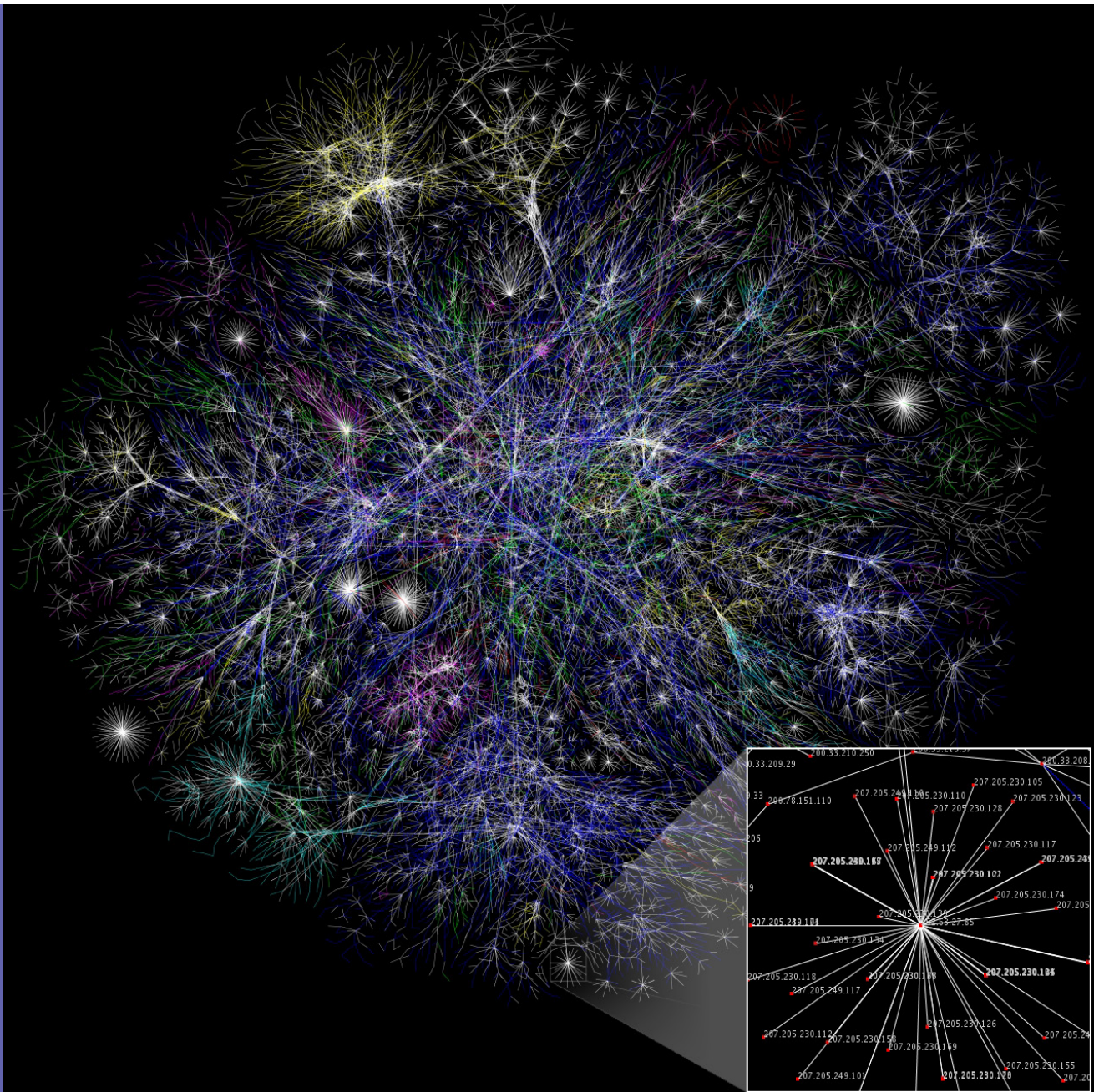


THE DEMOCRATIC NATURE OF THE INTERNET'S INFRASTRUCTURE

Discussion Paper 3/2023



THE DEMOCRATIC NATURE OF THE INTERNET'S INFRASTRUCTURE

Discussion Paper 3/2023

Konstantinos Komaitis



International IDEA
Strömsborg
SE-103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

© 2023 International Institute for Democracy and Electoral Assistance

International IDEA publications are independent of specific national or political interests. Views expressed in this publication do not necessarily represent the views of International IDEA, its Board or its Council members.



With the exception of any third-party images and photos, the electronic version of this publication is available under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 (CC BY-NC-SA 3.0) licence. You are free to copy, distribute and transmit the publication as well as to remix and adapt it, provided it is only for non-commercial purposes, that you appropriately attribute the publication, and that you distribute it under an identical licence. For more information visit the Creative Commons website: <http://creativecommons.org/licenses/by-nc-sa/3.0/>.

International IDEA
Strömsborg
SE-103 34 Stockholm
SWEDEN
Tel: +46 8 698 37 00
Email: info@idea.int
Website: <https://www.idea.int>

Cover illustration: Partial map of the Internet based on the January 15, 2005 data found on opte.org.
Published with a Creative Commons licence BY 2.5
Design and layout: International IDEA
Copyeditor: Andrew Robertson

DOI: <https://doi.org/10.31752/idea.2023.35>

ISBN: 978-91-7671-641-0 (PDF)

Acronyms and abbreviations

BGP	Border Gateway Protocol
IETF	Internet Engineering Task Force
ICANN	Internet Corporation for Assigned Names and Numbers
IGF	Internet Governance Forum
OSI	Open Systems Interconnection (see Appendix A)

Contents

Acronyms and abbreviations	iv
Executive summary	3
Introduction.....	4
Chapter 1	
The Internet, its design principles and democracy	6
Global reach, integrity	7
General purpose.....	8
Supports innovation without permission	9
Accessible	10
Collaboration.....	11
No permanent favourites.....	12
Chapter 2	
Recommendations	14
Conclusion	16
References	17
Appendix A	
Open Systems Interconnection	21
About the author.....	23
About International IDEA	24

EXECUTIVE SUMMARY

These days it is scarcely possible to have a conversation about democracy without mentioning the Internet. Similar to democracies, the Internet is a complex ecosystem, consisting of a multitude of actors and facilitating (at least in theory) the equal participation of anyone who is willing to adhere to a set of minimum requirements.

The strength of the Internet lies in its original design, which in some ways mirrors democratic ideas. As with the separation of powers in a true democratic state, the architecture of the Internet has no centre of control and allows power to flow from the bottom up and even from the margins, rather than always from above. With design principles like voluntary participation, collaboration, ease of access and autonomy, the Internet has been regarded as a tool capable of democratizing information, knowledge and societies at large.

During the past few years, policymakers have directed their attention towards the top layers of the 'Internet stack', those where the effect on democracy is more easily observable. Little attention has been paid to the infrastructure of the Internet—the part that is invisible to users yet constitutes the essence of what the Internet is really about.

This Discussion Paper seeks to alert democratic stakeholders to often ignored aspects of the digital threats to democracy, and to highlight the key weak spots of the Internet as an infrastructure upon which democracy itself partly rests.

The strength of the Internet lies in its original design, which in some ways mirrors democratic ideas.

INTRODUCTION

In the past decade, the perceived impact of the Internet on democratic values has shifted drastically, especially with regards to social media.

In the past decade, the perceived impact of the Internet on democratic values has shifted drastically, especially with regards to social media. According to a 2020 report by the Pew Research Center, there is a significant concern that ‘humans’ use of technology will weaken democracy ... due to the speed and scope of reality distortion, the decline of journalism and the impact of surveillance capitalism’ (Anderson and Rainie 2020). Yet, in the same period the Internet, as it exists today, has been a fundamental infrastructure for exercising democratic rights such as freedom of expression, association or political participation.

Although most of these worries concern the upper layers of the ‘Internet stack’—the consumer-facing applications, websites and products that dominate public understanding of the Internet—they create mistrust of the entire Internet ecosystem down to its very physical infrastructure. This poses serious challenges to the global Internet and contributes to the democratic deficit the world is currently experiencing. What is more, some authoritarian regimes such as China, Russia and Saudi Arabia are already using the Internet’s infrastructure as a weapon against debate and dissent. Digital authoritarianism comes in different shapes and sizes; it is not only limited to tactics of disinformation and propaganda, but includes also Internet shutdowns and surveillance through the use of artificial intelligence (AI) and facial recognition software (Lamensch 2021).

In the past few years, as the role and presence of Internet-based services have grown exponentially, policymakers have been directing their attention towards the top layers of the ‘Internet stack’, those where the effect on democracy is more easily observable. Correspondingly little emphasis has been placed on the infrastructure of the Internet, the part that is invisible to users.

Nevertheless, this is changing and not always for the better. In many of the most recent legislative initiatives emerging from democracies, we see a trend towards manipulating the Internet’s infrastructure, which might result in the

creation of single points of control. India (Karthik 2022), South Korea and the European Union (Komaitis and Park 2022), for instance, are discussing options to disrupt the interconnection market and the voluntary agreements that support seamless access to content and services. This would be to turn upside down the core principle of network neutrality: the idea that all data, content and applications should be treated without discrimination.

Furthermore, the Network Information Systems II (NISII) Directive, Europe's latest cybersecurity agenda, has a far-reaching extraterritorial oversight, creating the incentive for other countries to reciprocate 'which would significantly complicate the operation of a fundamental component of the Internet's global infrastructure' (RIPE 2021). Should such trends persist, there is a real danger that the Internet fragments. In the meantime, a diverse set of countries, including Indonesia, South Africa, Turkey and Vietnam, demand the data accumulated from social media use to be physically stored within their borders, creating the conditions for more control by state actors and a less global Internet. The number of Internet shutdowns has already grown to levels that should worry most democracies (see Access Now n.d.).

This brief paper seeks to inform policy discussions and policymaking geared towards the protection of the Internet as a fundamental infrastructure for democracy. Its democratizing promise regarding information and knowledge is contingent on—among other factors—an enabling architecture that creates the necessary conditions for this to happen. The design of the Internet may not be a sufficient condition (nor have been the direct outcome of a democratic experiment), but crucially these design principles are now at risk. Collaboration, participation and autonomy constitute features that reflect both the Internet and democracy. By focusing on the design of the Internet, this paper aims to highlight often ignored aspects of the digital threats to democracy, as well as the key weak spots of the Internet as an infrastructure upon which democracy partly rests.

By focusing on the design of the Internet, this paper aims to highlight often ignored aspects of the digital threats to democracy.

Chapter 1

THE INTERNET, ITS DESIGN PRINCIPLES AND DEMOCRACY

Part of what makes the design principles a worthwhile approach is that they have not changed since the Internet consisted of just two networks.

In 2012, the Internet Society attempted to capture the values that pertain to the Internet in a document called 'Internet Invariants: What really matters' (Internet Society 2012). The document provides a snapshot of what distinguishes the Internet from other technologies, outlining how the Internet's normative values represent engineering choices but also reflect democratic ideals.

In doing so, 'What really matters' helps us unpack the relationship between the Internet and democracy. Part of what makes the design principles a worthwhile approach is that they have not changed since the Internet consisted of just two networks, despite the Internet's significant evolution. After more than 20 years of the commercial Internet, it is unquestionable that the Internet has become inseparable from contemporary understandings of how democracies function, reflecting a fundamental transformation rivalled technologically only by the printing press and radio.

The Internet Society description of the Internet's constants (given here verbatim) include:

- *Global reach, integrity.* Any endpoint of the Internet can address any other endpoint, and the information received at one endpoint is as intended by the sender, wherever the receiver connects to the Internet. Implicit in this is the requirement of global, managed addressing and naming services.
- *General purpose.* The Internet is capable of supporting a wide range of demands for its use. While some networks within it may be optimized for certain traffic patterns or expected uses, the technology does not place inherent limitations on the applications or services that make use of it.
- *Supports innovation without requiring permission (by anyone).* Any person or organization can set up a new service that abides by the existing standards and best practices, and make it available to the rest of the Internet without requiring special permission.

- *Accessible.* It is possible to connect to the Internet, build new parts of it, and study it overall. Anyone can ‘get on’ the Internet—not just to consume content from others, but also to contribute content on existing services, put up a server (Internet node), and attach new networks.
- *Based on interoperability and mutual agreement.* The key to enabling inter-networking is to define the context for interoperation, through open standards for the technologies and mutual agreements between operators of autonomous pieces of the Internet.
- *Collaboration.* Overall, a spirit of collaboration is required. Beyond the initial basis of interoperation and bilateral agreements, the best solutions to new issues that arise stem from willing collaboration between stakeholders. These are sometimes competitive business interests, and sometimes different stakeholders altogether (e.g. technology and policy).
- *There are no permanent favourites.* While some technologies, companies and regions have flourished, their continued success depends on continued relevance and utility not strictly some favoured status ... Good ideas are overtaken by better ideas; to hold on to one technology or remove competition from operators is to stand in the way of the Internet’s natural evolution.
(Internet Society 2012)

What follows is an attempt to outline the way each of these design characteristics facilitates democratic politics, and how they are often under attack.

GLOBAL REACH, INTEGRITY

The Internet’s global reach is the result of conscious design decisions from its earliest days. Designing a system where ‘distributed routing’ would deliver a resilient and adaptable network of autonomous networks, allowing for local optimizations while maintaining worldwide connectivity (Komaitis and Park 2022) was part and parcel of ensuring an open infrastructure. In a 1988 paper, Internet pioneer David Clark stipulated that the ultimate design goal for the Internet is to ensure that ‘communication [can] continue despite loss of networks or gateways’ and that ‘the Internet must permit distributed management of its resources’ (Clark 1988: 107). It was once a radical idea to suggest that a user in Singapore, for example, should be able to frictionlessly access data in the same way as a user in Buenos Aires.

This open and global infrastructure delivers a variety of benefits. Democratic decision making would be strengthened by networked users reading, listening to, and learning from what is happening across the world and from each other, sharing best practices and avoiding repeating mistakes. Users, armed with nothing more than a device that connects them to the Internet, could

The Internet’s global reach is the result of conscious design decisions from its earliest days.

organize, coordinate and take action, strengthening freedom of expression and association. The hope was that the Internet's design would be able to mobilize people in creating technologies and networks, which would also democratize political life in various ways. The Internet would be 'open to anyone willing to participate, as a consumer, an information provider, an infrastructure builder, or an academic who wants to study how it all fits together' (Komaitis and Park 2022).

However, this vision has not been realized in its entirety and could become further compromised. The biggest threat to the Internet's global nature is fragmentation, or, in simple terms, the splintering of the Internet into smaller pieces. In the beginning only a handful of countries, in particular China and Iran, opted to prevent users from accessing the broader Internet and instead channel them to domestically-produced—and strictly monitored and controlled—applications and tools. In recent years, geopolitical zero-sum thinking and protectionism have expanded the threat of Internet fragmentation beyond authoritarian countries. A host of democracies, from the European Union to the United Kingdom, Canada, India and the United States (and more) are exploring more aggressive content moderation and regulation strategies that carry this risk (Komaitis 2023; Coe 2022; Buell 2021; Iyengar 2021; ITIF 2020). If the end goal of having a global communications infrastructure is the accessibility of information from anywhere in the world, then the inconsistency of content moderation laws will prevent such access. Furthermore, such an intense regulatory environment could have immense implications for public debate and participation (UN OHCHR 2021).

One of the reasons for the success of the Internet was that there never was an attempt to restrict its application to any specific technology.

GENERAL PURPOSE

One of the reasons for the success of the Internet was that there never was an attempt to restrict its application to any specific technology. 'Generality delivers flexibility. The Internet continuously serves a diverse and constantly evolving community of users and applications' (Komaitis and Park 2022).

For the Internet, a general-purpose network allows the co-existence of a diverse set of applications, actors and an environment that changes constantly. Services like social media and messaging have facilitated a different kind of democratization than the advent of competitive multiparty elections. They have given users the ability not only to exercise their democratic rights online, but to do so using the medium of their choice and not be restricted to a government-sanctioned and possibly limited one. The use of the encrypted messaging app Signal during protest movements all over the world is a recent example allowing protestors to evade government monitoring of communications. Not surprisingly, autocratic regimes such as China, Iran and Uzbekistan have disrupted access to Signal (as well as Twitter, Wikipedia and many others) explicitly to curtail the democratic rights of their populations.

Another complex challenge is managing the proliferation of misinformation, disinformation and fake news. In the Philippines, companies like Facebook constitute an infrastructure that defines both politics and online interactions (Ressa 2019). In the 2016 US presidential elections, social media companies played a role in jeopardizing American democracy (Kübler, Pauwels and Manke 2020). Since then, the spread of disinformation through social media has plagued democracies across the world. In Europe, for instance, 71 per cent of European citizens encounter fake news online several times a month (European Union 2020). Using different approaches, several governments have tried to impose measures to control disinformation—but these often double as tools to curtail freedom of expression. Measures to rein in political disinformation often bring diminished returns, due to the difficulty of creating adequate regulation for all existing platforms and even channels of communication (text, video or audio, for instance).

SUPPORTS INNOVATION WITHOUT PERMISSION

The success of the Internet rests also on the fact that interoperable building blocks allow innovation to happen constantly, without requiring any sort of permission from a central authority. On the Internet, everything is voluntary—participation, communities and the adoption of standards. People contribute because they want to and because they gain value from the Internet. As in pluralist democracies, Internet users can come together to form collectives based on shared interests; these collectives then create a set of interdependencies that encourage self-organization processes. From technical organizations, such as the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN) or the World Wide Web Consortium (W3C), to more user-interfacing platforms like Wikipedia and Reddit, voluntary participation, consensus and decentralized decision-making sit at the heart of how the Internet has developed and been managed. Similar to the way a democracy is at risk if it fails to allow the space for citizens to self-organize and deliberate, the Internet cannot operate without self-organizing and the democratic associations of its users.

China provides the starkest example of how top-down, state-driven and state-sanctioned standards could create the conditions for a less democratic Internet. As China takes a more central role in global technological competition, it is expected that the new technologies it proposes ‘will create a more network-centric Internet that enables fine-grained controls in the foundations of the network, changing the way people and things connect and how data is collected and used’ (Hoffmann, Lazanski and Taylor 2020). Huawei’s ‘New IP’ proposal (Internet Society 2022) provides such a paradigm.

The success of the Internet rests on the fact that interoperable building blocks allow innovation to happen constantly, without requiring any sort of permission from a central authority.

Accessibility by everyone, irrespective of status or background, constitutes a paramount principle for the Internet and is what makes it scalable and resilient.

ACCESSIBLE

When considering the reasons democracy and the Internet are so compatible, the presumption of equality provides an obvious link. Accessibility by everyone, irrespective of status or background, constitutes a paramount principle for the Internet and is what makes it scalable and resilient. 'Unrestricted access and common protocols deliver global connectivity and encourage the network to grow' (Komaitis and Park 2022).

The promise of the Internet was that contributions would not be judged on the basis of their creator's identity or background, but solely on their own merits. The best solutions come from people coming together on an equal footing. In the IETF, for example, participants represent themselves; rough consensus and running code sit at the forefront of how Internet standards are created. The Internet has created a 'global town square' that transcends the borders and restrictions imposed by nation states. With its open standards processes and their voluntary adoption, the Internet provides agency to anyone who wants to participate.

To realize the goal of accessibility for everyone, the Broadband Commission for Sustainable Development is working towards making broadband affordable and universal (Broadband Commission n.d.). With 2.7 billion people still offline, there is a great amount of work to be done towards connectivity. In the meantime, evidence also points to the fact that community-led initiatives are also necessary and effective in addressing the digital divide (Connectivity Capital 2022). Community networks constitute an additional way to gaining access to the Internet and have played a key factor in democratizing communities and information.

However, even where infrastructure supports connectivity, access to the Internet is not always a given. Even in highly-developed countries, women and racial and ethnic minorities suffer from a digital divide, in terms of both Internet access and related professional and practical opportunities (Fairlie 2016; NCES 2021; OECD 2018). Nor does systemic repression in patriarchal and 'honour-based' cultures disappear simply because individuals are online; here too, women especially face pressure to conform to gender norms and codes of behaviour (Pearce and Vitak 2016).

The other threat to connectivity comes from Internet shutdowns, which, over the years, have increased in both volume and intensity. In 2022, Internet shutdowns by governments across the world affected 2.7 billion people (Surfshark n.d.), costing the global economy approximately USD 24 billion (IGF 2023; Shahbaz, Funk and Vesteinsson 2022).

In some cases, state actors have used BGP (Border Gateway Protocol) routing to censor international traffic. In November 2019, in the wake of opposition political demonstrations, the Iranian Government was successful in cutting off most traffic from the global Internet, while continuing to operate a domestic network (Salamatian et al. 2021). Similarly, China has often used BGP hijacking

to carry out covert man-in-the-middle surveillance on Western countries and companies (Demchak and Shavitt 2018). Interference with BGP could be considered as limiting one of the stronger democratizing powers of the Internet—the transnational flow of accessible information.

COLLABORATION

As a global system, the Internet is a network of networks held together by a spirit of collaboration.

When information traverses the Internet, it may pass through a handful of networks, and the network from which the traffic originated probably has no formal relationship with the network that receives it. The reason why this works is collaboration, both in exchanging and carrying traffic from other networks, and in solving problems that may have originated several hops away. The basis for this collaboration is a number of open standards and practices that all network operators have adopted voluntarily ... Such collaboration between stakeholders has become an essential approach to addressing issues affecting the information society.

(Internet Society 2016: 9)

Stakeholders from all sectors and countries have learned to work together in different ways and have created democratic communities (e.g. the IETF, ICANN and the Internet Governance Forum—IGF) that, to this day, continue to advance the Internet through inclusiveness of diverse ideas and collaboration. This has produced tangible dividends. ‘The development of many Internet Exchange Points (IXPs) around the world, for example, has only been possible due to the close collaboration of local communities, technical experts, industry and governments’ (Internet Society 2016: 9).

In other words, Internet governance is based in multistakeholder, collaborative communities that are largely—if not entirely—separate from state-to-state interactions. This system of governance reflects and has reinforced other Internet constants, such as *interoperability and mutual agreement* and the *support of innovation without requiring permission*. It has maintained an Internet where technical needs take precedence over geopolitical competition. Achievements in Internet governance have been key to allowing the exercise of democratic rights online—and in many countries, before similar rights can be enjoyed offline.

Internet governance is based in multistakeholder, collaborative communities that are largely—if not entirely—separate from state-to-state interactions.

The Internet is an inherently decentralized technology, but for decentralization to work, the principal actors need to consider prerequisites such as oversight, accountability and clear policies and processes.

NO PERMANENT FAVOURITES

The Internet is an inherently decentralized technology, but for decentralization to work, the principal actors need to consider prerequisites such as oversight, accountability and clear policies and processes. Early participants in the management of the Internet—the IETF, ICANN and the Regional Internet Registries (RIRs)—operate under such prerequisites.

By contrast, in centralized systems hierarchy serves to maintain a distribution of power; accountability and oversight may be subordinated to the same purposes entirely. As the Internet became increasingly commercial and as user demand increased, a host of new actors emerged which have failed to uphold the values of the decentralized ecosystem. In fact, especially as infrastructure moves up the 'Internet stack', a new environment of app stores and cloud computing emerges that is more monopolistic, top-down and autocratic. Unlike the Internet, these new, proprietary environments are not ecosystems; they are what author Maria Farrell calls 'plantations' (Farrell 2022). This phrase captures that while from a technical point of view big technology companies are engineered, distributed systems, ultimately, what they offer to users is a monolithic version of the Internet:

In contrast to a functioning ecosystem, app stores are centrally controlled by a single power. Innovation runs along pre-set rails. Apps compete with each other, but only on criteria set by the system owners. Users choose only from what the controllers make available. The money, data and power generated in the app store flow disproportionately back to the owner. It's emphatically not an ecosystem but a hierarchy that permits ritualistic competition to drain off the energies of potential competitors. (Farrell 2022)

This monolithic view is often less open and overwhelmingly undemocratic. And, as technology companies begin to occupy different spaces in the Internet ecosystem, the challenge becomes how to avoid this shift.

Engineers anticipated this shift. As early as the 1960s, Paul Baran, a pioneer in the development of computer networks, predicted the rise of a centralized 'computer utility' that would offer computing much the same way that power companies provide electricity (Baran 1967). To be more precise, during the early days of the Internet, transit providers used to be responsible for carrying the traffic between cities, regions and continents. However, as the Internet grew, so did the actors that participated in its ecosystem. Today content providers and cloud computing companies have moved to perform core functions of the Internet, being the places where most of the 'interneting' takes place. As we move up to user-facing applications, we see something similar. The reality today is that most users will use the services of a single company, Alphabet, for communication (Gmail); entertainment (YouTube); e-commerce (Google shopping); information (Google search); navigation (Google maps); and mobile apps (Google Play).

Centralization creates single points of control, disempowers users, conditions them to certain behaviours, undermines participation and breaks trust by creating a paralysing feeling among users who lack the required transparency to make informed choices. Centralization creates the conditions for a less democratic order. Whereas the Internet still continues to work even when networks fail, services and websites can fail because the platforms they depend on (e.g. Content Delivery Networks, CDNs) fail. Practically, what transpires is the introduction of unnecessary chokepoints within the Internet's infrastructure, which are controlled by a small number of entities, yet they control a user's full Internet experience.

As a reaction to this concentration of power in the hands of a few players, some state actors have been taking on functions that indicate the development of an even more centralized, but state-managed, Internet environment. Most famously, the Chinese Communist Party has created an Internet environment that allows it to control online interactions of users (*Economist* 2018).

In sum, the capacity of the Internet to support democracy—through all of the above design features—is getting harder. According to the Freedom House annual 'Freedom of the Net' report, in 2022 governments were turning their backs on an open Internet and seeking more control of online spaces. 'New national laws posed an additional threat to the free flow of information by centralizing technical infrastructure and applying flawed regulations to social media platforms and user data' (Shahbaz, Funk and Vesteinsson 2022).

In sum, the capacity of the Internet to support democracy—through all of the above design features—is getting harder.

Chapter 2

RECOMMENDATIONS

Despite this move to greater control, ensuring the Internet continues to support democracies and civic participation cannot be achieved by governments stepping back and allowing private actors to lead. Instead, it is recommended that governments consider the following:

- 1. Conduct impact assessments for Internet policy proposals to ensure they meet their stated goals while preserving the foundation of the Internet** (Komaitis 2020). States should approach Internet regulation with caution, ensuring that it is
 - *fitting*: proportionate, not excessive, mindful of negative and unintended consequences, while preserving the Internet's open, global and end-to-end architecture;
 - *informed*: based on evidence and sound data about the scale and impact of the issues and proposed solutions at hand, using ongoing dialogue to deepen understanding and build consensus; and
 - *targeted*: focused on clear objectives and the appropriate building blocks towards attaining them.
- 2. Recognize that technological fixes are no replacement for education and public awareness campaigns.** Most of the issues currently overwhelming governments' regulatory agendas have to do with issues that are ingrained in societies. Misinformation, disinformation, fake news and propaganda are as old as society itself; they have become the number one threat to democracies around the world because of the Internet's scalability. Finland has made media literacy part of its national core curriculum starting as early as in preschool and currently ranks first out of 41 European countries in resilience against misinformation (Gross 2023).
- 3. Promote cross-sectoral collaboration and strong international partnerships as key to advancing a more democratic Internet.** The Internet is full of 'wicked' (complex, evolving, thereby indeterminate and inherently

difficult) problems. Participants, representing different interests or goals, have to proceed together because none can run the Internet alone. ‘To get to that level of agreement, participants—whether private companies with financial stakes in the situation, or governments or individuals—must be disposed and willing to collaborate with others to instantiate adoption’ (Daigle, Komaitis and Roberts 2016: 2). Rather than respond with protectionist measures (as the EU and US have done—Rohac 2022) it is vital for democracies to work together more closely if the global Internet is to survive (Dong Kwan Kim 2020).

4. Implement human rights considerations into Internet design and standard-setting processes.

‘Infrastructure technologies are not neutral. The ways they are designed, operated and managed have implications for who can access and disseminate content, how people and communities can associate and represent themselves online, and who has the ultimate power over these decisions. Normalizing the corporate responsibility to respect human rights by identifying adverse impacts and taking steps to mitigate them must be done not just among social media platforms and app companies, but also registries, registrars, and other infrastructure providers that the public doesn’t see every day’ (Article 19 2021). Identifying ways to apply the human rights framework to the way standards are set, and without impeding innovation, is critical.¹ The Request For Comments (RFC) 8280 provides a good starting point (see IETF n.d.a), while the work on privacy in the context of the Domain Name System (DNS) also provides some useful guidance (see IETF n.d.b).

5. G7 governments in particular should live up the commitment to ‘develop a values-driven, high-impact, and transparent infrastructure partnership to meet the enormous infrastructure needs of low- and middle-income countries’ (POTUS 2021). Democratic states should not only invest in their own infrastructure but also assist other countries, especially those where the unconnected population (37 per cent) lives, including by supporting and investing in infrastructure capacity building. Moving forward, infrastructure that is trustworthy and able to support the open Internet will be key in ensuring a more democratic world. Part of this infrastructure will be dedicated ‘to supporting access to platforms and services that depend upon an open, interoperable, secure, and reliable Internet and mobile networks with sound cybersecurity’ (POTUS 2021).

¹ The Internet Engineering Task Force (IETF) has formed a research group that aims to discuss human rights for Internet protocol design. For more information see IETF n.d.a (<https://datatracker.ietf.org/rg/hrpc/about>).

CONCLUSION

In its *Global State of Democracy 2022* Report, International IDEA finds that there is a 'declining public faith in the value of democracy' and that 'the recent series of global crises ... appear to indicate the emergence of a new status quo, defined by radical volatility and uncertainty' (International IDEA 2022). Unsurprisingly, this also applies to the Internet, its future governance and its societal effects.

In recent years, the Internet has been increasingly used as a battleground for nation states to achieve their geopolitical goals; it has also been used to interfere with elections and to undermine the functioning and prestige of democracy more generally. For these attacks and other malicious activities, the global and open architecture of the Internet is exploited, denting faith in the capacity of the Internet to democratize information and societies. However, the reality is that the Internet can still achieve all this and more—as long as its architecture continues to remain intact.

The Internet is an irreplaceable asset for democracy as long as it remains open, global and interoperable.

This requires that state actors both understand and protect what makes the Internet work. What really matters is the Internet's design: the enduring characteristics that allow the Internet to be a useful tool at the disposal of democracies. The Internet is an irreplaceable asset for democracy as long as it remains open, global and interoperable. Anything less than that, and it can easily turn into a tool for oppression and authoritarianism.

References

- Access Now, #KeepItOn (homepage), [n.d.], <<https://www.accessnow.org/keepiton>>, accessed 21 April 2023
- Anderson, J. and Rainie, L., 'Concerns about democracy in the digital age', Pew Research Centre, 21 February 2020, <<https://www.pewresearch.org/Internet/2020/02/21/concerns-about-democracy-in-the-digital-age>>, accessed 21 April 2023
- Article 19, 'Digital Freedom: Building an Internet infrastructure that promotes human rights', 8 June 2021, <<https://www.article19.org/resources/digital-freedom-building-an-Internet-infrastructure-that-protects-human-rights>>, accessed 20 April 2023
- Ball, J., 'Facebook and Google's New Plan? Own the Internet', Wired, 10 July 2021, <<https://www.wired.co.uk/article/facebook-google-subsea-cables>>, accessed 21 April 2023
- Baran, P., 'The future of computer utility', *The Public Interest*, 8 (1967), pp. 75–87, <https://www.nationalaffairs.com/public_interest/detail/the-future-computer-utility>, accessed 21 April 2023
- Broadband Commission for Sustainable Development, 'Achieving the 2025 Advocacy Targets', [n.d.], <<https://www.broadbandcommission.org/advocacy-targets>>, accessed 20 April 2023
- Buell, M., 'Canada's Proposed Online Harms Legislation and the Internet', Internet Society, 8 November 2021, <<https://www.internetsociety.org/resources/2021/internet-impact-brief-canadas-proposed-online-harms-legislation-and-the-internet>>, accessed 21 April 2023
- Clark, D., 'The design philosophy of the DARPA Internet Protocols', *Computer Communication Review*, 18/4 (1988), pp. 106–14, <<https://doi.org/10.1145/52325.52336>>
- Coe, P., 'The Draft Online Safety Bill and the regulation of hate speech: Have we opened Pandora's box?', *Journal of Media Law*, 14/1 (2022), pp. 50–75, <<https://doi.org/10.1080/17577632.2022.2083870>>
- Connectivity Capital (with Association for Progressive Communication, Internet Society, and Connect Humanity), 'Financing mechanisms for locally owned Internet infrastructure', September 2022, <https://connecthumanity.fund/wp-content/uploads/2022/09/Financing-Mechanisms-for-Locally-Owned-Internet-Infrastructure-Updated_Sep-21-2022.pdf>, accessed 20 April 2023
- Daigle, L., Komaitis, K. and Roberts, P., 'Keys to successful collaboration in solving wicked Internet problems', Internet Society, November 2016, <<https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-Collaboration-Behavior-20161122.pdf>>, accessed 20 April 2023
- Demchak, C. and Shavitt, Y., 'China's maxim—leave no access point unexploited: The hidden story of China telecom's BGP hijacking', *Military Cyber Affairs*, 3/1 (2018), <<https://doi.org/10.5038/2378-0789.3.1.1050>>
- Dong Kwan Kim, 'How cross-sector collaboration is driving the global climate agenda', World Economic Forum, 13 January 2020, <<https://www.weforum.org/agenda/>>

- [2020/01/how-cross-sector-collaboration-is-driving-the-global-climate-agenda>](#), accessed 20 April 2023
- Economist, The*, 'China has the world's most centralised Internet system', 28 June 2018, <<https://www.economist.com/special-report/2018/06/28/china-has-the-worlds-most-centralised-internet-system>>, accessed 20 April 2023
- European Union (Eurobarometer), 'Attitudes towards the Impact of Digitalization on Daily Lives', March 2020, <<https://europa.eu/eurobarometer/surveys/detail/2228>>, accessed 20 April 2023
- Fairlie, R. W., 'Are We Really A Nation Online? Ethnic and Racial Disparities in Access to Technology and Their Consequences', 20 September 2005 (for the 'Leadership Conference on Civil Rights Education Fund'), <<http://civilrightsdocs.info/pdf/reports/nation-online/digitaldivide.pdf>>, accessed 24 April 2023
- Farrell, M., 'Your platform is not an ecosystem', Crooked Timber, 8 December 2022, <<https://crookedtimber.org/2022/12/08/your-platform-is-not-an-ecosystem>>, accessed 21 April 2023
- Gross, J., 'How Finland is teaching a generation to spot misinformation', *New York Times*, 10 January 2023, <<https://www.nytimes.com/2023/01/10/world/europe/finland-misinformation-classes.html?smid=tw-nytimes&smtyp=cur>>, accessed 20 April 2023
- Hoffmann, S., Lazanski, D. and Taylor, E., 'Standardising the splinternet: How China's technical standards could fragment the Internet', *Journal of Cyber Policy*, 5/2 (2020), pp. 239–64, <<https://doi.org/10.1080/23738871.2020.1805482>>
- Information Technology and Innovation Foundation (ITIF) 'Misguided TikTok and WeChat bans risk fragmenting the Internet economy, says ITIF' (press release), 7 August 2020, <<https://itif.org/publications/2020/08/07/misguided-tiktok-and-wechat-bans-risk-fragmenting-internet-economy-says-itif>>, accessed 20 April 2023
- International IDEA, *The Global State of Democracy 2022: Forging Social Contracts in a Time of Discontent* (Stockholm: International IDEA, 2022), <<https://doi.org/10.31752/idea.2022.56>>
- Internet Engineering Task Force (IETF), 'Human Rights Protocol Considerations (hrpc)', [n.d.a], <<https://datatracker.ietf.org/rg/hrpc/about>>, accessed 21 April 2023
- , 'Recommendations for DNS Privacy Service Operators', RFC 8932, [n.d.b], <<https://datatracker.ietf.org/doc/rfc8932>>, accessed 21 April 2023
- Internet Governance Forum (IGF), 'IGF 2022 Policy Network on Internet Fragmentation', Output document, January 2023, <https://www.intgovforum.org/en/filedepot_download/256/24127>, accessed 21 April 2023
- Internet Society, 'Internet Invariants: What really matters', 3 February 2012, <<https://www.Internetsociety.org/Internet-invariants-what-really-matters>>, accessed 21 April 2023
- , 'Internet Society submission to the "Points of Discussions towards ICT Charter from G7 Ministers"', 24 February 2016, <<https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-G7-Questionnaire-submission-20160224-1.pdf>>, accessed 20 April 2023
- , 'Huawei's "New IP" proposal—frequently asked questions', 22 February 2022, <<https://www.internetsociety.org/resources/doc/2022/huaweis-new-ip-proposal-faq>>, accessed 21 April 2023

- Iyengar, R., 'India is a trying to build its own Internet', CNN Business, 8 March 2021, <<https://edition.cnn.com/2021/03/08/tech/india-internet-homegrown-apps/index.html>>, accessed 20 April 2023
- Karthik, A., 'Draft Telecom Bill 2022: How the reform may hinder innovation & growth of Indian tech start-ups', INC42, 2 December 2022, <<https://inc42.com/resources/draft-telecom-bill-2022-how-the-reforms-may-hinder-innovation-growth-of-indian-tech-startups>>, accessed 21 April 2023
- Komaitis, K., 'The silver lining of Internet regulation: A regulatory impact assessment', Techdirt, 11 August 2020, <<https://www.techdirt.com/2020/08/11/silver-lining-internet-regulation-regulatory-impact-assessment>>, accessed 21 April 2023
- , 'Internet Fragmentation: Why it Matters for Europe', EU Institute for Security Studies, 31 January 2023, <<https://eucyberdirect.eu/research/internet-fragmentation-why-it-matters-for-europe>>, accessed 21 April 2023
- Komaitis, K. and Park, K. S., 'The global trend that could kill the Internet: Sender Party Network Pays', 22 November 2022, <<https://www.techdirt.com/2022/11/22/the-global-trend-that-could-kill-the-Internet-sender-party-network-pay>>, accessed 21 April 2023
- Kübler, R., Pauwels, K. and Manke, K., 'How Social Media Drove the 2016 US Presidential Election: A Longitudinal Topic and Platform Analysis', Working Paper, Social Science Research Network, 27 July 2020, <<http://dx.doi.org/10.2139/ssrn.3661846>>
- Lamensch, M., 'Authoritarianism has been reinvented for the digital age', Centre for International Governance Innovation, 9 July 2021, <<https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age>>, accessed 21 April 2023
- National Center for Education Statistics (NCES, US Department of Education), 'Students' Internet access before and during the coronavirus pandemic by household socioeconomic status', NCES Blog, 20 September 2021, <<https://nces.ed.gov/blogs/nces/post/students-internet-access-before-and-during-the-coronavirus-pandemic-by-household-socioeconomic-status>>, accessed 24 April 2023
- Organization for Economic Co-operation and Development (OECD), *Bridging the Digital Gender Divide: Include, Upskill, Innovate* (Paris: OECD, 2018), <<https://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf>>, accessed 24 April 2023
- Pearce, K. E. and Vitak, J., 'Performing honor online: The affordances of social media for surveillance and impression management in an honor culture', *New Media & Society*, 18/11 (2016), <<https://doi.org/10.1177/1461444815600279>>
- President of the United States (POTUS), 'Fact sheet: President Biden and G7 Leaders Formally Launch the Partnership for Global Infrastructure and Investment', 26 June 2022, <<https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment>>, accessed 21 April 2023
- Ressa, M., 'Facebook let my government target me: Here's why I still work with them', *Time*, 17 January 2019, <<https://time.com/5505458/facebook-maria-ressa-philippines>>, accessed 21 April 2023
- RIPE Network Coordination Centre, 'Response to the European Commission's Proposed NIS 2 Directive', March 2021, <https://www.ripe.net/participate/internet-governance/multi-stakeholder-engagement/ripe-ncc-response-to-nis-2-directive_march-2021.pdf>, accessed 21 April 2023

- Rohac, D., 'The EU and America are sliding into protectionism', *The Spectator*, 3 December 2022, <<https://www.spectator.co.uk/article/the-eu-and-america-are-sliding-into-protectionism>>, accessed 20 April 2023
- Salamatian, L., Douzet, F., Salamatian, K. and Linonier, K., 'The geopolitics behind the routes data travel: A case study of Iran', *Journal of Cybersecurity*, 7/1 (2021), <<https://doi.org/10.1093/cybsec/tyab018>>
- Shahbaz, A., Funk, A. and Vesteinsson, K., *Freedom House, Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet* (Washington, DC: Freedom House, 2022) <<https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-Internet>>, accessed 21 April 2023
- Surfshark, 'Internet Censorship', [n.d.], <<https://surfshark.com/research/internet-censorship/internet>>, accessed 21 April 2023
- United Nations Office of the High Commissioner for Human Rights (OHCHR), 'Moderating online content: Fighting harm or silencing dissent?', 23 July 2021, <<https://www.ohchr.org/en/stories/2021/07/moderating-online-content-fighting-harm-or-silencing-dissent>>, accessed 20 April 2023

Appendix A

OPEN SYSTEMS INTERCONNECTION

In the early days, the Internet was closely associated with the Open Systems Interconnection (OSI) model, created by the International Organization for Standardization (ISO). The OSI model provides a map for how networks should communicate with each other and, over the years, has become the universal language for computer networking, allowing communication systems to coexist. It is divided into seven abstract layers, each stacked on top of the last.

In today's inter-networked world, the OSI model provides a useful analogy and is not something that the modern Internet strictly follows (though it continues to remain useful for troubleshooting network problems). The OSI model is useful for communicating ideas, but not for implementation. However, as the Internet evolved there was the realization that the OSI model neither accurately describes nor is ideal for understanding networks.

In a nutshell, the OSI model is static, while the Internet is dynamic: it continually welcomes new services and actors. For example, in the past few years, large technology companies like Facebook and Google have invested heavily in new transatlantic cables (Ball 2021), which makes them also important participants in what would be the physical layer. Equally, telecommunications providers (DT, Telefonica, etc.) are also engaged in cloud infrastructure and other more content-oriented services. Looking at the Internet under the linear OSI model creates misconceptions about its actors, the services they provide and the role they play in the entire 'Internet stack'.

What makes the Internet's design principles a better 'way in' to understanding the present and potential future of networks—and their relationship to democracy—is the fact that, by contrast, they have not changed. Ever since the Internet consisted of just two networks (today it is thousands spread across the world) they have remained the same. By definition, the Internet can only survive if everyone buys into these principles. Otherwise, and less compatibly with democracy, there will be only networks.

Figure A.1. The Open Systems Interconnection model

7. Application layer

Human–computer interaction layer, where applications can access the network services.

6. Presentation layer

Ensures that data is in a usable format and is where data encryption occurs.

5. Session layer

Maintains connections and is responsible for controlling ports and sessions.

4. Transport layer

Transmits data using transmission protocols including TCP and UDP.

3. Network layer

Decides which physical path the data will take.

2. Data link layer

Defines the format of data on the network.

1. Physical layer

Transmits raw bit stream over the physical medium.

Source: ISO/IEC 7498-1:1994(en), Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model—Part 1, <<https://www.iso.org/standard/20269.html>>, accessed 18 April 2023.

About the author

Konstantinos Komaitis, PhD, is a veteran of developing and analysing Internet policy to ensure an open and global Internet. Konstantinos has spent almost 10 years in active policy development and strategy as a Senior Director at the Internet Society. He is currently a non-resident fellow at the Digital Forensic Research Lab of the Atlantic Council.

About International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization with 34 Member States founded in 1995, with an exclusive mandate to support and advance democracy worldwide.

WHAT WE DO

We produce comparative, policy-friendly knowledge and provide technical assistance on issues relating to elections, parliaments, constitutions, money in politics and political representation, all under the umbrella of the UN Sustainable Development Goals. We assess the performance of democracies around the world through our unique Global State of Democracy Indices and reports. Our work is expanding to address issues related to climate change and democracy.

We use our knowledge to provide technical assistance and expert advice to governments and civil society around the world. We publish books, databases, and primers annually in several languages on topics ranging from voter turnout to Indigenous peoples' rights in constitution-building. Gender equality and inclusion are mainstreamed in all our work.

We engage in conversations and convene agenda-setting dialogues and partner with like-minded organizations, including the African Union, the European Union and the United Nations, to achieve greater impact.

WHERE WE WORK

Our headquarters is in Stockholm, and we have regional and country offices in Africa, Asia and the Pacific, Europe, and Latin America and the Caribbean. International IDEA is a Permanent Observer to the United Nations and is accredited to European Union institutions.

<https://www.idea.int>



International IDEA
Strömsborg
SE-103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

The strength of the Internet lies in its original design, which in some ways mirrors democratic ideas. As with the separation of powers in a true democratic state, the architecture of the Internet has no centre of control and allows power to flow from the bottom up and even from the margins, rather than always from above. During the past few years, policymakers have directed their attention towards the top layers of the 'Internet stack', those where the effect on democracy is more easily observable. Little attention has been paid to the infrastructure of the Internet—the part that is invisible to users yet constitutes the essence of what the Internet is really about.

This paper seeks to alert democratic stakeholders to often ignored aspects of the digital threats to democracy, and to highlight the key weak spots of the Internet as an infrastructure upon which democracy itself partly rests.