

Incident Response


Art, Science and Engineering

Maarten Van Horenbeeck
maarten@first.org

你好

- [@maartenvhb](#)

- Director of Security Engineering at 

- Director and former Chairman of 

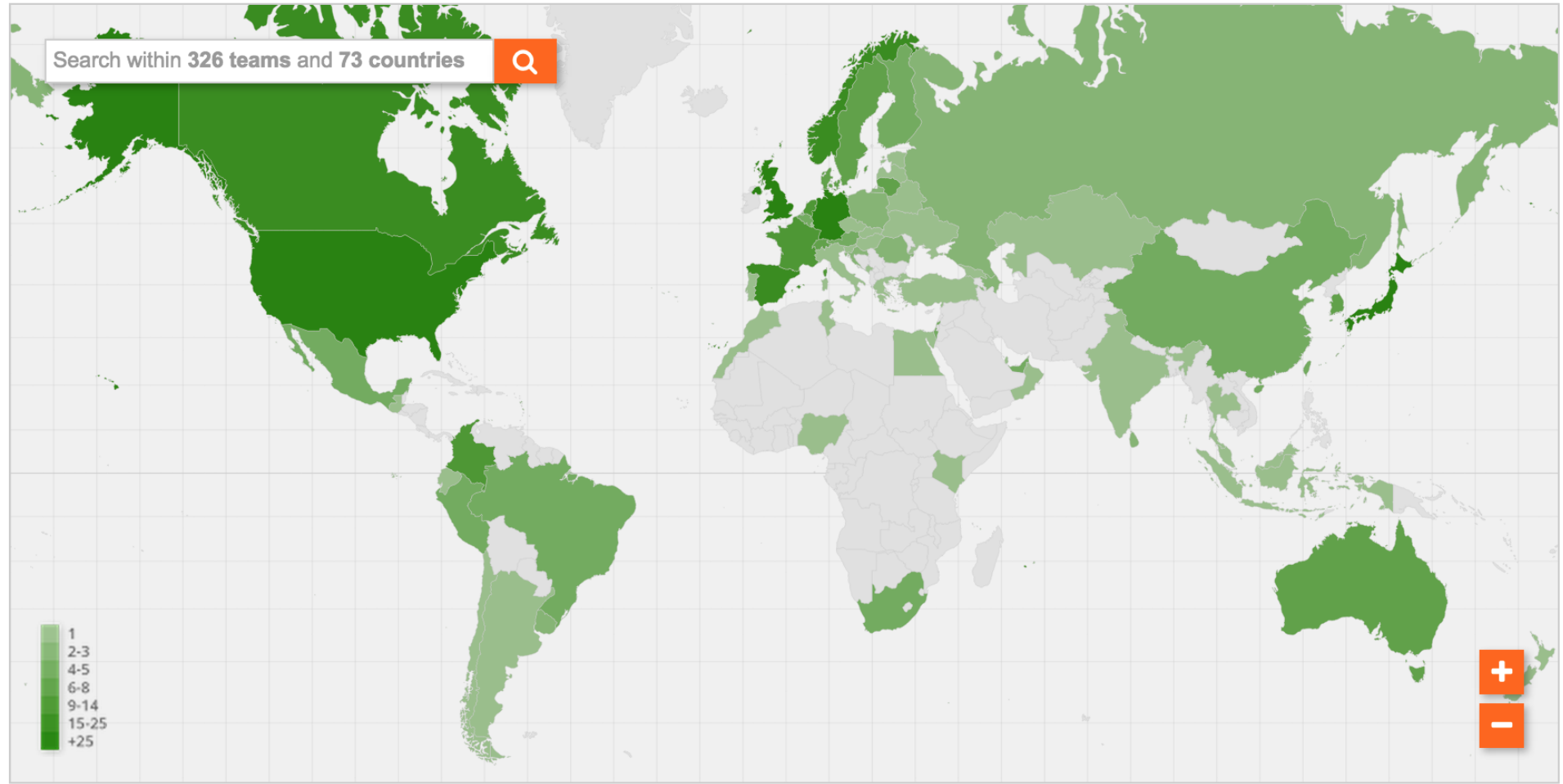
- **Incident Responder.**



Search within 326 teams and 73 countries



- 1
- 2-3
- 4-5
- 6-8
- 9-14
- 15-25
- +25



1988



Ithaca, New York

Population 30,513



Morris worm

The times, they are a-changing.

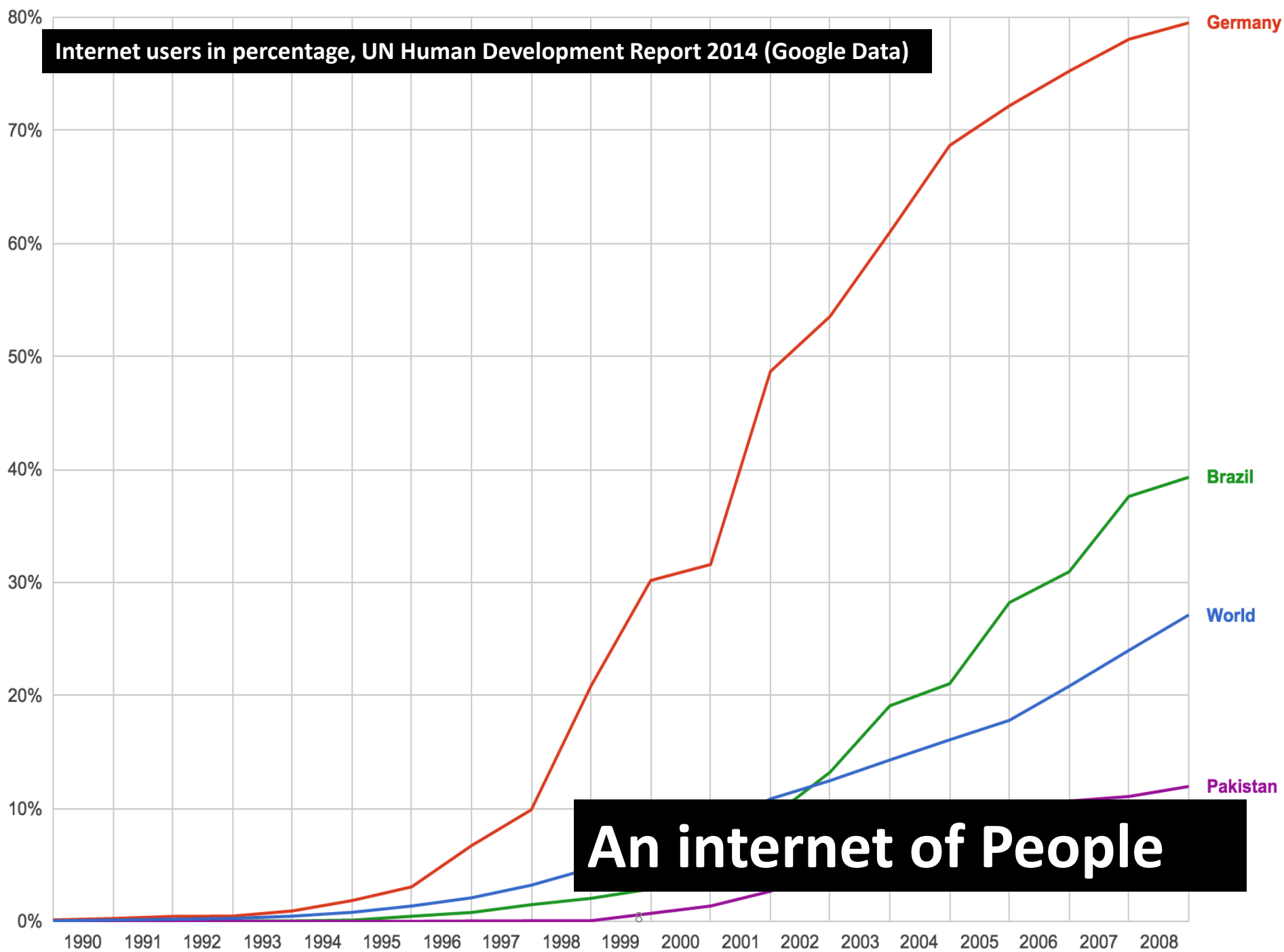
Bob Dylan, 1964

An internet of Things



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

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



An internet of People



Art, science and engineering



The image shows two pages of an open book with dense, small text. The text is arranged in columns and appears to be a technical or scientific document, possibly a dictionary or a manual. The left page has a line of text that is being pointed to by the person's right index finger. The right page contains several lines of text, some of which are bolded or otherwise highlighted. The text is too small to read clearly, but it seems to be organized in a structured manner, possibly with headings or sub-sections. The overall appearance is that of a professional or academic reference work.

- **Art:**
 - *“Quality according to aesthetic principles of what is appealing”*
- **Science:**
 - *“Branch of knowledge or study dealing with facts or truths showing general laws”*
- **Engineering:**
 - *“Creating large structures using scientific methods”*

Our common history

1986

الصَّلَاةُ وَالسَّلَامُ عَلَيْكَ يَا رَسُولَ اللَّهِ
الصَّلَاةُ وَالسَّلَامُ عَلَيْكَ يَا حَبِيبَ اللَّهِ
الصَّلَاةُ وَالسَّلَامُ عَلَيْكَ يَا نَبِيَّ اللَّهِ
الصَّلَاةُ وَالسَّلَامُ عَلَيْكَ يَا رُؤُفَ الرَّحِيمِ
الصَّلَاةُ وَالسَّلَامُ عَلَيْكَ يَا رَحْمَةَ الْعَالَمِينَ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ
مركز الخدمات العامة لجمعية خيرية
0300-4387411, 0315-4225918
www.dawateislami.net



Lahore, Pakistan

Population 5.143 million



Path=A:

Absolute sector 0000000, System BOOT

Displacement	Hex codes																ASCII value
0000(0000)	FA	E9	4A	01	34	12	00	07	14	00	01	00	00	00	00	20	-0J04: 0T 0
0016(0010)	20	20	20	20	20	20	57	65	6C	63	6F	6D	65	20	74	6F	Welcome to
0032(0020)	20	74	68	65	20	44	75	6E	67	65	6F	6E	20	20	20	20	the Dungeon
0048(0030)	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0064(0040)	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0080(0050)	20	20	63	29	20	31	39	38	36	20	42	61	73	69	74	20	(c) 1986 Basit
0096(0060)	26	20	41	6D	6A	61	64	20	28	70	76	74	29	20	4C	74	& Amjad (pvt) Lt
0112(0070)	64	2E	20	20	20	20	20	20	20	20	20	20	20	20	20	20	d.
0128(0080)	20	42	52	41	49	4E	20	43	4F	4D	50	55	54	45	52	20	BRAIN COMPUTER
0144(0090)	53	45	52	56	49	43	45	53	2E	2E	37	33	30	20	4E	49	SERVICES..730 NI
0160(00A0)	5A	41	4D	20	42	4C	4F	43	48	20	41	4C	4C	41	4D	41	ZAM BLOCK ALLAMA
0176(00B0)	20	49	51	42	41	4C	20	54	4F	57	4E	20	20	20	20	20	IBRAL TOWN
0192(00C0)	20	20	20	20	20	20	20	20	20	20	20	4C	41	48	4F	52	LAHORE
0208(00D0)	45	2D	50	41	4B	49	53	54	41	4E	2E	2E	50	48	4F	4E	E-PAKISTAN..PHON
0224(00E0)	45	20	3A	34	33	30	37	39	31	2C	34	34	33	32	34	38	E :430791,443248
0240(00F0)	2C	32	38	30	35	33	30	2E	20	20	20	20	20	20	20	20	,280530.

Row=begin of file/disk End=end of file/disk

ESC=Exit PgD=forward PgUp=back F2=chg sector num F3=edit F4=get name

2000



Manila, Philippines

Population 23 million



LOVE-LETTER-FOR-YOU.txt.vbs

2007

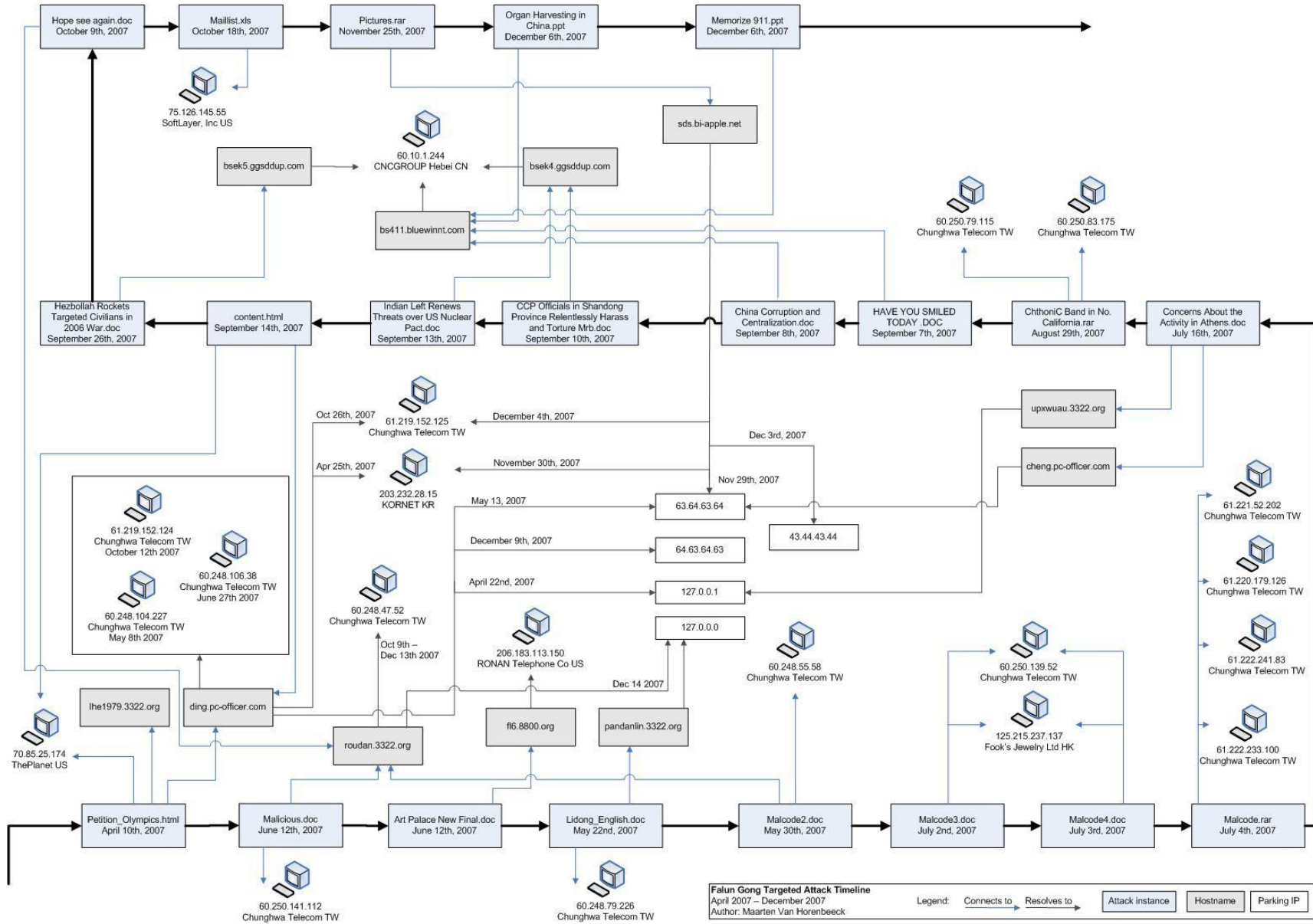


Brussels, Belgium

Population 1.2 million



Targeted attacks



2010



Natanz, Iran

Population 12,060



STUXNET

.stub, mrxnet.sys



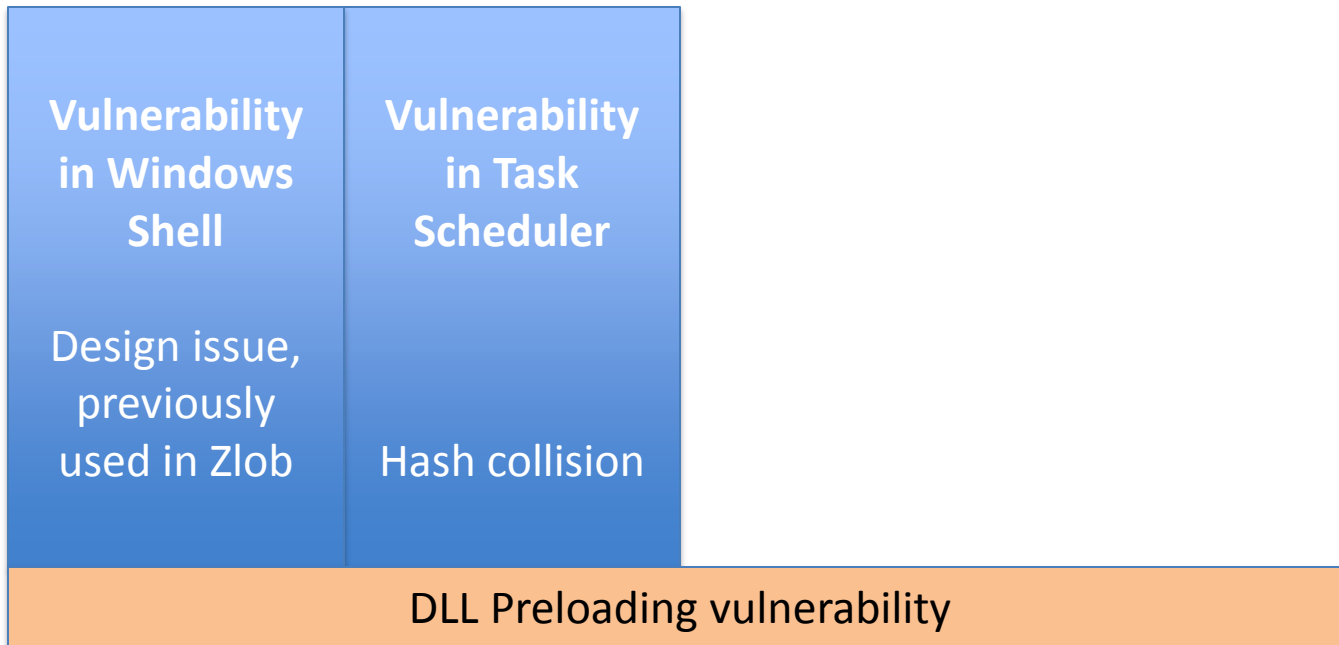
Stuxnet

**Vulnerability
in Windows
Shell**

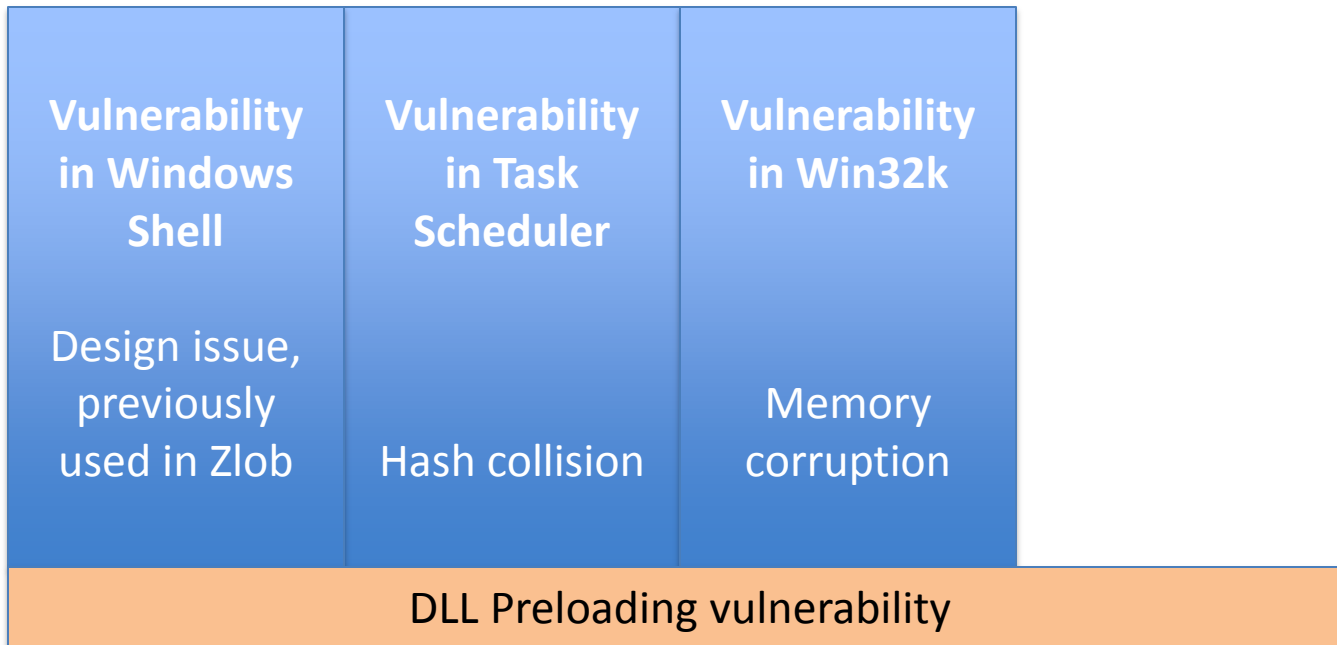
Design issue,
previously
used in Zlob

DLL Preloading vulnerability

Stuxnet



Stuxnet



Stuxnet

Vulnerability in Windows Shell	Vulnerability in Task Scheduler	Vulnerability in Win32k	Vulnerability in Print Spooler
Design issue, previously used in Zlob	Hash collision	Memory corruption	Design issue
DLL Preloading vulnerability			

2011



Khartoum, Sudan

Population 6.5 million



Duqu

2011



Beverwijk, The Netherlands

Population 40,049



DigiNotar

DigiNotar



★ Is This MITM Attack to Gmail's SSL ? 

 ADD A REPLY

by alibo 8/27/11

Hi,
Today, when I trid to login to my Gmail account I saw a certificate warning in Chrome .
I took a screenshot and I saved certificate to a file .

this is the certificate file with screenshot in a zip file:
<http://www.mediafire.com/?rrklb17slctityb>

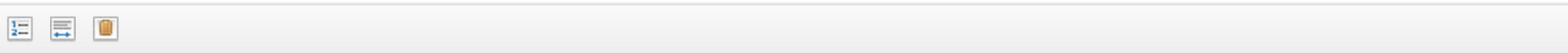
and this is text of decoded fake certificate:
<http://pastebin.com/ff7Yg663>

when I used a vpn I didn't see any warning ! I think my ISP or my government did this attack (because I live in Iran and you may hear something about the story of Comodo hacker!)



1. Hello
- 2.
3. I'm writing this to all the world, so you'll know more about us..
- 4.
5. At first I want to give some points, so you'll be sure I'm the hacker:
- 6.
7. I hacked Comodo from InstantSSL.it, their CEO's e-mail address `mfpenco@mfpenco.com`
8. Their Comodo username/password was: user: `gtadmin` password: `globaltrust`
9. Their DB name was: `globaltrust` and `instantsslcms`
- 10.
11. Enough said, huh? Yes, enough said, someone who should know already knows...
- 12.
13. Anyway, at first I should mention we have no relation to Iranian Cyber Army, we don't change DNSes, we
- 14.
15. just hack and own.

DigiNotar

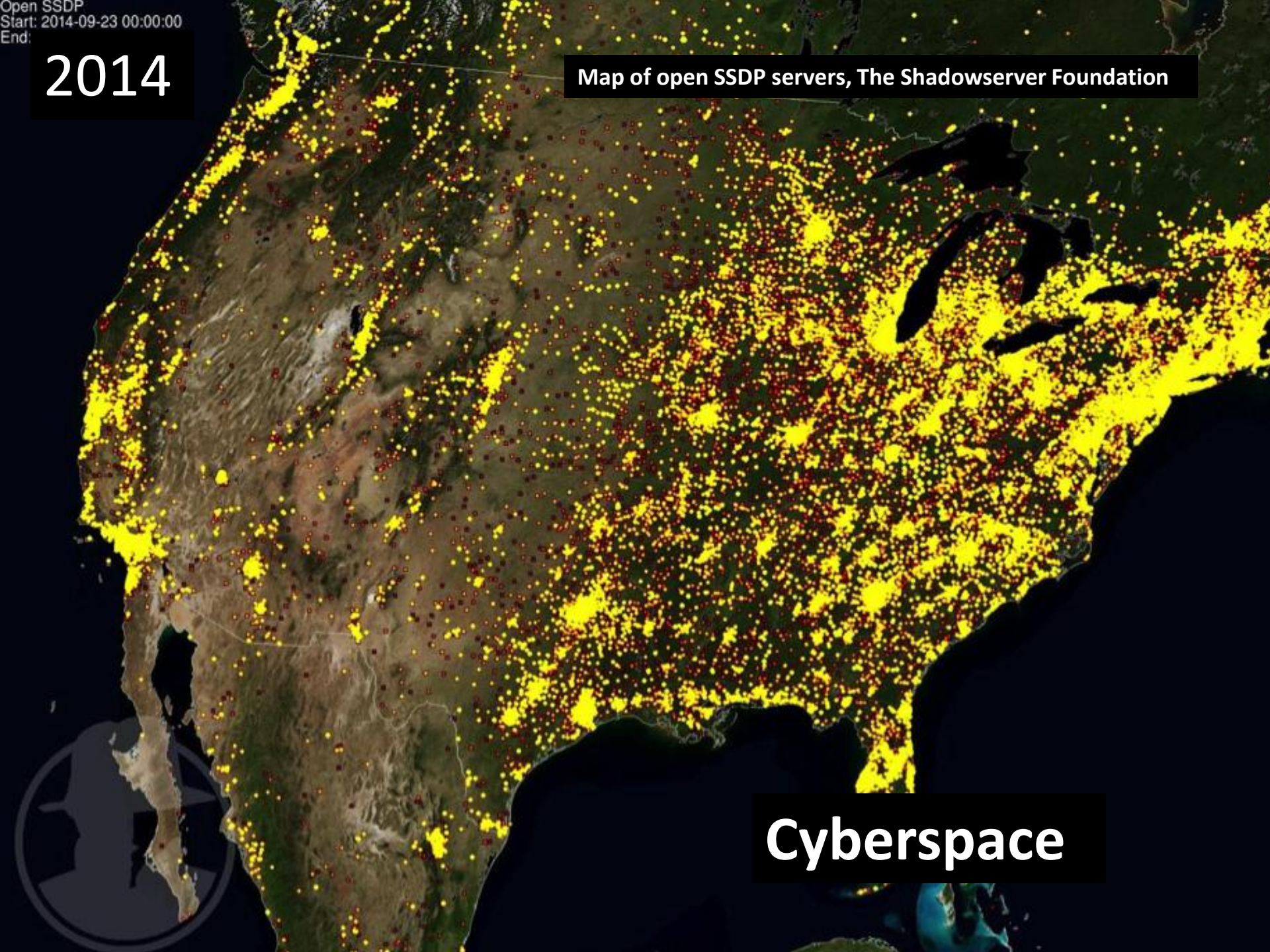
- 
1. Hi again! I strike back again, huh?
 - 2.
 3. I told all that I can do it again, I told all in interviews that I still have accesses in Comodo resellers, I told all I have access to most of CAs, you see that words now?
 - 4.
 5. You know, I have access to 4 more so HIGH profile CAs, which I can issue certs from them too which I will, I won't name them, I also had access to StartCom CA, I hacked their server too with so sophisticated methods, he was lucky by being sitted in front of HSM for signing, I will name just one more which I still have access: GlobalSign, let me use these accesses and CAs, later I'll talk about them too..
 - 6.
 7. I won't talk so many detail for now, just I wanted to let the world know that ANYTHING you do will have consequences, ANYTHING your country did in past, you have to pay for it...
 - 8.
 9. I was sure if I issue those certificates for myself from a company, company will be closed and will not be able to issue certs anymore, Comodo was really really lucky!
 - 10.
 11. I thought if I issue certs from Dutch Gov. CA, they'll lose a lot of money:
 12. http://www.nasdaq.com/aspx/dynamic_charting.aspx?selected=VDSI&timeframe=6m&charttype=line
 - 13.
 14. But I remembered something and I hacked DigiNotar without more thinking in anniversary of that mistake:
 15. <http://www.tepav.org.tr/en/kose-yazisi-tepav/s/2551>

Open SSDP
Start: 2014-09-23 00:00:00
End:

2014

Map of open SSDP servers, The Shadowserver Foundation

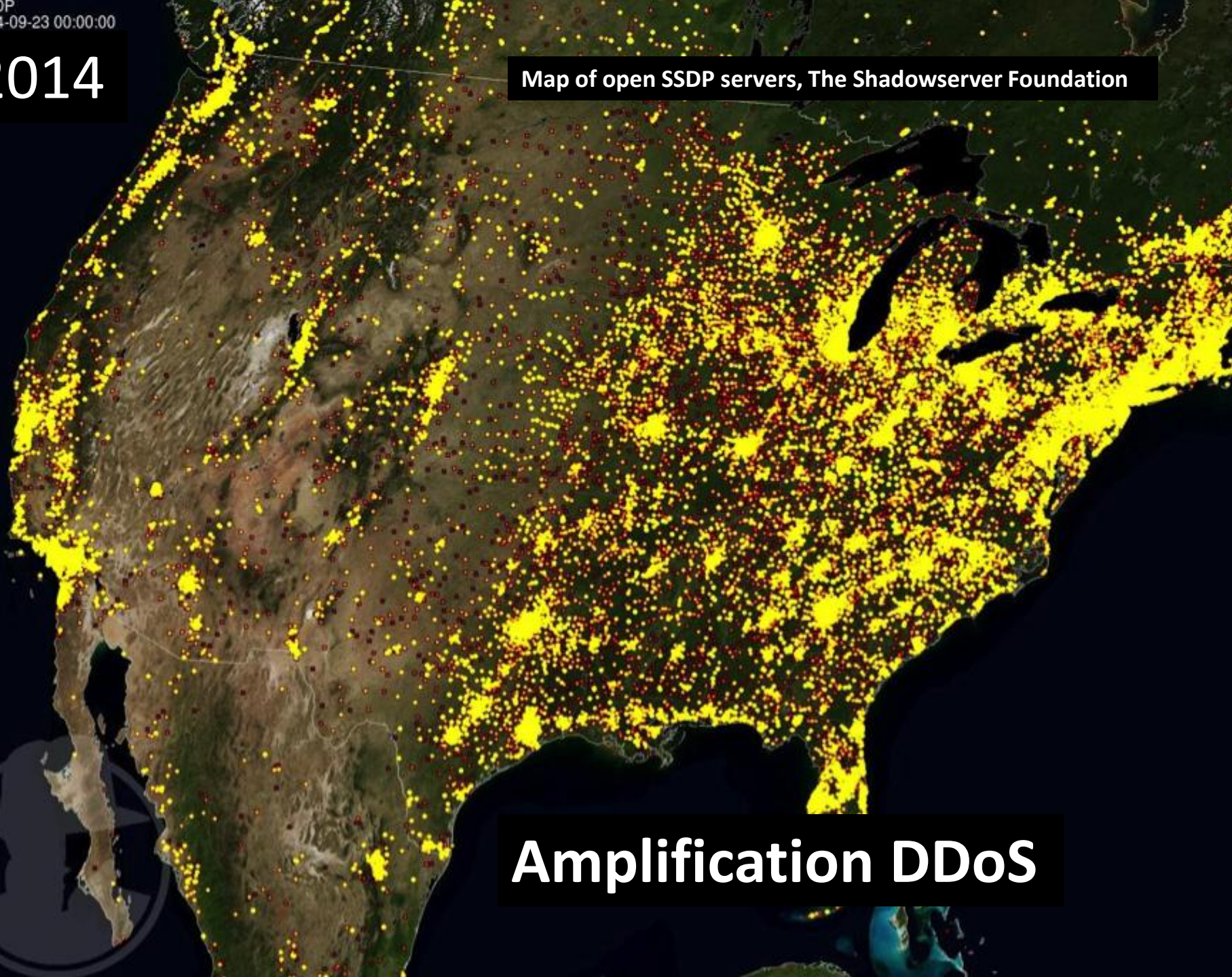
Cyberspace



Open SSDP
Start: 2014-09-23 00:00:00
End:

2014

Map of open SSDP servers, The Shadowserver Foundation



Amplification DDoS



Network Working Group
Request for Comments: 2827
Obsoletes: [2267](#)
BCP: 38
Category: Best Current Practice

P. Ferguson
Cisco Systems, Inc.
D. Senie
Amaranth Networks Inc.
May 2000

**Network Ingress Filtering:
Defeating Denial of Service Attacks which employ
IP Source Address Spoofing**

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

Abstract

Recent occurrences of various Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point.

2014

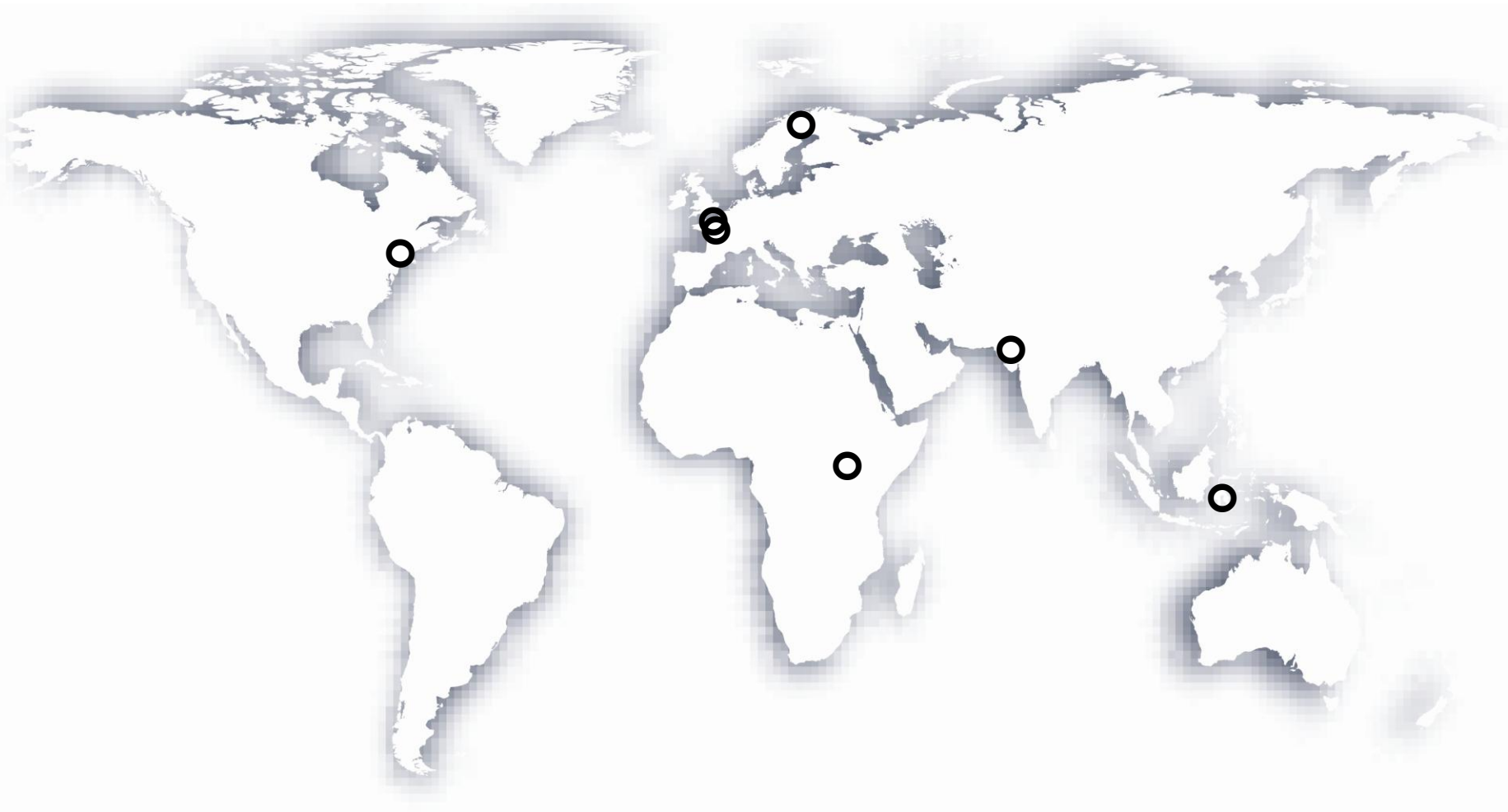


Oulu, Finland

Lowest temperature on record -34 C

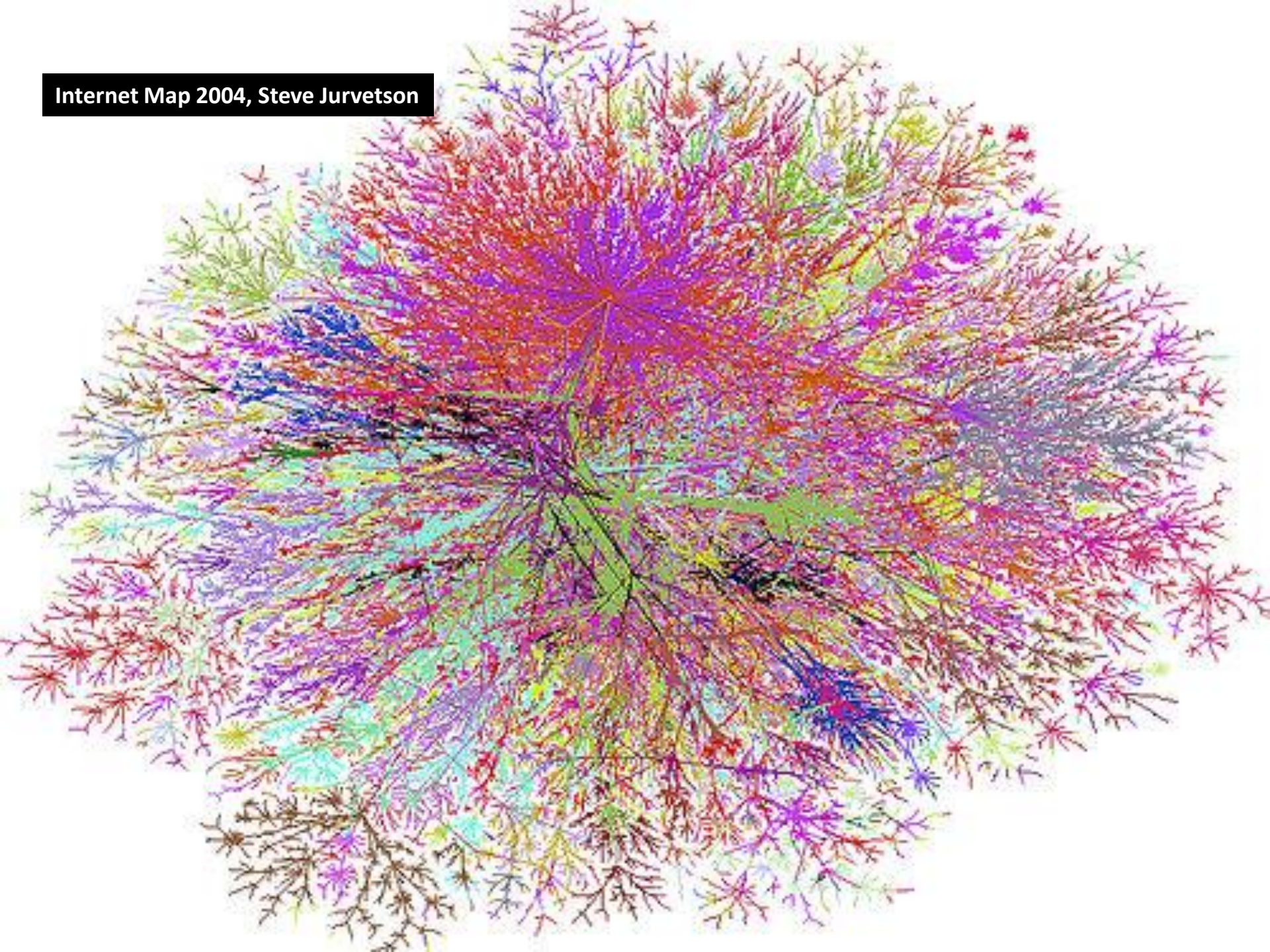


Heartbleed



Dealing with complexity

Internet Map 2004, Steve Jurvetson





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

Dealing with complexity

- **“Know who you’re selling to”**
 - Build a community where we can reach others...
 - ... and understand what others do.
- **“Transportation”**
 - Build the right tools for the job. Let automation do the hard work, humans the smart work.
- **“Lingua franca”**
 - Develop standards to work together better.

Dealing with complexity

- **You make partners before you need them**
 - Connect with industry groups and competitors
 - Participate and share information
- **Know which technologies you know, and which you don't**
 - Do you have or partner with reverse engineers?
- **When something is the right thing to do, do it**
 - Track and participate in standards
 - We all should have done this with BCP38 😊
- **Researchers help protect your organization**
 - Cherish and encourage their work

多謝