The evolution of cyber defense

Maarten Van Horenbeeck
Chairman, FIRST

FIRST™
Improving Security Together

Forum of Incident Response and Security Teams

Things

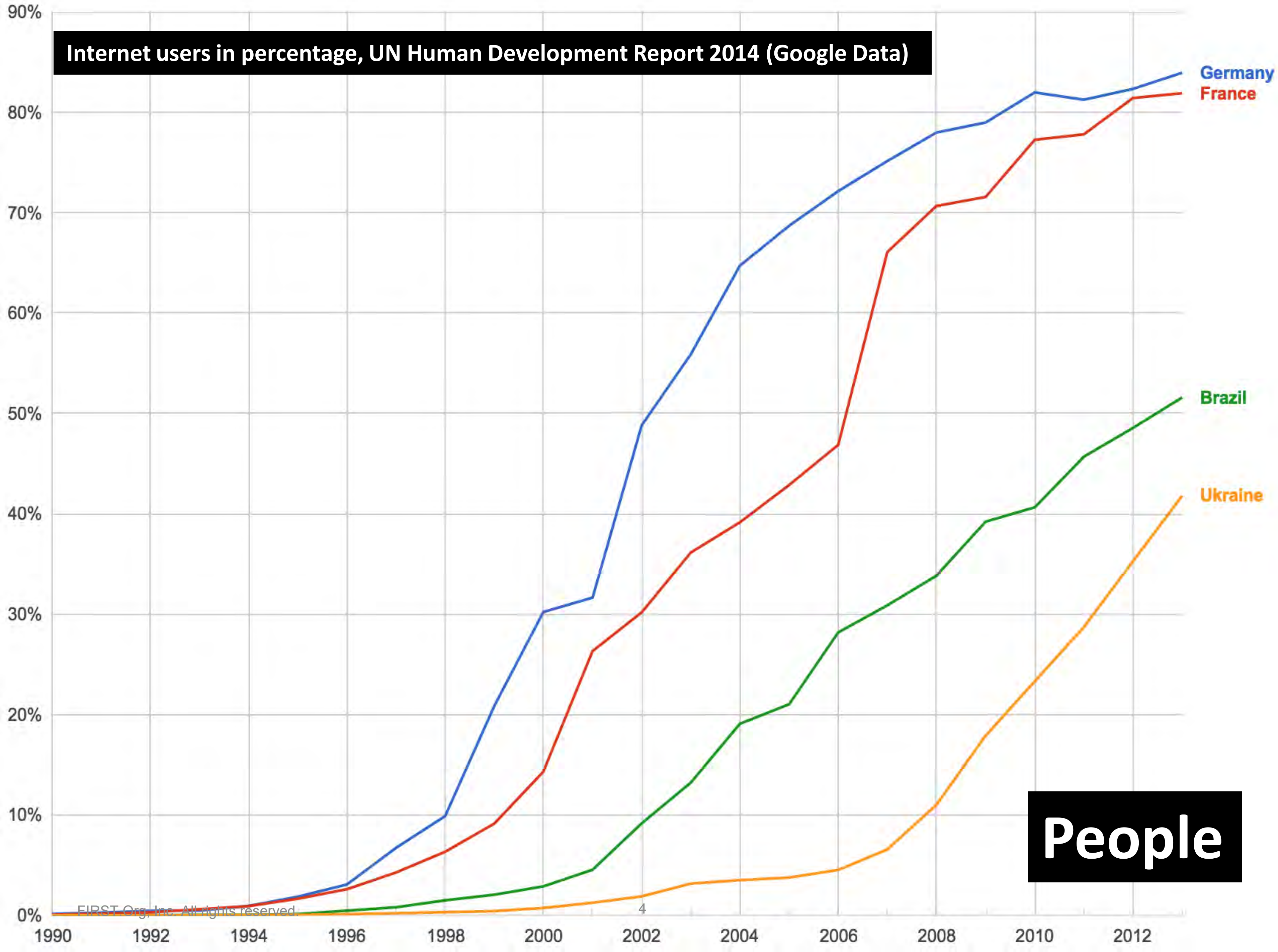
ource: Traffic Signal Preemption in Millersville,PA by Wikipedia user Niagara

The Internet of Things

- The network will continue to grow
  - Cisco predicts 50 billion devices by 2020
  - Mobility will be the norm
  - Sensors may decide on kinetic action

- Incident Response will become more complex
  - Network addressing
  - Embedded software vulnerabilities
  - Density of traffic flows and relations

Internet users in percentage, UN Human Development Report 2014 (Google Data)

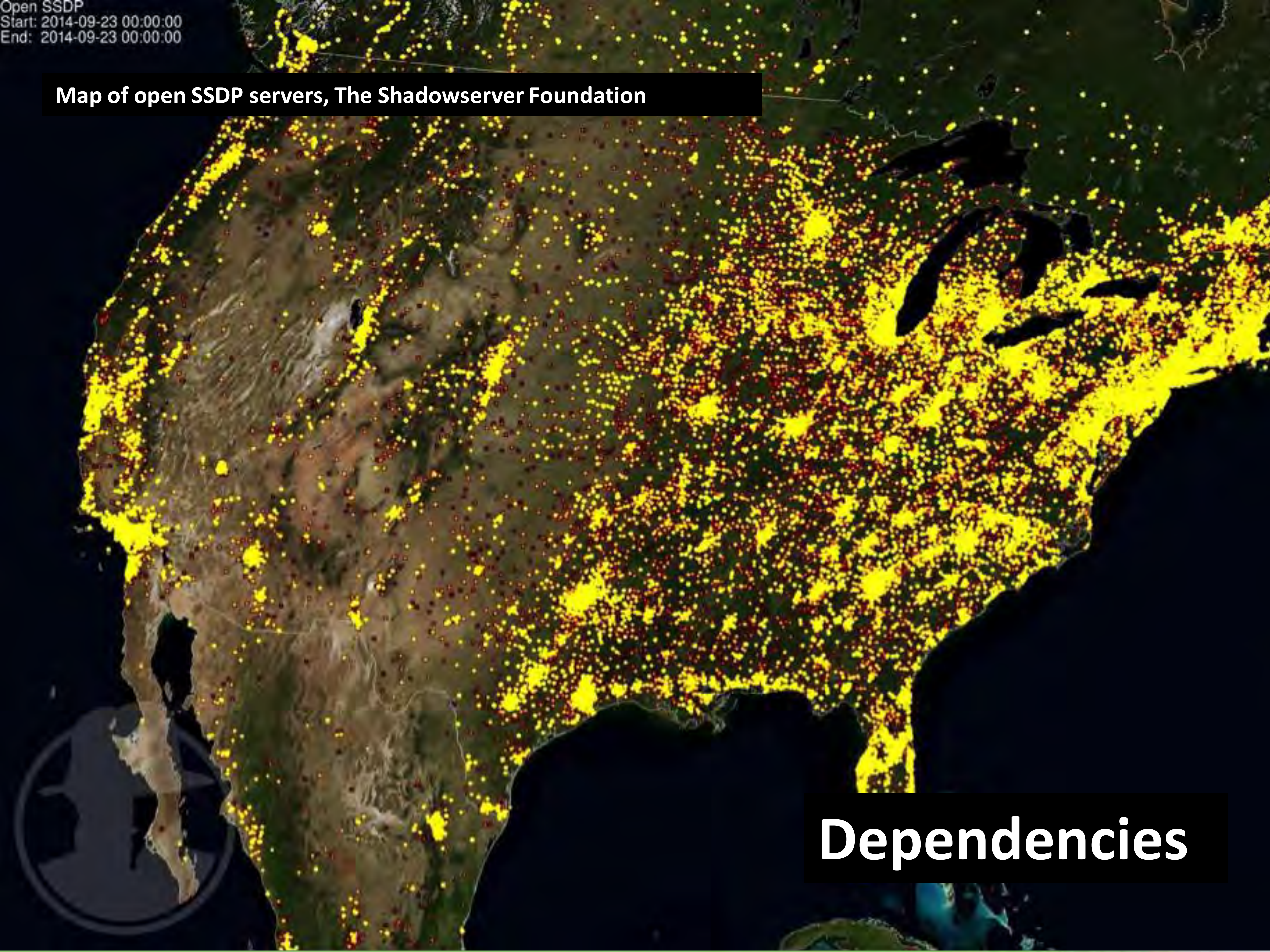


People

The Internet of People

- The amount of users is growing
  - Microsoft predicts 4 billion users by 2020
- Users are increasingly mobile
  - GSMA predicts 3.8 billion mobile users by 2020
- Increasingly varied knowledge and expectations
  - Privacy and safety
  - Diversity of internet use cases

Dependencies



Map of open SSDP servers, The Shadowserver Foundation

Our history

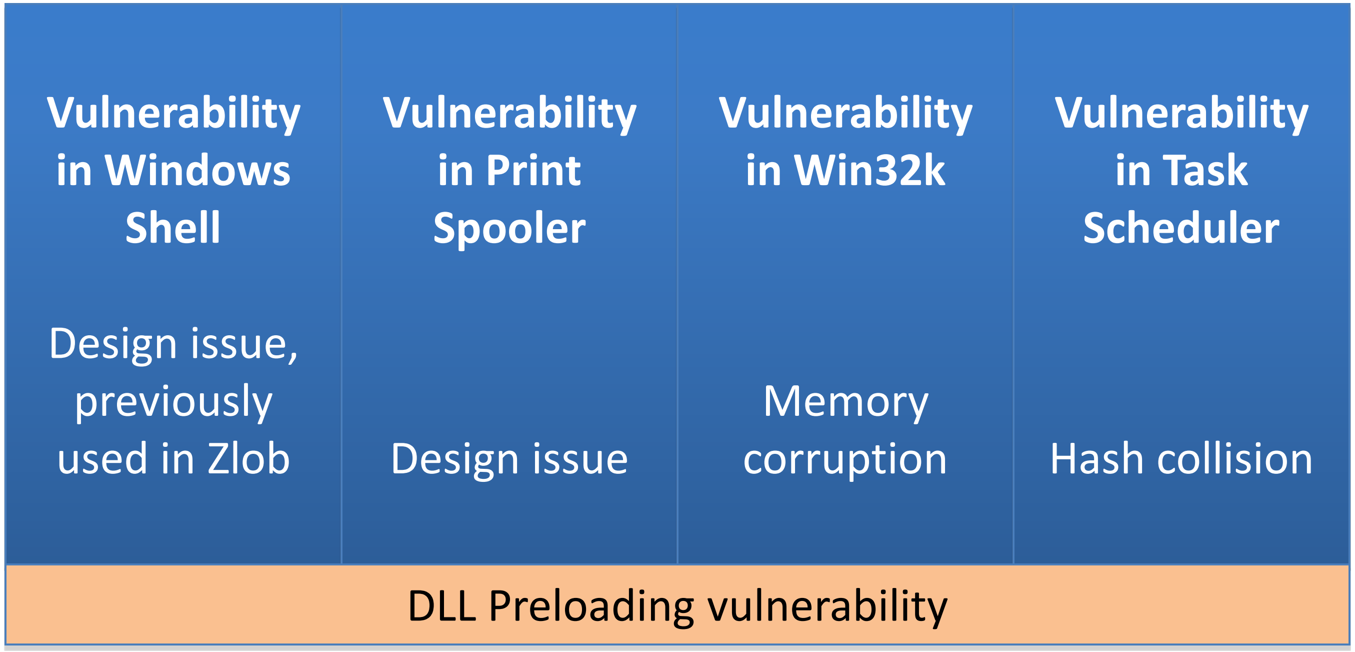
- **Pakistani Brain (1986)**
- Internet Worm (1988)
- Stuxnet (2010)
- DigiNotar (2011)
- Bash vulnerability (2014)

Our history

- Pakistani Brain (1986)
- **Internet Worm (1988)**
- Stuxnet (2010)
- DigiNotar (2011)
- Bash vulnerability (2014)

Stuxnet

- Real life use of 0-day vulnerabilities



Vulnerability in Windows Shell

Design issue, previously used in Zlob

Vulnerability in Print Spooler

Design issue

Vulnerability in Win32k

Memory corruption

Vulnerability in Task Scheduler

Hash collision

DLL Preloading vulnerability

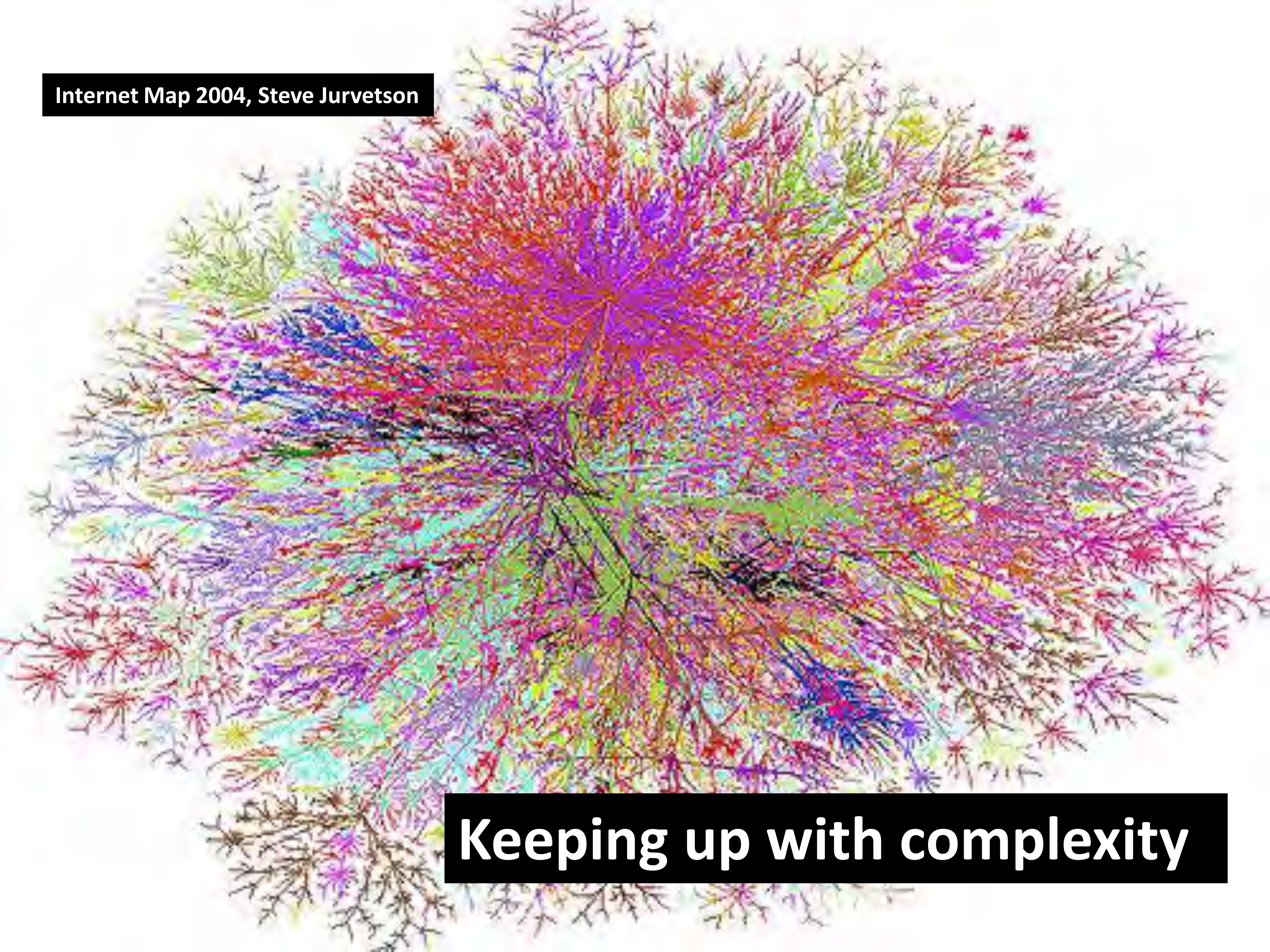
Our history

- Pakistani Brain (1986)
- Internet Worm (1988)
- Stuxnet (2010)
- **DigiNotar (2011)**
- Bash vulnerability (2014)

Our history

- Pakistani Brain (1986)
- Internet Worm (1988)
- Stuxnet (2010)
- DigiNotar (2011)
- **Bash vulnerability (2014)**

Keeping up with complexity



Internet Map 2004, Steve Jurvetson

How do we keep up?

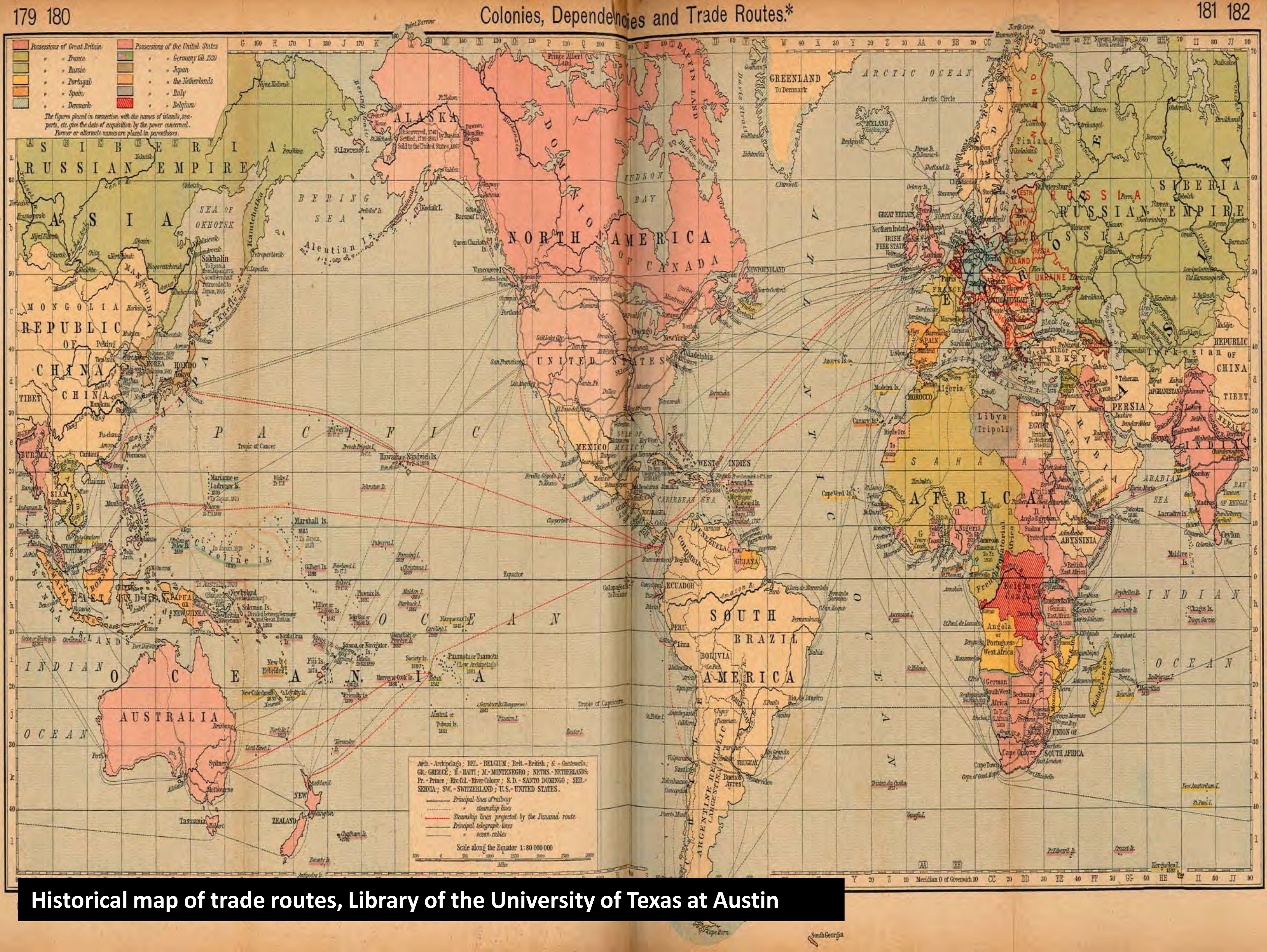
- Engage **multi-stakeholder** communities
  - A cyber balance of power?

- **Automate** and **standardize** technical sharing
  - Help define priorities and “what is useful”
  - Ensure we speak the same technical language
  - Machine-to-machine information exchange
  - **STIX/TAXII**, **M**alware **I**nformation **S**haring **P**latform

How do we keep up?

- Think through the **economics**
  - It's all about incentives
  - Make cyber attacks more expensive

- Build **trust**, **community** and **capability**
  - Develop capability and share sparse skills
  - Confidence building



Historical map of trade routes, Library of the University of Texas at Austin

Questions?

maarten@first.org

Improving Security Together

Forum of Incident Response and Security Teams