Will the Internet Still Be Resilient During the Next Black Swan Event?

Andrew Campling
Director, 419 Consulting Ltd.
Andrew.Campling@419.Consulting

Dominique Lazanski
Director, Last Press Label
dml@LastPressLabel.com

Submission to IAB Workshop on COVID-19 Network Impacts

Introduction

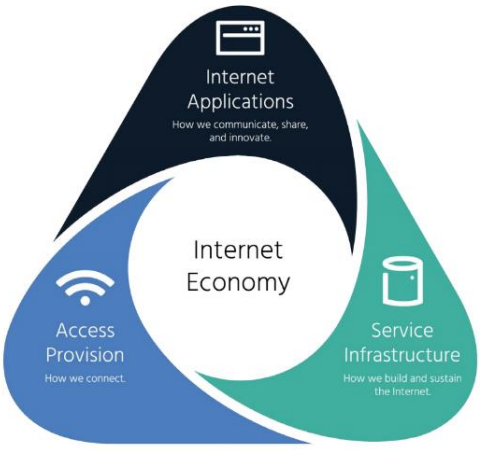
The Internet has fared well under in the pressure and demands of working from home due to lockdowns and social distancing during the Covid-19 pandemic of 2020. However, current developments, which are tending towards consolidation, present potential issues and challenges if and when the next major disruption impacts the globe. Consolidation of the core Internet building blocks is expanding, with this trend continuing during the Covid-19 crisis. Because of this, it would have been worse if Covid-19 and its subsequent implications, like remote working during lockdown, happened in 5 years' time.

In this brief paper we will then see how the Internet – fixed and mobile – has been doing during Covid-19. We will also look at consolidation and consolidation trends. which are emerging to date, taking into consideration whether these trends are in the best interests of end users. And finally, we will make some conclusions about future Internet architecture and resilience and argue that current trends continue as they are the Internet would not be as stable or resilient.

What is Consolidation?

Consolidation is the process by which a number of things are combined to make a larger entity. In the case of the Internet, different layers of the Internet are experiencing consolidation from the application layer to the technical layer. Large companies, like Facebook and Google, account for a significant amount of content and applications online today. Additionally, these companies are building out infrastructure and developing technical protocols which, ultimately drives the traffic – and data – into these few companies. For example, Google has 81% of all searches online and 94% of all mobile searches as of 2020.[1]

[1] According to the *Investigation of Competition in Digital Markets,* Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, United States House of Representatives, 6 October 2020. https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf



In its report "Consolidation in the Internet Economy"[2], the Internet Society examined how consolidation will impact on Internet Economy, which it defined as covering Internet applications, service infrastructure and access provision (see the diagram opposite).

The Internet Society's report considered, amongst other things, the impact of consolidation on the Internet's technical evolution and use. Whilst the report concluded that more research was required, it did note that there could be adverse effects on user choice, innovation and trust.

There have been papers and discussion at the IETF and during IAB events relating to consolidation. At the IAB's Design Expectations vs. Deployment Reality in Protocol Development Workshop 2019, Andrew Sullivan discussed the concentration in web services, network services and standard services. Both Christian Huitema and Julien Maisonneuve noted concentration as an effect of economies of scale and network effects in business models.[3] Jari Arkko discussed the impacts of consolidation on the Internet infrastructure in a document for the IETF[4], with the document identifying issues including loss of resilience and increased risk of surveillance. It goes on to note that "it seems prudent to recommend that whenever it comes to Internet infrastructure services, centralised designs should be avoided where possible".[5] This seems like good advice. However, contrary to this recommendation, current trends are towards consolidation.

How did the Internet Cope Under Covid-19 in Europe? (In Spite of Consolidation)

Back in March 2020, it was reported that the broadband performance of major UK providers from 24 January to 23 March remained the same and in fact did not deviate from the usual performance patterns seen before 2020.[6] British Telecom (BT) reported a decrease in mobile data traffic of 5% in March 2020 as most people connected to their WIFI at home. And because of working or staying at home, BT saw a 35-60% increase of daytime traffic of up to 7.5 Tb/s.[7] In April, Vodafone reported that on their fixed broadband lines, usage increased over 50% in Italy and Spain and upstream data flows, due to video conferencing increased 100% while downstream increased around 44% across their European networks.

---

[2] https://future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf Accessed 6 October 2020

[3] See https://www.iab.org/activities/workshops/dedr-workshop/position-papers/ for all DEDR papers. Accessed 8 October 2020.

[4] https://datatracker.ietf.org/doc/html/draft-arkko-arch-infrastructure-centralisation-00 Accessed 6 October 2020

[5] IBID page 5.

[6] https://www.thinkbroadband.com/news/8699-millions-working-from-home-and-home-schooling-how-is-broadband-performing Accessed 4 October 2020.

[7] https://newsroom.bt.com/the-facts-about-our-network-and-coronavirus/ Accessed 4 October 2020.

However, the biggest increase came in streaming tv, films and online games of almost 50% across Europe.[8] And other European operators reported much the same.[9]

The resilience of the Internet and its decentralised architecture coped well with the change in work and travel habits in the early part of 2020 and increased traffic on fixed and mobile Internet usage. The overall trend for DNS traffic continues to be increasing[10] as does the trend for cybercrime during Covid-19, according to Interpol.[11] But overall, once again, the Internet is hold is doing well against increased traffic, potential attacks, and more streaming online.

Current Trends in Consolidation

Current trends in Internet architecture and global governance could upend the decentralised, resilience of the Internet that we know today. This section considers the trends which could promote and accelerate consolidation whilst reducing the diversity of Internet technologies.

DNS over HTTPS (DOH)

The development of encrypted DNS, specifically DNS-over-HTTPS (DoH), has been driven by a desire to show full end-to-end encryption of network connections. The protocol was deemed complete and the DoH working group[12] wound up in March 2020 despite the absence of both resolver discovery and selection mechanisms, a shortcoming that may be addressed in due course via the IETF's recently constituted ADD working group[13].

In the meantime, client software is developing with interim discovery solutions which almost always favours the large, cloud-based resolver operators. This is leading to a situation where users are being presented with a very small number of pre-configured resolver options irrespective of their location – in some client software as few as three or four options may be presented[14]. This compares very poorly with the current position where many times that number of resolvers per country are currently operating.

If the ADD working group isn't able to ratify a viable discovery option in relatively short order it is possible that bulk of DNS traffic will be consolidated onto a handful of global operators compared to the thousands that operate in a highly decentralised manner today. The impact that such a loss of diversity of providers, hardware and software may have on the long-term resilience of DNS should not be underestimated[15]. Nor should the

[8] https://www.vodafone.com/covid19/news/update-on-vodafone-networks Accessed 4 October 2020.
[9] See, for example, https://ripe80.ripe.net/wp-content/uploads/presentations/32-ripe80_covid.pdf Accessed 4 October 2020.
[10] https://www.akamai.com/uk/en/resources/visualizing-akamai/ Accessed 4 October 2020.
[11] https://ripe80.ripe.net/wp-content/uploads/presentations/30-Presentation-EC3-RIPE80.pdf Accessed 4 October 2020.
[12] https://datatracker.ietf.org/group/doh/about/ Accessed 8 October 2020
[13] https://datatracker.ietf.org/group/add/about/ Accessed 8 October 2020
[14] At the time of writing, the Firefox browser presents a list of three pre-configured resolver options to North American users: Cloudflare, NextDNS and Comcast.
[15] https://techcrunch.com/2020/07/17/cloudflare-dns-goes-down-taking-a-large-piece-of-the-internet-with-it/ Accessed 6 October 2020

attractiveness of these potential network chokepoints to attack be overlooked, whether to access the unencrypted data or to disrupt operations.

A further side effect of the development of DoH should also be noted: by routing the DNS over HTTPS, it becomes much easier to track user activity through the use of cookies. Therefore a protocol that was developed to enhance user privacy and security could actually undermine both: privacy through the use of cookies and security by consolidating DNS traffic onto far fewer resolver operators that are far more attractive targets for malicious actors of various types.

Encrypted Server Name Indication (eSNI)

Options to encrypt the Server Name Indication (SNI) have been explored by the relevant IETF working group but to date it has not been possible to develop a solution without shortcomings. As an example, if only sensitive or private services use SNI encryption then the mere presence of that encryption is itself a signal that a client is going to such a service. This flaw in the encrypted SNI (eSNI) options under evaluation required a rethink in the approach being taken.

The solution now proposed, Encrypted Client Hello (ECH, previously called ECHO) assumes that private origins will co-locate with or hide behind a provider (CDN, application server etc.) which can protect SNIs for all of the domains that it hosts[16]. Whilst there is logic in this approach, the consequence is that the would-be standard encourages further consolidation of data to aid privacy. What it does not appear to consider is the attractiveness of this larger data pool to an attacker, compared with more dispersed solutions.

Consolidating data into a central location would be a focus for cybersecurity attacks as a 'one stop shop'. Attackers can access data all in one place. Arguably, it is the most efficient way for attackers to find and exfiltrate data online. Though centralised data allows for economy of scale, one overall solution for security and a way to manage data efficiently for large companies, it also creates a single point of failure as well as performance limitations, among other issues.[17] Choosing one, centralised, location for data storage would be accelerated by the rollout and use of eSNI.

Digital Sovereignty

One of the justifications for end-to-end encryption, and therefore for the use of protocols such as DoH and ECH, is to protect would-be dissidents from undemocratic governments. The assumption being made was that those governments would be unable to overcome the protections being offered.

Another trend that occurred, coincidentally, during the Covid-19 pandemic is the evidence that both China and Russia are blocking DoT and DoH traffic. It was reported in August 2020, that a potential 'upgrade' to the Great Firewall of China in July 2020 allowed for China to block HTTPS connections with newer, encryption protocols like TLS 1.3 and ENSI.[18] Furthermore, recent research reveals that Google is blocked in China due to censorship and

[16] https://tools.ietf.org/html/draft-ietf-tls-esni-07 Accessed 6 October 2020

[17] https://www.computer.org/publications/tech-news/trends/centralized-cloud-security-an-asset-or-a-liability Accessed 7 Octboer 2020.

[18] https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/ Accessed 4 October 2020.

Google 8.8.8.8 traffic is blocked at 99%.[19] Russia is seeking to achieve the same outcome, but is planning to do so by making it illegal to encrypt traffic through the use of TLS 1.3, DoH, DoT and ENSI.[20] According to reports, the update to the Russian IT law is likely to be approved in October 2020.

At first thought, this might not seem like an issue of consolidation. However, a discussion on the Ripe Labs website seems to foreshadow this current discussion. Entitled, *"Centralised DoH is bad for Privacy, in 2019 and beyond"*, the discussion centres all traffic going through Cloudflare, a US company, thereby causing privacy issues for traffic traversing infrastructure that is, by nature, American.[21] This centralisation is one of the many reasons why blocking or banning encrypted traffic is a must for Russia and China. Not only is the traffic unable to be intercepted, but most of the traffic goes through a handful of large providers. The very fact that the two countries with significant Internet traffic are not allowing TLS 1.3, DoT or DoH traffic means that consolidation is happening in Western countries and that there is likely to be a decreasing amount of traffic going into these countries as more and more providers, who reside outside of China and Russia, adopt TLS1.3, DoT and DoH.

Consolidation: An Analogy

As more people work from home, access to information, servers and private networks normally accessed in the office by using the corporate intranet now needs to be accessed at home by the use of VPN. VPNs have become a choke point in Internet traffic between home and 'the office', but also VPNs have become the target of security attacks as well.[22] VPN traffic in a corporate environment is challenging to get a hold of, but some metrics are available for global demand. According to research from April 2020, demands for VPNs have increased to about 44% in the second half of March 2020. This, alone, gives some indication of the change in working behaviour on VPN usage.[23]

The uptick in VPN usage provides an excellent analogy for consolidated traffic using DoH/DoT. Though many providers may adopt DoH/DoT, the majority of encrypted traffic will transit through a handful of larger providers and, as a result, create a choke point for traffic. Anecdotally, we have all experienced issues when using a VPN and trying to do a video call during peak times for meetings in the last 6 months. Limiting video, restricting social media access, and blocking certain websites, as corporate policy, may help with VPN traffic bandwidth. But could this be an analogy for what the future of Internet traffic could look like in a fully encrypted, DoH implemented world? And if so, is this an analogy for what

---

[19] Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang and Jianping Wu. 2019. An End-to-End, Large-Scale Measurement of DNS-over Encryption: How Far Have We Come?. In Internet Measurement Conference (IMC'19), October 21–23, 2019, Amsterdam, Netherlands. ACM, New York, NY, USA, p. 9.

[20] https://www.zdnet.com/article/russia-wants-to-ban-the-use-of-secure-protocols-such-as-tls-1-3-doh-dot-esni/ Accessed 4 October 2020.

[21] https://labs.ripe.net/Members/bert_hubert/centralised-doh-is-bad-for-privacy-in-2019-and-beyond Accessed 4 October 2020;.

[22] https://redmondmag.com/articles/2020/09/29/new-microsoft-security-report.aspx Accessed 4 October 2020.

[23] https://www.cnet.com/news/vpn-use-surges-during-the-coronavirus-lockdown-but-so-do-security-risks/ Accessed 4 October.

a consolidated Internet, at the technical and application layers at the very least, would look like?

The Internet is for End Users

The IAB's recent publication, RFC 8890[24], declares that the Internet is for end-users. The document's abstract states that "when there is a conflict between the interests of end users of the Internet and other parties, IETF decisions should favor end users". It is questionable whether those developments that have allowed or even accelerated the continuing consolidation of various aspects of the Internet infrastructure and related Internet economy are in the best interests of end users and all users of the Internet.

Conclusion

If the trends identified in this paper continue on their current trajectory, Internet consolidation will lead to issues like traffic congestion and centralised data as well as greater exposure to cybersecurity and privacy risks. In 10 years' time when a new, yet unseen pandemic or other global emergency emerges, the Internet would be not a solution, but a headache.

In light of the current trend of consolidation, we propose the following for consideration:

- In developing Internet protocols, attention should be paid to not weaken the overall resilience of the Internet. In other words, there should be a focus on potential impacts to global Internet infrastructure.
- Along the same lines, when developing new technologies and protocols the potential to enable consolidation should be taken into account. The Internet should not be further consolidated on any of the layers of the Internet.
- In addition, when developing new technologies and protocols, security considerations should be extended to consider whether user privacy may be compromised, for example by allowing individual developers to decide whether to take advantage of additional tracking opportunities.
- Follow RFC 8890 by ensuring that true multi-stakeholder engagement takes place, ensuring that the real-world impacts of the Internet and proposed future developments, both technical and policy, are understood so that decisions can be made that truly favour the interests of end users.
- Programmes or future research opportunities within the IETF, IRTF and IAB which would improve or strengthen resilience and redundant decentralisation of Internet infrastructure should be debated and discussed.

Consolidation is growing and the impact of Covid-19 would have been worse and could potentially be worse if the current trends of consolidation, as we laid out in the brief paper, continue apace. We would welcome further discussion on our proposals for future debate and discussion.

[24] https://www.rfc-editor.org/rfc/rfc8890.html Accessed 8th October