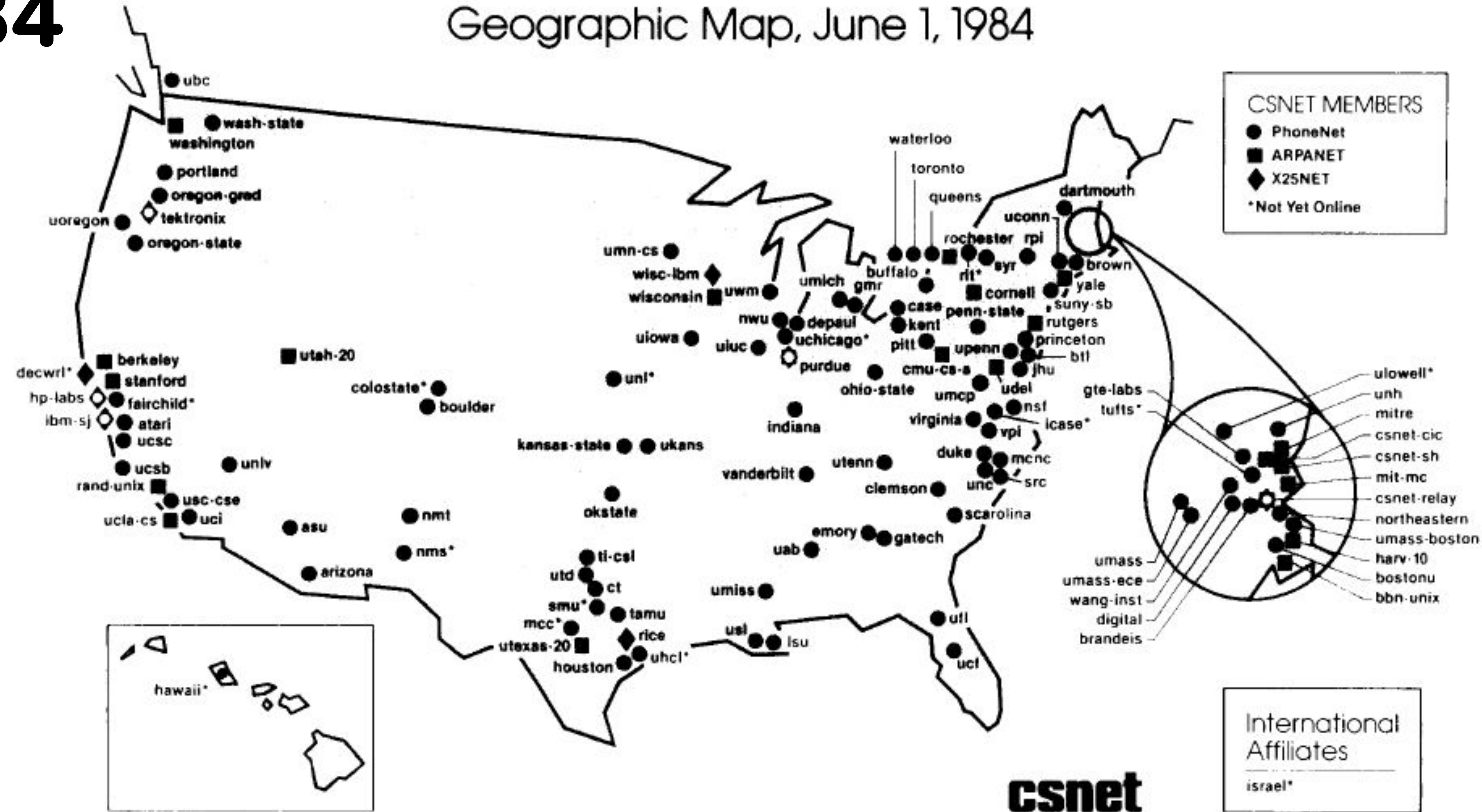
January 1, 1983

The ARPANET switched to using TCP/IP, marking the birth of the modern Internet

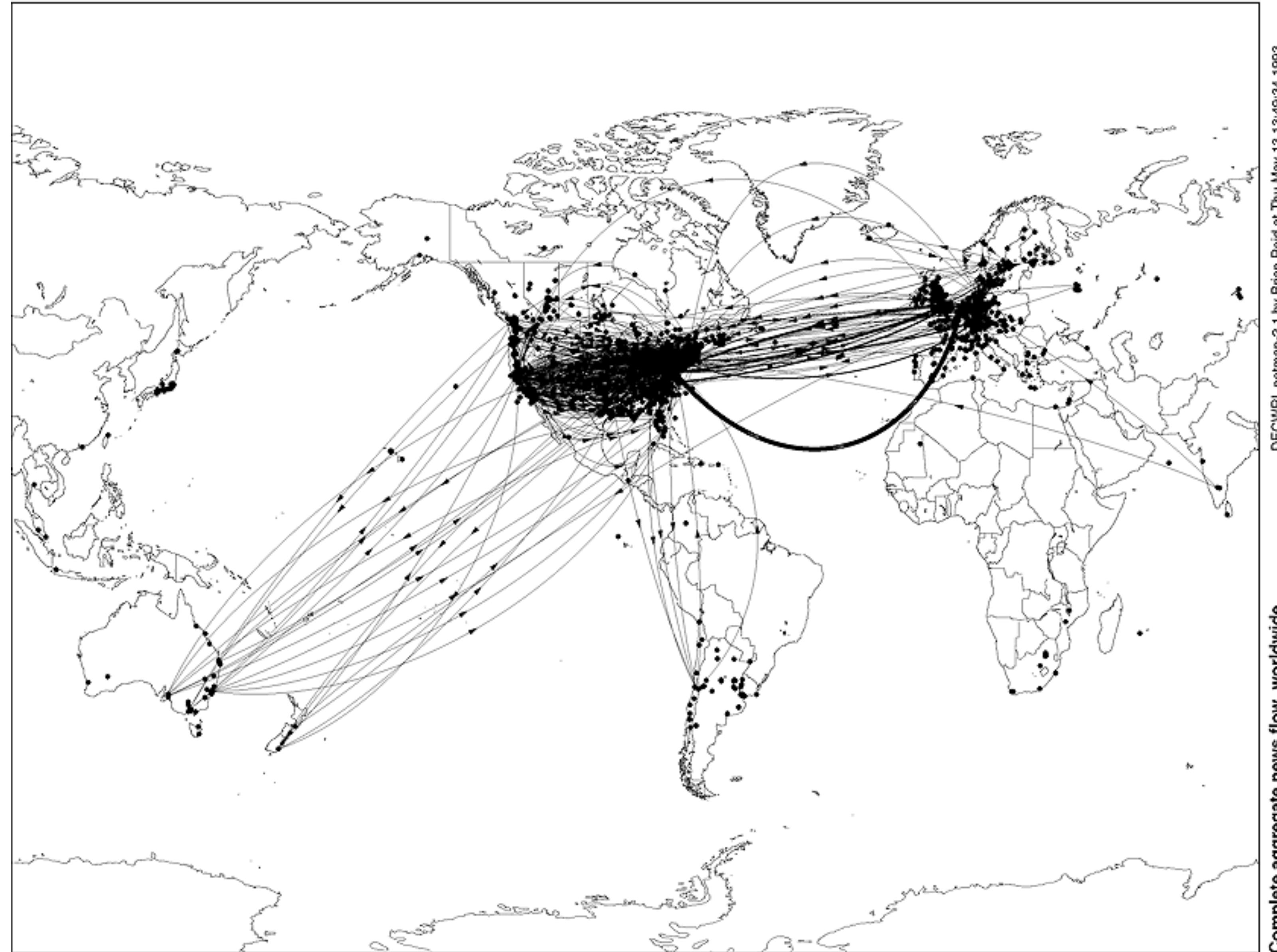


1984

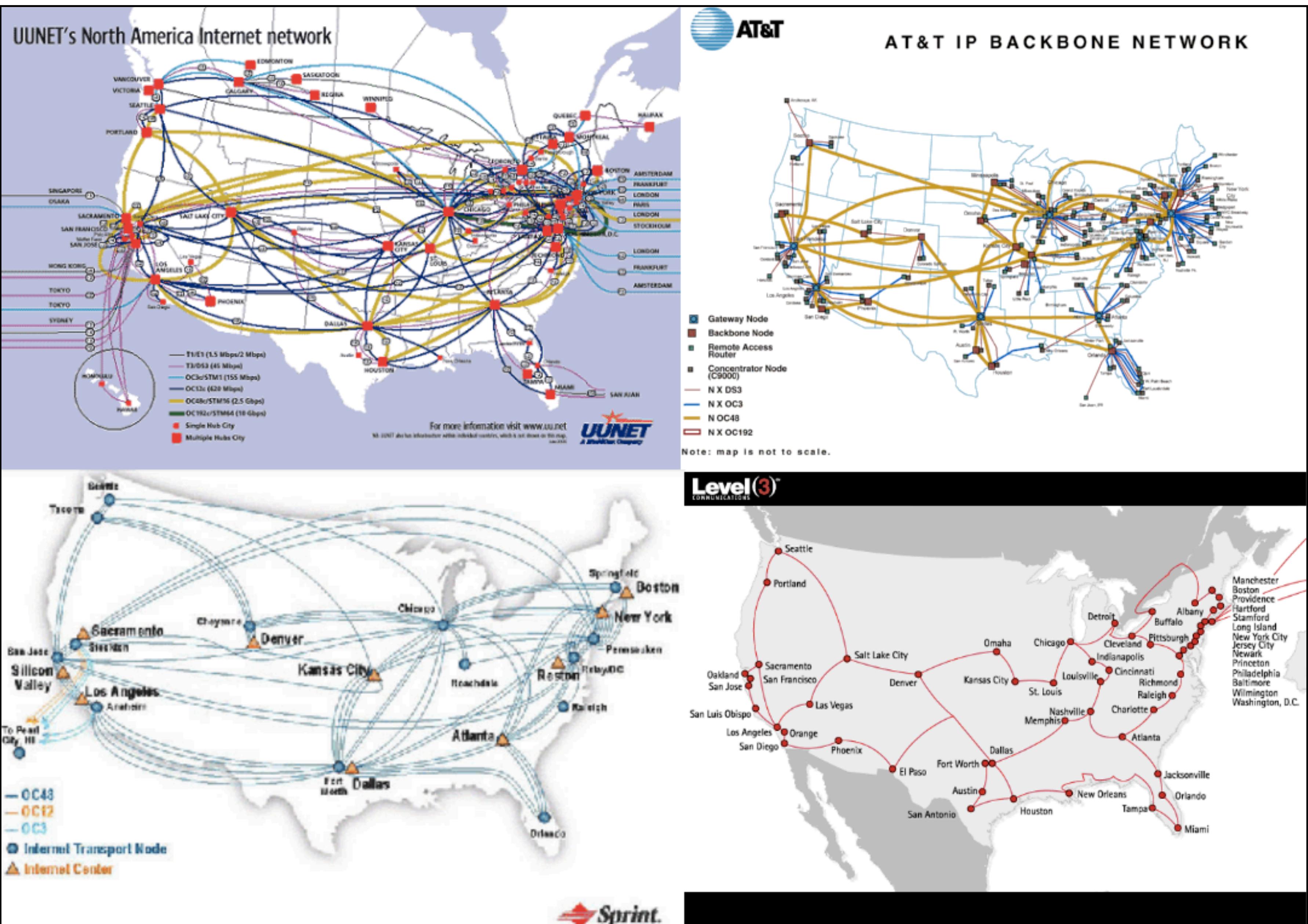
Geographic Map, June 1, 1984



1993

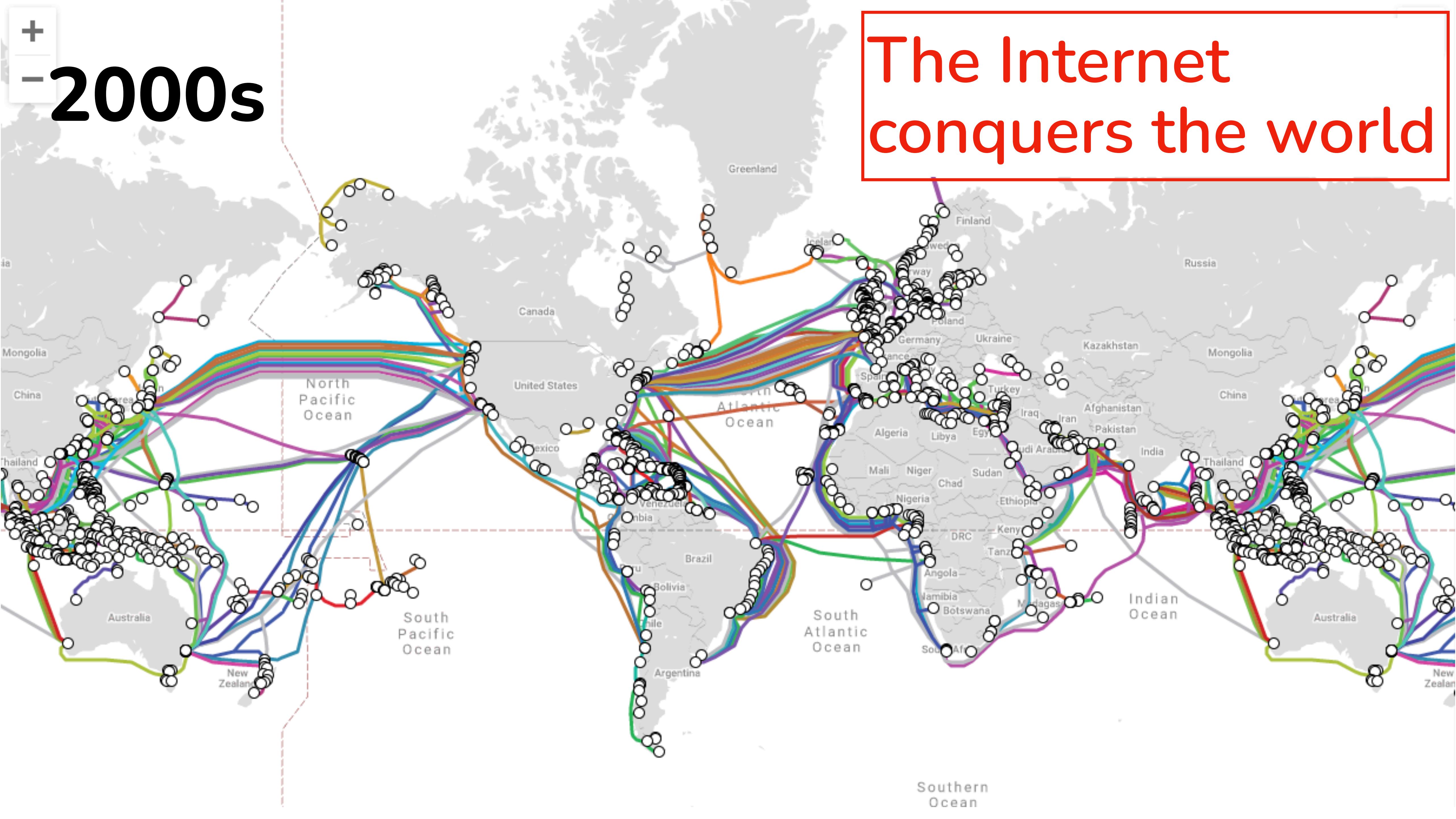


1994

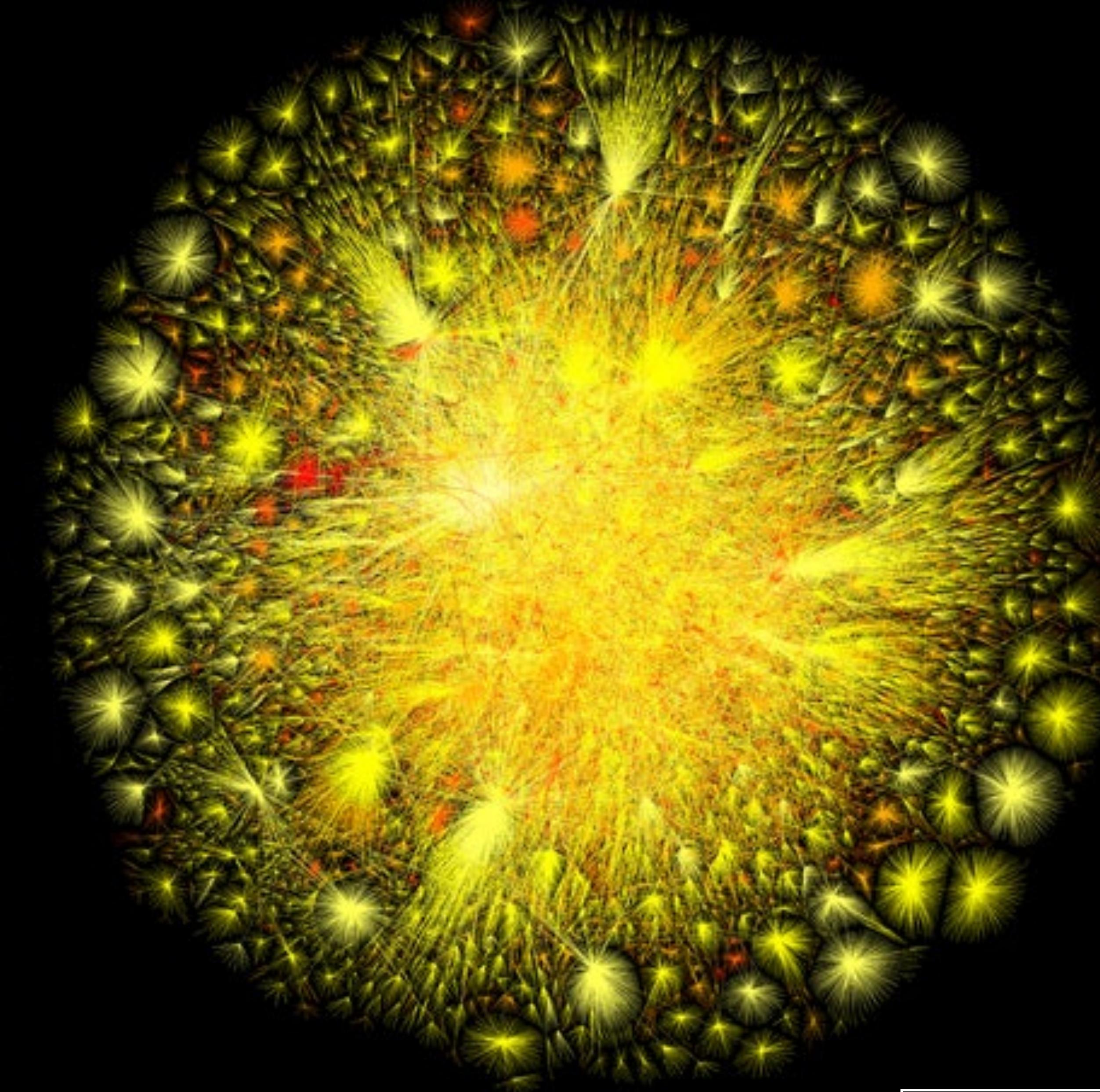
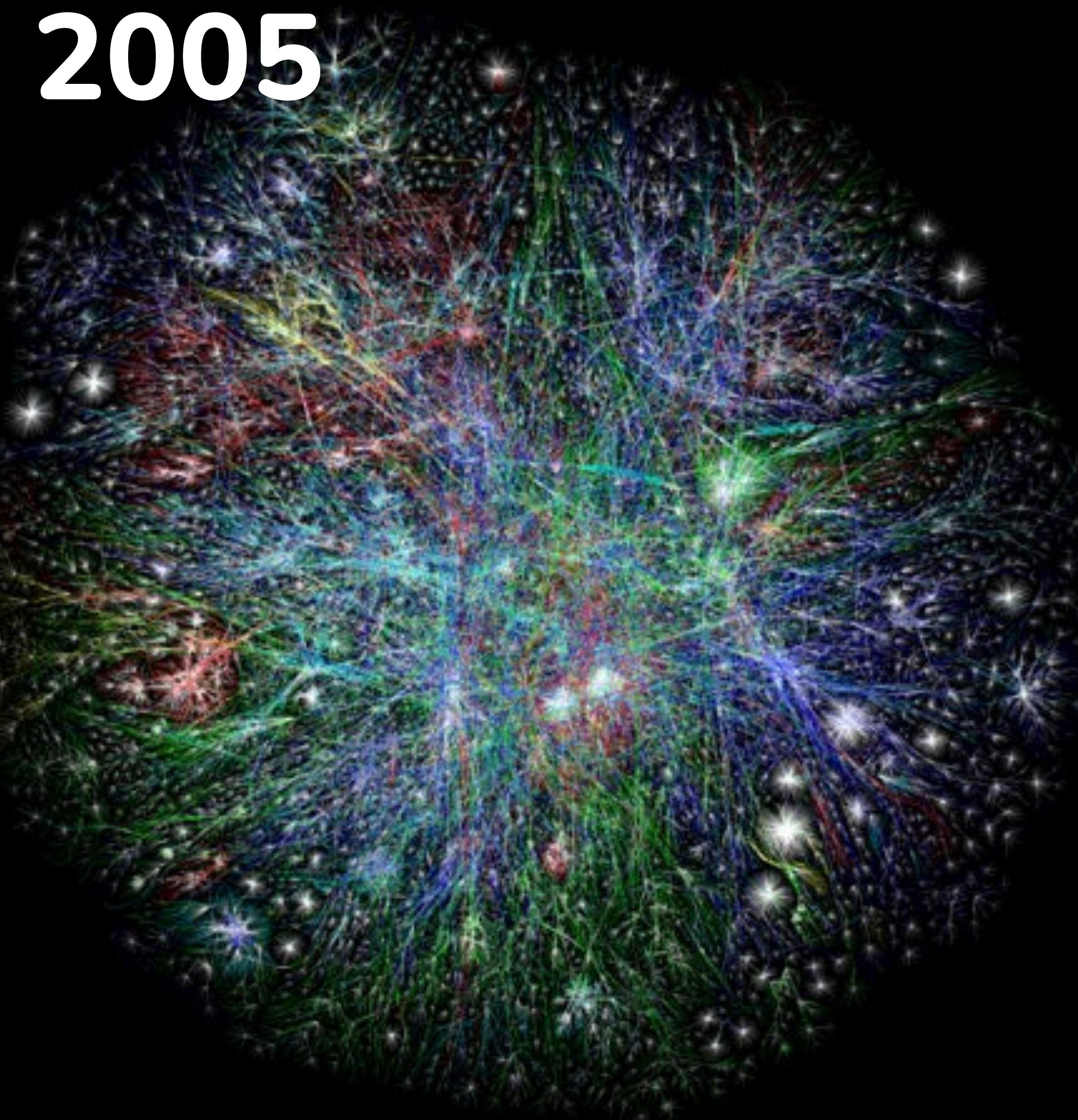


The Internet conquers the world

-2000s



2005



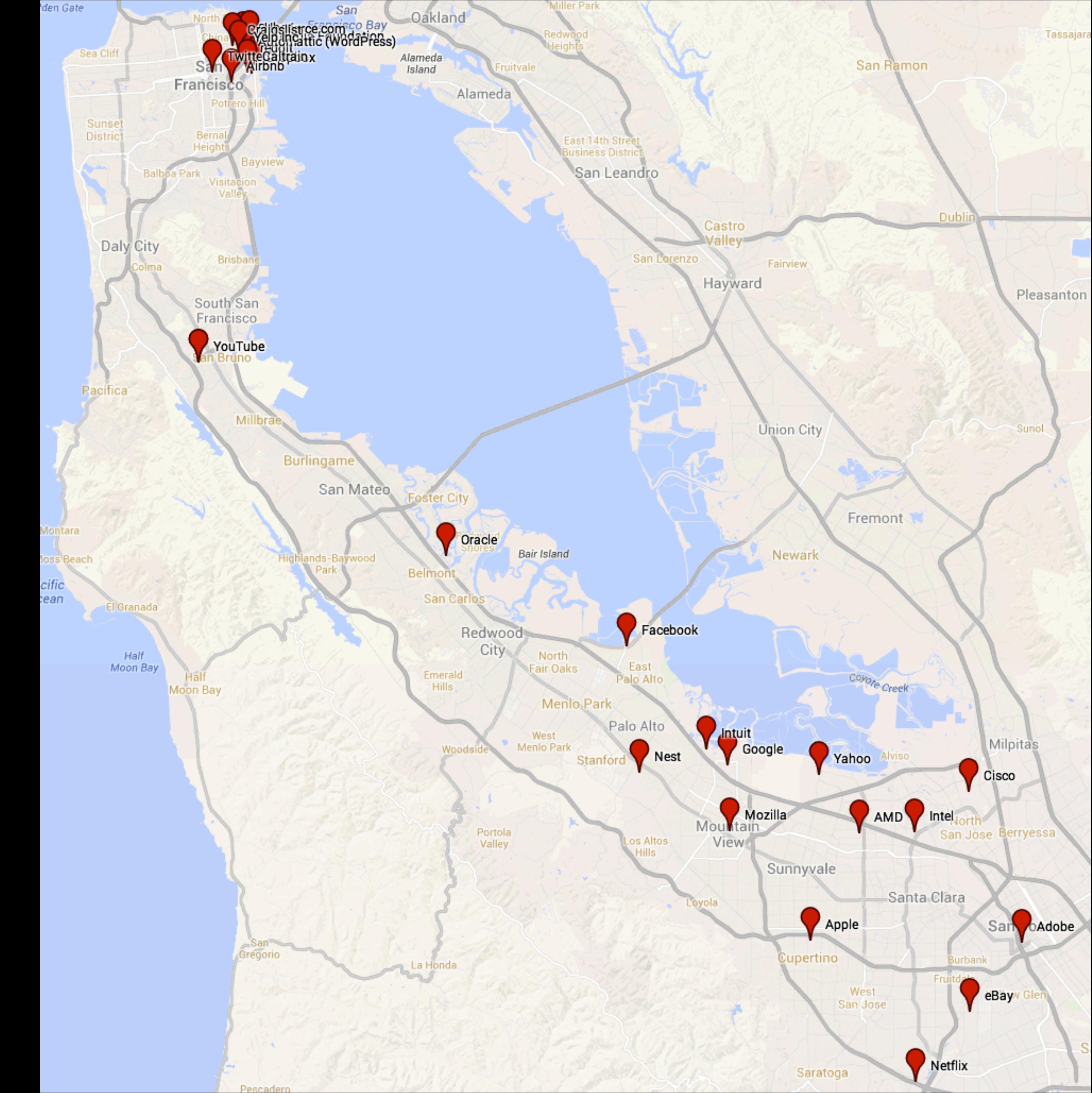
opte project



How big is the Internet?

www.internetlivestats.com

The capital of the Internet



The Internet is one of humanity's greatest achievements

It is the basis for all human communication at any distance

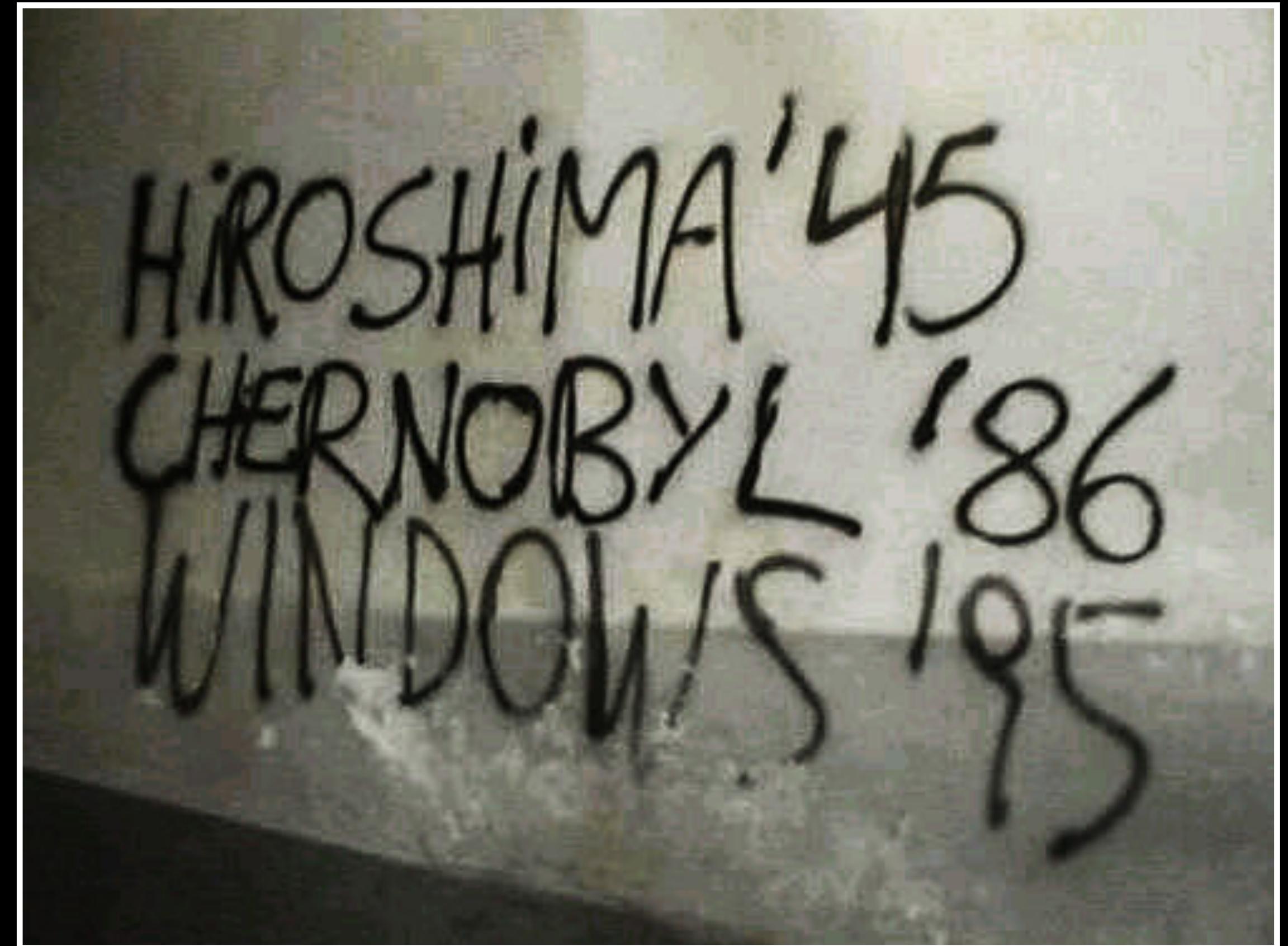
It is the ultimate repository of human's knowledge

It is the foundation of all world-scale software services

It is increasingly the basis for sensing and actuation in our world

and we are just getting started!

The Story Part II



It is the basis for all human communication at any distance

It is the ultimate repository of human's knowledge

It is the foundation of all world-scale software services

It is increasingly the basis for sensing and actuation in our world

What can possibly go wrong?



Threats

Multiple classifications depending on

result (type of incident)

severity (impact of the incident)

structure (type of opponent)

motive (reasons for attack)

threat vs threat actor

Types of security incidents

Class	Type	Description
Abusive content	Spam	"Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discretization or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals
	(Child) Sexual Exploitation/Sexual/Violent Content	Child Sexual Exploitation (CSE), sexual content, glorification of violence, etc.

Types of security incidents

Class	Type	Description
Malicious code	Infected system	System infected with malware, e.g. PC, smartphone or server infected with a rootkit. Most often this refers to a connection to a sinkholed C2 server
	C2 server	Command-and-control server contacted by malware on infected systems
	Malware distribution	URI used for malware distribution, e.g. a download URL included in fake invoice malware spam or exploit-kits (on websites)
	Malware configuration	URI hosting a malware configuration file, e.g. web-injects for a banking trojan

Types of security incidents

Class	Type	Description
Information gathering	Scanning	Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning
	Sniffing	Observing and recording of network traffic (wiretapping)
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats)

Types of security incidents

Class	Type	Description
Intrusion attempts	Exploitation of known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.)
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force). This IOC refers to a resource, which has been observed to perform brute-force attacks over a given application protocol
	New attack signature	An attack using an unknown exploit

Types of security incidents

Class	Type	Description
Intrusions	Privileged account compromise	Compromise of a system where the attacker gained administrative privileges
	Unprivileged account compromise	Compromise of a system using an unprivileged (user/service) account
	Application compromise	Compromise of an application by exploiting (un-)known software vulnerabilities, e.g. SQL injection
	System compromise	Compromise of a system, e.g. unauthorised logins or commands. This includes compromising attempts on honeypot systems
	Burglary	Physical intrusion, e.g. into corporate building or data-centre

Types of security incidents

Class	Type	Description
Availability	Denial of service (DoS)	Denial of Service attack, e.g. sending specially crafted requests to a web application which causes the application to crash or slow down
	Distributed denial of service (DDoS)	Distributed Denial of Service attack, e.g. SYN-Flood or UDP-based reflection/amplification attacks
	Misconfiguration	Software misconfiguration resulting in service availability issues, e.g. DNS server with outdated DNSSEC Root Zone KSK
	Sabotage	Physical sabotage, e.g. cutting wires or malicious arson
	Outage	Outage caused e.g. by air condition failure or natural disaster

Types of security incidents

Class	Type	Description
Information content security	Unauthorised access to information	Unauthorised access to information, e.g. by abusing stolen login credentials for a system or application, intercepting traffic or gaining access to physical documents
	Unauthorised modification of information	Unauthorised modification of information, e.g. by an attacker abusing stolen login credentials for a system or application or a ransomware encrypting data. Also includes defacements
	Data loss	Loss of data, e.g. caused by harddisk failure or physical theft
	Leak of confidential information	Leaked confidential information like credentials or personal data

Types of security incidents

Class	Type	Description
Fraud	Unauthorised use of resources	Using resources for unauthorised purposes including profit-making ventures, e.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes
	Copyright	Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez)
	Masquerade	Type of attack in which one entity illegitimately impersonates the identity of another in order to benefit from it
	Phishing	Masquerading as another entity in order to persuade the user to reveal private credentials. This IOC most often refers to a URL, which is used to phish user credentials

Types of security incidents

Class	Type	Description
Vulnerable	Weak crypto	Publicly accessible services offering weak crypto, e.g. web servers susceptible to POODLE/FREAK attacks
	DoS amplifier	Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks, e.g. DNS open-resolvers or NTP servers with monlist enabled
	Potentially unwanted accessible services	Potentially unwanted publicly accessible services, e.g. Telnet, RDP or VNC
	Information disclosure	Publicly accessible services potentially disclosing sensitive information, e.g. SNMP or Redis
	Vulnerable system	A system which is vulnerable to certain attacks, i.e., misconfigured client proxy settings (e.g., WPAD), outdated operating system, XSS vulnerabilities, etc

Types of security incidents

Class	Type	Description
Others	Uncategorized	All incidents which don't fit in one of the given categories should be put into this class or the incident is not categorized
	Undetermined	The categorization of the incident is unknown/undetermined

Threats according to potential for harm

	Class	Type(s)	
Critical	Others	APT	
Very high	Malicious code Intrusion Availability	Malware distribution Theft Sabotage	Malware configuration Interruptions
High	Abusive content Harmful code Intrusion Intrusion attempt Availability Data compromise Fraud	Child pornography Infected system App compromise Unknown attack DoS Unauthorized access Phishing	Inadequate sexual or violent content C&C server Privileged account compromise DDoS Data leak Unauthorized data modif.

Threats according to potential for harm

	Class	Type(s)	
Medium	Abusive content	Harmful speech	Login attempts
	Info gathering	Social engineering	
	Intrusion attempt	Exploitation of known vulns	
	Intrusion	Unprivileged account compromise	
	Availability	Misconfiguration	Copyright
	Fraud	Unauthorized use of resources	
	Masquerade		
	Vulnerable	Weak crypto DDoS amplifier Information disclosure	
Low	Abusive content	Spam	Sniffing
	Info gathering	Scanning	
	Others	Others	

Threats according to impact

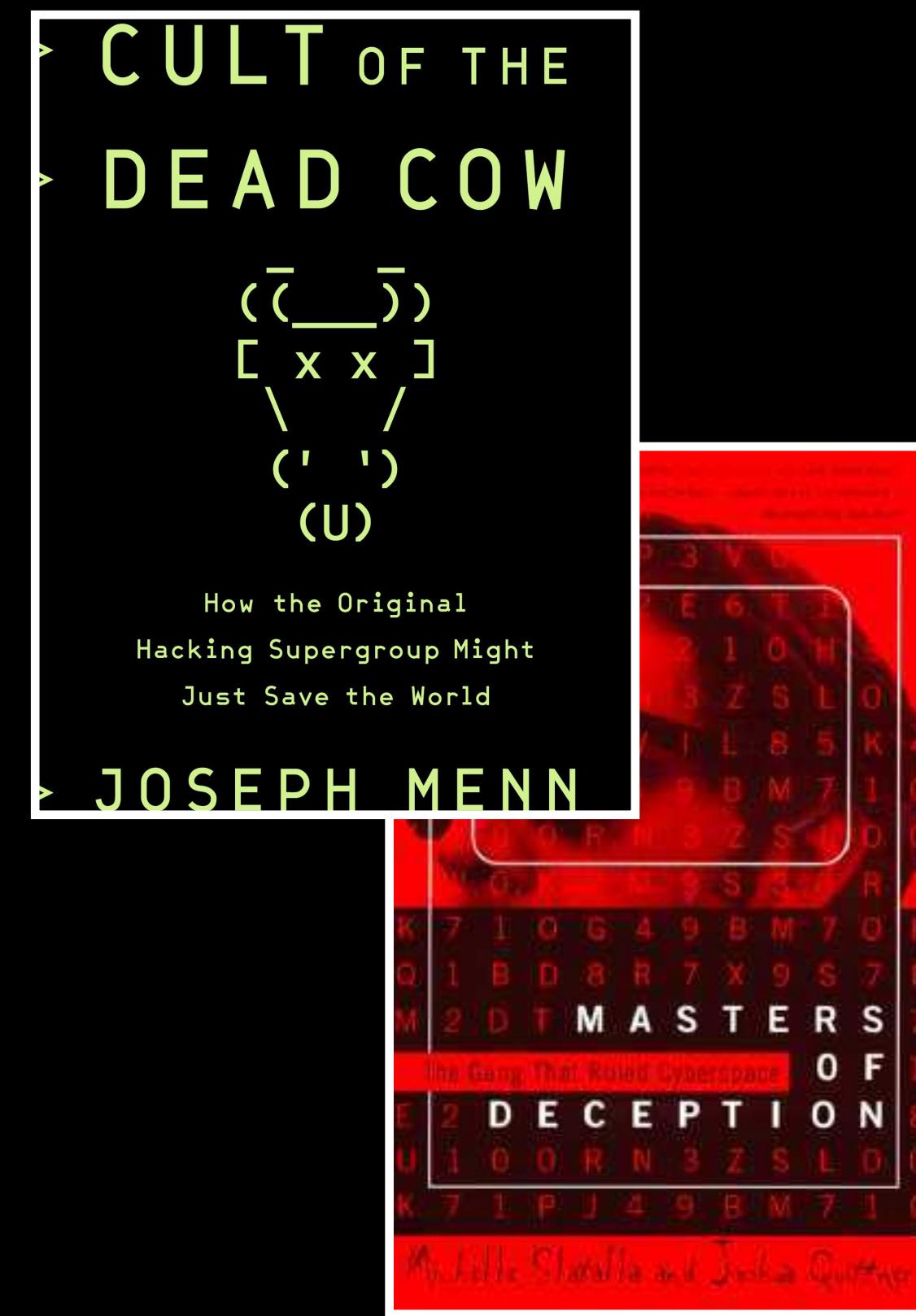
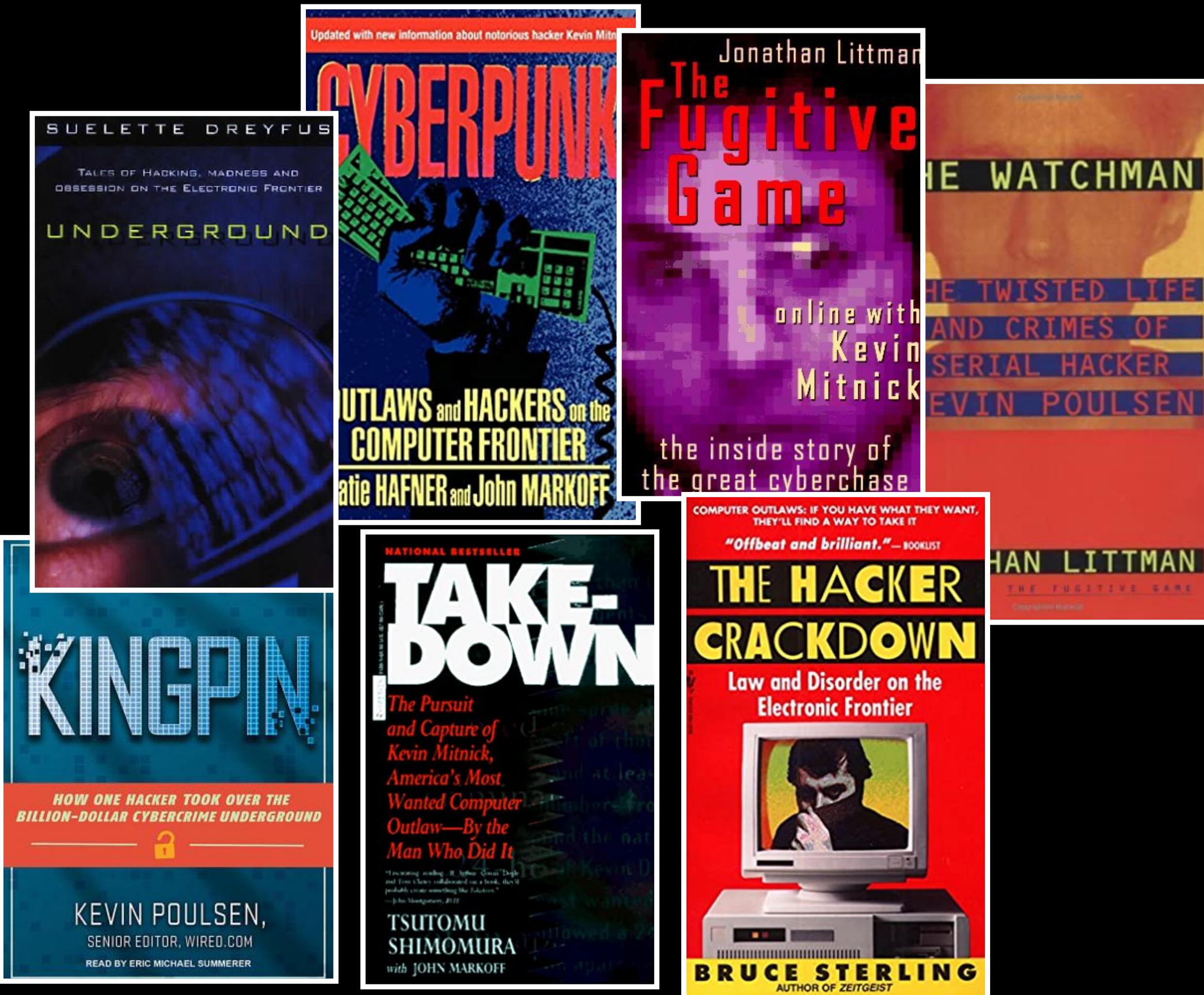
	National security Citizens' lives	Critical infras. Essential service	% affected systems	Recovery time & cost	Economic impact	Reputational impact
Critical	potentially	yes	90%+ systems 50%+ users	100+ person-day	0,1% GDP	very high continuous intl. news coverage
Very high
High
Medium
Low	no	no	1 isolated system	<1 person- day	[0.001%, 0.0001%] GDP	isolated, no news
No impact	no	no	negligible	negligible	negligible	negligible

Threats according to structure

	Unstructured	Structured	Highly structured
Who	individuals small groups	groups	units
Organization	little to none	well organized and planned	well organized and planned
Funding	no	good	extensive & sustained over time
Intelligence	OSINT easily detectable	OSINT private / insiders	all
TTPs	documented	documented 0days	documented 0days
Target	opportunistic	specific	strategic
Motivation	bragging, personal, economic, ...	gain of IP/secrets, military/political dominance	state reasons

How did we get here?

The early(-ish) days



And then things changed forever

Early-to-mid 2000s

From

- no payload
- noisy
- large scale, same threat
- 10s per week

To

- spammers, info stealers, ...
- quiet & evasive
- micro distribution
- 10,000s per day

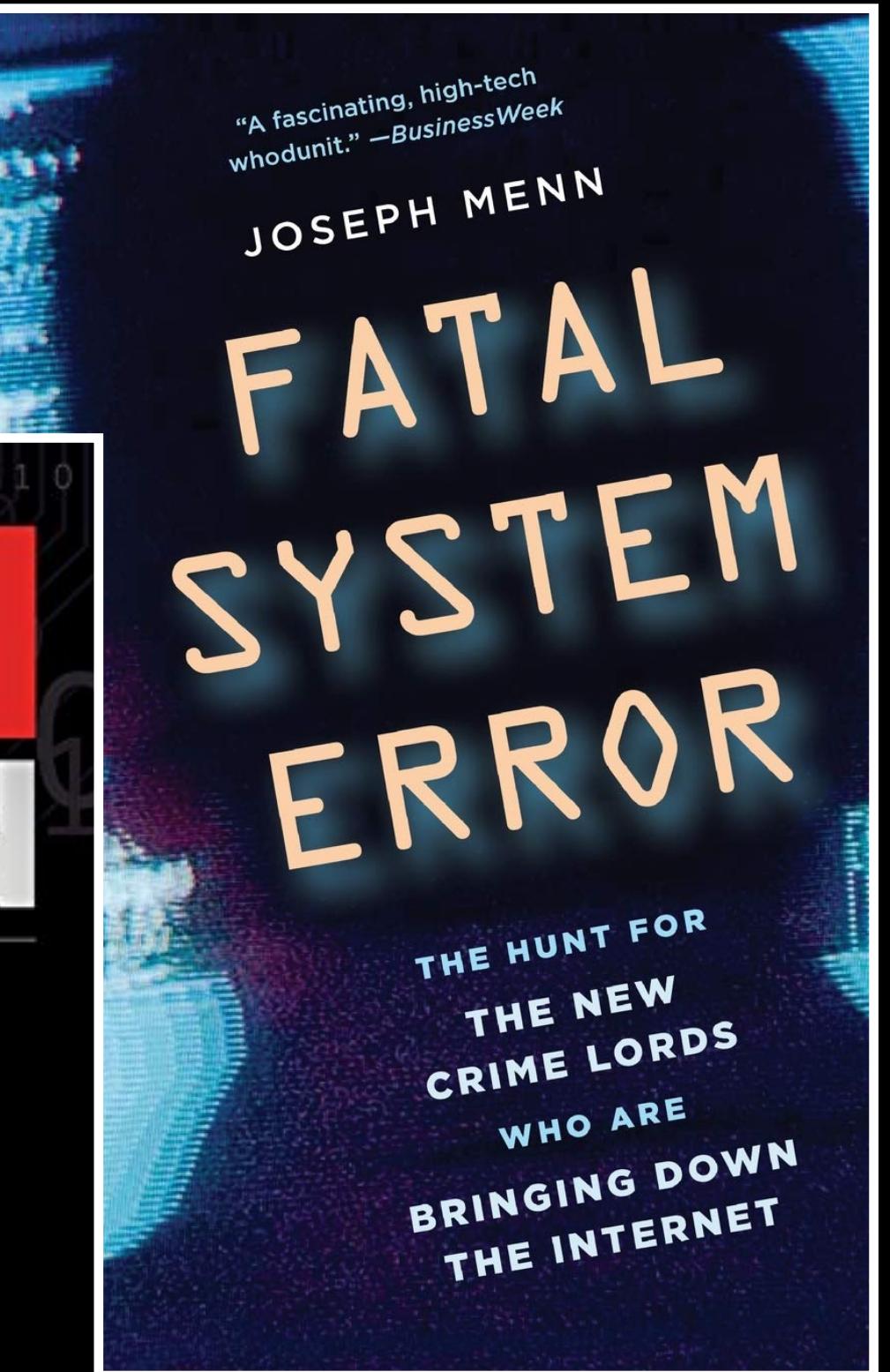
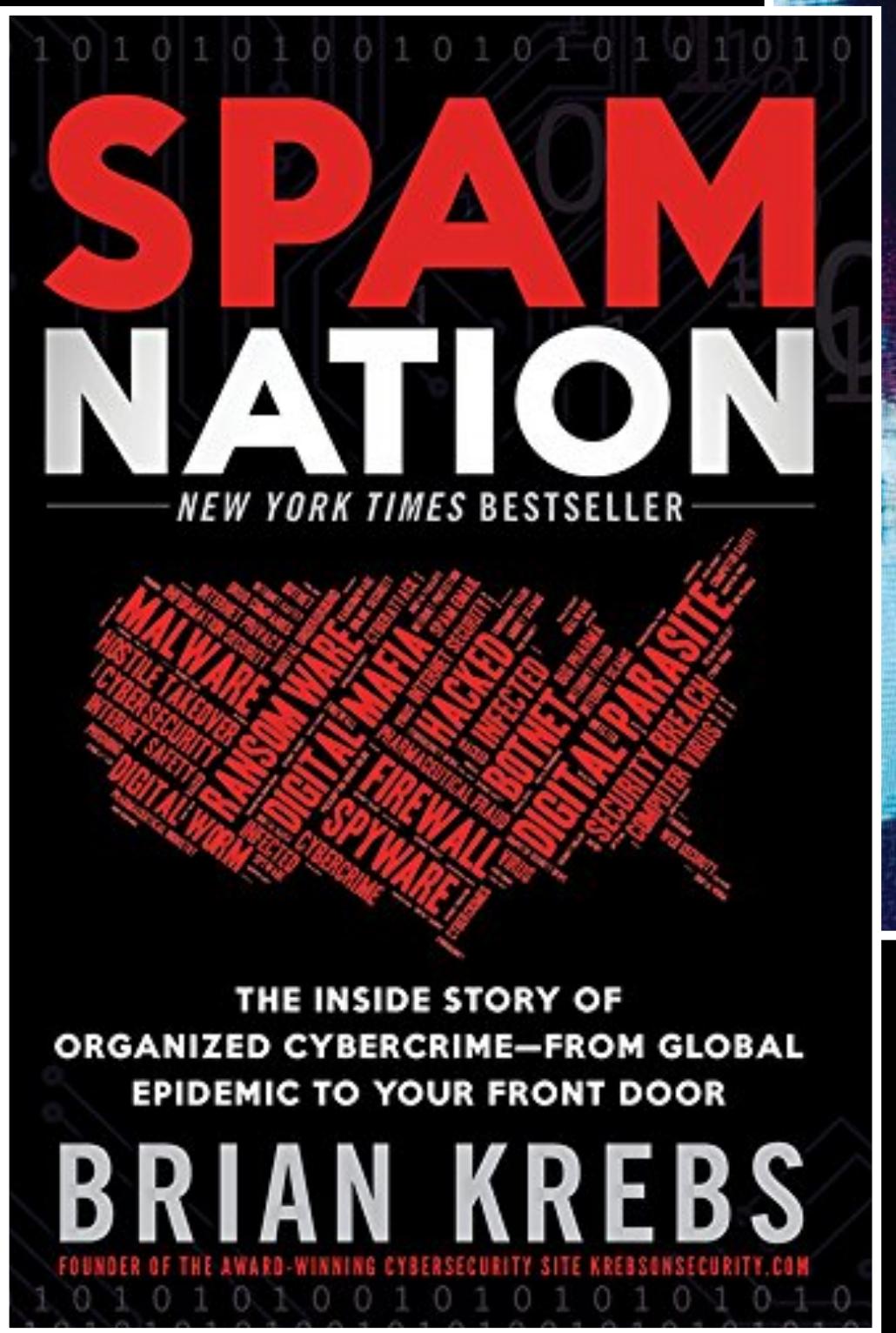
fame

profit

The underground economy of cybercrime

Underground markets where actors
specialize
scale up
globalize

(as manufacturing did in the late 18th century)



NSA FILES: DECODED

What the revelations mean for you.

Exclusive
Revealed: how US secretly collects private data from AOL, Apple, Facebook, Google, Microsoft, Paltalk, Skype, Yahoo and YouTube
the guardian
guardian.co.uk

Files prove existence of undercover operation codenamed Prism

Exclusive
Revealed: how UK spied on its G20 allies at London summits
the guardian
guardian.co.uk

● Politicians' calls and emails intercepted by UK intelligence
● Delegates tricked into using fake internet cafes
● Analysts at GCHQ sent logs of phone calls round the clock
● Documents revealed by US whistleblower Snowden
● Revelations come as UK prepares to host G8 leaders



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Where is X-KEYSCORE?
the guardian
guardian.co.uk

Exclusive Secret tool searches email

exclusive
UK used Google and Facebook to spy on us
the guardian
weekend edition

Pressure on government over secret intelligence gathering

Tour de France Froome's show of strength gives rivals something to worry about
the guardian
guardian.co.uk

Glastonbury special

New leaks show how US is bugging its European allies
DROPMIRE

Cameron pushed into early vote on marriage tax break
MIF
MANCHESTER INTERNATIONAL FESTIVAL
4 - 21 July 2013
See page 3

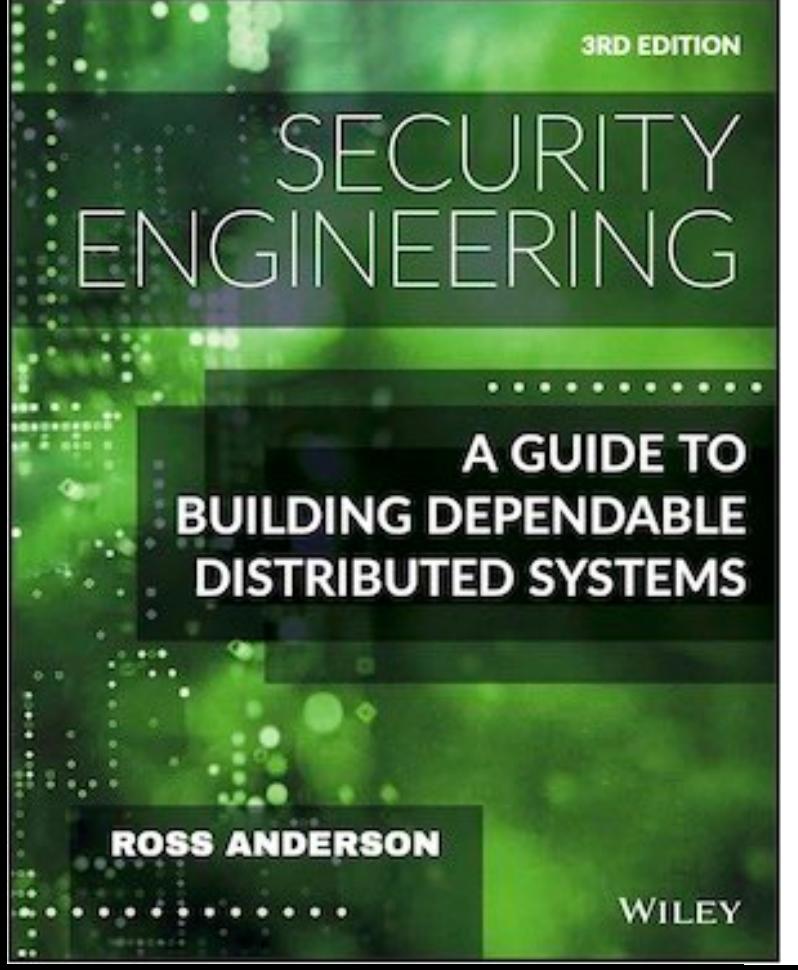
The 2010s

Platforms

Stabilization of
the cybercrime
ecosystem

Online
abuse &
hostility

Opponents



Chapter 2

Who is the Opponent?

The
Spooks

The
Crooks

The
Geeks

The
Swamp

Why is security hard?

At the start of this century, security technology was an archipelago of mutually suspicious islands – the cryptologists, the operating system protection people, the burglar alarm industry, right through to the chemists who did banknote inks. We all thought the world ended at our shore. By 2010, security engineering was an established and growing discipline; the islands were being joined up by bridges as practitioners realised we had to look beyond our comfort zones. The banknote ink chemist who didn't want to understand digital watermarks, and the cryptologist who could only talk about confidentiality, were steadily marginalised.

Now, in 2020, everyone needs to have a systems perspective in order to design components that can be integrated usefully into real products and services. And as these are used by real people, and often at global scale, our field is embracing the humanities and social sciences too.

Ross Anderson, “Security Engineering”, 3rd Edition, Ch.29

Many persistent security failures
are incentive failures

Many persistent security failures
are usability failures

Many persistent security failures
are complexity failures

Technical and—especially—social complexity

New technologies have unanticipated consequences



addictive

invasive

alienating

spying

apocalyptic

Many persistent security failures are politics failures

*What would our technology look like if it aspired to keep everyone safe?
Who loses and who gains when “computer says no”?*

Tech monopolies and the nature of power

Facebook becoming the de facto arbiter of political speech

Google and Apple dictating policy on coronavirus contact tracing

Amazon, Microsoft and Google dictating policy on facial recognition

Thierry Breton  @ThierryBreton · Apr 22

I just had a good exchange with #Apple CEO @tim_cook on the need to ensure that contact tracing apps are fully:

- ✓ anonymised
- ✓ voluntary
- ✓ transparent
- ✓ temporary
- ✓ secured

and interoperable across operating systems and borders.

#Deconfinement apps must respect our #privacy.



Tim Cook

158 742 2K 