CENTR Tech Trends Watch

April 2020

The Tech Trends Watch is a new, regular part of CENTR's reporting on current affairs which takes into account ongoing trends in technology development from a range of standards development organisations and other technology forums. Its purpose is to trace out those trends that may have an impact on the addressing and numbering communities, and assess how those developments tie in with external stakeholders such as policy-makers and other industry sectors.

The new European Commission is taking a more aggressive stance on industrial policy, pushed by concerns in the larger member states like France and Germany that the European Union is increasingly depending on foreign technology providers only.

For instance, there are no larger European web service providers, with US-based companies dominating in both cloud and web. Similarly, even internet network equipment is still mostly provided by one US entity, Cisco, and the rest by Chinese competitors.

As the US becomes increasingly oriented towards domestic problems and the East Asia region, some EU member states are trying to grapple with the risk of an increasingly volatile American administration ordering a company like Amazon to selectively close down servers.

The issues could also be more subtle though.

The Wilfried Martens Centre recently highlighted the lack of strong European patents in the mobile handset chip[1]. As more and more European companies become downstream implementers of advanced upstream chip technologies, this could create serious dependencies on the licensing models advanced by the US administration - even if those licensing models are not inherently in the implementers' interests[2].

It will remain difficult for European governments and the European Commission to organize themselves around consistent, self-interested policies. But the collateral damage caused by poor attempts to shape such policies could have a serious impact on the future opportunities for internet infrastructure entities such as the DNS sector.

Firstly, the two European companies that are making network equipment are actually mobile network companies rather than internet network companies. Ericsson and Nokia come, at least in part, from a different network topology than the internet community.

---

[1] Brussels Bytes, 5G and the future of the European telecom sector with Roslyn Layton, https://soundcloud.com/martenscentre/episode-3-5g-and-the-future-of-the-european-telecom-sector-with-roslyn-layton

[2] See e.g. https://fair-standards.org/key-principles/

The wireless environment creates real physical and technical constraints on how to choose, for instance, suitable congestion control mechanisms[3]. The technical challenges that arise from these constraints are quickly catching up with an increasingly wireless connectivity landscape. But mobile networks are also more intrinsically connected to nation-states, through the government-auctioned spectrum licenses required to legally operate services, so the EU has difficulties leveraging its size to support local network equipment vendors. Instead, much of the European discussion on mobile networks for the future has been steered by US national security concerns pertaining to Chinese vendors[4]. However, bringing national security into European discussions distances both local manufacturers, strategies and technology development even further from the European field, cornering it instead in each of the 27 states.

Much like European governments, European mobile network vendors are trapped between geopolitical behemoths. It follows naturally that it is companies from other jurisdictions that are taking the lead on opening bolder discussions on what a next generation internet protocol could look like[5].

Secondly, even where European actors are providing web services, they are not well-integrated into the internet governance community. Of course, telecommunications operators are putting even more effort into internet standards organisations such as the IETF than they are putting into the mobile network standards body, 3GPP.

Nevertheless, other players, such as OVH, 1&1 or R22 are strangely absent from the discussions on future generation data center routing protocols in both the IEEE and the IETF. They are also strangely absent from the discussions on abuse management or networking policies in RIPE. In fact, if anything, they are receiving heavy criticism by these communities for not being collaborative enough[6].

Thirdly, there are more fundamental problems, such as French companies having mostly French customers, and German companies having mostly German customers. Locally-strong entities like the Czech Seznam, a search engine which is not only driving interesting technical developments in their local market but that has also remained competitive and interesting for end-consumers in that market, are virtually unknown outside the Czech Republic.

Part of this is a language issue: the European Union is a broad umbrella after all. But part of it is also active ignorance in Western European states. There is a preference for optimizing policy against US or China-based entities, rather than exploring feasible policy options for the successful, innovative and popular companies that could be driving technology developments for the web and internet environments in Europe. The European Union, and each of its individual member states, in this sense end up being oddly self-deprecating.

The DNS community mostly depends on internet connectivity broadly continuing to operate in the same way that it has done since the 1980s. It also depends on internet governance and technical standardization to remain broadly credible, engaging and attractive to the actors that are impacted by its decisions. But to be, successful conservatives, European DNS entities cannot remain happy to simply defend a status quo, they

---

[3] M. Polese et al, A Survey on Recent Advances in Transport Layer Protocols, pre-print July 2019, arXiv:1810.03884v2 [cs.NI] https://arxiv.org/abs/1810.03884

[4] Stiftung Neue Verantwordung, 5G vs National security, 12 February 2019. https://www.stiftung-nv.de/de/publikation/5g-vs-national-security

[5] See, e.g. New IP.

[6] https://www.ripe.net/ripe/mail/archives/anti-abuse-wg/2020-February/005603.html

must also be cognisant of the real challenges created by the particular network technology and features that the internet provides, and of the "digital sovereignty" struggles of their local governments.

1. DNSSEC key signing ceremony highlights structural problems in trust model

The COVID-19 lockdowns on both sides of the Atlantic created disruptions in the DNS security (DNSSEC) root key signing ceremony in the last quarter.

For the first time ever, the travel restrictions caused IANA to have to use emergency protocols for the ceremony, involving only local US-based staff in the end[7]. It highlights a weak point in the trust model of DNSSEC: its dependency on a single jurisdiction and the ability of trusted stewards to travel in and out of that jurisdiction.

In the past years, there have been repeated discussions in IT and security circles about the increasingly unreliable visa procedures of the US. Adi Shamir, an Israel-based security researcher and the S in RSA, was denied an entry visa in 2019 when he was intending to visit his eponymous conference RSA Security Conference[8]. The IETF has also attempted to reduce its presence in the US to ensure that as many people as possible can reliably attend its meetings[9].

Intensified discussions around digital sovereignty in the European Union[10], around next generation networks at the International Telecommunications Union (ITU) led by China[11], and a recent (or renewed) criticism from Russia against the multistakeholder model[12], highlight a medium- to long-term need to take a long hard stare at some of the underlying foundations of DNS security.

As work intensifies to shift more and more features from the traditional TCP/IP stack into the application layers - the web or HTTP(S) stack - this is going to become an ever more important problem to address for those who want the internet to continue working, more or less, in the way that it is doing now and with a similar set of stakeholders.

---

[7] See e.g. https://mm.icann.org/pipermail/root-dnssec-announce/2020/000126.html

[8] Adi Shamir visa snub: US govt slammed after the S in RSA blocked from his own RSA conf, https://www.theregister.co.uk/2019/03/05/rsa_cofounder_us_visa_row/

[9] IETF 102, change of venue https://mailarchive.ietf.org/arch/msg/ietf-announce/WS9N8eeO35tbe876-_6GmrgnSvY/

[10] See e.g. https://www.diplomatie.gouv.fr/en/french-foreign-policy/europe/president-macron-s-initiative-for-europe-a-sovereign-united-democratic-europe/

[11] CENTR (Monika Ermert, eLance), Report on IETF107 https://centr.org/library/library/external-event/centr-report-on-ietf107.html

[12] Commentary of the Russian Federation on the initial "pre-draft" of the final report of the United Nations open-ended working group on developments in the field of information and telecommunications in the context of international security https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf

2. New IP - actually sort of old

As recently reported by CENTR in its IETF107 report[13], recent discussions at the International Telecommunications Union (ITU) have raised many eyebrows in the internet community. The Chinese delegation (since the ITU is a multilateral organisation where entities need to incorporate under the umbrella of a government) has raised the topic of next-next generation networks - requirements that they suggest will be imperative for advancing connectivity beyond 2030[14].

Both the IETF[15] and RIPE NCC[16] have reacted strongly against these proposals, calling them an affront to the decentralized internet model and a dramatic, and harmful, change to the currently open architecture of the internet. Nevertheless, the ITU discussions are not as outlandish as one might initially come to believe.

For one, centralization is not a completely outlandish concept in the internet community. Trust models, such as those underlying the certificate systems for cryptography - including the ones ensuring the authenticity of DNS records through DNSSEC - are intrinsically centralized. They are made slightly less dependent on a single jurisdiction and entity through procedure only.

Even beyond that though, work on Time-Sensitive Networking (TSN) in both the IEEE 802.1 and on deterministic networking in the IETF DETNET working groups is already moving in approximately the direction of rethinking traditional and ad hoc routing. In these bodies, there has been some careful fencing of such technical developments to "limited domains" (a concept introduced by Sheng Jiang and Brian Carpenter in an IETF INTAREA draft in November 2018[17]), meaning, not the general, public internet.

Centralization, in some sense, is however ongoing in other spaces too. The newest generation of WLAN, Wifi 6, already incorporates stronger, centralized features to increase through-put and improve congestion control[18]. Better bridging between wired and wireless networks may also require stronger coordination mechanisms from some centralized entity.

The use-cases considered by the 3GPP-SA1 group are also of such a nature that they may require more fundamental rethinking of how connectivity works. Haptic networking is one example[19], but the common API framework is another[20].

All of these examples conspire to the observation that the resistance against New IP might be more motivated by objections against the entity doing the proposing (Chinese government) and the forum in which the proposal is put forth (ITU), than a genuine concern that the technical problems raised by this proposal are as such invalid or not worthy of discussion.

---

[13] See footnote 11.

[14] ITU, "Network 2030 - A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond" (May 2019) https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf

[15] LS on New IP, Shaping Future Network, https://datatracker.ietf.org/liaison/1677/

[16] Do We Need a New IP? https://labs.ripe.net/Members/marco_hogewoning/do-we-need-a-new-ip

[17] IETF draft-carpenter-limited-domains-00 https://datatracker.ietf.org/doc/draft-carpenter-limited-domains/

[18] https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6

[19] "Adaptive 5G Low-Latency Communication for Tactile Internet Services", VOL. 107, Proceedings of the IEEE.

[20] 3GPP TS 23.222, Common API Framework for 3GPP Northbound APIs. ftp://3gpp.org/Specs/2019-12/Rel-16/23_series/23222-g60.zip

With the governance complications in mind, we must understand the limitations of some of the internet governance bodies for Chinese players especially. A quick overview of the public reports on attendance at the IEEE 802 groups shows that Huawei participation has quickly declined in favour of Futurewei participation[21] since last year (2019), when the US administration decided to step up the trade conflicts with China. These shifts are also visible at the IETF and the 3GPP: geopolitics risks making it costly and intractable for Chinese companies to work with US-based standards bodies.

Unfortunately, the problems are not restricted to outright trade hostilities. More and more features are being incorporated into network equipment and wireless personal devices, a development which is not likely to abate any time soon. This brings in jurisdictional aspects of intellectual property rights strategies too.

It simply matters whether something is incorporated in California, in New Jersey, in France or given legitimacy by international treaties. While in the DNS and numbering space it may not be immediately obvious, it is perfectly evident to hardware manufacturers that rely on patent licensing revenue models that jurisdiction makes a difference even in the absence of full-on national security and trade conflicts.

Saying that " this is the way it has been done until now and it always worked" is not good enough: it avoids the complications that arise from a geopolitical tech landscape in flux. Ultimately these are not just technical problems, but economic and political problems too: who gets independence, power and revenue. As more technical features creep into the hardware layers, we are just likely to see more of the hardware economics play a role in where new ideas are discussed and who ends up raising them.

3. Further delays in the next release of the 5G specification

Release 17 of the 5G specification is set to be delayed by several more months due to all 3GPP meetings being cancelled in the wake of COVID-19[22].

The 5G vision is locked on Industry 4.0 applications. Together with so-called "verticals", companies which operate in manufacturing, factory settings and other environments where feature requirements are highly specialised[23], network equipment vendors are chasing down some long-known difficulties with latency guarantees and security in constrained environments. While discussions around better quality of service, deterministic routing or bridging between wired and wireless networks are hardly new issues, the new potential customer bases for network equipment vendors is. The telecommunications operators, while still well-connected with regulators and governments, have not always been the most technically forward-thinking customers.

While many internet specifications, such as open authentication tokens or TCP layer security (TLS) are working their way into the mobile networks, the Release 16 common API framework (a set of procedures and APIs that enable non-network operators to provide services to other non-operators, such as printing or similar over a 5G network) (CAPIF) from December 2019 does not preclude alternatives to DNS for

[21] Last slides in 802.11 WG Opening Reports by chair (see last 12 meetings): https://mentor.ieee.org/802.11/documents?is_dcn=opening&is_group=0000

[22] https://list.etsi.org/scripts/wa.exe?A2=ind2003A&L=3GPP_TSG_SA&O=D&P=65

[23] IEEE 802 Nendica Report: The Lossless Network for Data Centers (2018-08-17), IEEE 802 Nendica Report: Flexible Factory IoT — Use Cases and Communication Requirements for Wired and Wireless Bridged Networks (2020-04-17), Siemens Financial Services: Practical Pathways to Industry 4.0 The obstacles to digital transformation and how manufacturers can overcome them (White Paper 2018).

addressing[24]. Even the IETF DETNET group seems to be mentioning the DNS in their reference architecture mostly to placate the more conservative members of the internet governance community[25].

ICANNorg remains confident that the inertia of the mobile network sector will impede any immediate commercial overhaul of the addressing market[26]. However, while optimistic conservatism has its merits, and it is true that many legacy network applications will continue to rely on the DNS for the foreseeable future, it seems warranted to keep an eye on mobile network developments.

The close cooperation between equipment manufacturers and their new Industry 4.0 sectorial partner in mobile standards organisations could indicate a future shift to different resilience, robustness and security models for addressing, at least as it relates to industrial environments and users of connectivity that operate within such environments.

From the perspective of the emerging European Union industrial policy, the cooperation between the largest European equipment vendors and continental European industry 4.0 players could also forecast strong political buy-in into these new technologies.

4. One more step towards onion-services

In February, the coordination platform for certificate authorities, CA Browser Forum, approved domain-validated certificates[27] for .onion-addresses[28] in what seems to be one step among many in contemporary technology developments into internet-ancillary domains.

Onion-addressing does not rely on the DNS, in the sense that it does not rely on ICANN or IANA to be looked up[3]. While they are not the first domain-names to fall outside of the ordinary internet addressing schemes[29], they are the first such special-use domains intended for general-purpose services and the first to demand equality with traditional DNS in terms of cryptographic certificates.

One of the expectations expressed ahead of the CA/B Forum vote was that this step towards even footing with traditional DNS services will make onion-addressing more compatible with web browsers' ordinary security features and thereby more tractable for a larger range of users[30]. While Tor is still some way off from attracting a majority of connectivity customers to its secure network, this step has to be recognised in the larger context of mobile networks, mobile operating systems and secure networking developments.

---

[24] 3GPP TS 23.222, Common API Framework for 3GPP Northbound APIs. ftp://3gpp.org/Specs/2019-12/Rel-16/23_series/23222-g60.zip

[25] RFC8655 Deterministic Networking Architecture. https://datatracker.ietf.org/doc/rfc8655/

[26] ICANN OCTO Report 004, 5G Technology, January 2020. https://www.icann.org/en/system/files/files/octo-004-en.pdf

[27] CA/Browser Forum Ballot SC27v3: Version 3 Onion Certificates https://cabforum.org/2020/02/20/ballot-sc27v3-version-3-onion-certificates/#Ballot-SC27v3-Version-3-Onion-Certificates

[28] RFC7686: The ".onion" Special-Use Domain Name https://datatracker.ietf.org/doc/rfc7686/

[29] IANA, Special-Use Domain Names. http://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml

[30] Seth David Schoen, EFF. [cabfpub] DV issuance for next-generation onion services. https://cabforum.org/pipermail/public/2017-November/012451.html