Dynamic Coalition on Core Internet Values (DC-CIV) - Final

The Internet was developed in a collaborative and respectful setting. The researchers and engineers had in mind a flexible and adaptable system that accommodated new communication technology and new applications (and protocols to support them), while adhering to a global notion of interoperability at the IP layer.

As the Internet has evolved and expanded to link half of the population of Earth, the environment in which it operates has changed. The Internet has challenged existing business models, it has opened opportunity for self-expression with global reach to everyone with access and it has ignited new businesses and economic growth. It has provided a mechanism for sharing all the world's knowledge in nearly real time. At the same time, it has enabled new and harmful practices including invasion of privacy, injection of malware, unprecedented surveillance, identify theft, spread of disinformation and denial of service attacks. Our challenge is to preserve all the beneficial aspects of the Internet while defending its users against the hostile aspects of Internet access and use. Governments see these contrasting aspects of the Internet and seek to apply laws and regulations to protect citizens from harm and to corral bad business practices. The matter is made more complex by the global character of the Internet and its general insensitivity to national boundaries. If there are solutions to these problems, they will be found in a multistakeholder collaboration among the technical community, civil society, the private sector and governments working together to establish policies the preserve the best of the Internet and inhibit the worst.

Core Internet values: Evolution over the past 12 months

The coalition's emphasis last year was on defining a set of Core Internet Values and evaluating the state of these values at the time. With the evolution of the Internet not showing any sign of slowdown, the past year saw a multitude of new threats to Internet Ecosystem, from a serious increase in cyber-attacks to a multiplication of political and commercial threats, both in the developing and developed world. It appears that no country is completely safe from attempts at eroding Core Internet Values. How far can this erosion go without seriously hindering the vector for innovation that the Internet has been since its inception? This year, the coalition looked at a subset of these values and their evolution in the past 12 months.

Global – The Internet is a global medium open to all, regardless of geography or nationality.

The past year has seen a significant rise in the Internet being blocked or restricted due to local conflicts. Governments seeing the Internet as a threat have blocked social media websites and apps during times of turmoil, such as military coups, social unrest, or elections. Blocking has taken place at both the network level (dropping/cutting of routes) and at the application level (blocking of a specific type of traffic through deep packet inspection). Blocking is also commonly being used by law enforcement to combat the abuse of the Internet which in some cases have created fragmentation for users.

Interoperable – Interoperability is the ability of a computer system to run application programs from different vendors, and to interact with other computers across local or wide-area networks regardless of their physical architecture and operating systems. Interoperability is feasible through hardware and software components that conform to open standards such as those used for internet.

Interoperability in the last year has seen both gains and challenges.
The main gains are in the increased acceptance of IPv6 in operational networks and the expansion of HTML5, which on the Web platform (itself an application from the point of view of the layered architecture of the Internet) allows for animation and other functions to be native instead of supplied by a plug-in. Some significant landmarks have been passed in IPv6 operations (percentage adoption in US carrier networks).
The main challenge continues to be the expansion of apps; more silent challenges are the threatened adoption of “national” protocols and addressing systems in some countries, and the purchase and wrapping of systems like Skype into new corporate containers and architectures (in this last case, moving from decentralized, peer-to-peer switching to the owning company’s cloud.)

The Internet remains interoperable in its underlying technology, and the past 12 months have not seen any significant shift in this core value except if one takes into account new services. Polarisation in the types of services offered is ongoing. Major social media websites have all released apps that bypass the interoperable nature of the Internet by creating walled gardens (On the Internet, a walled garden is an environment that controls the user's access to Web content and services. In effect, the walled garden directs the user's navigation within particular areas, to allow access to a selection of material, or prevent access to other material.) . Content shared in these walled gardens can seldom be transferred across to other walled gardens.

Within the physical layer, there has been no significant shifts to a single technology. In services such as email, no technology has overwhelmed the others. The physical layer is rife with upcoming challenges coming from the increased adoption and the planned expansions of the Internet of Things (IoT). The IoT will not be connected by WiFi only; many radio systems will come into play. Standards and the corresponding associations may force layer crossings, or adaptations to specific wireless communication systems - spectrum and chips - that may be harder to interoperate. Consortia may attempt to limit interoperability in order to create a more fluid experience, better domain handovers, etc., and also argue that these changes contribute to security.

New angles have sprung up with Interoperability in the past year, however. There are challenges coming from the Internet of Things (which need to form closed environments across all layers, from a standard for the chips and the radios to the way information is managed and privacy secured). These include some possible evolutions of fifth-generation mobile networking technology (5G), which will try to impose gateways (and establish cross-layer controls due to

"network slices," which also has an impact on the end-to-end principle and others), and Internet Protocol version 6 (IPv6) implementations.

IoT is also driving the need for strong authentication across many device brands so that software update sources and sources of control or data gathering can be verified. IoT interoperability across brands will be driven by user expectations.

On the positive (progress in interoperability, that is), the expansion of IPv6 should be noted, as with other core values addressed in this document, not only in that there are more addresses being handed out and used but in that more applications and important Internet services are using IPv6; the progress of HTML5, and the care that the Internet Engineering Task Force (IETF) is taking in securing communications at low levels without a break in interoperability is also noteworthy.

Interoperability imply Open standards and this is described next.

Open – As a network of networks, any service, application, or type of data (video, audio, text, etc.) is allowed on the Internet, and the Internet's core architecture is based on open standards.

The global and free nature of the Internet, core values underpinning its development, faces both new and growing challenges around the world, particularly as certain nations look to create local intranets to circumvent access to the global Internet. Although Internet fragmentation has long been considered a threat to the Internet, mounting evidence suggests that it could become more of a reality in the coming period. China, the home to the second-largest Internet user base in the world, already has a closed and heavily regulated Internet, for instance, while Iran rolled out its "national Internet" in August 2016 and Russia continues to advocate for a closed Internet and fewer Internet freedoms. A similar change is predicated in China; Pakistan enacts strong laws that may close domains; and even European countries are enacting rules that may limit the openness of communications over the Internet. Moreover, the Association of Progressive Communications (APC) along with multiple civil society activists and other members of the Internet governance community in Brazil are deeply concerned that the 2016 ousting of former president Dilma Rousseff will see Internet freedom significantly decrease in the coming years as processes and policies Rousseff supported, such as NETmundial, Marco Civil da Internet, and the multi-stakeholder CGI.br initiative, will likely be undermined. Although advocating for Internet rights is outside of this Dynamic Coalition's remit, curtailing Internet access, limiting Internet content, and cutting off a population of end users -- especially via technical means -- from the global Internet significantly undermines the global and free nature of the Internet.

The same goes for domain names: The United States Immigration and Customs Enforcement Agency seizes domains that are under control of top-level domains (TLDs) operated in the U.S. - often a blunt instrument that may affect innocent third-level domains. Generally, legally appealing these seizures is likely to be a complex process, especially when third parties that are completely unrelated to the reason for the seizure are affected.

Attempts to make Internet governance in the higher layers less open are also ongoing. The United Nations Conference on Trade and Development (UNCTAD) Working Group on Enhanced Cooperation (WGEC) and the treaty-oriented negotiations among some country groups may operate within this trend.

Decentralized – The Internet is free of any centralized control.

This is still the case today. Technological control of the Internet's design principles appears to not be under threat, with technical standards still developed according to core principles in the IETF. The domain name system (DNS), with its 13 root servers, remains free from centralised control. A successful Internet Assigned Numbers Authority (IANA) stewardship transition has transferred stewardship of the root server updates to the Internet Corporation for Assigned Names and Numbers' (ICANN) multi-stakeholder community and more.
On the content level, however, an increasing number of governments are now filtering content either directly or by proxy through laws that Internet Service Providers (ISPs) need to follow. An example is the United Kingdom's "Family Friendly Internet." Another example is the well-known "Great firewall of China."

Is the Internet under threat of political control? A brief closely investigating this question is needed, but is not directly within the DC-CIV's remit.

End-to-end – Application-specific features reside in the communicating end nodes of the network rather than in intermediary nodes, such as gateways, that exist to establish the network.

The difficulty with which IPv6 has managed to impose itself as the technology that will enable the Internet to have enough Internet Protocol (IP) addresses that would allow this end-to-end architecture to be maintained is a matter of concern. Analysts are seeing a growth of Carrier-Grade Network Address Translation (CG-NAT), which "breaks" this end-to-end core value. CG-NAT does so by causing some applications to malfunction and blocks the ability for any service to be run or accessed by end users. The architecture developed by CG-NAT is one of a one-way distribution of content, downloading, with little or no possibility for an end user to offer content for upload. Peer-to-peer networks and applications are negatively impacted by CG-NAT. Moreover, operating one's own content delivery network is impossible.

The past year has seen a growth of IPv6 connectivity and use, with an increasing amount of content made available using this protocol, and this should provide further incentives for more ISPs to offer IPv6, especially now that traffic is increasing. The difficulty comes with the cost of running a scalable dual-stack IPv4/IPv6 network and one that relies solely on IPv4 and CG-NAT. Case studies performed by ISPs having chosen the IPv6 option, such as Sky Broadband and EE, have demonstrated that CG-NAT is both not scalable and more costly to implement on a large scale. Furthermore, the security-related challenges brought forward by difficulty in tracing the source of traffic behind a CG-NAT device paint the future of CG-NAT with a dark

brush. Ultimately, IPv6 is looking increasingly likely to succeed, which bodes well for ongoing and robust end-to-end architecture.
Network neutrality is one of the principles or policies derived from the end-to-end principle. Its nature and the negotiations around it have shifted from technical principle to commercial traffic-management negotiations in the last year as a new model has emerged in which OTT/OSPs have now created large CDNs and therefore do not have to negotiate for large volumes of traffic with network operators. Zero-rating is a network-neutrality-related issue whose definition and assessment is ongoing and varies widely across countries.

User-centric – End users maintain full control over the type of information, application, and service they want to share and access.

Traffic filtering has increased, often based on the ill-defined concept that filtering brings security. The significant and thus worrying trend showing a significant increase in cybersecurity threats – from viruses to worms, malware, denial of service attacks and ransomware – helps ISPs and telecommunication companies make the case that more control of network traffic, and therefore traffic filtering, is necessary.
The extension of traffic control to include social, economic, and/or political filters, such as the filtering of pornography, peer-to-peer file-sharing services, and/or social media, is on the increase; thus, the Internet is less user-centric today than it was last year.

Robust and reliable – While respecting best-effort scenarios for traffic management, the interconnected nature of the Internet and its dense mesh of networks peering with each other have made it robust and reliable.

The IPv4 Internet has been incredibly robust both when it comes to reachability across the globe and reliability. IPv4 traffic peering agreements amongst ISPs have resulted in a very dense intermeshed network that is able to self-heal in most situations, at least in the Global North. There remains challenges in some countries, especially in the Global South, but best practices and the development of resilient routes to the rest of the Internet have made single points of failure rare. Except in cases of political struggle where there was actual intent to turn the Internet off in a geographic area, there have been few cases of an intentional blackout at the country level. Accidental traffic slowdowns caused primarily by submarine cable cuts have been equally as common as in 2015 but less likely to affect Internet users with a total blackout on a wide scale, although some countries, like Vietnam, have been subjected to transient service when supplied mostly by a single cable. IPv6 connectivity was somehow less reliable; until recently, the density of the interconnectivity that made the mesh of IPv6 networks was lower than for IPv4. As a result, it was not uncommon that an incident on a part of the network would affect traffic significantly, either by introducing a significantly longer delay through traffic needing to take a much long route or by splitting that part of the network off altogether – thus rendering it inaccessible. The gradual increase in density of the IPv6 mesh has alleviated this and understandably, this has translated to an increase in IPv6 network reliability. The IPv4/IPv6 dual stack might have actually increased robustness of the network.

There have been several “kill switch” instances over the last year, among which are deliberate blackouts to avoid copying in national student examinations as well as more politically-motivated ones.

Finally, there has been a sustained increase in malicious software exploiting weak security in devices to launch attacks to impact the Internet negatively. It was not an issue in the early Internet development. Times have changed. Should there be a new core value that should drive efforts at standardization and protocol development?