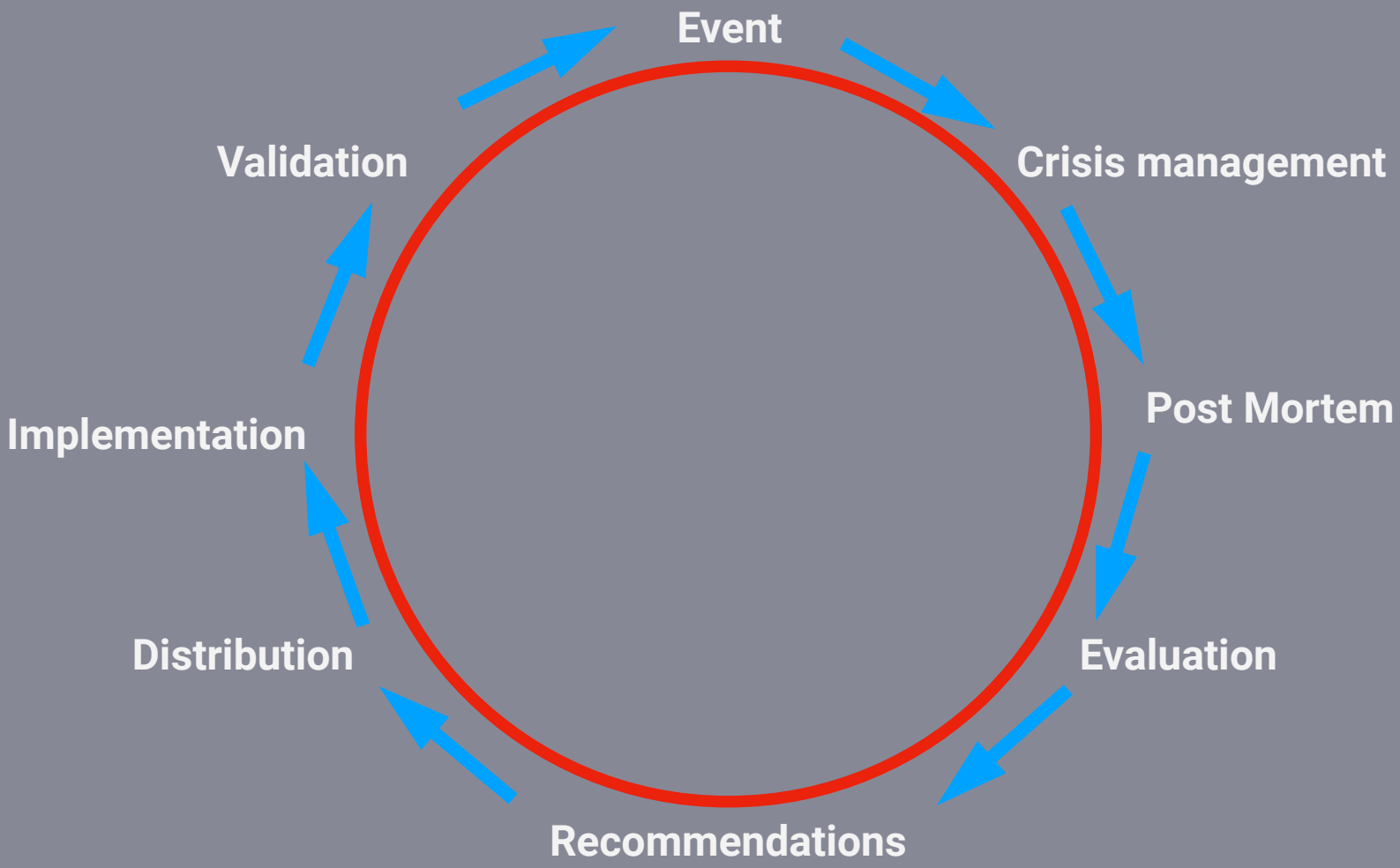
# Technical challenges to protecting state sovereignty online

**Patrik Fältström**
**Technical Director and Head of Security**


Event
Crisis management
Post Mortem
Evaluation
Recommendations
Distribution
Implementation
Validation


Kungl. IngenjörsVetenskaps Akademien

# From pipes to a lasagna

Kungl. IngenjörsVetenskaps Akademien

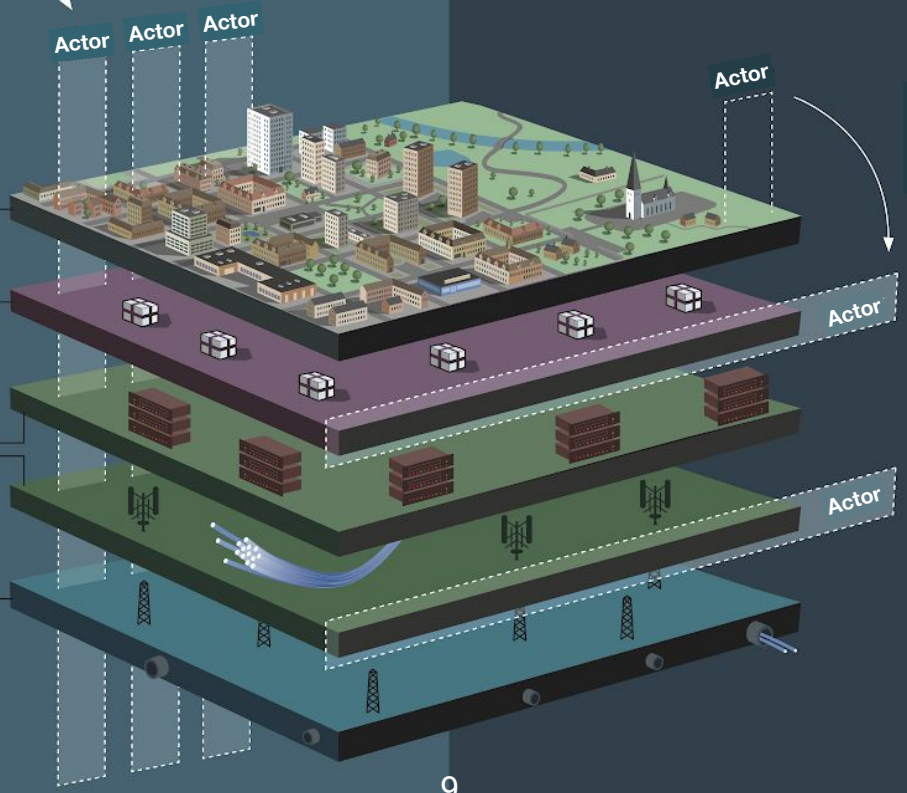
**Traditional deployment in ”pipes” implies a tight control throughout the infrastructure**

**Services**
Companies, public sector and others offer services like web, email and apps to companies, citizens and consumers.

**Internet Access**
Internet- and mobile operators give companies and consumers access to Internet.

**Active infrastructure**
Transmission providers ensure transport of data to internet- and mobile operators.

**Passive infrastructure**
Ducts, fibre, masts etc. Built by municipalities, private companies and others.

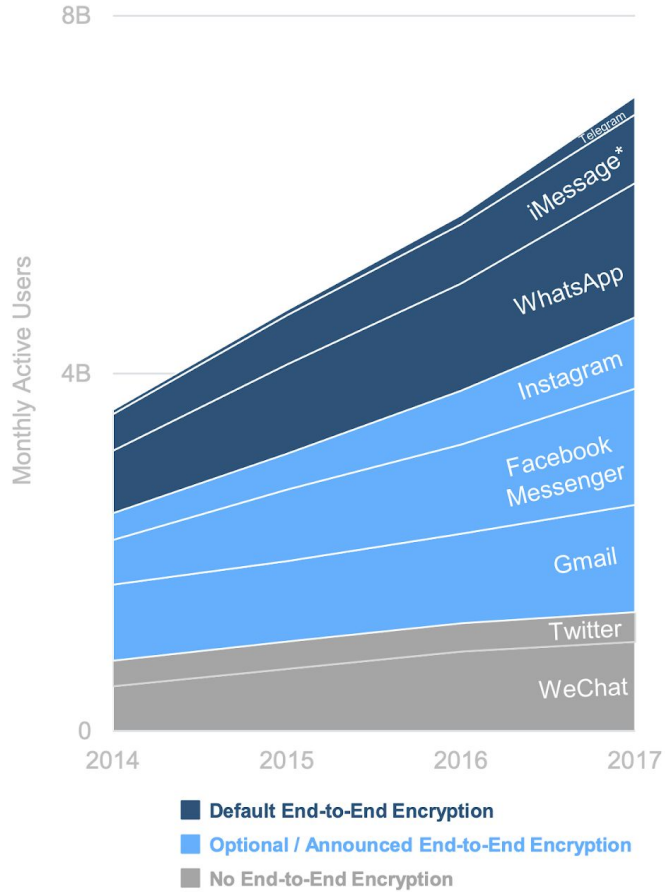



**A continuous change towards a partial horizontal management implies control throughout the infrastructure get new constraints**

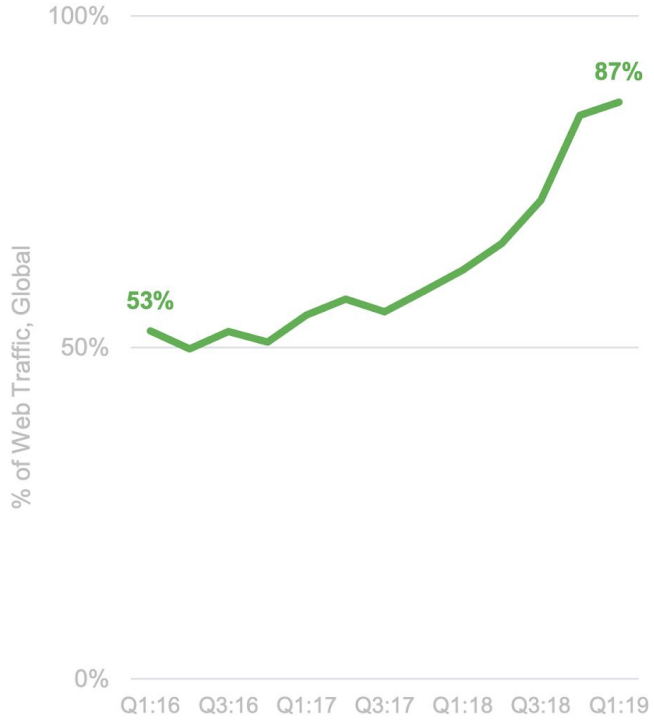
**Pros:**
- Simpler management of control
- Increased ability to innovate
- Standardization leads to replaceability of products and services

**Cons:**
- ”Markets” on different layers that do not work as efficient as possible
- Lack of control and planning
- Low skills regarding procurement
- Non-optimal risk management for the society as a whole

## Select Messenger MAUs

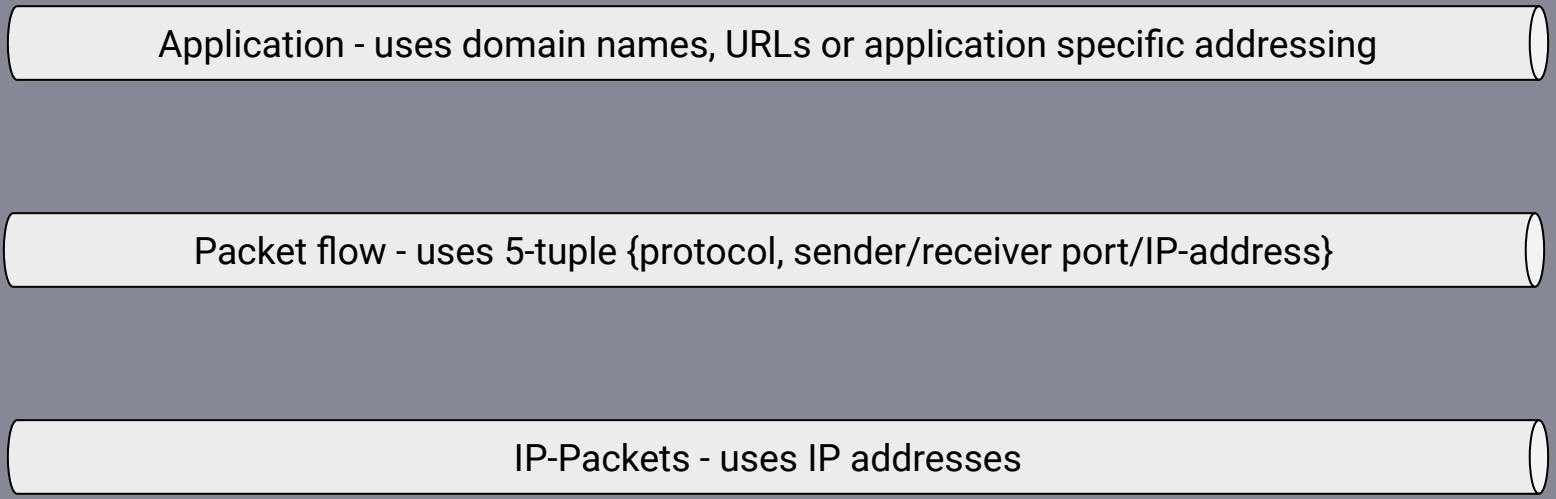


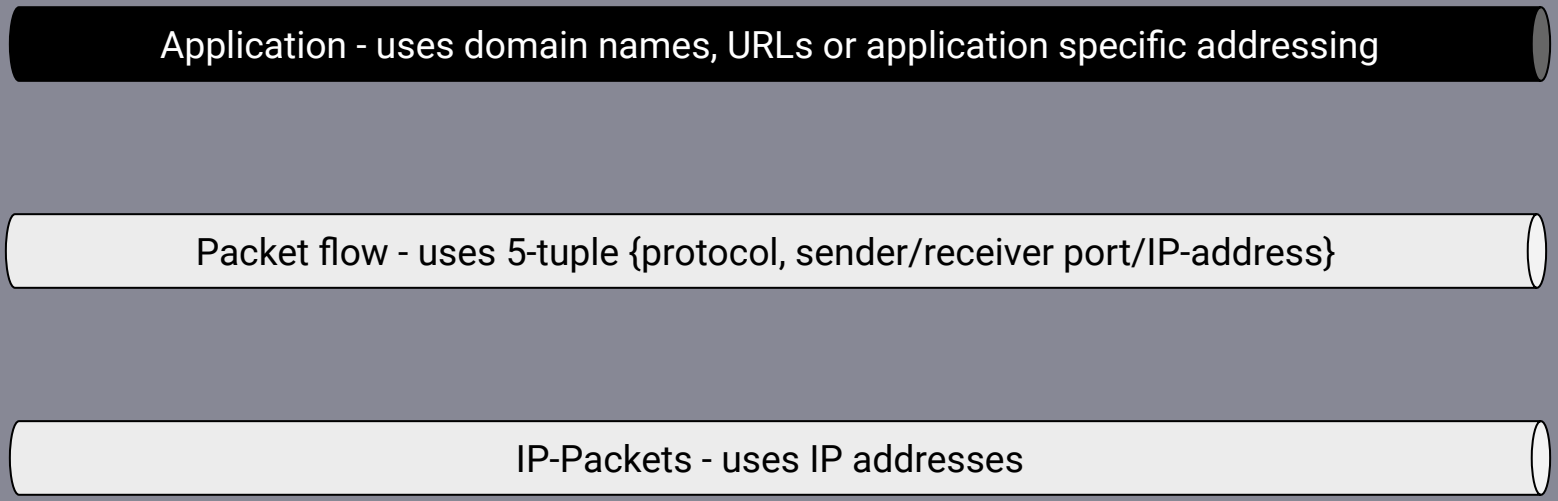

## % of Web Traffic Encrypted

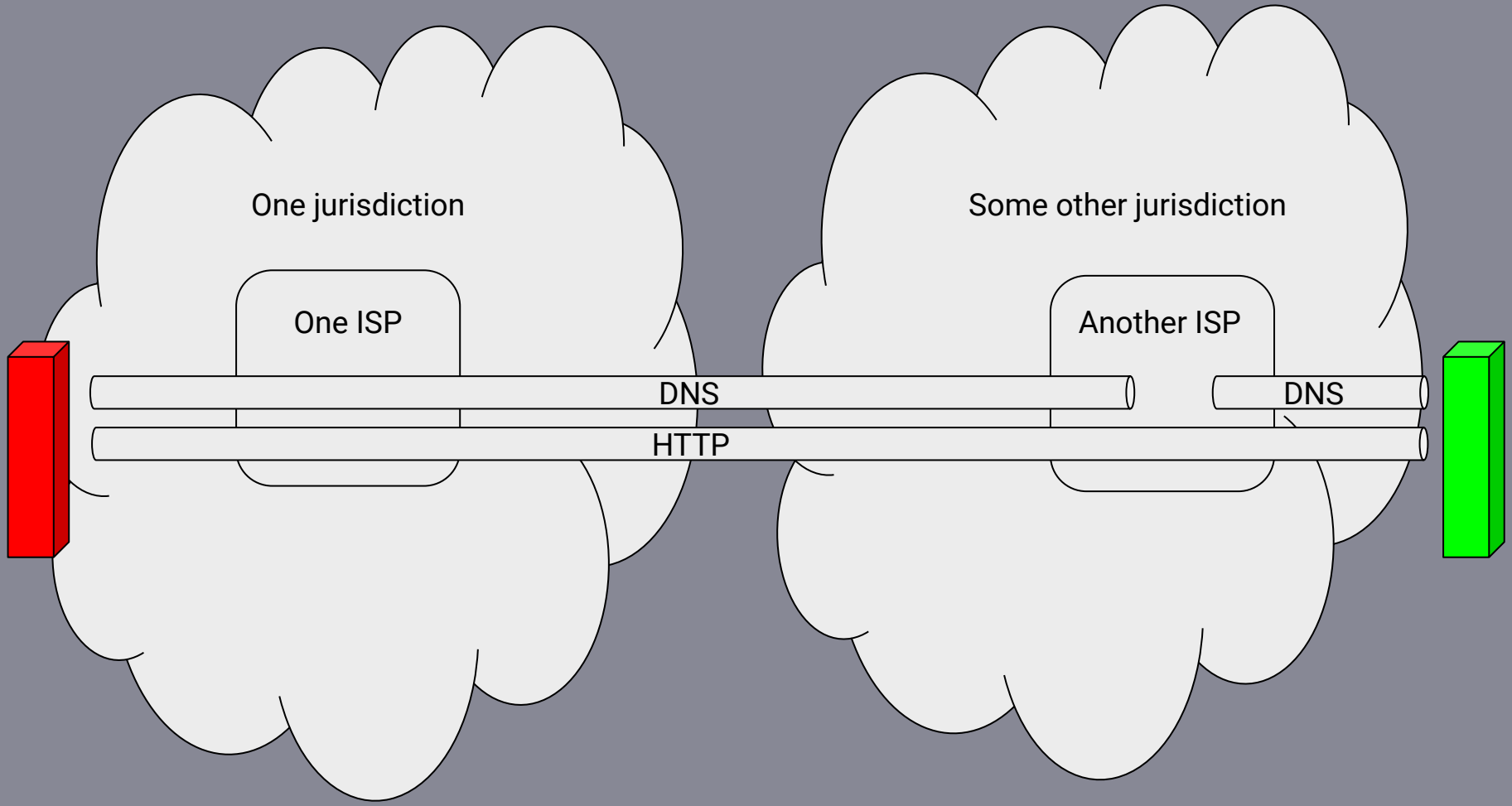


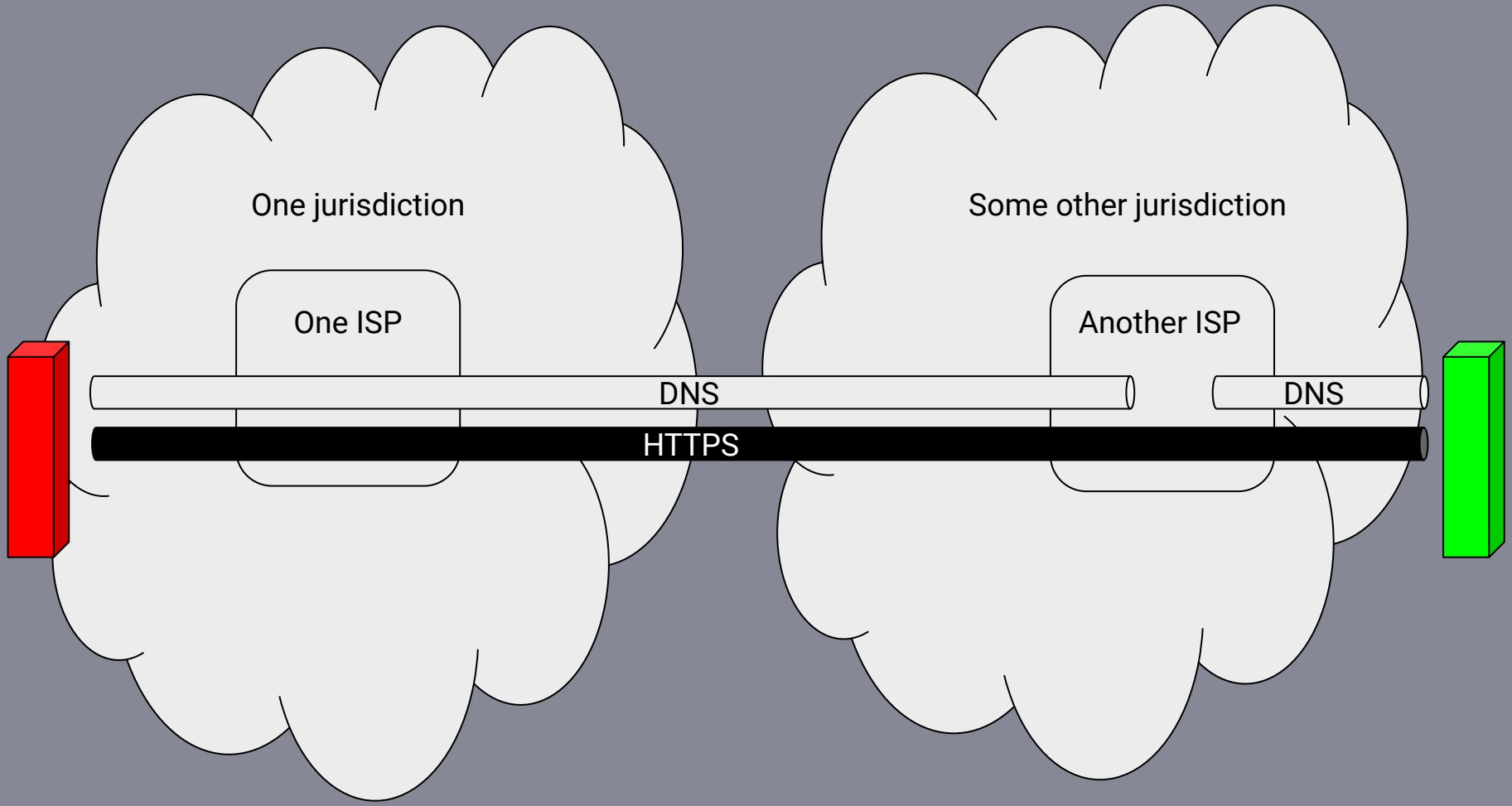

BOND
Internet Trends
2019

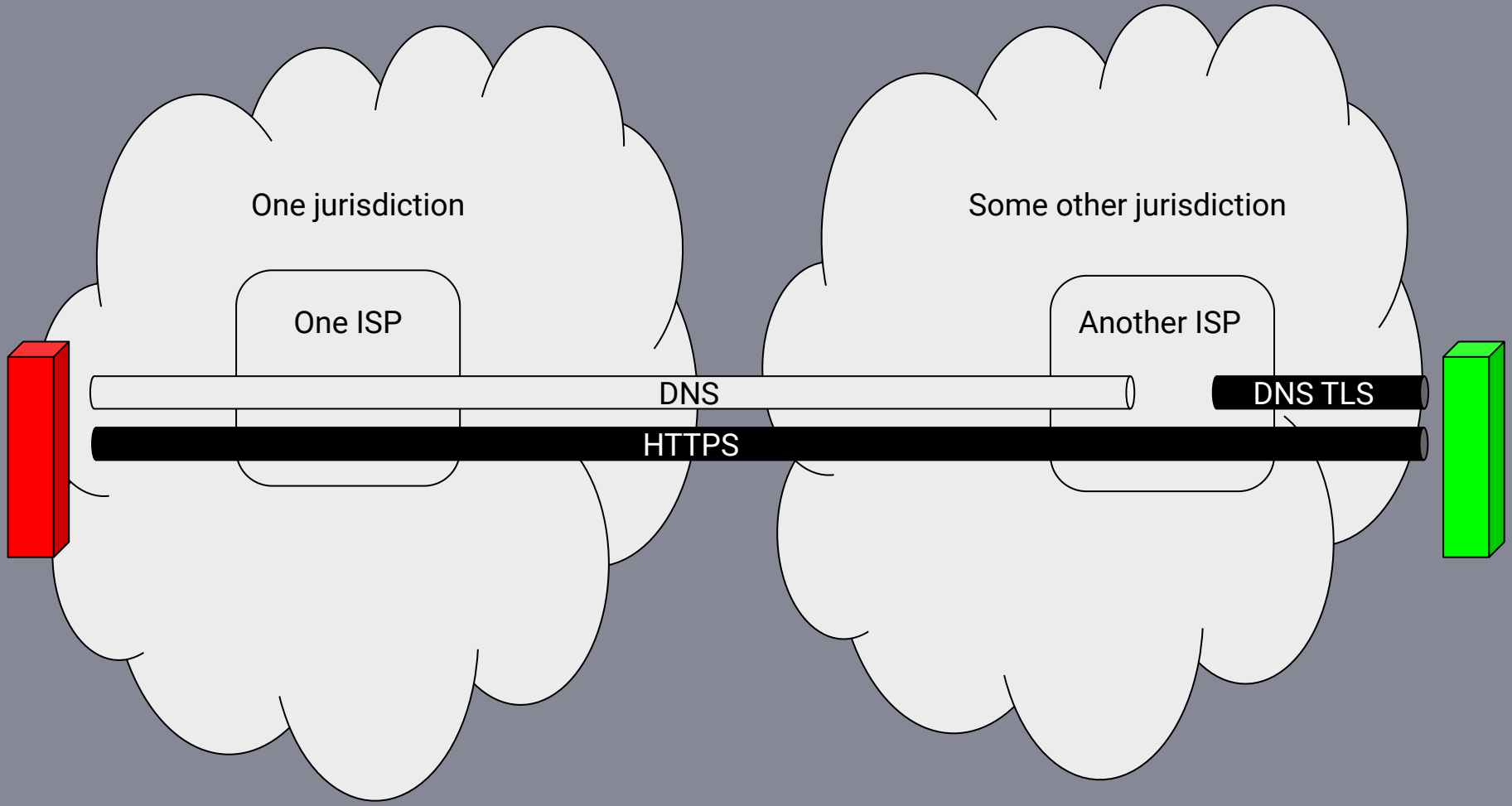
Source: Google, Tencent, Twitter, Facebook, Apple, Telegram releases & Morgan Stanley estimates. Note: *iMessage2 MAUs calculated by install base of Apple iPhones, as estimated by Credit Suisse (2014-2017). WhatsApp employs end-to-end encryption by default. Facebook Messenger has end-to-end encryption capabilities but users have to manually enable them. Instagram does not have end-to-end encryption but Facebook is planning to add that feature & make Facebook Messenger encrypted by default (1/19). All Gmail messages are encrypted at rest and in transit. Fortinet Q3:18 Quarterly Threat Landscape Report (11/18). HTTPS = Hyper Text Transfer Protocol Secure is the secure protocol over which data is sent between the browser and the website the user is connected to.

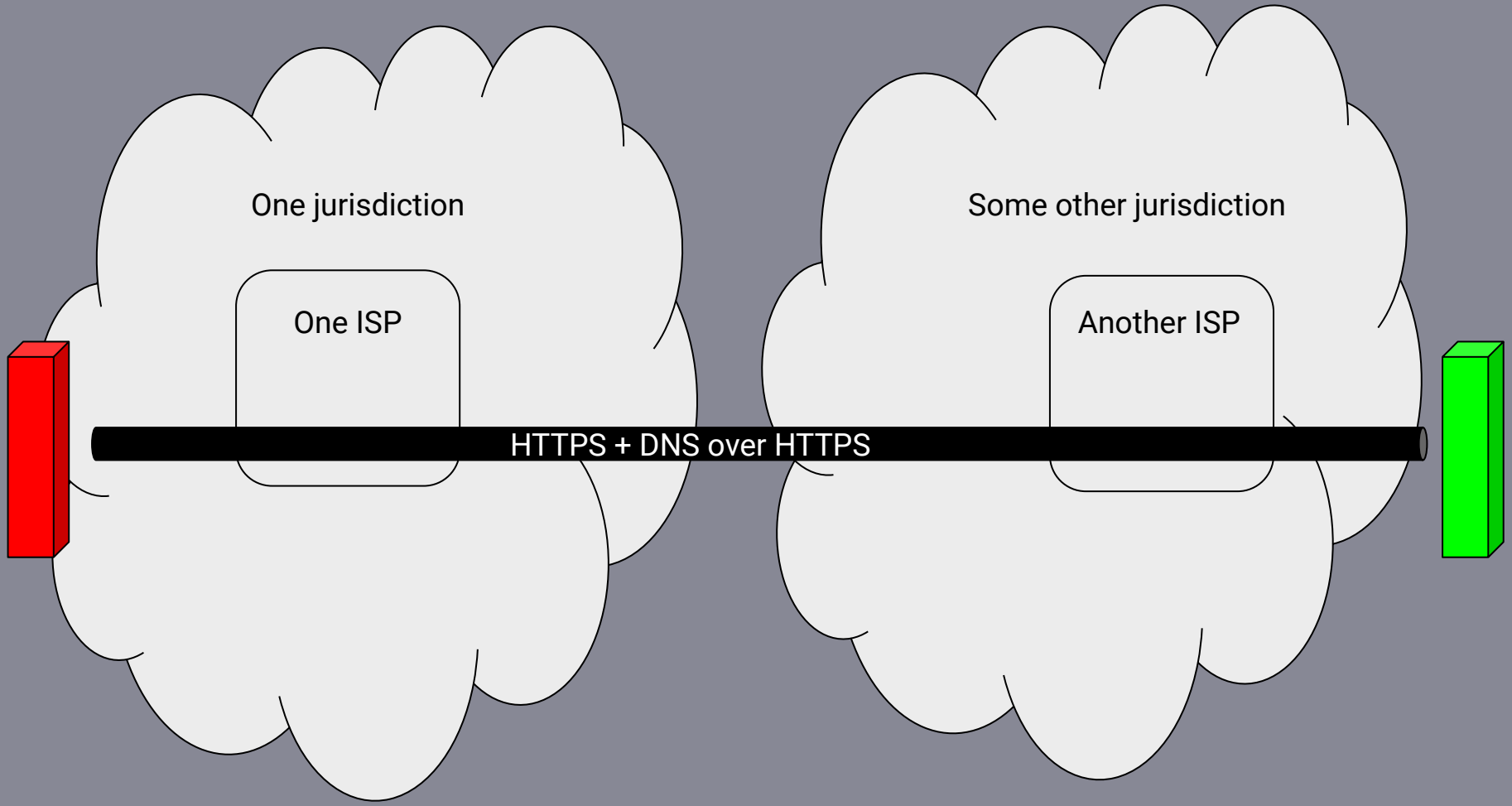

Application - uses domain names, URLs or application specific addressing
Packet flow - uses 5-tuple {protocol, sender/receiver port/IP-address}
IP-Packets - uses IP addresses


Application - uses domain names, URLs or application specific addressing
Packet flow - uses 5-tuple {protocol, sender/receiver port/IP-address}
IP-Packets - uses IP addresses


One jurisdiction
One ISP
Some other jurisdiction
Another ISP
DNS
DNS
HTTP


One jurisdiction
Some other jurisdiction
One ISP
Another ISP
DNS
DNS
HTTPS


One jurisdiction
One ISP
Some other jurisdiction
Another ISP
DNS
DNS TLS
HTTPS


One jurisdiction
One ISP
Some other jurisdiction
Another ISP
HTTPS + DNS over HTTPS

# Summary

- Other examples exists
- Cross border transactions
  - How to handle conflicting jurisdictions?
  - Specifically when local parties are blind?
  - Who is responsible for what?
- Data being secured
  - Digital signatures
- Data being hidden
  - Encryption
- All good things!
  - Hide and secure things from the bad guys
- But also bad!
  - Also bad guys uses the same tools