DNS over HTTPS (DoH)

An Inconvenient Misalignment

Dr. Paul Vixie, CEO
Farsight Security, Inc.

2020-10 (FIRST LAC2020)

Abstract

- Encrypted DNS has been a hot topic for discussion in the world of Internet standards this past year. Its potential impact on enterprise networks has been a prominent part of that discussion. This webinar will explain the two methods for encrypting DNS (DNS over HTTPS and DNS over TLS, known as DoH and DoT), the perceived advantages of each over the other and of encrypting DNS in general, and the potential threats and dangers encrypted DNS presents to enterprise networks. We will then examine the publicly-stated implementation strategies of Google, Apple, Microsoft, and Mozilla as it relates to operating system and browser support for encrypted DNS. The presentation will end with recommendations and advice for how enterprise networks may adjust to the presence of applications and operating systems with support for encrypted DNS inside their networks.

Peace of Westphalia, 1648 (from *Wikipedia*)

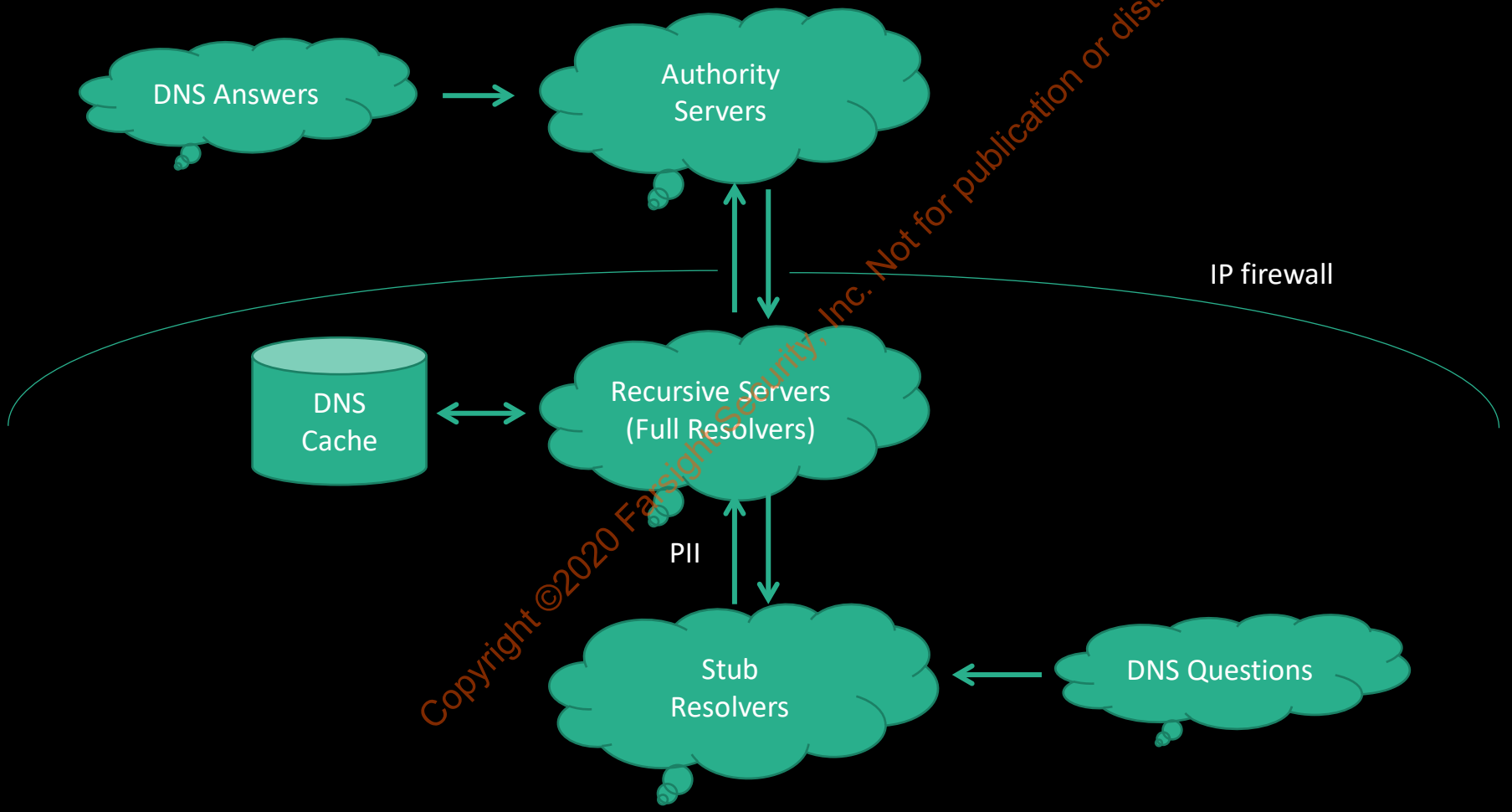
- “The Peace of Westphalia established the precedent of peace established by diplomatic congress. A new system of political order arose in central Europe, based upon peaceful coexistence among **sovereign** states.
- Inter-state aggression was to be held in check by a **balance of power**, and a norm was established against interference in another state's domestic affairs.
- As European influence spread across the globe, these Westphalian principles, especially the concept of sovereign states, became central to international law and to the **prevailing world order**.”

Domains of Operations (Public, Private)

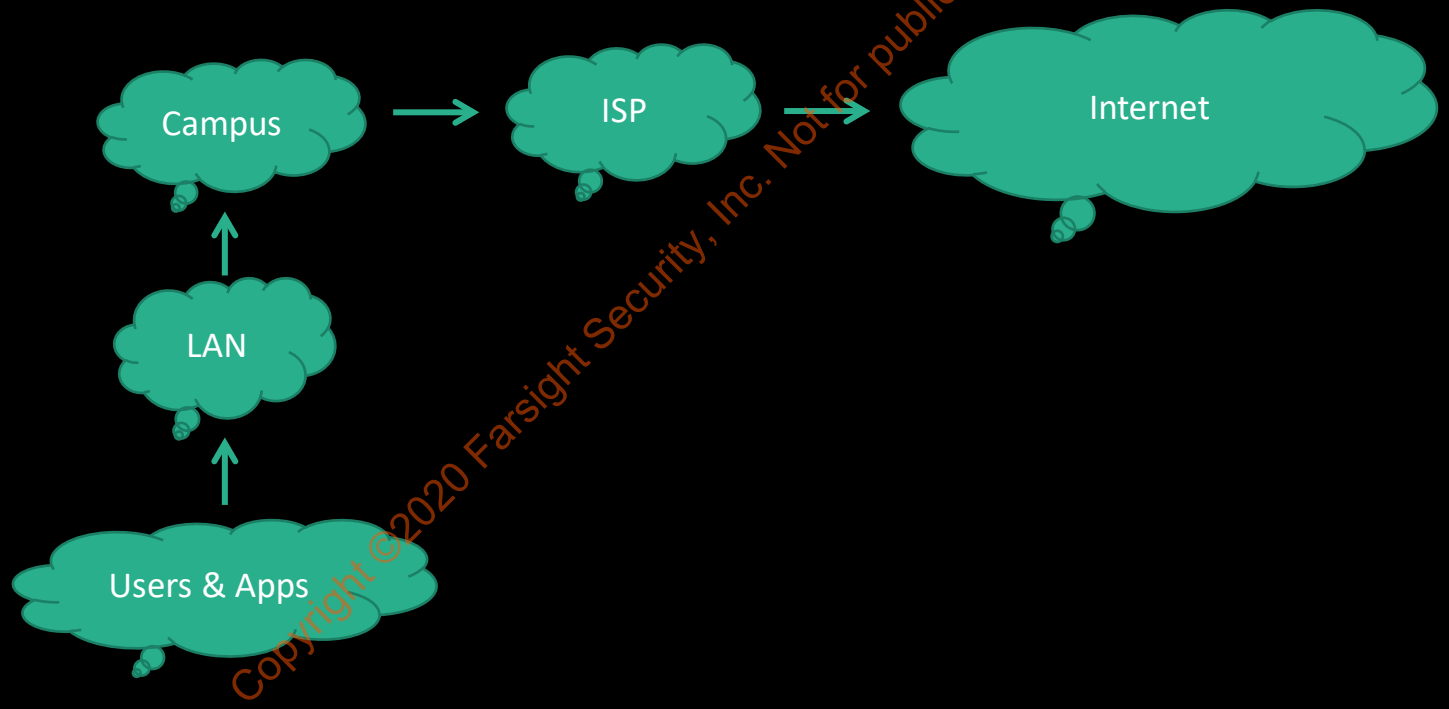
1. *Land*
2. *Sea*
3. Air
4. Space
5. I.T.
6. *Quantum*

Hierarchy of values: supremacy, parity, awareness

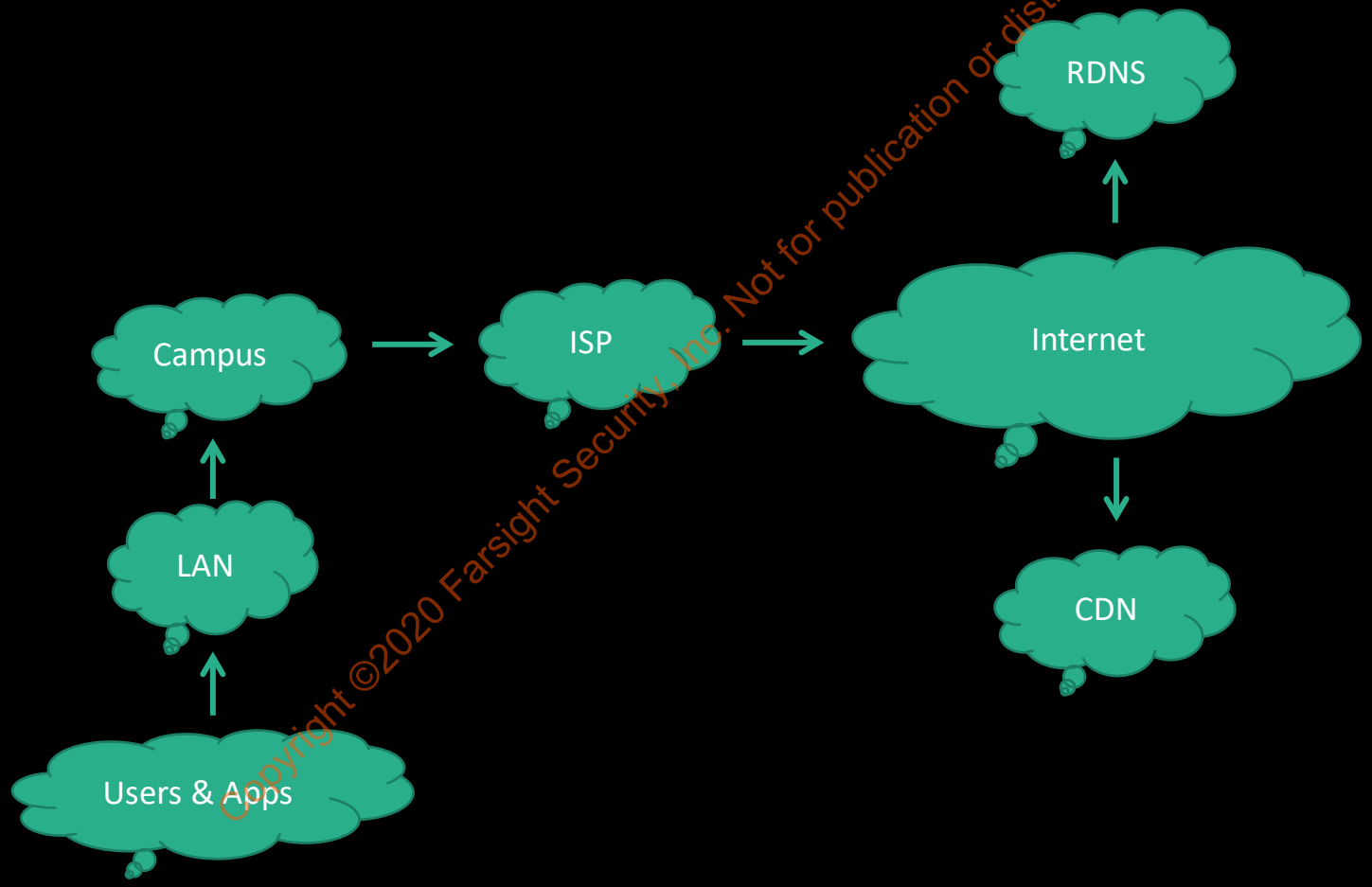
DNS System Architecture (Traditional)



Internet System Topology, ~1999



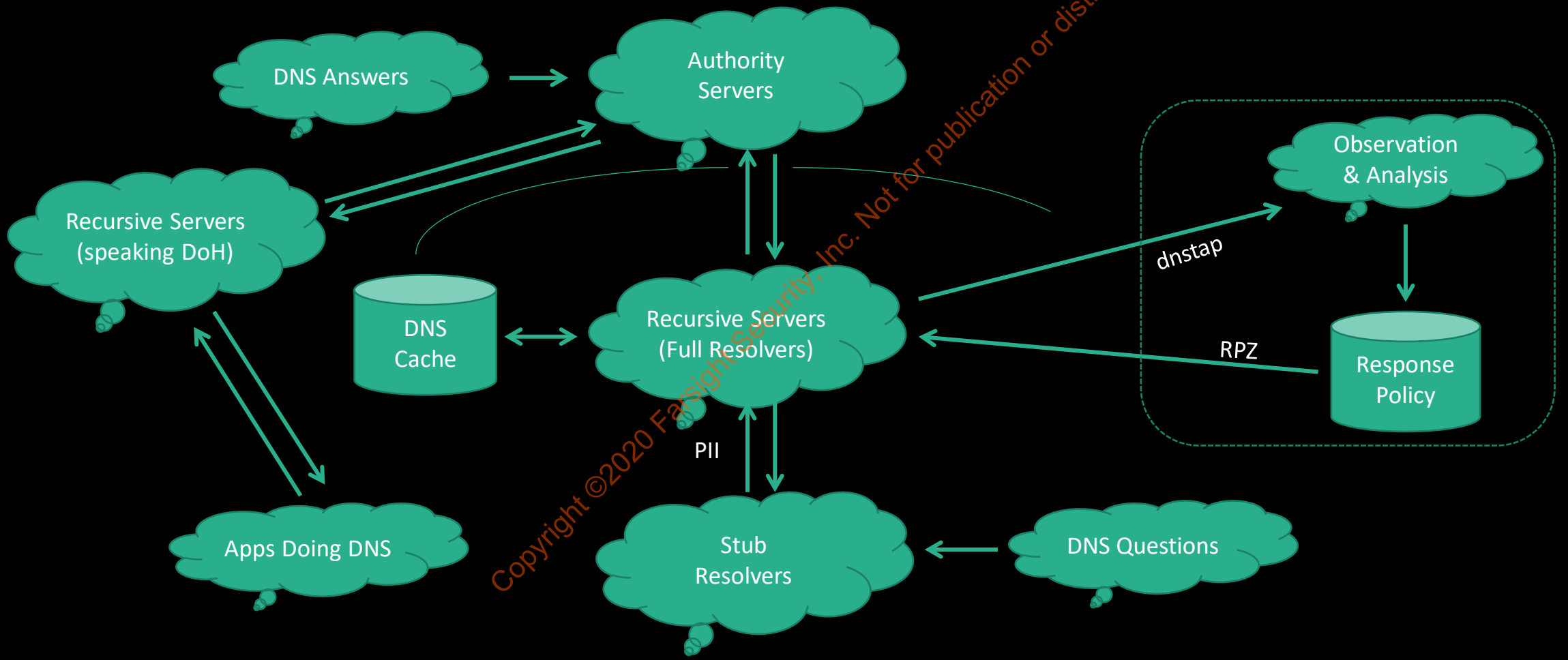
Internet System Topology, ~2020



Action and Reaction: encrypted DNS

- Ability to surveil and perturb DNS transactions is widely abused
  - By ISP's, by OpenDNS, and by governments (see also *Edward Snowden*.)
- So, IETF created DNS Over TLS (DoT), which is being deployed now
  - This is a new transport for any/all DNS transactions, above or below RDNS
  - This is TCP/853, better than TCP/53, and w/ TCPFO often better than UDP/53
  - Network operators can forbid, but cannot surveil or intercept, DoT
- Then, IETF created DNS Over HTTPS (DoH), also being deployed now
  - This is a new transport for stub-to-RDNS, but, meant to be firewall-proof
  - Since it uses TCP/443 a network operator "may think twice before blocking it"
  - DoH disintermediates parental controls at home, and company policy at work

DNS System Architecture, As Amended



Problems with DoH, part 1

- It's a political project, not a technical one
  - Encrypting stub-to-RDNS but not subsequent flows adds no actual privacy
  - An eavesdropper can guess DNS answers based on what happens afterward
  - Guessing the questions once you know the answers is trivial data science
- To stay out of jail in an authoritarian regime, you need a VPN
  - And once you have a VPN, what value would DoH add?
- Also note, many names are resolvable locally but not remotely
  - Most companies have their own internal-only TLD's like .CORP or .FORD
- The web is not the whole Internet; browsers can launch helper apps
  - Helper apps will use the normal stub resolver, getting different DNS answers

Problems with DoH, part 2

- DoH cannot differentiate between these network operators:
  - Parents, who use RDNS filtering as part of their family Internet controls
  - Sysadmins, who use RDNS filtering to block spam and malware
  - Security teams, who use RDNS monitoring to detect new malware infections
  - Authoritarian government, who uses RDNS for “thought control”
  - ISPs who wish to surveil their customers to aid in targeted advertising
- DoH’s costs would be tolerable if there was an accompanying benefit
  - However, DoH is a political act, adding no actual effective privacy
- Some people think CCP has practical resource limits for GFW
  - Some people don’t

Selected quotation – July 2014 – https://medium.com/message/81e5f33a24e1

- “The NSA is doing so well because software is bullshit.”
- “Next time you think your grandma is uncool, give her credit for her time helping dangerous Russian criminals extort money from offshore casinos with DDoS attacks.”
- “C is good for two things: being beautiful and creating catastrophic zero-days in memory management.”
- “When we tell you to apply updates we are not telling you to mend your ship. We are telling you to keep bailing before the water gets to your neck.”

Managed Private Networks (MPN)

- Endpoints are fundamentally unsecurable
  - IoT; abandonware; supply chain poisoning; 0-days; intruders
- Allowing some kinds of traffic, disallowing others
  - Firewalls: IP, web, DNS
- Economics of scale force an anomaly detection posture
  - Bad actors must therefore try to “blend in”
- Nation-state and ISP networks are not private
  - But they want some of the powers of MPN’s (observation; filtering)
- DoH is not deliberately targeted against any of this
  - Most IP growth is mobile; most revenue is from tracking and advertising

Internet vs. Web

- It's going to become broadly necessary to control TCP/443 (HTTPS):
  - TLS 1.3 + ESNI means no more HTTPS MITM – requires proxy for all outbound
  - Every IP offering DoH will be widely blackholed, because of malware DoH use
- Possession is said to be 90% of the law
  - On the Internet (network of networks) that meant: "my network; my rules"
  - On the Web (network of eyeballs) that means: "my network; DoH's rules"
- As a form of Internet governance, DoH shows the worst of all worlds
  - Which is: *code is law* (or: *the rule of the strongest*)
- Whoever can ship the most code, makes the rules
  - Eventually this will mean LTE/5G for free in all IoT devices

Avoiding Collateral Damage

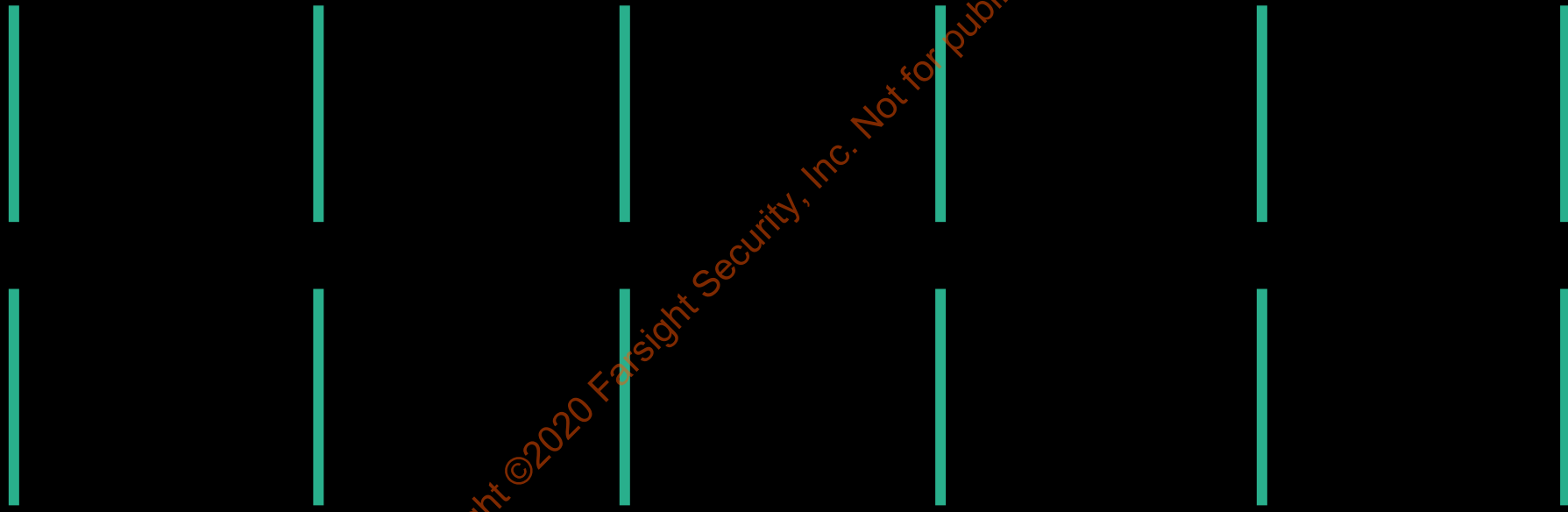
- Google's DNS clients (Chrome, Android) will attempt to upgrade the protocol from cleartext-UDP to DoT or DoH, *using the same servers*.
  - Microsoft (Windows) and Apple (OSX, IOS), roughly likewise.
- Google's DoH servers are promised to run on well known addresses (8.8.8.8) so that they can be blocked using common firewall methods.
  - IBM/Quad9 (9.9.9.9) and Cisco OpenDNS/Umbrella, roughly likewise.
- Mozilla is turning on DoH by default (in the USA), bypassing locally configured servers in favour of their *Trusted Recursive Resolvers*.
- APNIC/Cloudflare (1.1.1.1), a Mozilla TRR, retains address agility.

Return of the Corporate State

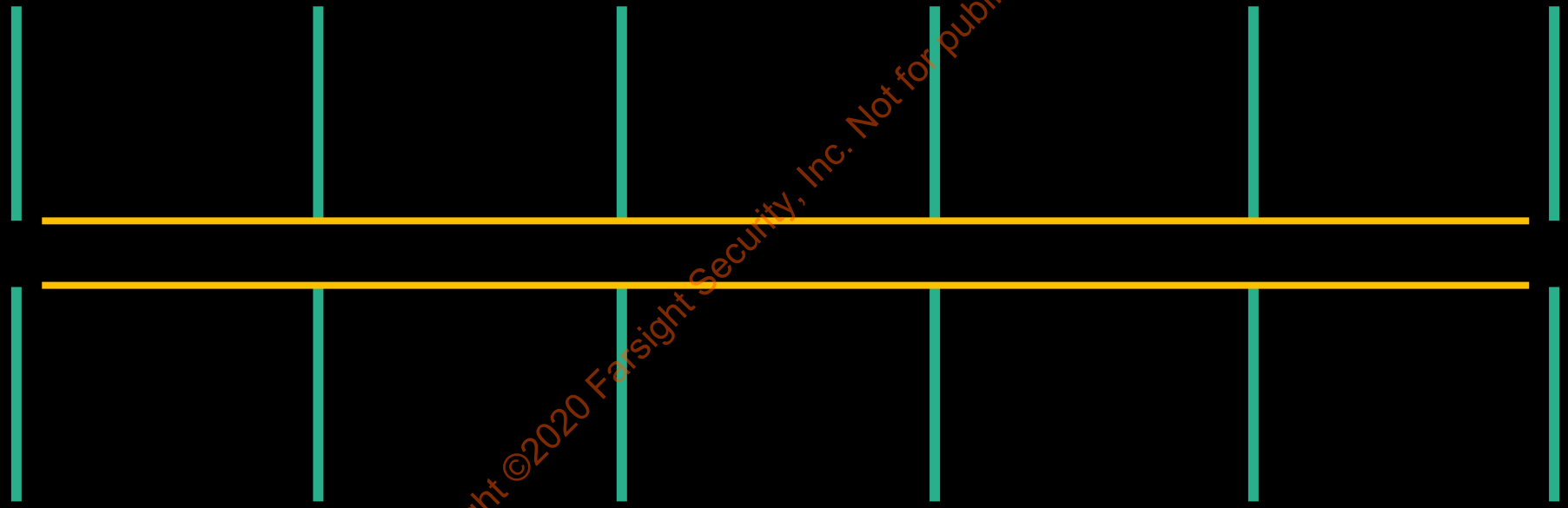
> 4. The user will be informed that we have enabled use of a TRR and have the opportunity to turn it off at that time, but will not be required to opt-in to get DoH with a TRR.

- Mozilla Corporation (of Firefox) is deploying DoH on an opt-out basis
  - Their first Trusted Recursive Resolver (TRR) is Cloudflare™
  - Both the opt-out policy, and the choice of a US company, are controversial
- The UK objected, and demanded a “summit meeting” in London
  - Mozilla agreed to leave the UK out of their DoH roll-out “for now”
- This leaves open the question: how many other countries will object?
  - And: how many other browser/app vendors will implement similar policies?

Cooperation Is Alignment



Cooperation ~~Is~~ Was Alignment



Expensive (Imposed) Choices

- Faced with Internet Standards for RDNS bypass, a NetOp can either:
  - Allow malware, intruders, supply chain poison, BYOD to bypass DNS controls
  - Stop thinking any network can ever be secure, move beyond “perimeters”
  - Create smaller networks having explicit whitelists for must-be-reached
  - Allow Chromecast, Chrome, IoT unlimited access to their motherships
- …Or:
  - Follow the tradition: *possession is 9/10th of the law*
  - Establish an AUP and enforce it for all outbound communications
  - Get creative about what (few) requires a proxy and what (many) does not
  - Firewall every app and every IoT, make manufacturers share the burden

Now Under Consideration: Resolverless DNS

- Web content providers and their CDN's want better performance
  - Which means, faster time-to-next-eyeball
- Most content includes many object references (images, scripts)
  - The time taken for a browser to look up these DNS names is measurable
  - (and may involve "ad blocking")
- Therefore an IRTF WG is studying "Resolverless DNS"
  - Here, DNS data will be "pushed" as part of a normal web content fetch
  - DNSSEC signatures won't be included; TLS is considered "secure enough"
- This terrifically broadens the attack surface of web site defacement
  - Bit coin mining JS can now be downloaded without triggering EP protections

End Notes

- Every innovator solves the problems their/they customers have
  - Not every innovator knows or cares about systemic costs
- DNS is the first and only system of its kind that has scaled by 10^9
  - Distributed, coherent, reliable, autonomous, and hierarchical – unique!
- As in politics, economics, and climate change, this future is brutal
  - Our consent is no longer sought, and can be withheld only at notable cost
- Westphalian era is not strictly, completely, over
  - However, Space and I.T. operational domains ignore “borders”
  - “You can keep what you can defend” means something different vs. 1648
  - Many corporations today have I.T. supremacy over most countries