Future Challenges of the Internet

Fred Baker

Agenda

- I’ll discuss four challenges:
  - Politics
  - Security
  - Addressing
  - Deployment frontiers
- I’m not sure they are “future”. The are certainly “challenges”

Politics

Extra-territorial law?

Recent examples

- GDPR (European Union)
    - https://businesslawtoday.org/2018/04/extraterritorial-scope-gdpr-businesses-outside-eu-need-comply/
- Net Neutrality, on again, off again (US)
    - https://www.dslreports.com/shownews/Senators-Press-Ajit-Pai-on-DDOS-Attack-His-Agency-Made-Up-141999
- European Commission Copyright proposal
    - https://www.siliconrepublic.com/enterprise/eu-copyright-proposal-letter
- US DOC/NTIA Inquiry on Internet Policy Priorities
    - https://www.ntia.doc.gov/federal-register-notice/2018/notice-inquiry-international-internet-policy-priorities

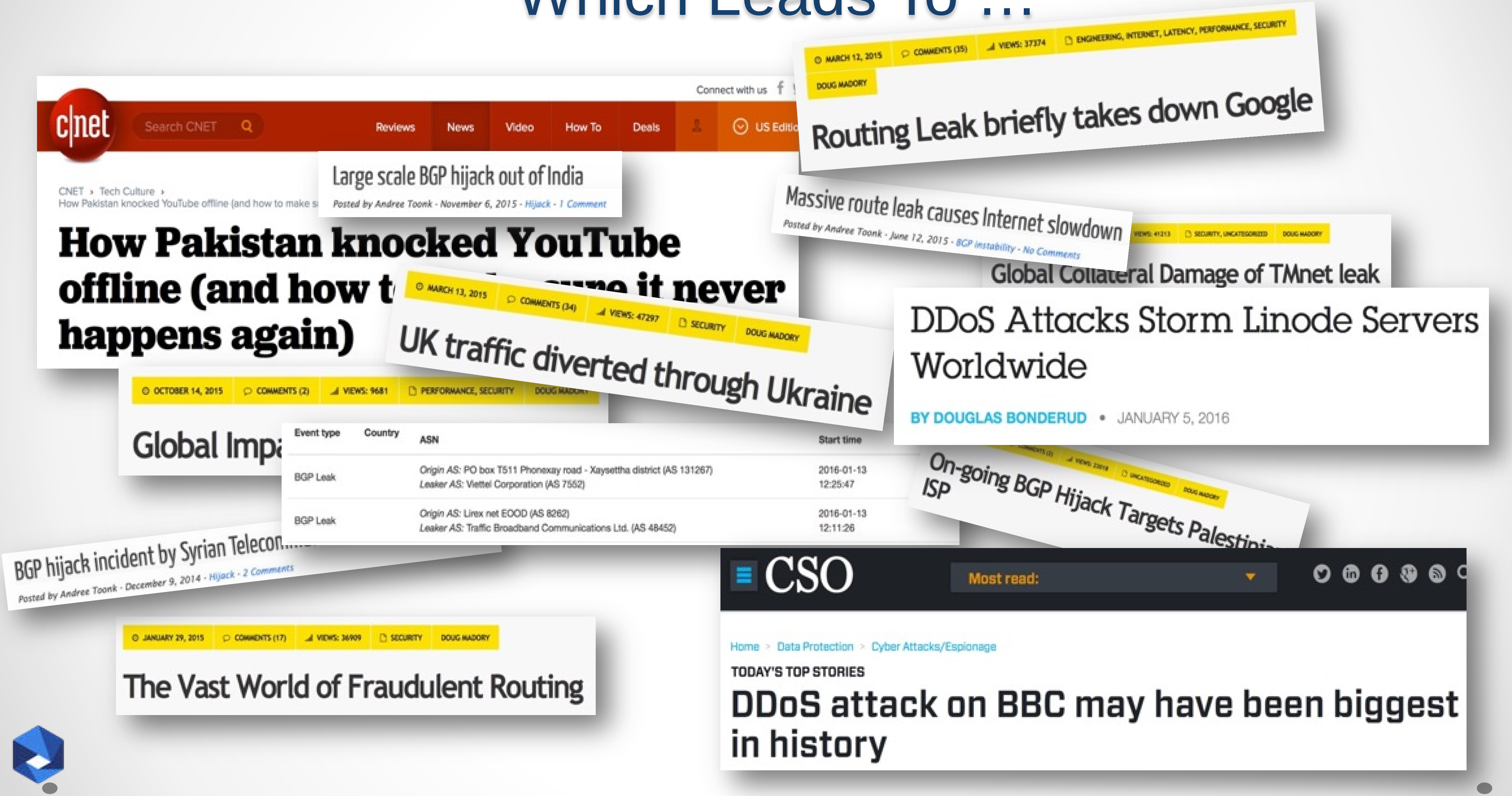
Security

Mutually Agreed Norms for Routing Security (MANRS)

The Honor System: Routing Issues

- Border Gateway Protocol (BGP) is based entirely on trust between networks
- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

Which Leads To …



MARCH 12, 2015 | COMMENTS (35) | VIEWS: 37374 | ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY | DOUG MADORY

Routing Leak briefly takes down Google

Connect with us

c|net Search CNET Reviews News Video How To Deals US Editio

CNET › Tech Culture ›
How Pakistan knocked YouTube offline (and how to make s

How Pakistan knocked YouTube offline (and how t… …sure it never happens again)

Large scale BGP hijack out of India

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

Massive route leak causes Internet slowdown

Posted by Andree Toonk - June 12, 2015 - BGP instability - No Comments

VIEWS: 41213 | SECURITY, UNCATEGORIZED | DOUG MADORY

Global Collateral Damage of TMnet leak

MARCH 13, 2015 | COMMENTS (34) | VIEWS: 47297 | SECURITY | DOUG MADORY

UK traffic diverted through Ukraine

DDoS Attacks Storm Linode Servers Worldwide

BY DOUGLAS BONDERUD • JANUARY 5, 2016

OCTOBER 14, 2015 | COMMENTS (2) | VIEWS: 9681 | PERFORMANCE, SECURITY | DOUG MADORY

Global Impa

Event type	Country	ASN	Start time
BGP Leak		*Origin AS:* PO box T511 Phonexay road - Xaysettha district (AS 131267) *Leaker AS:* Viettel Corporation (AS 7552)	2016-01-13 12:25:47
BGP Leak		*Origin AS:* Lirex net EOOD (AS 8262) *Leaker AS:* Traffic Broadband Communications Ltd. (AS 48452)	2016-01-13 12:11:26

VIEWS: 23018 | UNCATEGORIZED | DOUG MADORY

On-going BGP Hijack Targets Palestinia… ISP

BGP hijack incident by Syrian Telecom…

Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments

JANUARY 29, 2015 | COMMENTS (17) | VIEWS: 36909 | SECURITY | DOUG MADORY

The Vast World of Fraudulent Routing

CSO Most read:

Home › Data Protection › Cyber Attacks/Espionage

TODAY'S TOP STORIES

DDoS attack on BBC may have been biggest in history

The Threats: What's Happening?

Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	Source address validation

MANRS Actions

• Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

• Global Validation

Facilitate validation of routing information on a global scale

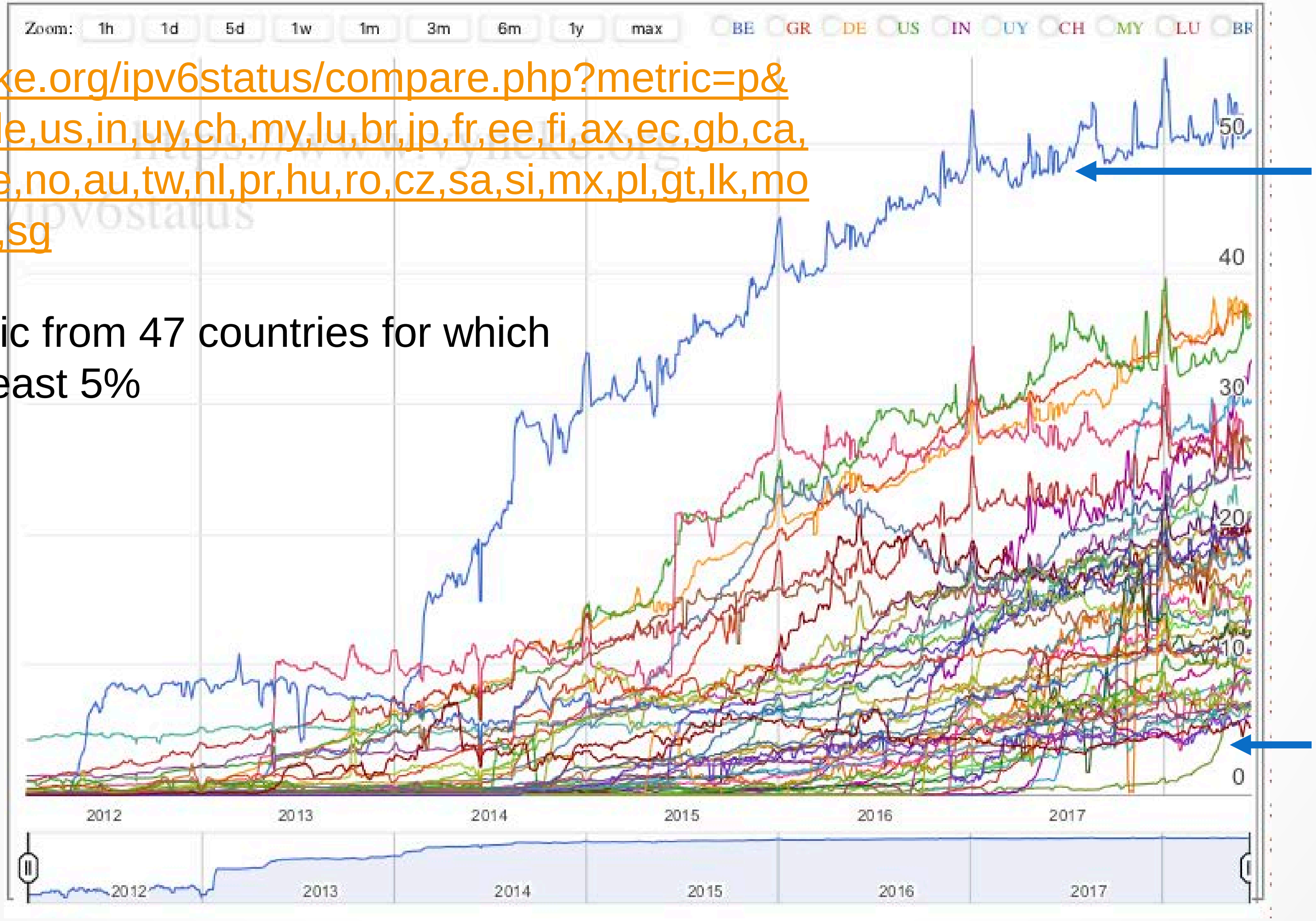
Publish your data, so others can validate

Addressing -
IPv6 Deployment

Global IPv6 traffic as seen by Google

https://www.vyncke.org/ipv6status/compare.php?metric=p&countries=be,gr,de,us,in,uy,ch,my,lu,br,jp,fr,ee,fi,ax,ec,gb,ca,pt,tt,ie,th,vn,nz,pe,no,au,tw,nl,pr,hu,ro,cz,sa,si,mx,pl,gt,lk,mo,at,se,ar,zw,bo,fo,sg

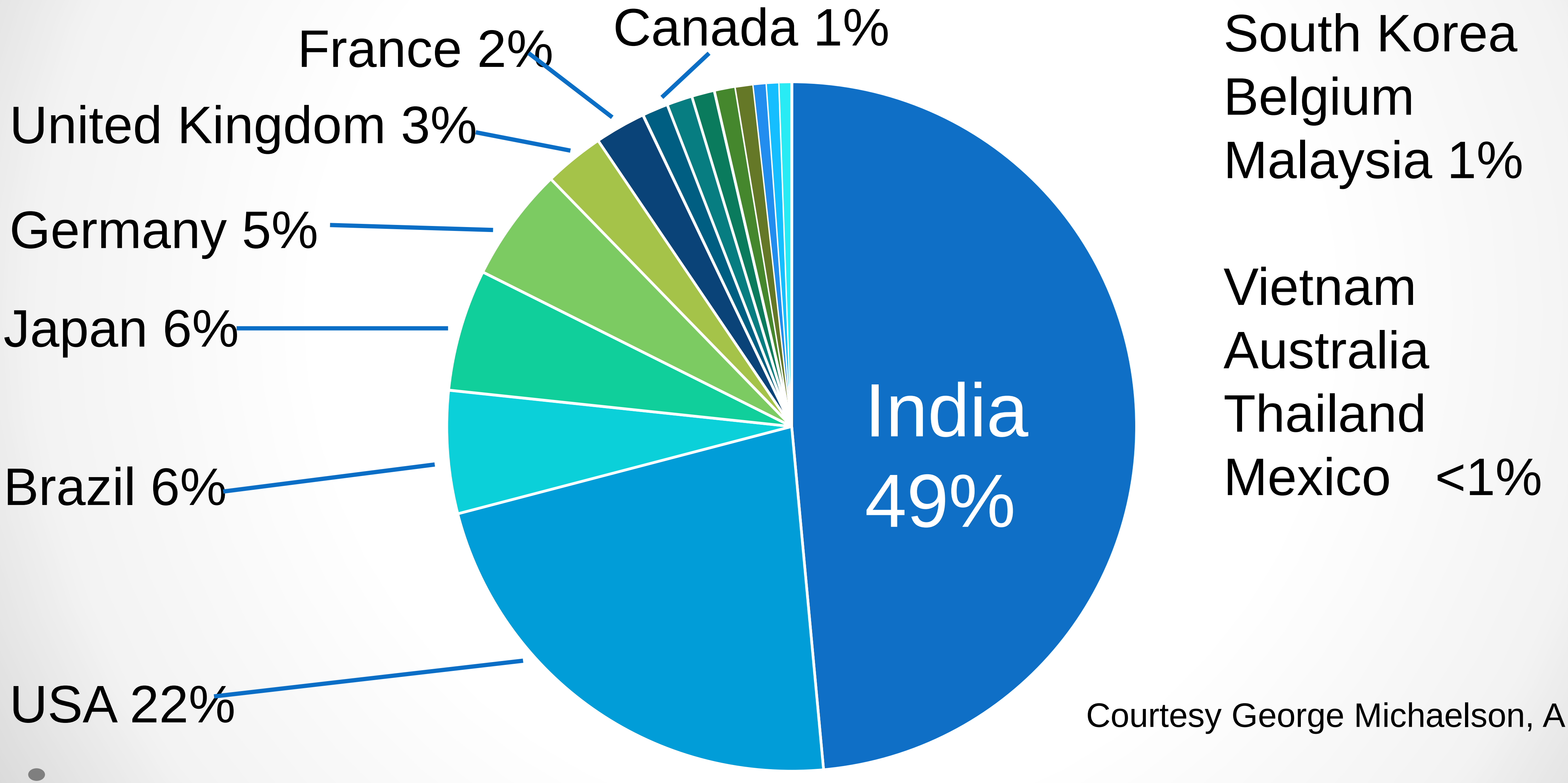
Google sees traffic from 47 countries for which IPv6 traffic is at least 5%



Belgium

Taiwan

Top 15 economies in IPv6 Traffic



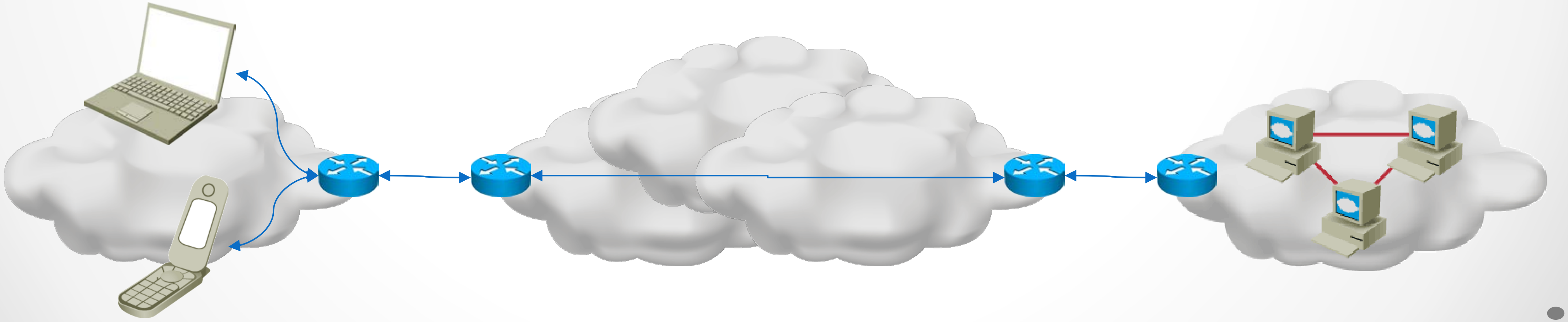
Courtesy George Michaelson, APNIC

Observations: what's doing well

- A number of networks are reporting high IPv6 use, notably mobile networks
  - Reliance JIO and Verizon Wireless similarly report that about 90% of its traffic uses **IPv6**. T-**Mobile** is among the providers in the process of turning IPv4 off. Other major **cellular IPv6** providers include AT&T **Wireless**, Sprint, Telus, Tele2, EE, KDDI, Softbank, OTE, Rogers and many others.
  - *That was a year ago* – ISOC's 2017 IPv6 report
- Residential Broadband, especially with managed routers
  - My kids tease me about IPv6. But each one uses it more than they know…
- Data Centers and Content
  - Some data center and content operations report high IPv6 availability/use
  - Cloudflare, Mythic Beasts
  - Google, Facebook, etc

The elephant in the room: Enterprise

- When a dual stack device tries to access an IPv6-capable device, it may use IPv6
  - Visible in Google/APNIC/Akamai statistics: turn on IPv6, and suddenly see traffic
- *When a dual stack device tries to access an IPv4-only device, it uses IPv4*
  - Very common with enterprise web presence, email, etc
  - *Enterprise in general hides behind IPv4/NAPT on the illusion that it provides security*
- *"End to end" is application, platform, and routing path*



Fundamental issues are legal and economic

- Address cost:
  - IPv4 addresses cost money, price likely to peak in 2018-2019 due to expected IPv6 market impact and size of available IPv4 address pools
  - IPv6 addresses essentially free
- Management and maintenance cost
  - Diagnosing IPv4 networks can be complex and error-prone
  - IPv6 flat address space simplifies management issues
- Can you associate a single address (or address+port) with a single subscriber?
  - Carrier Grade Network Address Translation often does not meet legal requirements.

Deployment frontiers

Future Internet

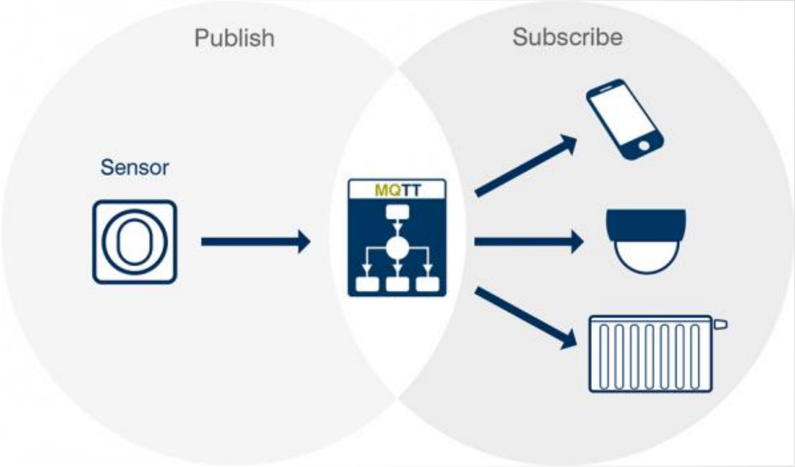
Internet of Things

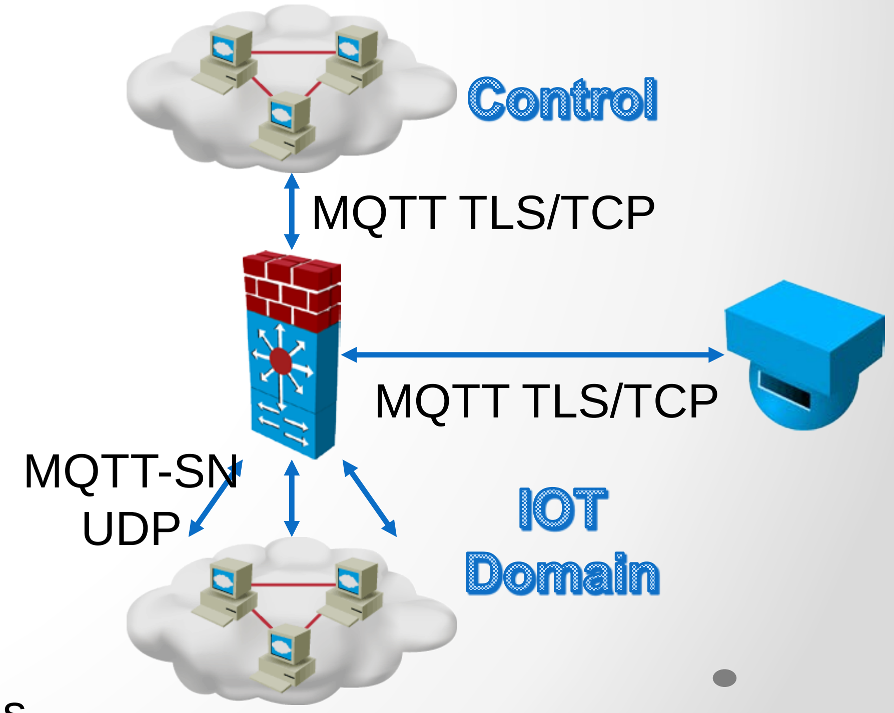
We hear a lot about the Internet of Things

- IOT is at least two broad markets:
  - **Devices that are essentially stand-alone computers in people’s homes of offices running an access application**
    - Google Assistant, Alexa, Microsoft Cortana, Apple Siri, and so on
    - **Usually responsible for its own security, as laptops are**
  - **Devices that are often trivially simple and parts of larger services**
    - Robots
    - Video or audio surveillance
    - Smart Grid
    - Automotive engineering
    - Building Management
    - Etc.
    - **Often part of a security *system***

MQTT: an example of a secured IOT System

- MQTT: OASIS Standard
  - TLS/TCP connection from cloud system to device or gateway
  - Sleeping nodes: managed UDP access to gateway
- Publish/Subscribe
  - Focuses on messages, not devices
  - Delivers messages from "publishers" to "subscribers"
  - IOT domain could be link layer only
- Message exchange
  - Cloud access via TLS/TCP to security/distribution gateway
  - "Always On" IOT uses TLS/TCP as well
  - Sleeping Nodes
    - Request messages from gateway to reduce battery consumption





Note: this is a worked example, not the only way to accomplish this

IOT Security

- Various frameworks are being promoted: OTA, US NIST, US DHS, among others
- My general thought is that many IOT devices are manufactured using ODM approaches and suffer many of the idiocies that other ODM consumer products such as routers have experienced for the same reasons.
- “These 60 dumb passwords can hijack over 500,000 IoT devices into the Mirai botnet”
  - https://www.grahamcluley.com/mirai-botnet-password/

IOT Security

- In general, I think that IOT security policies and approaches should be comparable to the policies and approaches used for any other secure systems
  - Example: use up to date software and software patches!
  - Example: password authentication has many problems, and is better if one uses cryptographic technologies or two factor authentication.
  - *That often means deploying secure systems of devices, and not putting IOT directly on the Internet.*

Future Challenges of the Internet

Fred Baker