More than Glimpse of Internet

Internet Behaviour and Insight

Wallis Choi
Dyn Asia Pacific
2017.02

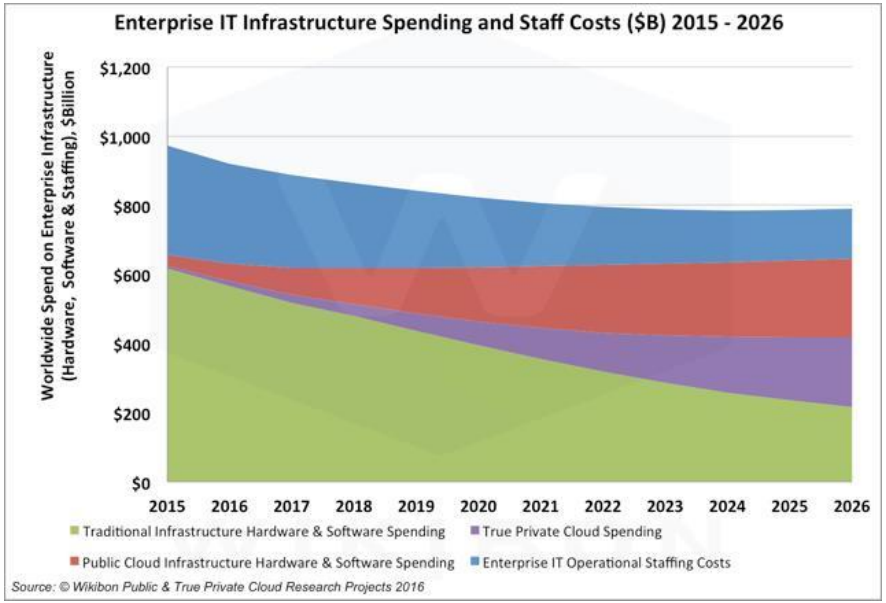
INTERNET
PERFORMANCE.
DELIVERED.

dyn.com @dyn


Trends and Challenges
Unique Big Picture Data Approach
What could we see?
Dyn

Cloud Growth in the Forecast

We're in the midst the most significant shift in IT over the last 30 years.



IDC predicts external cloud adoption will increase from 22% today to 32.1% in 24 months achieving 45.8% growth

http://www.idc.com/getdoc.jsp?containerId=prUS41039416

And cloud IT infrastructure spending will be 46% of total expenditures on enterprise IT infrastructure.

http://www.idc.com/getdoc.jsp?containerId=prUS25946315

Dyn

Warning: Storms on the Internet Horizon

Scale, Complexity & Volatility of the Internet on the Rise

- **SCALE:**

  3.6 Billion Users (1/2 the world's population)

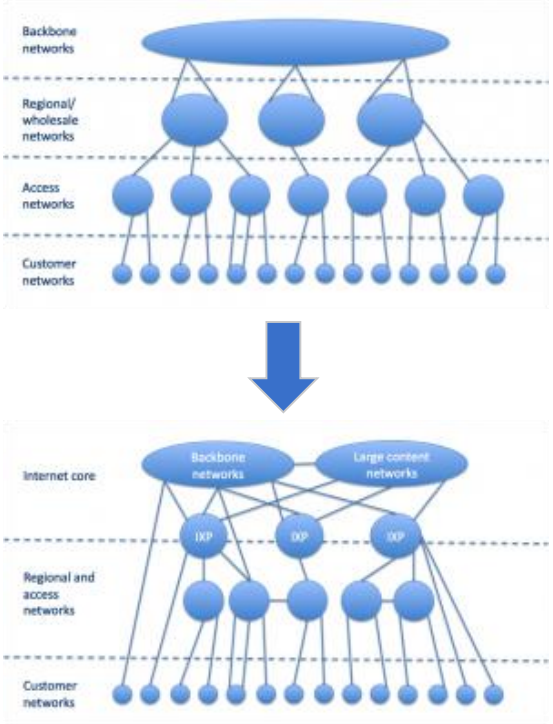
  10 B Devices/Things → Growing by US population every year → *Global IP Traffic to Triple over next five years*

- **COMPLEXITY:**

  Moving from hierarchical to flatter, more connected internet model

- **VOLATILITY:**

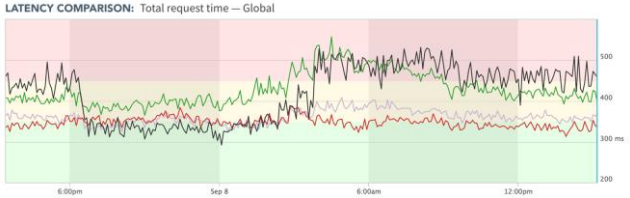
  Cheap, on-demand compute bites back: DDoS attacks up 100%-200% YoY; Route hijacks on the rise (both malicious and accidental)



Dyn

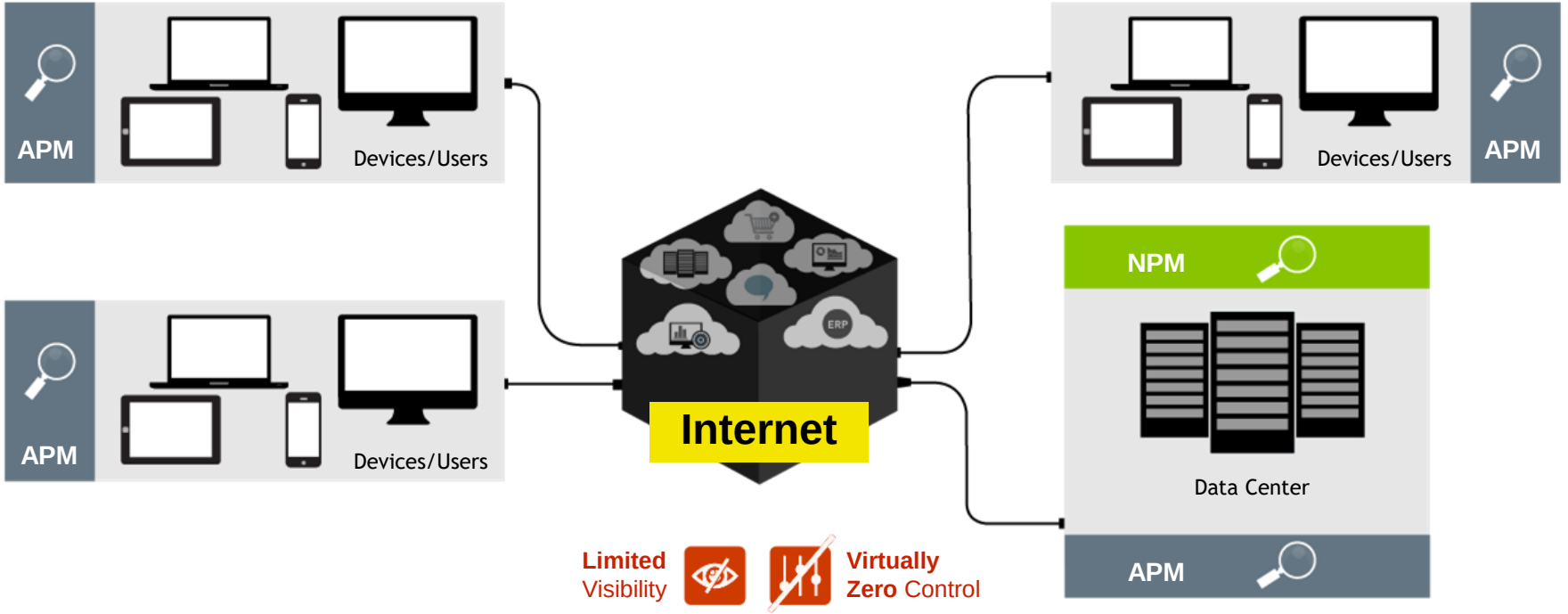
It’s always cloudy

somewhere on the internet



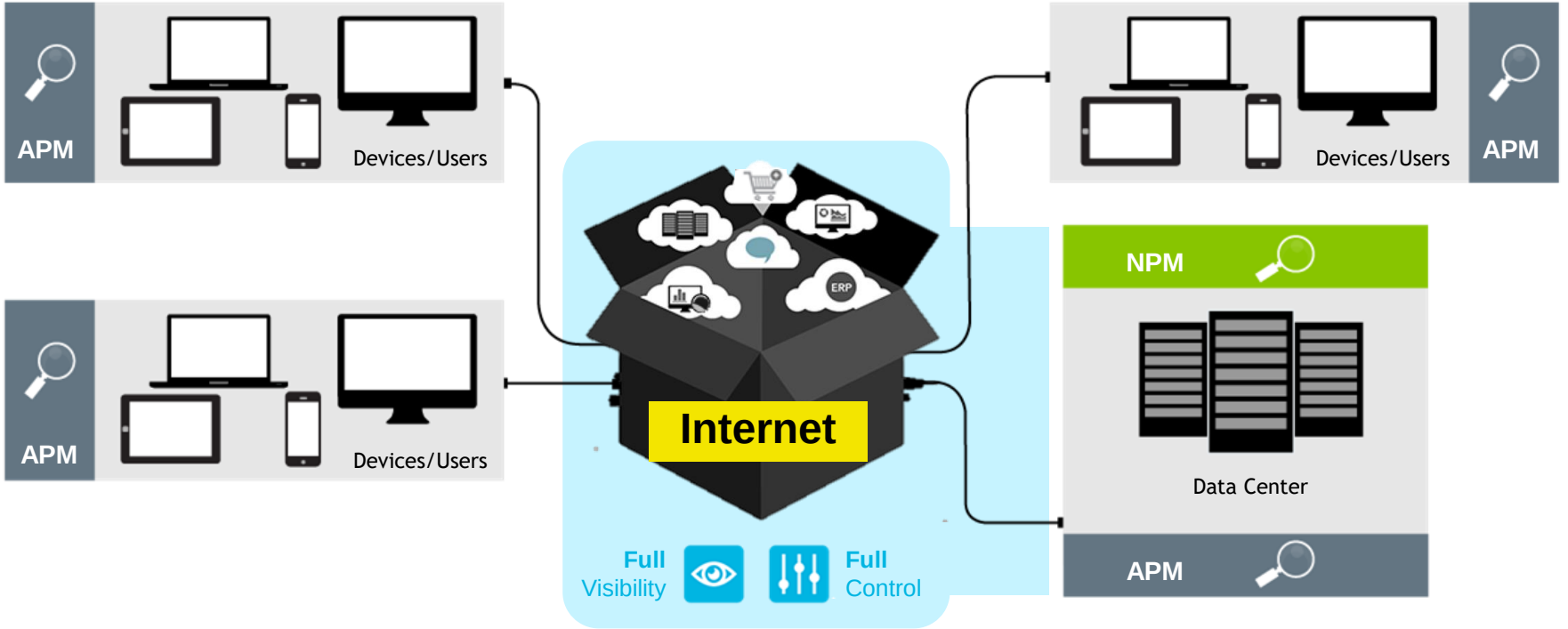
Dyn

Shift to SaaS and Cloud-based Infrastructure brings both Opportunity and Risk



To Enterprise IT, the move to the Internet has become an opaque "black box" =
Limiting visibility and virtually eliminating performance control

Visibility and Control instead of a Black Box

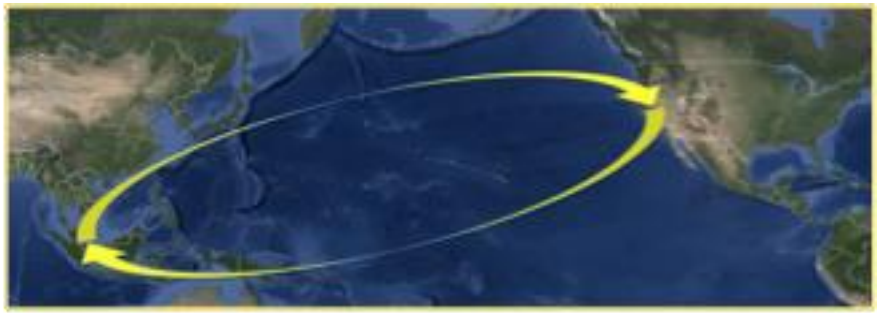


Visibility and Control to get the most from your Cloud-based infrastructure

Reduce Costs ***Decrease Risk*** ***Boost Revenue***

Dyn

Usual or Unusual?



Source: Dyn Research

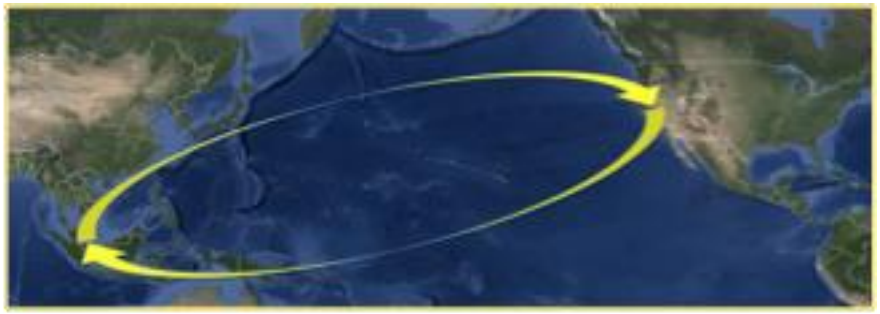
Scenario 1

Traffic between two floors of the same office building in Singapore takes over 350ms round trip, traveling via San Jose, California

Scenario 2

Traffic from Western Europe to the US takes around 70ms round trip, traveling via Iceland's incumbent provider

Usual or Unusual?



Source: Dyn Research

Scenario 1 — USUAL

NTT won't peer with Tinet in Singapore; Tinet must drag traffic to San Jose to hand it off to NTT, who drags it home again to Singapore.

Scenario 2 — UNUSUAL

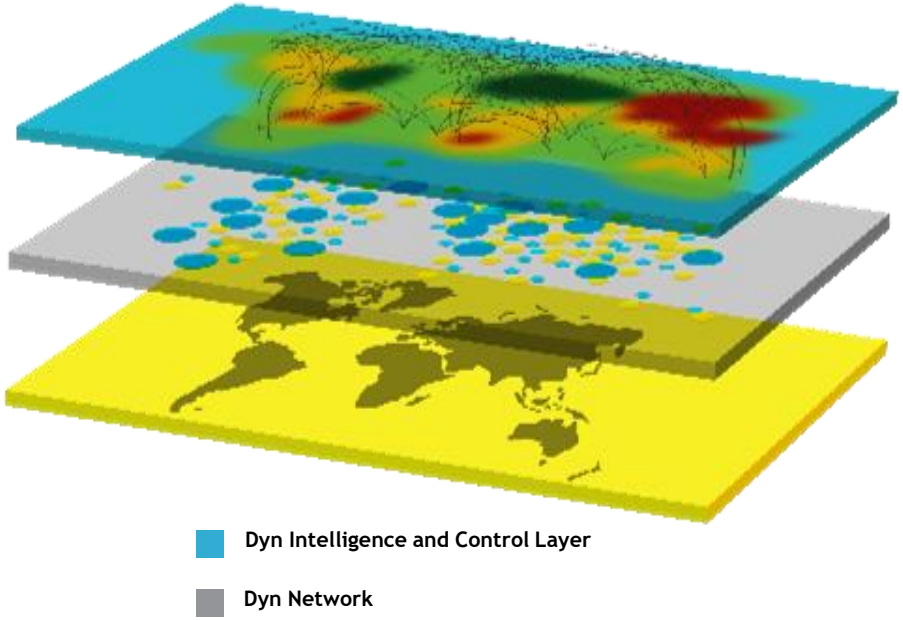
Iceland's ISP Siminn, hijacked routes of major firms for weeks and passed the traffic along. In general, traffic never flows via Iceland (cost, geo).


Trends and Challenges
Unique Big Picture Data Approach
What could we see?
Dyn

Unique “Big Picture” Data Approach

Curing Internet blindness

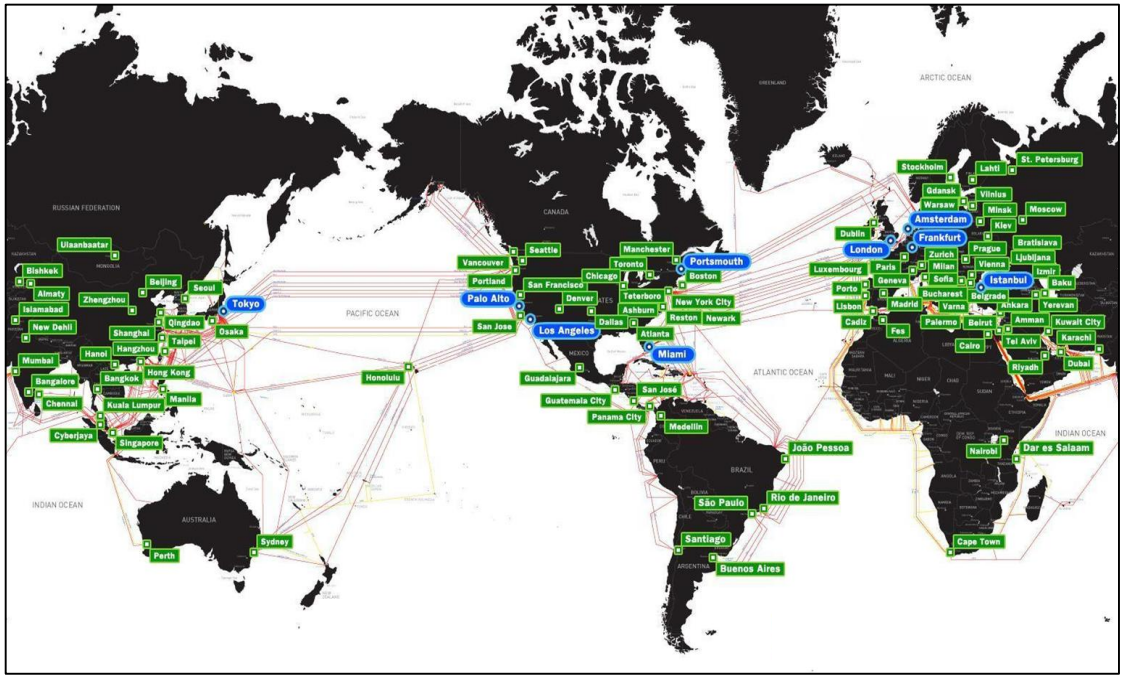
- **Dyn** monitors the entire Internet across multiple datasets
- Multi-dimensional data from sources such as:
  - Authoritative & Recursive DNS
  - Real-User Monitoring
  - Protocol & Performance Measurement
  - BGP Routing & Topology
- Correlation across datasets reveals high value problem root causes
- Only Dyn has non-archived datasets reaching back to 2002 for unique historic context



Active Management Infrastructure

Active monitoring of BGP

- Real-time global routing table from over 700 sessions
- Over Hundreds of collectors sending traceroutes to over millions targets daily
- Updates and alerts 30 seconds from real time



"It's good to see this great data being exposed for operational purposes. — The internet is so critical for for almost every business today."

– Gartner (Jonah Kowall, VP).

Dyn


Trends and Challenges
Unique Big Picture Data Approach
What could we see?
Dyn

Typical BGP MITM Attack w/ Dyn Alarm

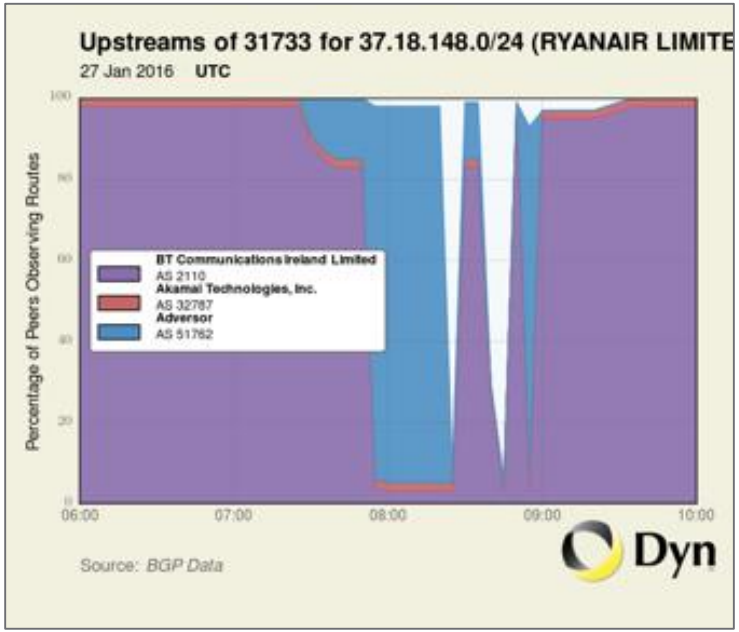

```
AS6697 (Beltelecom, BY) announced 1 pfx(s) that are
potentially hijacks of currently routed address space:

   XXX.YYY.151.0/24 (ZZZZ, GB), seen by 310 peers for an
   average of 1.16 hours.  This is a more specific of
   prefix: XXX.YYY.128.0/19 (ZZZZZ), Origin=NNNN (ZZZZZ,
   GB)
```

Dyn

DDOS Mitigation Success/Failure

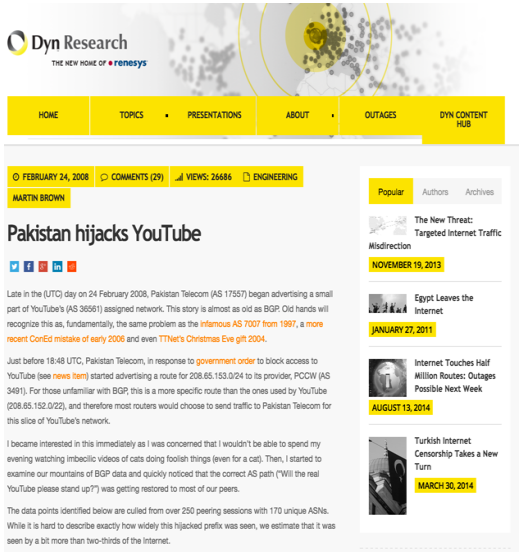
Sometimes the cure is similar to the poison

- Used **cleanpipe** for **DDoS mitigation**
- Uneven transitions to cleanpipe, including brief losses of Internet connectivity
- Cleanpipe failed to propagate customer routes globally
- 80% of Dyn's peers didn't have connectivity for a period
  - This is reflected by the white area on the diagram to the right



Anatomy of a Hijack: YouTube

- **Normal: YouTube announced through a /22 block**
  - 36561 208.65.152.0/22
- **Pakistan govt. attempted to block an ‘offensive’ video**
- **Pakistan Telecom implemented this by attempting to block YouTube within the country by announcing a more specific /24 prefix**
  - 17557 208.65.153.0/24
- **Propagated globally and redirected all YouTube users to Pakistan Telecom**
  - 3491 17557 208.65.153.0/24
- **YouTube unavailable for 4 hours globally**
- **YouTube reacted by announcing /24s. Still a partial hijack**
- **Finally, YouTube announced /25s**



http://research.dyn.com/2008/02/pakistan-hijacks-youtube-1/

Hijack 2: Going Nuclear

- March 2015: Vega (AS12883) starts announcing British Telecom prefixes
- Initially, 14 prefixes, later 167 prefixes including UK's Atomic Weapons Establishment (AWE)
- Traceroutes confirm traffic heads into Ukraine through Vega, but reaches its destination at AWE via BT
- Man-in-the-middle attack (a hijack variant)

MARCH 13, 2015 | COMMENTS (37) | VIEWS: 57457 | SECURITY | DOUG MADORY

UK traffic diverted through Ukraine

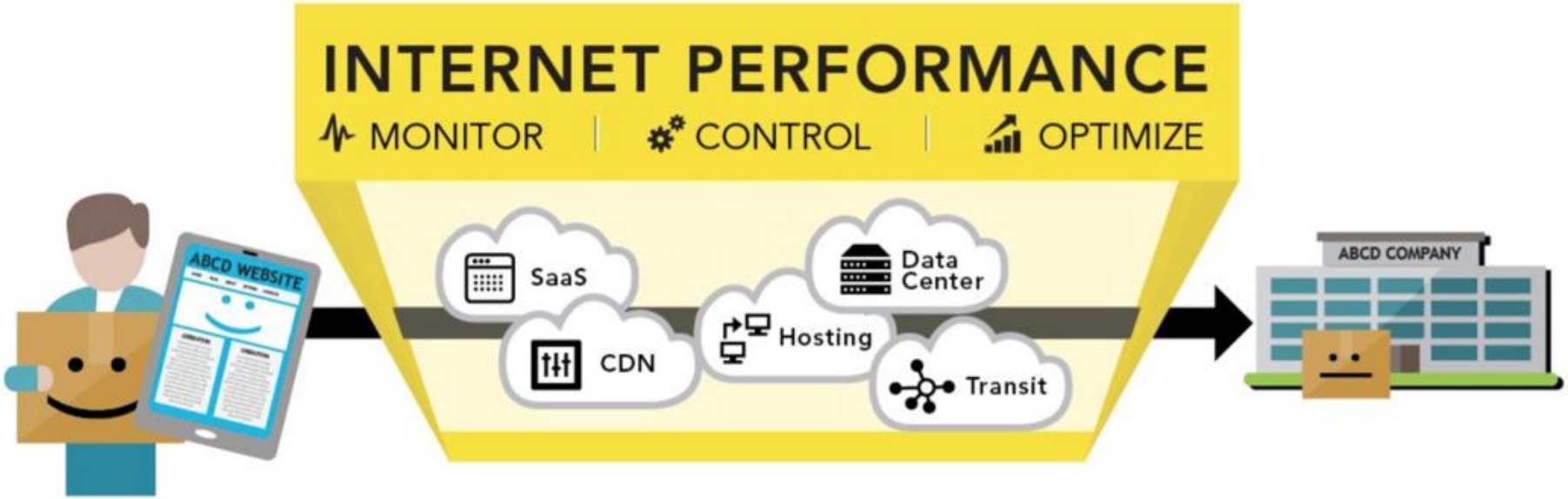
On the heels of the BGP leak yesterday that briefly impaired Google services around the world, comes another routing incident that impacted some other important Internet services.

Beginning on Saturday, Ukrainian telecom provider, Vega, began announcing 14 British Telecom (BT) routes, resulting in the redirection of Internet traffic through Ukraine for a handful of British Telecom customers. Early yesterday morning, Vega announced another 167 BT prefixes for 1.5 hours resulting in the rerouting of additional traffic destined for some of BT's customers, including the UK's Atomic Weapons Establishment, the "organization responsible for the design, manufacture and support of warheads for the United Kingdom's nuclear deterrent."

http://research.dyn.com/2015/03/uk-traffic-diverted-ukraine/

Dyn

Through Measurement, you are in Control



Dyn

THANK YOU!