Dynamic Coalition on Core Internet Values Activity Report

(Period December 2021 – December 2022)

This report summarises the activity of the DC on Core Internet Values (DC-CIV) since its session at the Hybrid IGF in Katowice in December 2021 and until the hybrid IGF in Addis Ababa in December 2022.

BACKGROUND ABOUT THE DC (STANDING EXPLANATION SAME AS LAST YEAR)

Over the last ten years our work as an IGF Dynamic Coalition is focused on defining and emphasizing Core Internet Values, which comprise of the technical architectural values by which the Internet was built, and, more importantly, what can be called 'social' or, in other words, 'universal' values that emerge from the way the Internet works.

The first is that the Internet is a ***global*** medium open to all, regardless of geography or nationality. It's ***interoperable*** because it's a ***network of networks***. It doesn't rely on a single application. It relies on ***TCP/IP, a common, open protocol***. It's ***free of any centralized control***. The only supposed control is the domain naming system, which provides a single translation system between domain names and IP addresses, and that's, of course, needed by design. It's ***end to end***, so traffic from one end of the network to the other end of the network goes unhindered. It's ***user centric***, and users have control over what they send and receive. And it's ***robust and reliable***.

These values have been under stress due to various developments, particularly during the Pandemic. Also, as the Internet expands with newer products, services and applications, there are emerging needs for focused pursuits on important aspects of the Internet, for instance, ***freedom from harm***. (In 2017, the Coalition put together a discussion paper focusing on freedom from harm as proposed by Vint Cerf in the context of addressing the rise of criminal use of the Internet and the solutions towards prevention of harm to the users of the Internet, including the harm that arises unintended from the staggering growth of IoT technologies, causing billions of devices connected to the Internet which in turn bring about new regulatory concerns.)

The Coalition was formed following the IGF Egypt workshop in 2009 titled "Workshop on Fundamentals: Core Internet Values" chaired by the then Internet Society President Lynn StAmour. As a DC, meetings were held at the IGF annually since IGF2010 and has also held sessions at EuroDig.

ACTIVITIES CONDUCTED IN THE PAST YEAR 2022

Activities within the IGF (e.g. participation in the annual IGF meeting, relations with other IGF workstreams)

The DC-CIV participated in DC coordination meetings[1]. It also wrote a substantive paper to prepare for the IGF 2022 session.

The 2022 IGF session of the DC-CIV[2], on the topic of "Geopolitical neutrality of the Global Internet" - was chaired by Olivier Crépin-Leblond and co-Chaired by Alejandro Pisanty, UNAM.
It included the following panellists:

- Bastiaan GOSLINGS, Senior Policy and Governance advisor, RIPE NCC, Technical Community, WEOG.
- Bill WOODCOCK, Executive Director, Packet Clearing House, Business Community, WEOG.
- Iria PUYOSA, International Research Advisory Council Member - Advisor on Social Media and Peacebuilding, Toda Institute, Washington DC, Civil Society, GRULAC.
- Veronika DATZER, policy advisor in German Parliament, Government, EEG.
- Vint CERF, Internet Evangelist, Google, Business Community, WEOG.

The topic was triggered by developments in Europe whereas Russia's military intervention in Ukraine spilled directly into Internet Governance. The Internet Community was under pressure with calls to "block" Russia from the Internet, and among various technical demands, to take down the former Soviet Russia's country code top level domain .SU and the current country code top level domain .RU. ICANN and the Regional Internet Registry RIPE NCC, declined to be drawn into a debate on a geographical Internet shutdown, which is antithetical to their core operating values of neutrality and impartiality. The Internet is a Network of Networks, global, not only in a geographical context, but by several shades of the term 'global' in terms of being free of cultural, ideological, political bias, and global in terms of the technologies that converge into it. The decision taken was to separate geopolitics from the Internet which would make the Internet into two or more 'Splinternets' in place of the unfathomably valued One Internet.

Yet, some leading members of the Internet Community signed a common statement "Towards the Multistakeholder Imposition of Internet Sanctions" - opening the door to the Internet Community having some means to decide on whether sanctions such as disconnection from the Internet would be appropriate.

The discussion of the above experts yielded a fascinating set of key points which are reproduced here, as they were carried directly to the IGF Leadership Panel.

(Vint Cerf, Google)

- Maintaining a generally neutral , connected and resilient core Internet infrastructure is of vital importance. Combating bad behaviors sometimes can be locally implemented (dropping DOS traffic, seizing abusive domain names, filtering "bad" content, detecting and filtering malware, spam and phishing).

[1] DC Coordination Group: https://www.intgovforum.org/multilingual/content/dc-coordination-activities
[2] Session "Geopolitical neutrality of the Global Internet ": https://intgovforum.org/en/content/igf-2022-dc-civ-dc-civ-geopolitical-neutrality-of-the-global-internet

- The major problems today are at the application layer whether this is misinformation, disinformation, CSAM, phishing, surveillance, etc. Finding ways to create incentives for good practices and to discourage bad ones is a challenge. When incentives don't work, we need ways to hold badly acting parties accountable. This will require international cooperation in cases where harns are inflicted across jurisdictional boundaries.
- It is important that attempts to apply sanctions proportionately and to follow the principle of subsidiarity. It is a mistake to apply sanctions at the wrong layer in the architecture. For example, shutting down the Internet to deal with bad behavior by some parties is an overreach that creates a lot of harm for those innocently relying on the operation of the network.

—-------

(Bill Woodcock, Packet Clearing House)

- The implementation of sanctions via Internet means currently faces two principal challenges: On the network side, network operators typically under-comply or over-comply, due to difficulties in appropriately scoping enforcement actions. On the governmental side, sanctions regimes are not typically published in a uniform, consistent, or machine-readable format, they're not published in a single predictable location, and they're not harmonized with other regimes.
- Many very specific implementation issues exist as well, starting with governments' predilection for transliterating foreign-language or foreign-character-set names of sanctioned entities in diverse and inconsistent ways, rather than using the most-canonical form of each name, in its native language and character set. Network operator implementation has been occurring within the Sanctions.Net community since March of 2022, and governmental harmonization efforts have been occurring principally within the Digital directorate of the OECD.
- Most conversation about Internet sanctions implementation has been positive and collaborative, since governments wish to see their sanctions regimes respected, and network operators wish to comply with the law and protect their customers. Dissenting voices have questioned the legitimacy of sanctions regimes from both the right and the left, principally fearing governmental overreach.

—--------

(Veronika Datzer, Advisor at German Parliament)

- It is impossible for politics to refrain from the internet because it already is. This process cannot be reversed. We therefore need political solutions because the technical infrastructure of the internet must remain neutral.
- Solutions to making the internet a peaceful place must not include internet sanctions as these impact all people and can have dramatic adverse consequences. They must be based on a multistakeholder model and co-create what it means to establish a peaceful internet, as such an understanding should not be imposed.
- We need to be in close cooperation between the technical community and the political community.

—---------

(Iria Puyosa, Toda Institute)

- The global multistakeholder governance ecosystem should center the protection of human rights to safeguard internet core values. Sanctions against States that violate international law may be necessary in cases of widespread human rights violations or credible allegations of crimes against humanity enabled by State agencies' internet usage.
- The global internet may need to create a multistakeholder policy advisory body that provides guidelines on targeted sanctions that may be enforced if necessary. Nonetheless, sanctions must be targeted, specific, and proportional. Also, a robust and reliable due process must be established for making these decisions
- The establishment of rules and processes to define and enforce sanctions should not be decided by a small number of governments (such as those belonging to the OECD). The policy formulation process should involve countries from different regions of the world. Otherwise, the sanctions regime may be considered unilateral and provide an excuse for the "sovereign internet" model leading to the splinternet.
- All of the countries are working their model of sovereignty and Internet some are taking an approach that is completely different than that model we're used to, the open, free, Internet.

—-------

(Bastiaan Goslings, RIPE NCC)

- It is not in the mandate of technical organisations like RIPE, not within the policies that determine how these organizations are run, to make decisions on sanctions. Policies are set by multistakeholder communities across an entire service region, which includes many jurisdictions. If there are sanctions, they need to be decided following due process, democratic fashion demonstrating that the sanctions are proportionate to the goals to be achieved. Economic sanctions are set by the European Union.
- RIPE has no authority to actually enforce what they are doing as it operates as a trusted technical organisation, a neutral authoritative entity in this case, but no enforcement power of any kind. Networks using the RIPE database operate on Trust.
- Anyone can decide they do not trust this system and operate their own registry. From that perspective, it is a vulnerable system.

The take-aways from this session are reproduced here due to their significance for future DC Core Internet Values work. The significance of this year has been the spilling-over of a real world conflict that included both online and offline hostilities. With this line having been crossed, it is very unlikely to see the clocks turn back. The Internet, a network of networks, is based on trust and collaboration and both are eroding at an unprecedented rate. Some of the points made during the session would have been completely unthinkable a few years ago. Whilst the DC-CIV has reported on an increasing number of incidents putting Core Internet Values into jeopardy, it is the first time the concept of “enforcement” has been suggested in this realm, as if the spirit of collaboration is being replaced by new values that require taking action – whether unilateral, multilateral, top down or bottom up.
We might be witnessing a significant change in the game.

CORE INTERNET VALUES TRACKING

The global changes caused by the Pandemic to the economy, work flows and society have been significant. With 2022, the world thought it was time to recompose its economy and put the pandemic behind us as a bad period to recover from, and along with it, there was hope that the erosion of Core Internet Values was going to slow down, perhaps even be reversed.

This was clearly not the case.

The focus from governments on combatting "online harm" was strengthened. Progress was made by governments towards the implementation of significant legislation addressing this topic. Whether it is breaking the end to end services and nature of the Internet, implementing a National DNS infrastructure, performing significant content filtering, weakening encryption or requiring identification for using the Internet – the Core Internet Values have never been so much at risk.

The roundtable sessions that were organised in 2021 and the topics addressed in 2022 are very likely to be followed by further roundtable sessions that will bring all actors to the table. Participants in the DC engaged in dialogue with legislation makers and other stakeholders to find solutions for the future of the Internet, without negatively impacting Core Internet Values. Unfortunately, successes have been sparse this year. Nevertheless, there is always hope, as long as stakeholders continue to engage in dialogue. This dialogue has broken down in some parts of the world in 2022. Let us hope renewed dialogue is found in 2023. The IGF will have a significant part to play in this.

Report submitted by Olivier MJ Crépin-Leblond, DC Core Internet Values Chair
15 February 2023