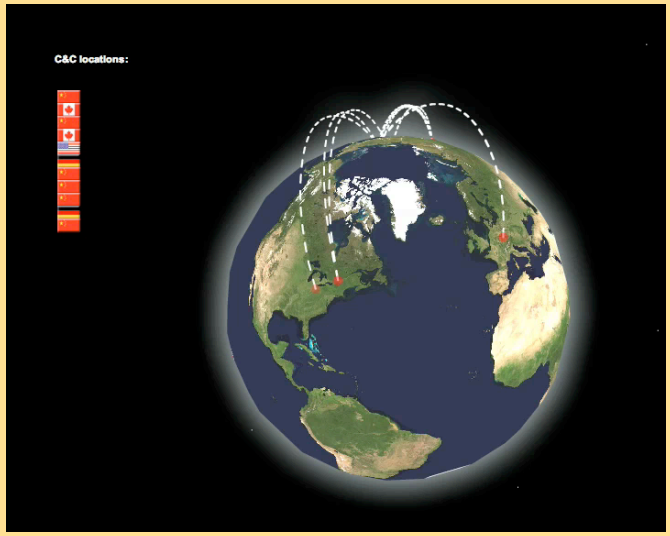
29 June 2009

Show Me The Evil



Dave Deitrich
Chief Technology Officer
Team Cymru

FIRST 21
Track 1 – 16:00-17:00
3F Genji West & North

About Team Cymru (1998-Present)

WHO?

Qui?
Wer?
¿Quién?
Кто?
من؟
谁?
どなたですか？
누구세요?
?מִי

WHY?

Pourquoi?
Warum?
¿Por qué?
Почему?
لماذا؟
为什么？
何故ですか？
왜요?
?לָמָּה

About this Presentation

¿Tan malo es? *Jak je to špatné?* *Hur illa är det?*

كيف هي سيئة؟ *Cât e de rău?* *Hoe erg is het?*

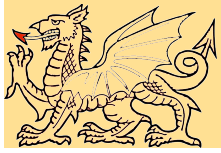
如何坏是什么？ *Come è brutto?* कितना बुरा है?

Comment est-il mauvais? *Насколько это плохо?*

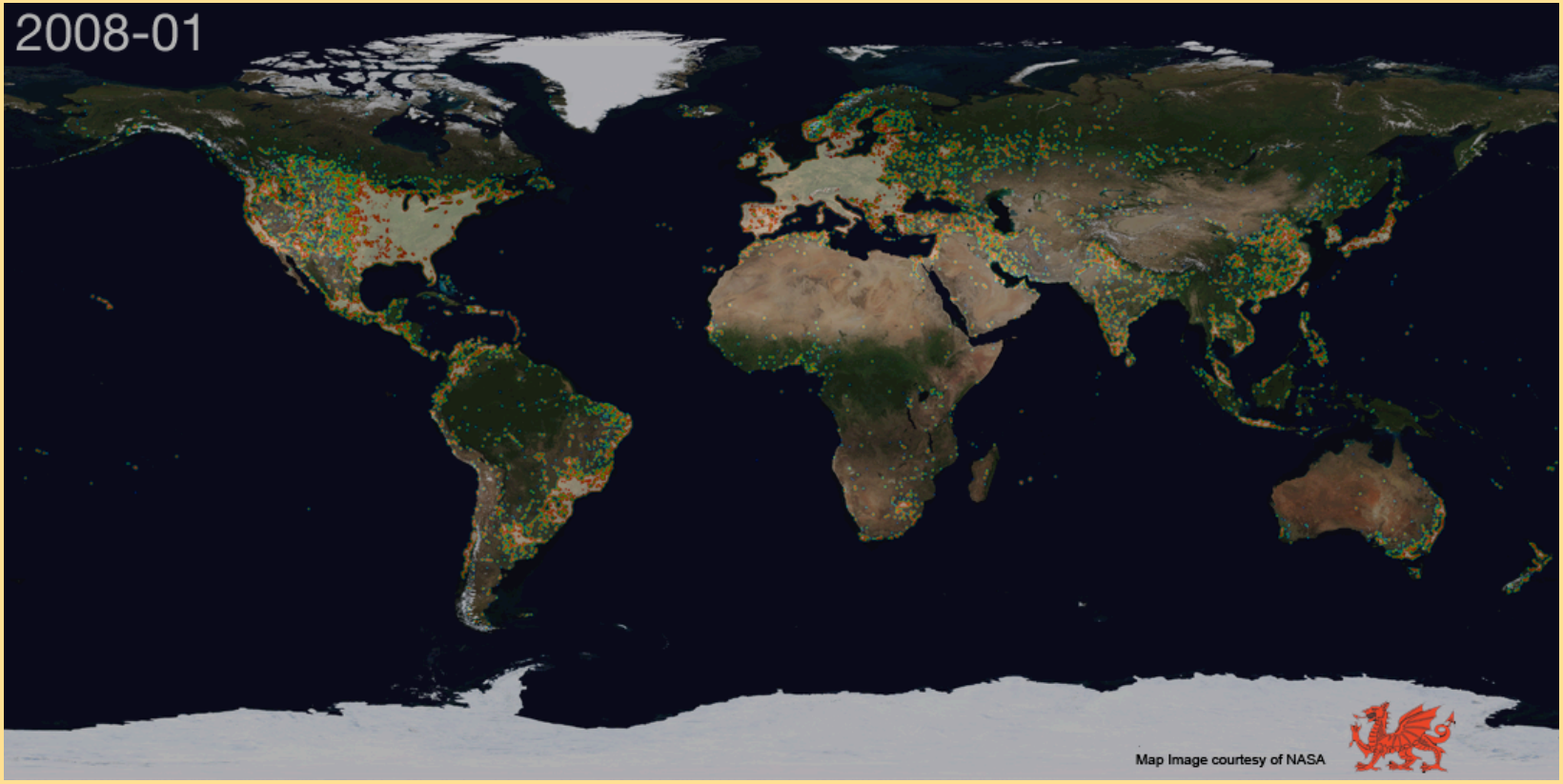
Wie schlimm ist es? *Ne kadar kötü?* ?כמה רע זה

どのように悪いのでしょうか？ **วิธีเลวคือมันได้หรือไม่**

얼마나 안 좋은 가요? *Kako je to loše?* *How bad is it?*

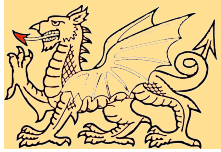


Internet “Evil” in 2008



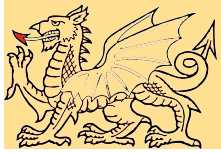
Bad Neighborhoods (By Count)

Country	Count
China	12,960,231
United States	9,046,360
Germany	6,324,031
Brazil	6,123,311



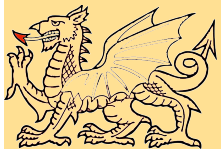
Bad Neighborhoods (By Percent)

Rank	Country	Count	% Malicious Ips
#1	Dominican Republic	194,777	48.06%
#2	Equatorial Guinea	825	40.28%
#3	Algeria	106,629	40.13%
#4	Djibouti	1,514	36.96%
#43	Brazil	6,123,311	20.58%
#107	Germany	6,324,031	7.43%
#115	China	12,960,231	6.89%
#201	United States	9,046,360	0.62%

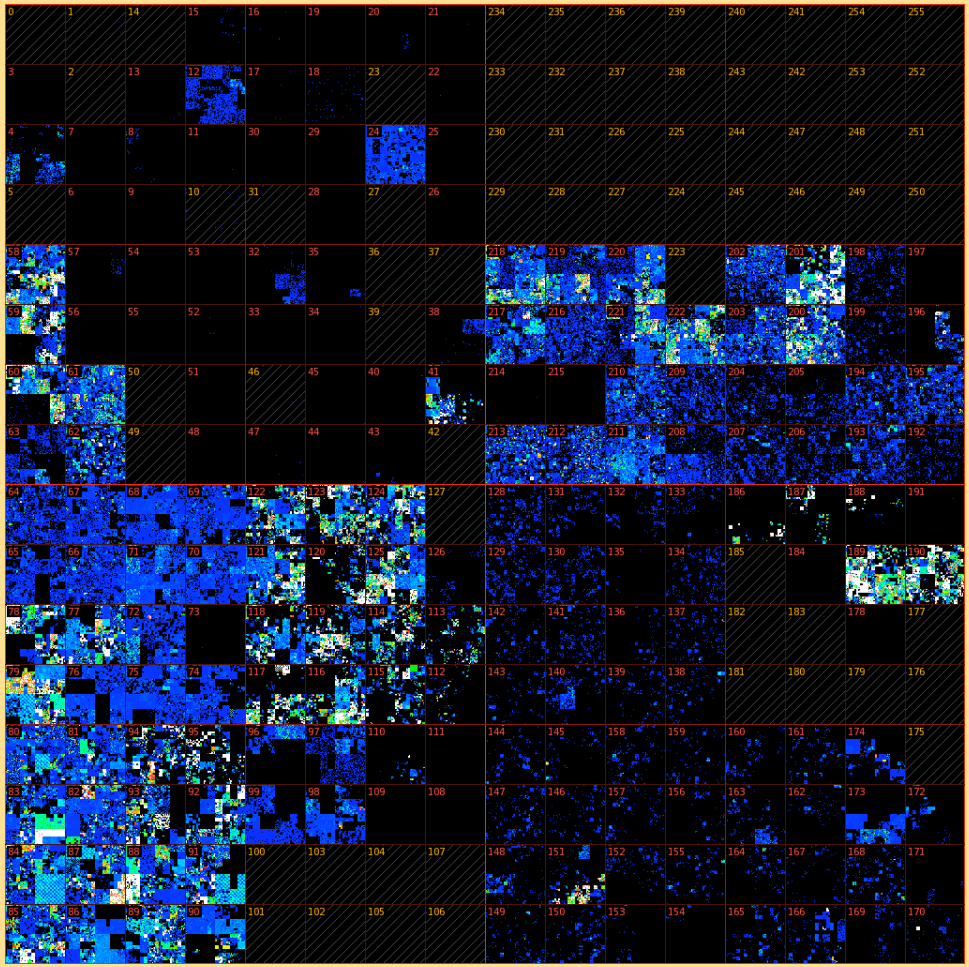


Bad Neighborhoods (By /8 Network)

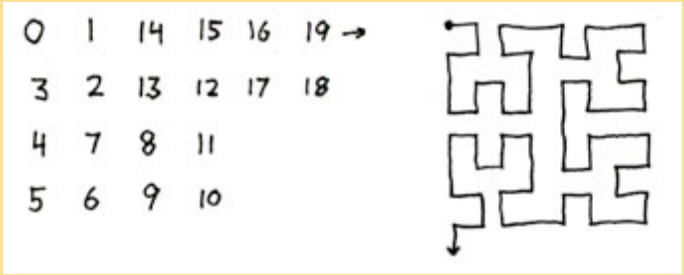
Network	Prefixes	Designation	Countries	Count
201/8	3,890	LACNIC	21	3,774,135
189/8	2,466	LACNIC	2	3,703,918
190/8	5,699	LACNIC	23	3,505,554
88/8	973	RIPE NCC	45	3,324,326
79/8	1,055	RIPE NCC	47	3,289,545
78/8	1,528	RIPE NCC	53	2,956,894



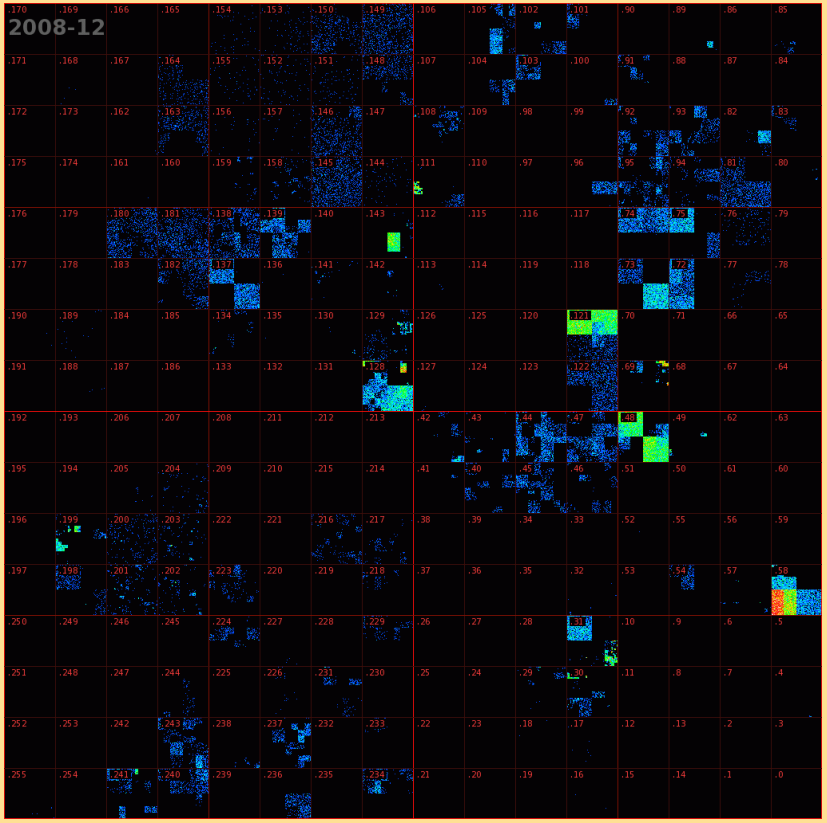
Bad Neighborhoods (Hilbert Curve)



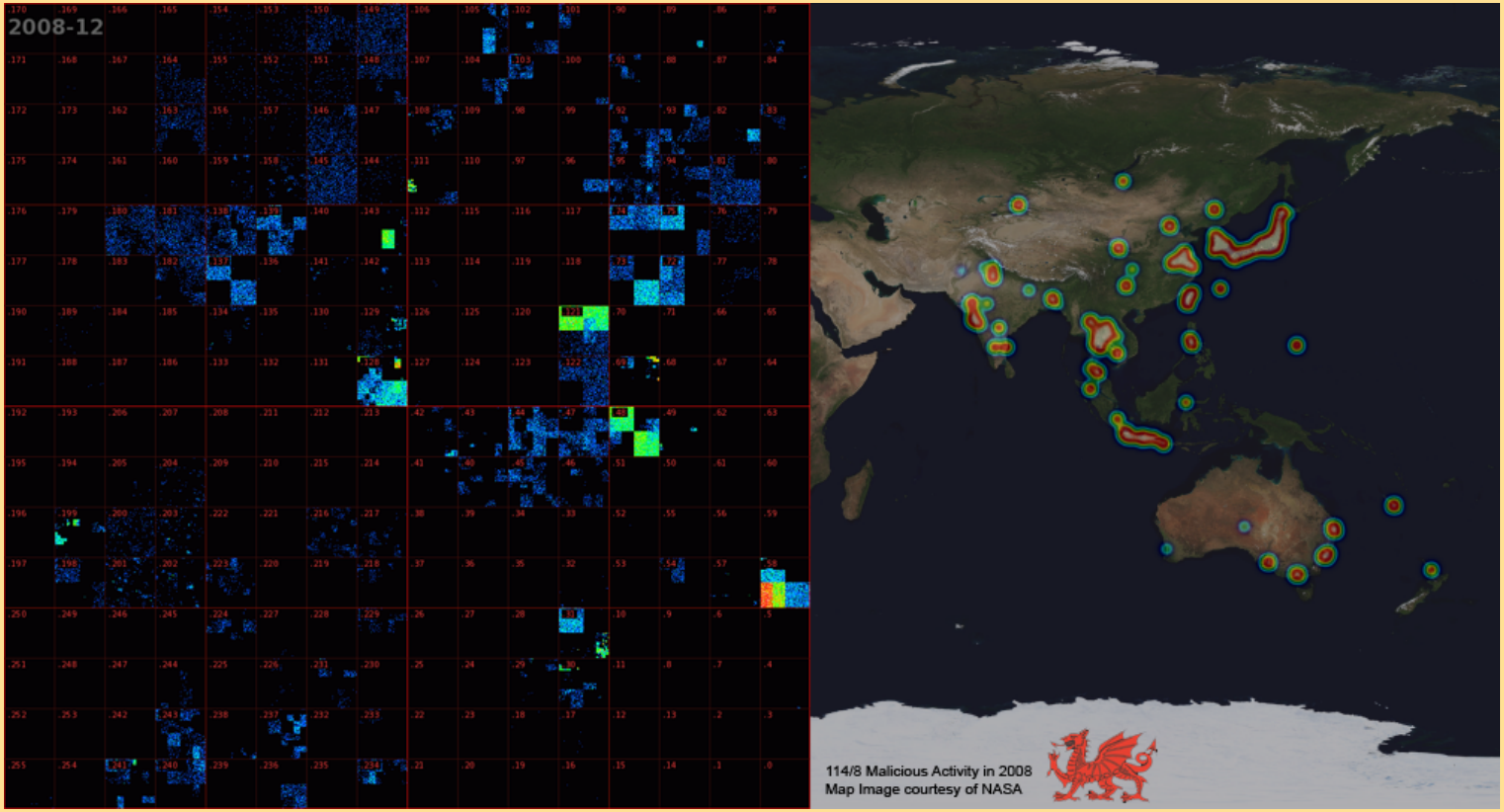
Hilbert Graph
http://xkcd.com/195/



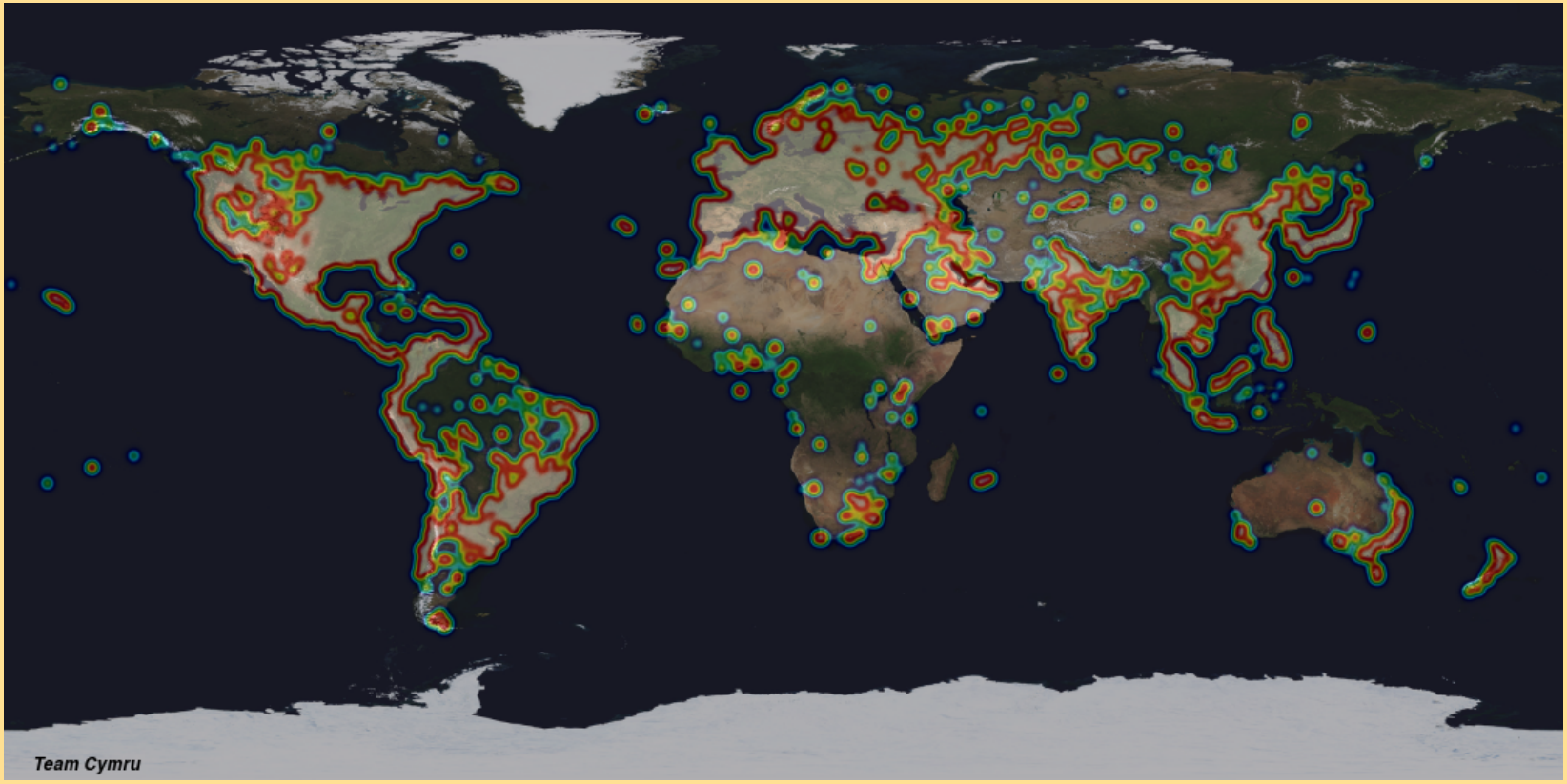
History of 114.0.0.0/8



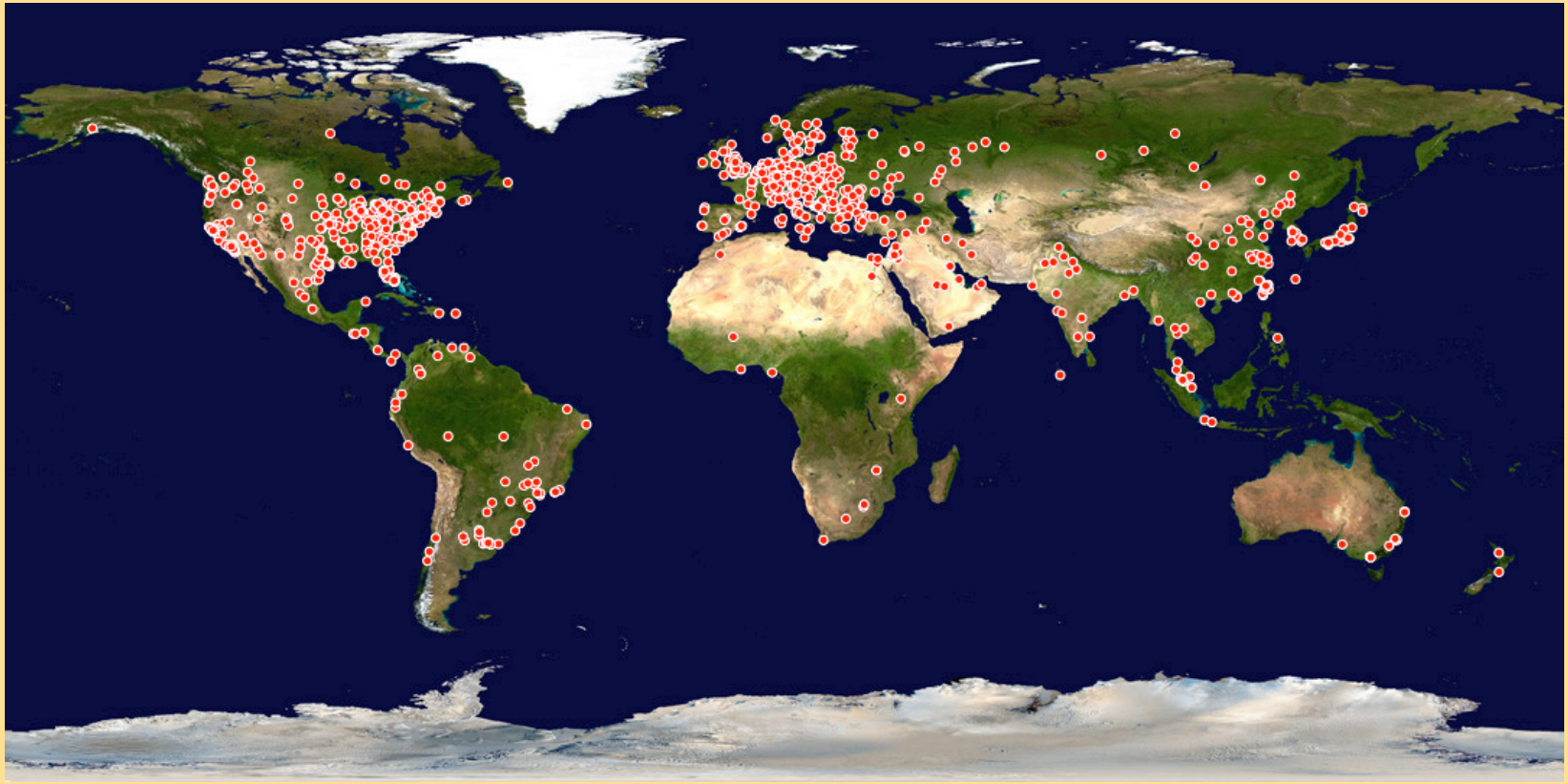
History of 114.0.0.0/8



Bots and Botnets

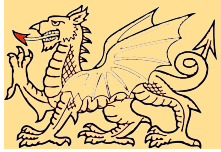


Bots and Botnets (C&Cs)

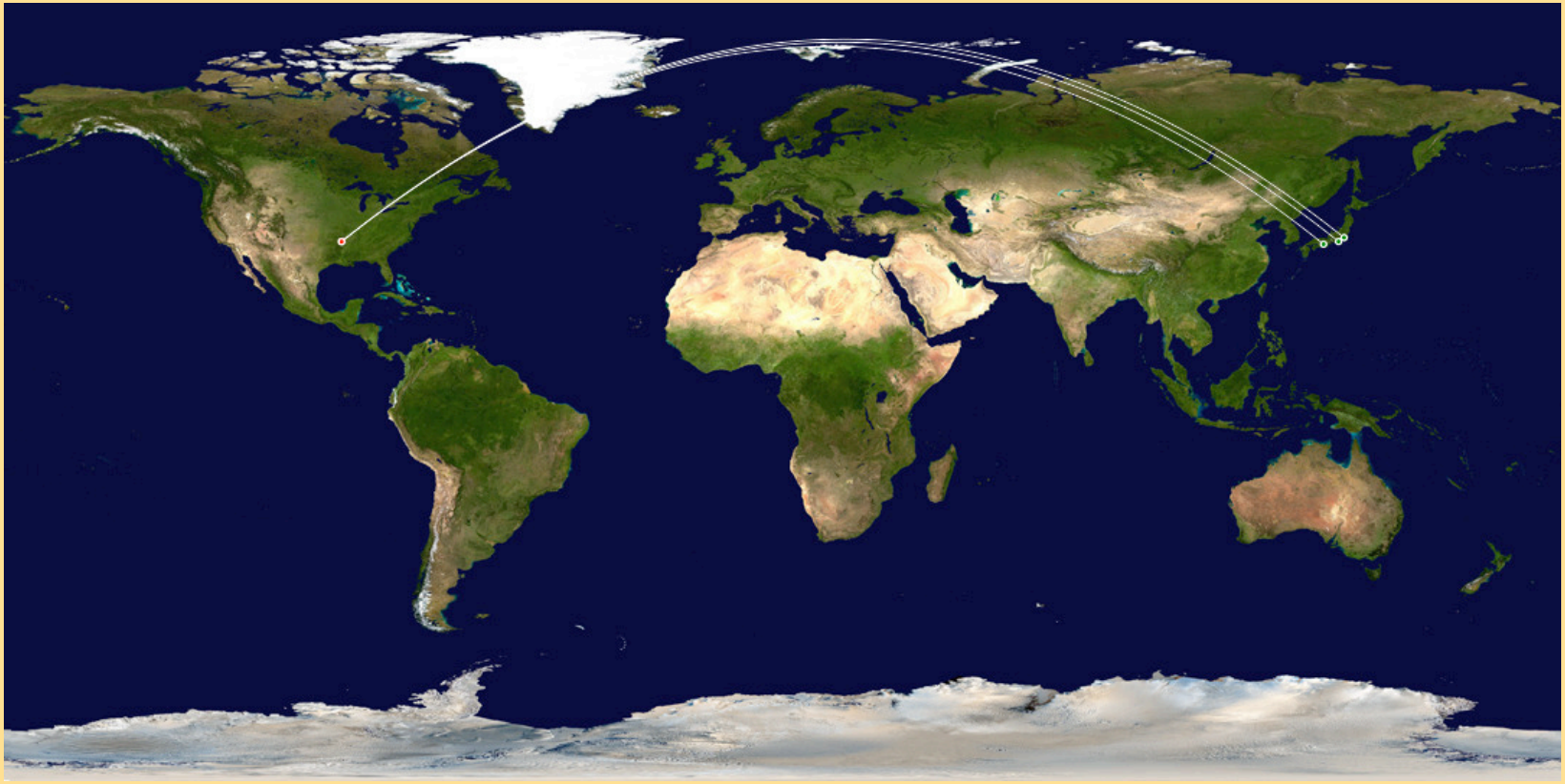


Bots and Botnets (C&Cs)

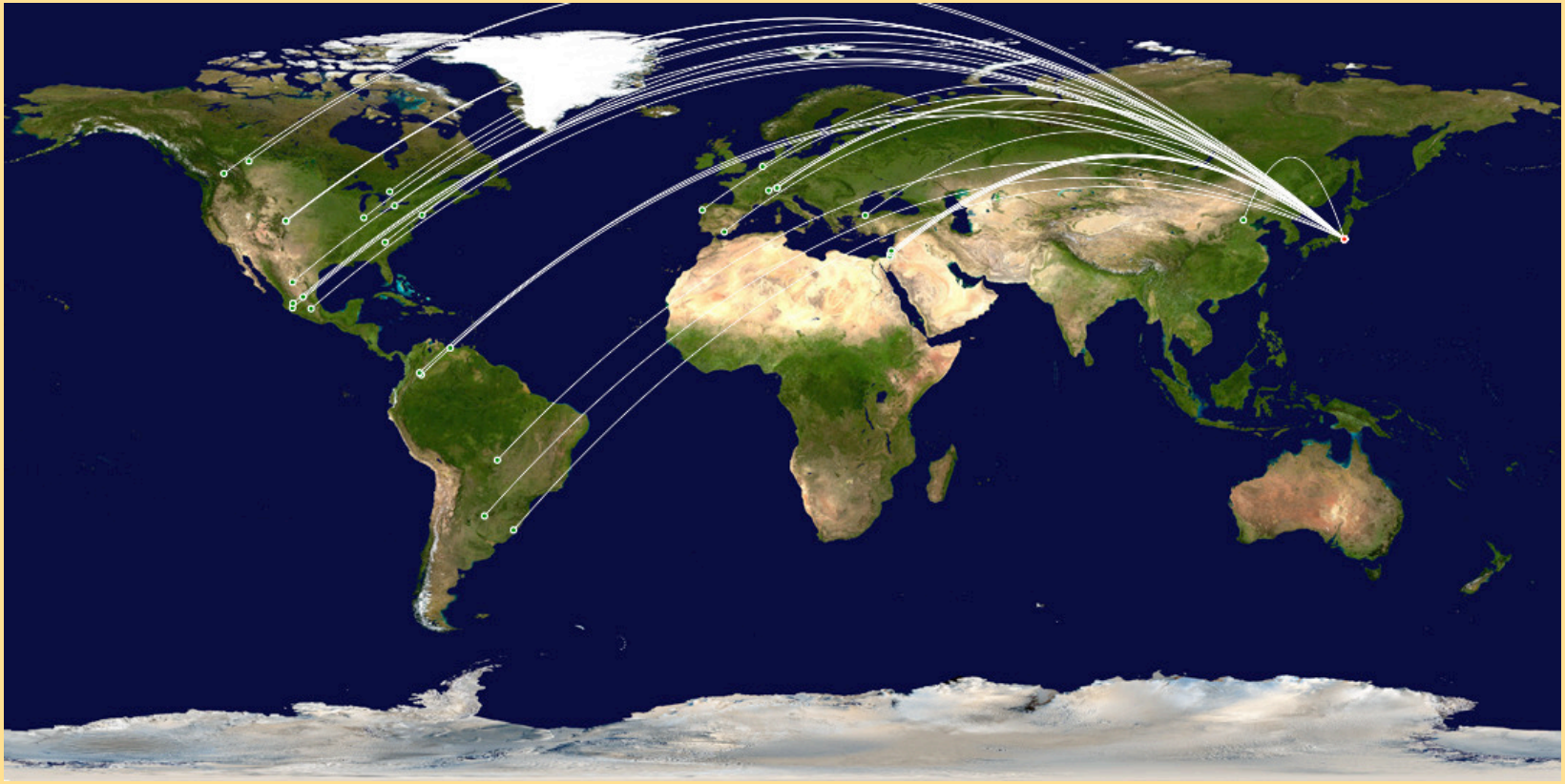
Country	# of Botnet Controllers (2008)
United States	1,941
Germany	294
Korea, Republic of	212
United Kingdom	159
Canada	138
China	134
Russian Federation	104



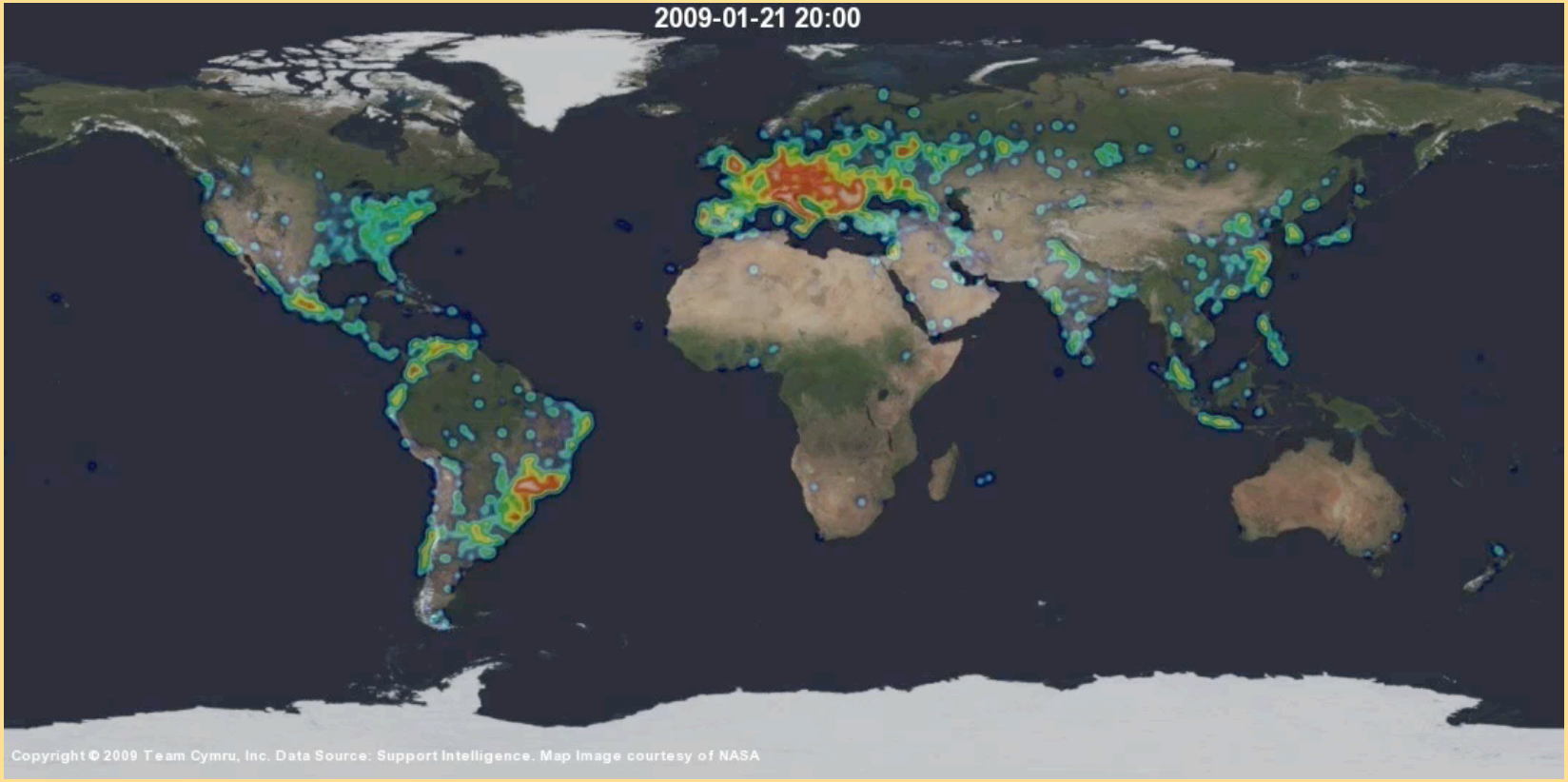
Target Japan! (Bots)



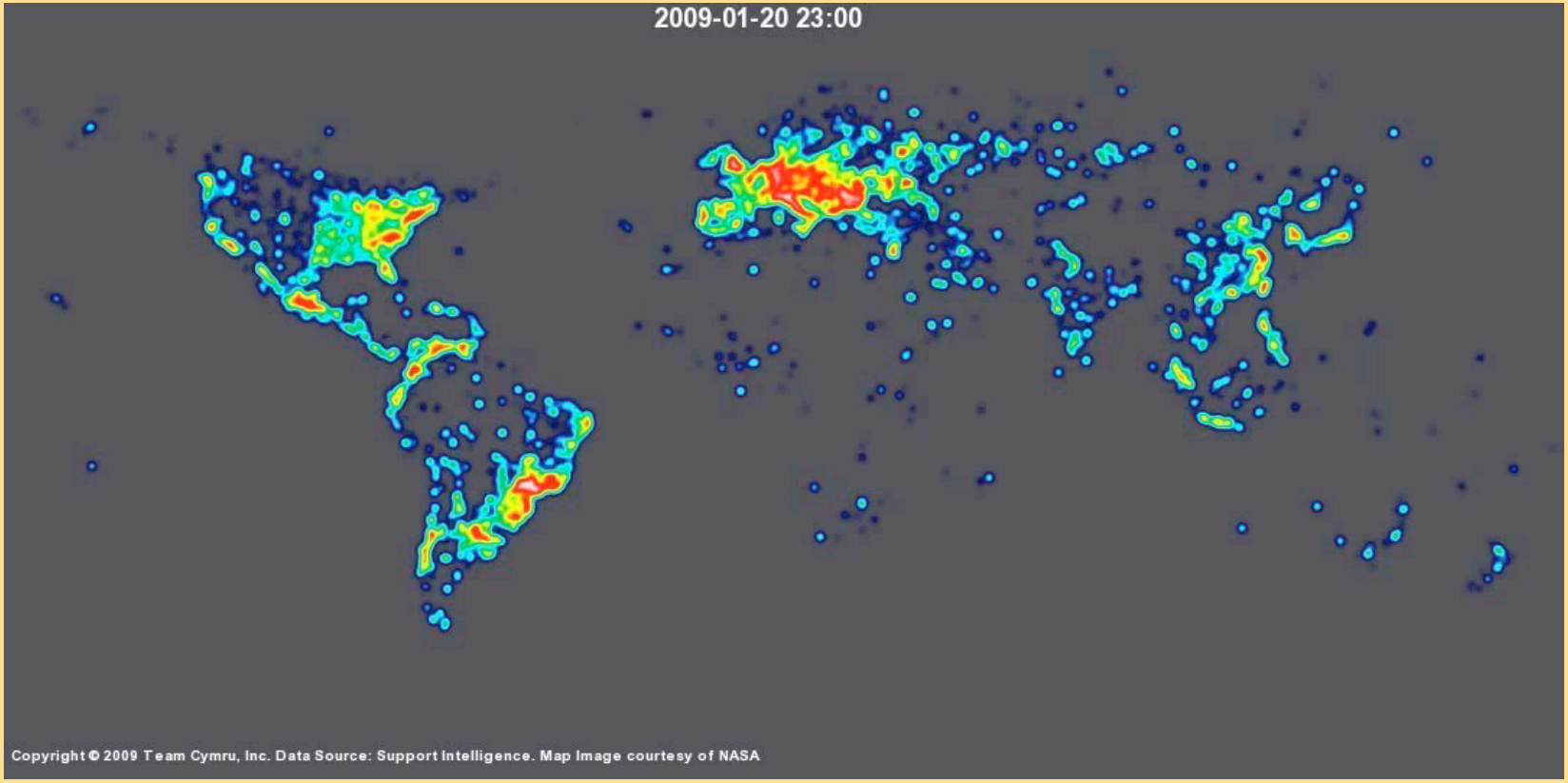
Target Japan! (C&Cs)



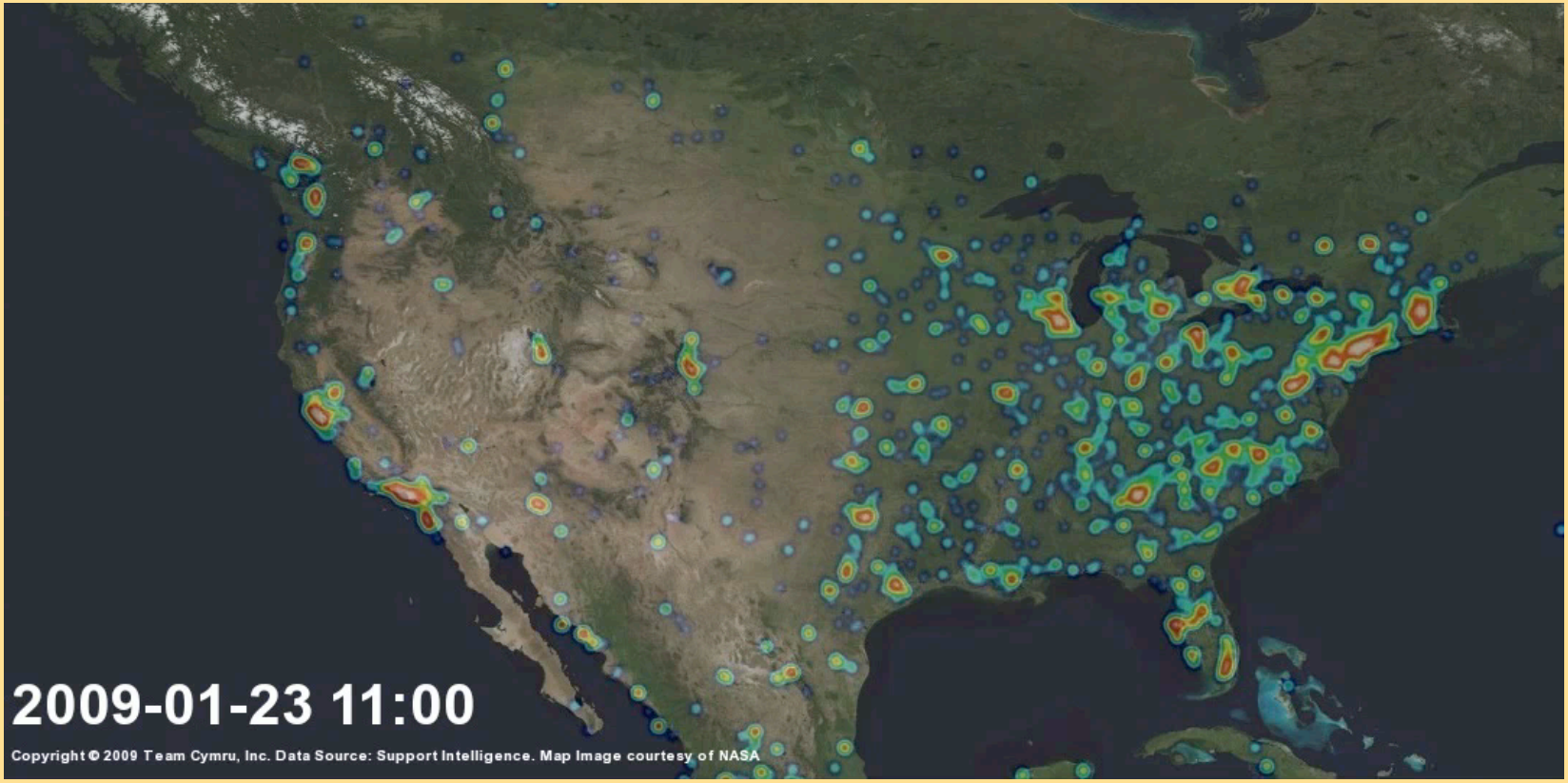
Conficker / Downadup



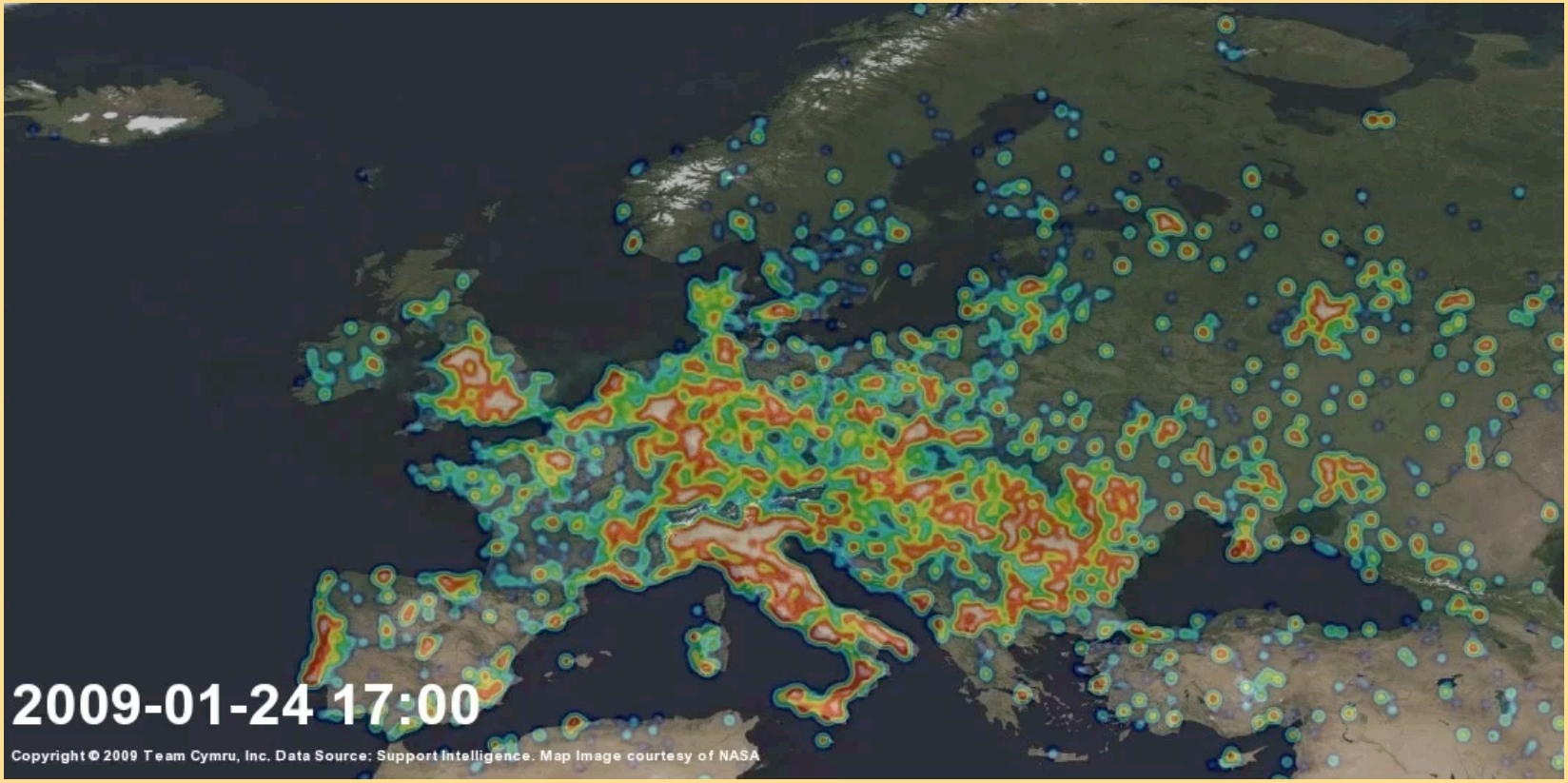
Conficker (No Map)



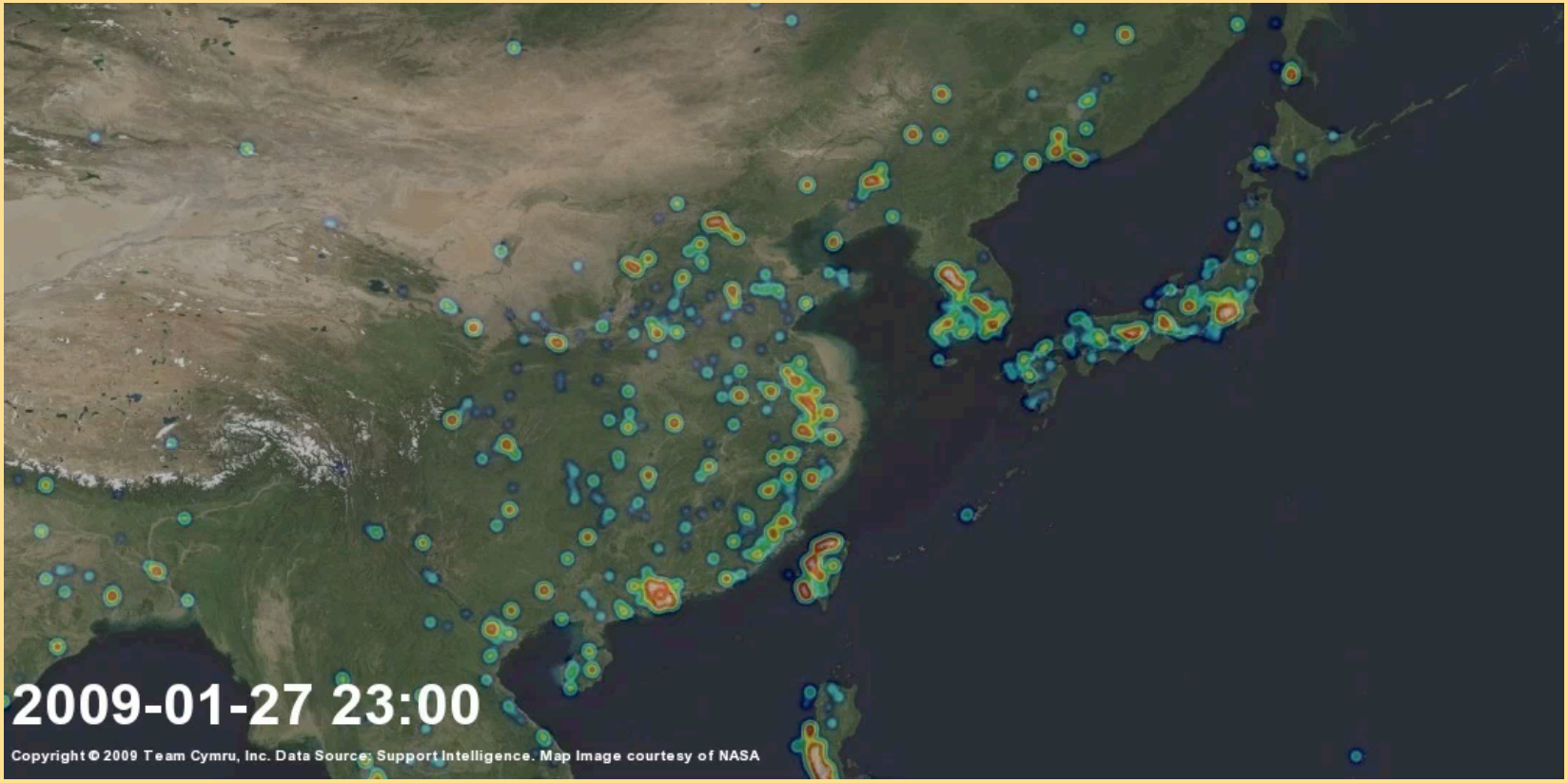
Conficker (North America)



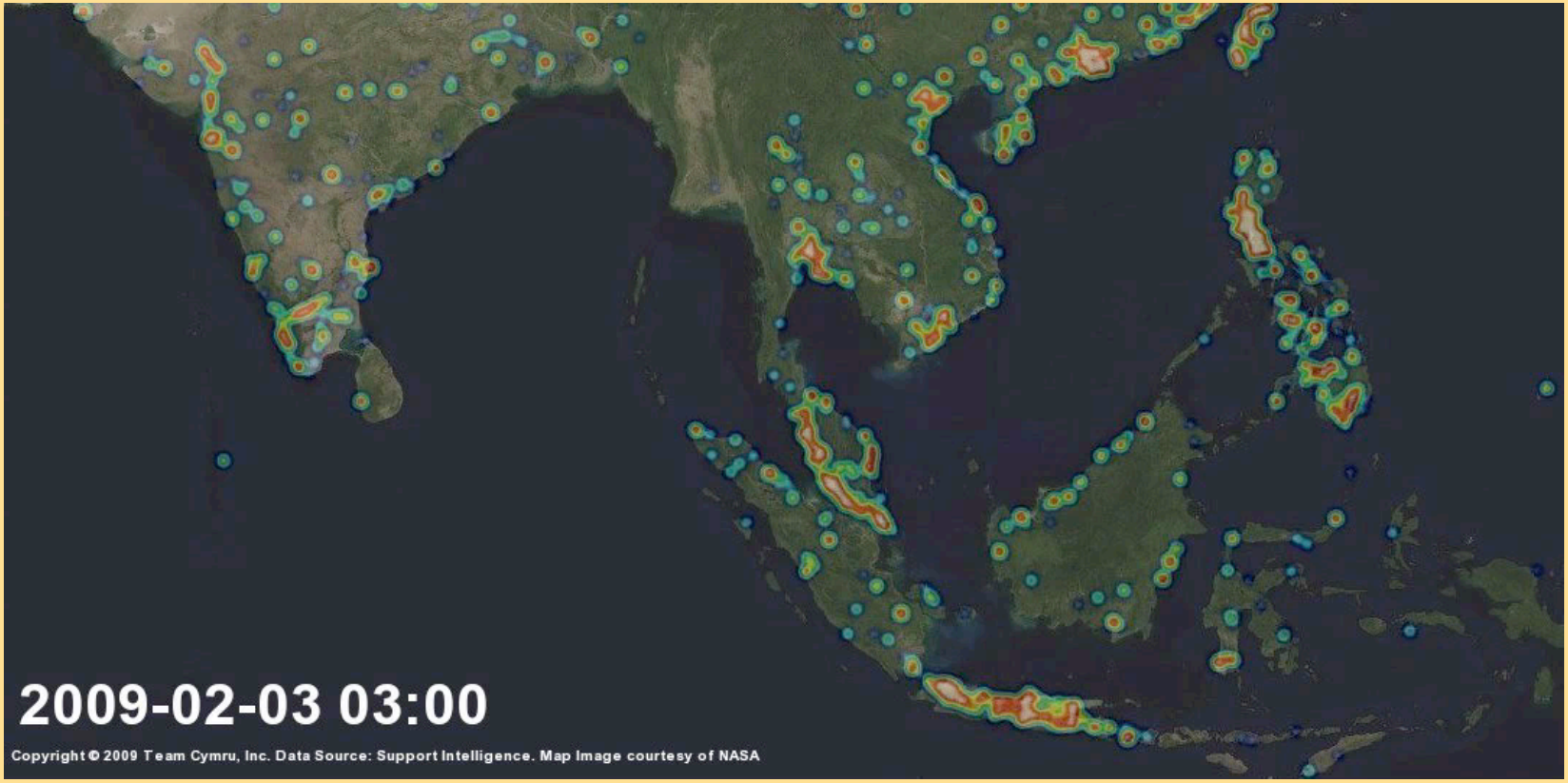
Conficker (Europe)



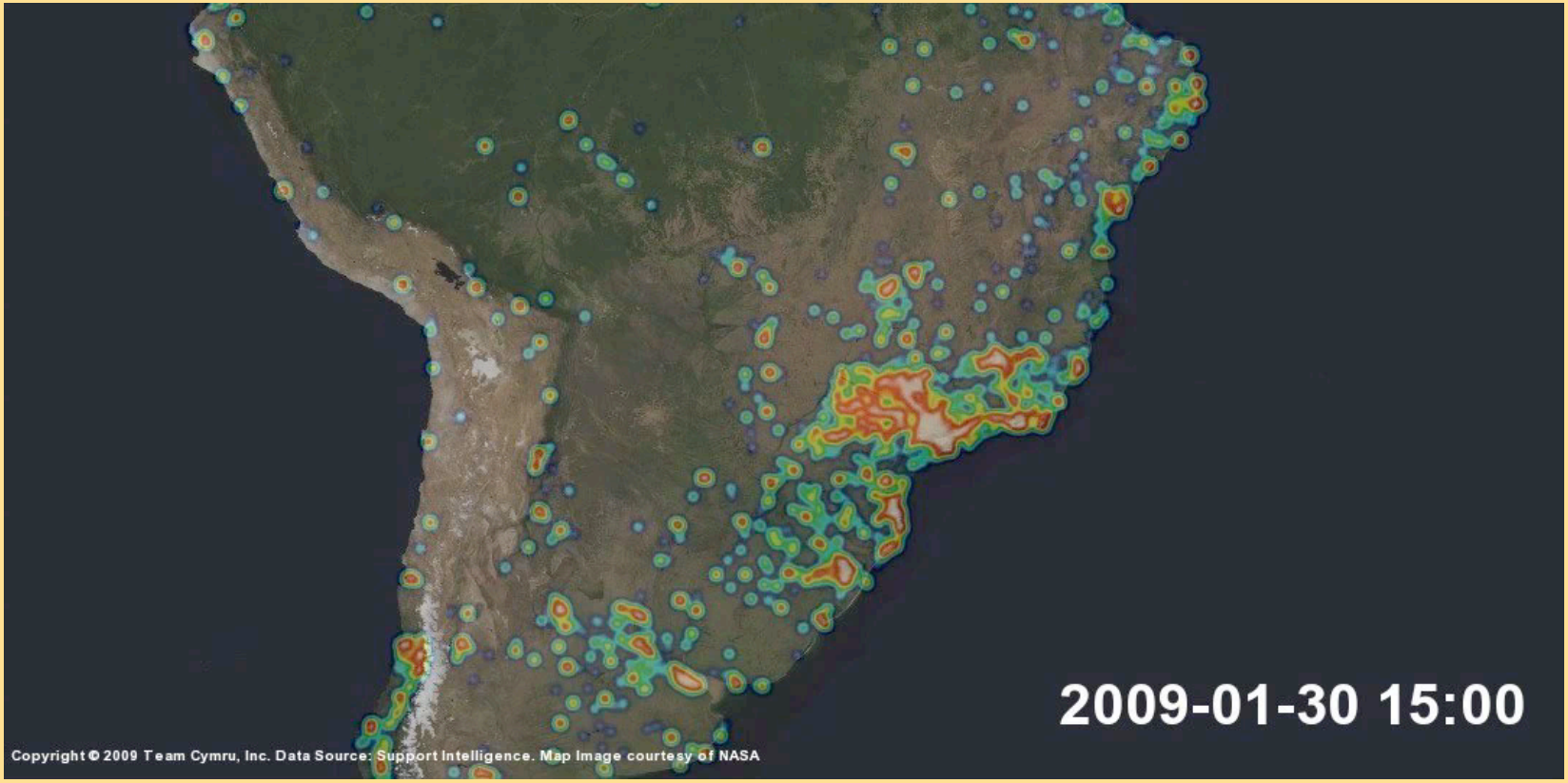
Conficker (North Asia)



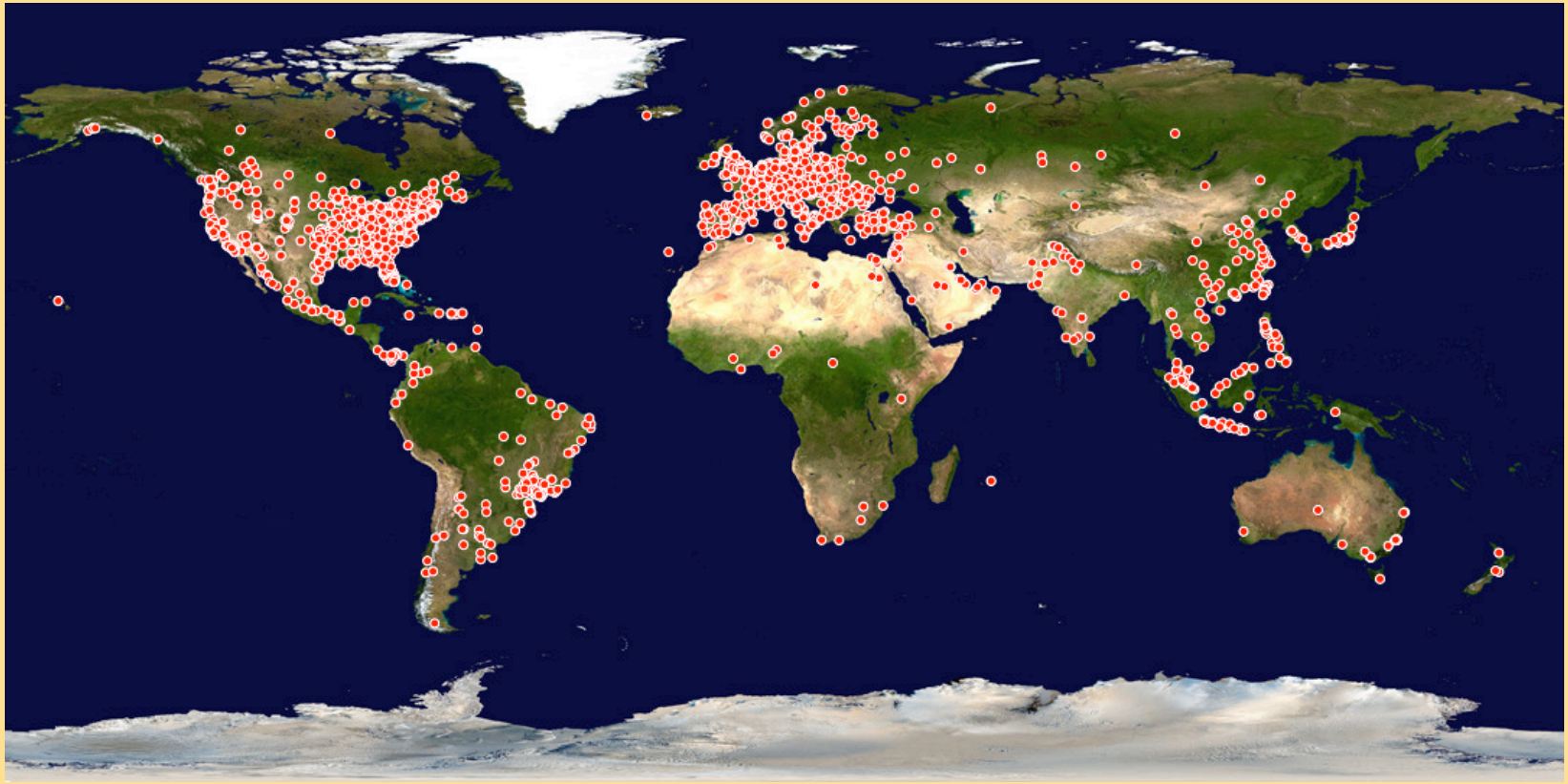
Conficker (South Asia)



Conficker (South America)

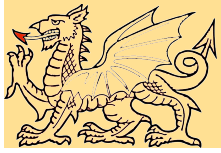


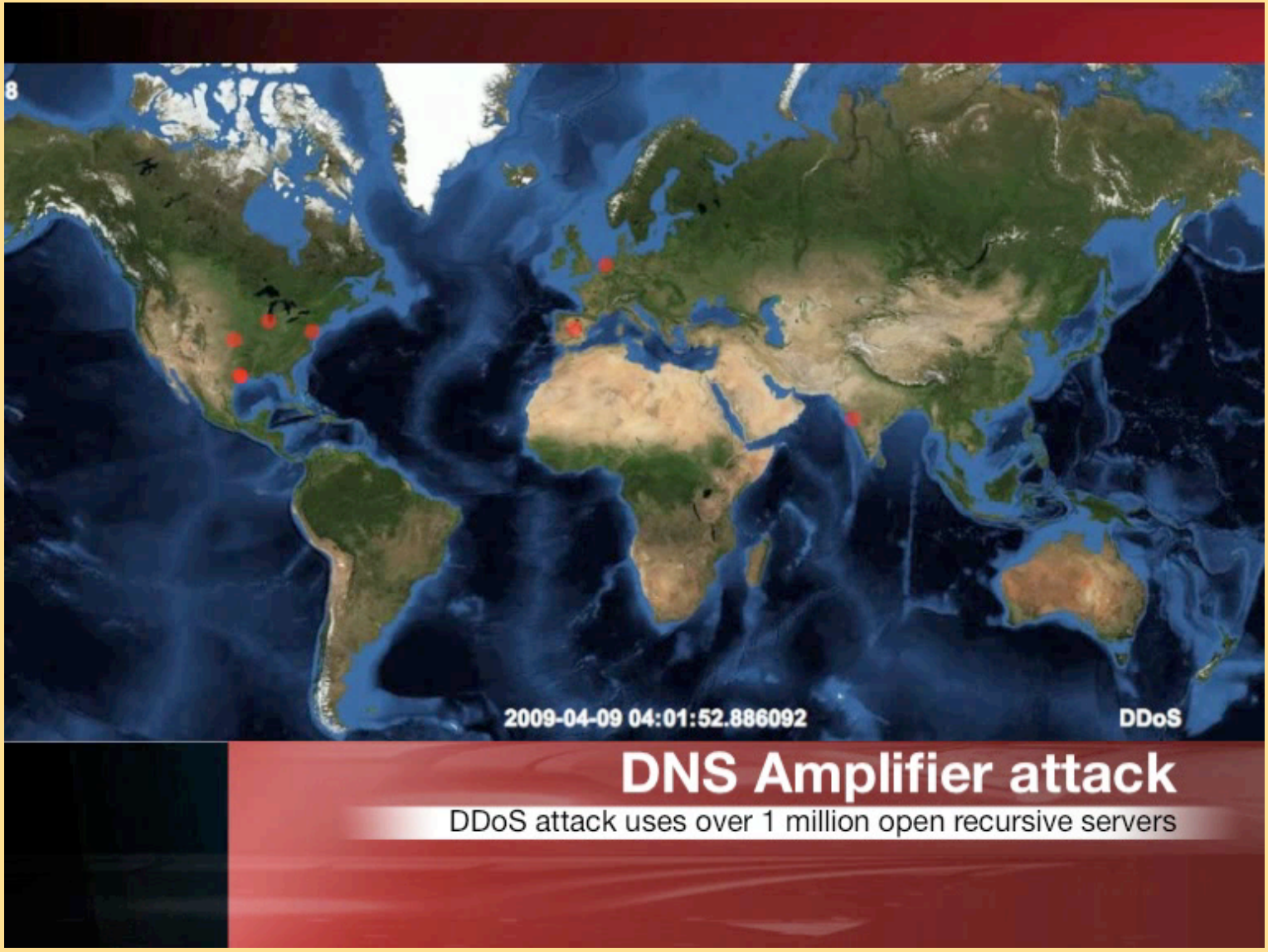
DDoS Attacks in 2008



DDoS Attacks in Japan 2008

- 118 total attacks
- Top target cities
  - Tokyo: 65 attacks
  - Osaka: 14 attacks
- Top target networks
  - AS17676 GIGAINFRA BB Tech. (29 attacks)
  - AS4713 NTT Communications (17 attacks)
  - AS17506 UCOM Corporation (12 attacks)



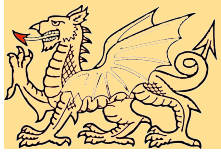


A Global Problem…

Questions?

Special Thanks

- Support Intelligence (Data)
  - http://www.support-intelligence.com
- Maxmind and Quova (GeoIP)
  - http://www.maxmind.com
  - http://www.quova.com
- NASA Visible Earth
  - http://visibleearth.nasa.gov



Contact Info

- deitrich@cymru.com
- www.team-cymru.org
- Team PGP key at www.cymru.com/teamcymrukey.txt

THANK YOU!

ありがとうございます!