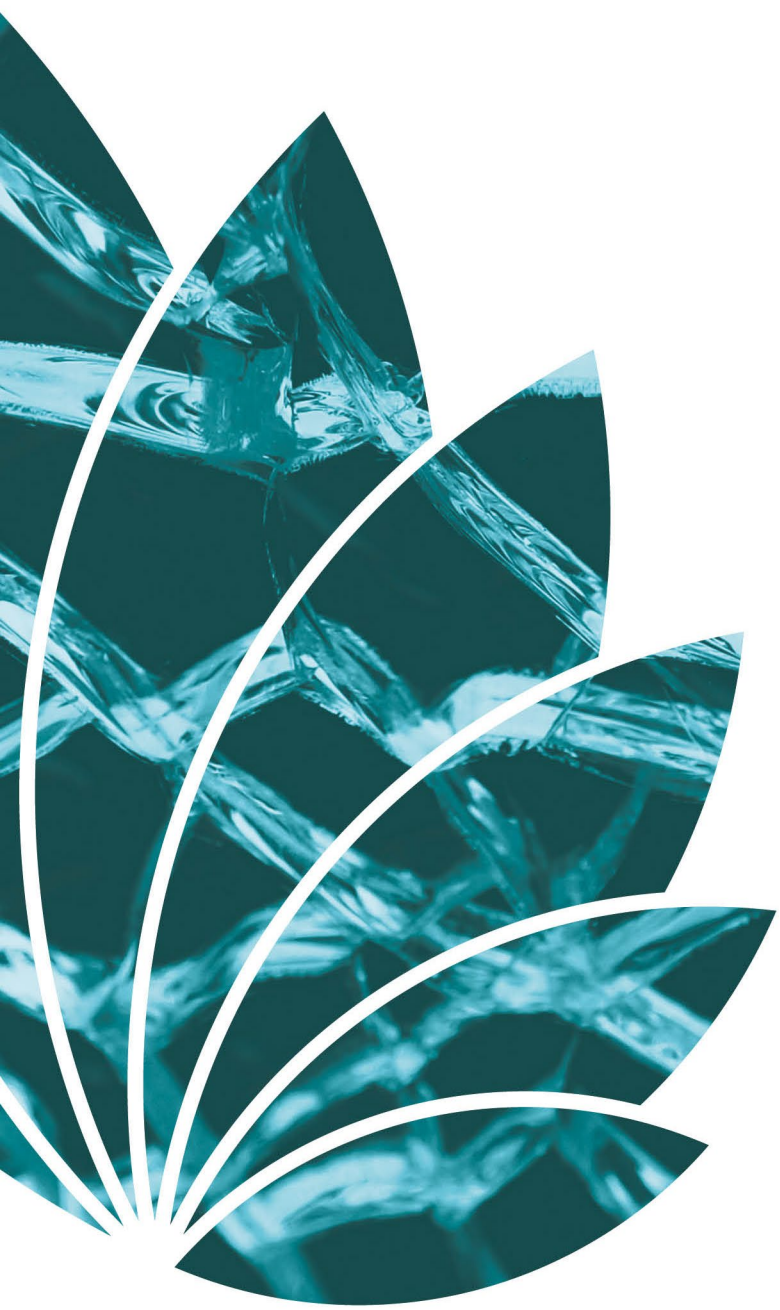
RESEARCH IN FOCUS

# Internet Fragmentation: Why It Matters for Europe

*Konstantinos Komaitis*
*January 2023*



EU CYBER DIRECT
EU Cyber Diplomacy Initiative

This publication has been produced in the context of the EU Cyber Direct – EU Cyber Diplomacy Initiative project with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or any other institution.

Cover image credits: Dominik Hofbauer/Unsplash

Implementing organisations:
EU Institute for Security Studies
Carnegie Endowment for International Peace
Leiden University

Funded by the European Union

# Contents

## Abstract

Has the world witnessed the end of the open internet? As globalisation is going through major reordering, the internet sits at the centre of how governments respond to various global challenges. The idea of an open internet has changed drastically in the past few years as states intervene more, mainly through domestic regulation. Internet fragmentation is now a reality, manifested through a combination of technical, commercial and governmental actions.

Europe's approach to fragmentation is not straightforward. Internationally, Europe is a strong advocate of an open and global internet and, in general, it invests in collaborating with partners to promote this idea. When it comes to its own policies, however, Europe is in fact contributing to fragmentation. An extremely busy legislative agenda has created the conditions for Europe to be contributing, in some ways, to a less open and more fragmented internet. The focal point of this agenda is Europe's 'digital sovereignty' approach, which, to an extent, appears to be incompatible with an open internet.

Europe has an important choice to make. What sort of internet does it want: an open, global, interoperable internet or one that is fragmented and limited in choice?


## Introduction

Has the world witnessed the end of the open, global and interoperable internet? Is the future one in which the global internet, with its openness and decentralised structure, surrenders itself to the pressures of fragmentation? What does this mean for Europe?

There is no doubt that globalisation has been going through a serious reorganisation, informed by critical global issues such as climate change, high inflation rates and an energy crisis in Europe. In recent years, the world has experienced a steady decline[1] in democracies, mainly driven by a wave of nationalism across the world that has contributed to a more inward-looking approach on the part of state actors. However, the interdependencies brought by globalisation in recent decades cannot simply be ignored. International trade of goods and services; the constant movement of people around the world, willingly or through force; and the way data traverses borders continue to command some degree of global coordination. The battle that state actors now face is how to be more autonomous and eliminate global dependencies while retaining levels of interconnectness that allow them to respond effectively to unpredictable emergencies, such as the recent Covid-19 pandemic.

The internet – the network of networks supporting all the activities that are happening in cyberspace – plays a critical role in balancing this battle. State actors have identified in the internet the tool that can allow them to stay connected, while asserting sovereignty over the way technology facilitates that. Over the years, we have seen an increase in national laws that end up creating chokepoints in the way networks are able to 'talk' to one another.[2] While the internet's architecture generally allows data to route around obstacles, this is not possible when the state decides to intervene. In this regard, there is a sense that the internet is fragmenting, breaking into smaller internets, which mainly operate as isolated islands.

Discussions about fragmentation are not new – in fact, they date as far back as the 1990s – but they became mainstream in the aftermath of Edward Snowden disclosing information regarding the US government's mass surveillance programme. Soon after his revelations, a host of governments engaged

[1] Sarah Repucci and Amy Slipowitz, Freedom in the World 2022: The Global Expansion of Authoritarian Rule, Freedom House (2022), available at: https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

[2] India is a good example here. As well as holding the top spot for the most internet shutdowns, India also requires cable ships that enter its waters to install monitoring equipment for bandwidth terminating in India, making it a chokepoint in international communications.

in conversations and policy proposals that would demand the localisation of certain types of data within jurisdictional boundaries; some went as far as to make recommendations that would allow states to interfere with the internet's traffic patterns.[3] The idea was to control communication flows in a way that would prevent possibilities for external snooping. internet fragmentation emerged as part of the political discourse to counter that narrative.[4] Fragmentation has dominated most of the internet governance discussions ever since.

Fragmentation, however, is not limited to state intervention. Over the years, other manifestations of fragmentation have emerged, both commercial and technical, and have been thought to contribute to a less global and less interoperable internet. All across the internet ecosystem, from the underlying infrastructure all the way up to applications and content, different types of fragmentation appear and provide an ununified internet experience. It is important, therefore, to be conscious of the scope of fragmentation and to be mindful of its dimensions, especially when we talk about its impact.

**Part of the complexity surrounding fragmentation is that there is no unified understanding of the term among stakeholders participating in internet governance discussions.**

Part of the complexity surrounding fragmentation is that there is no unified understanding of the term among stakeholders participating in internet governance discussions. For the technical community, fragmentation is condensed to obstacles in the internet's infrastructure that do not allow interoperation and interconnectness between networks.[5] From the private sector viewpoint, fragmentation is often seen in the form of national policies that aim towards data localisation or seem to restrict the free flow of data in any way. Finally, for civil society, fragmentation is seen through the lens of policies that aim to limit access to content or to censor certain types of content, driven by either commercial or state interests. All these interpretations are valid and important in finding solutions, but, unless they are seen as complementary, stakeholders will continue to talk past each other.

It is easy to forget the value of an open and global internet in this current climate. The international order feels less like an order and more like a continuous struggle to preserve the last traces of a peaceful world. The temptation is to look inwards, to erect more physical borders in order to retain control and diminish the uncertainty that interconnectivity brings. This, however, will only exacerbate a situation that is already fragile. If there is any chance for moving forward, it is only through collaboration. And an open internet facilitates this: it provides a common ground. Europe must resist the temptation of fragmentation and instead focus on identifying ways to pursue its own digital agenda while preserving an open internet. The following sections provide an overview of what fragmentation is, its different dimensions and why it is urgent for Europe to make a choice as to what kind of an internet it wants.

[3] Matthew Taylor, Nick Hopkins and Jemima Kiss, 'NSA surveillance may cause breakup of internet, warn experts, The Guardian (1 November 2013), available at: https://www.theguardian.com/world/2013/nov/01/nsa-surveillance-cause-internet-breakup-edward-snowden

[4] At the time of the Snowden revelations, for instance, Germany's largest telecommunications provider, Deutsche Telekom, suggested that regional traffic be routed only through domestic connections ('Deutsche Telekom hopes to hide German internet traffic from spies', Reuters, available at: https://www.reuters.com/article/germany-spying-telekom-idCNL6N0I209320131012). Although this idea never passed the stage of proposal, Europe has created a much stricter framework for the way data travels across the US. This has caused a significant problem of data flows between the two allies, and recently US President Biden signed an executive order that paves the way forward for a new EU–US data agreement (White House, 'Fact Sheet: President Biden signs executive order to implement the European Union-U.S. Data Privacy Framework', available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/).

[5] Examples here would include incompatible root zone files, DNS resolution issues, incompatibility between IPv4 and IPv6 addresses, etc.

## 1. An open cyberspace: why it matters

The common wisdom used to be that the internet would make societies more open and free. It would connect people, routing around any cultural and political obstacles, while creating new opportunities for self-expression and empowerment. It would provide people with unprecedented access to information and innovation, which, in turn, would ensure their participation in an open way.

From its early days, the design of the internet was intended to create a logical network and absorb existing heterogenous networks, while allowing them to perform independently. The idea was that the internet would act both as a set of building blocks for these networks and as the glue that keeps them together.[6] For this to happen, the internet had to be open to any device. Any computer would be able to connect to the network provided that it was willing to interoperate, something that technically would be easy to do.[7]

These features have earned the internet the title of a 'generative technology': 'a system that produce[s] unanticipated change through unfiltered contributions from broad and varied audiences'.[8] These features and adjacent protocols have remained unchanged from when the internet consisted of two networks of subscribers to today, when half of the population is online. These unfiltered contributions have introduced us to web browsers, search engines, voice over internet protocol (VoIP), real-time streaming, ecommerce, wifi, email, even our Global Positioning System (GPS) systems; they have been the main source of the unprecedented innovation that has led to today's economic growth and social empowerment.

The other important thing about the internet is that it is not a monolith, meaning that it is not – nor should it be viewed as – 'one' thing. It is in constant transition, which is driven by a host of actors (the private sector, governments, the technical community, civil society and academia). Part of this transition involves the user-faced experience. This is the place where content exists through web-based applications, mobile applications and application stores. The Internet of Things (IoT) and standard-based software also proliferate there. However, this is also the place where social threats appear and trigger discussions about state intervention. Often these social threats are perceived as 'internet threats', creating the conditions for internet fragmentation.

From a technical standpoint, the original shared vision guiding the internet's development was that every device on the internet should be able to exchange data packets with any other device that was willing to receive them. This degree of interoperability has nurtured an internet that we consider to be organic, unfragmented and open. The internet is a distributed system – an ecosystem of multiple, overlaying networks, devices, applications, people, and commercial and governmental interests. But, most fundamentally, it has some invisible attributes, otherwise known as 'invariants'[9] due to the fact that they don't change even as the internet continues to evolve. These are as follows.

- The internet has a global reach and integrity, and is not constrained in terms of supported applications and services.
- The internet is for everyone – there is no central authority that designates or permits different classes of internet activities.
- The internet requires some basic agreements and social behaviour between technologies and between humans.

[6] Neil Randall, *The Soul of the Internet* (London: Thomson Learning, 1997).
[7] Brian Carpenter, 'Architectural principles of the internet' (1996), available at: https://www.rfc-editor.org/rfc/rfc1958
[8] Jonathan Zittrain, *The Future of the Internet and How to Stop It* (Yale University Press, 2008).
[9] 'Internet invariants: what really matters', Internet Society (2012), available at: https://www.internetsociety.org/internet-invariants-what-really-matters/

- Although no specific technology defines the internet, there are some basic characteristics that describe what works.
- And, finally, the more the internet stays the same, the more it changes.

The idea that the internet is open and global has a profound and far-reaching impact. The internet provides significant economic benefits and the potential to enhance social welfare for people around the world. It introduces new ways for people to communicate, express and participate; it opens up new access channels to services and products and provides unprecedented access to a wealth of knowledge and information. The benefits the open internet provides are considerable for everyone, including marginalised and vulnerable communities, who often are the least connected. According to the International Telecommunications Union (ITU) Global Connectivity Report,[10] 'universal and meaningful connectivity' to the internet 'has become the new imperative for the 2020–2030 decade'.

Today the internet is, generally, global; at least, the infrastructure that supports it is. 'At the networking layer, it is mostly true that the internet has global reach: in principle, it is still true that any endpoint can send packets to any other end point.'[11] In practice, however, technical, political and commercial behaviours impair the internet's capability for global reach, causing fragmentation.

The following section provides an overview of fragmentation and its impact.

## 2. Defining fragmentation and its impact

Internet fragmentation must be seen both as a driver and as a reflection of an international order that is increasingly growing fragmented. For instance, the effort by the US government in recent years to ban[12] TikTok, the Chinese video app, is one of the multiple manifestations of this observation: growing tensions between the US and China result in a less global internet. The same applies to all other geopolitical tensions, whether regional or international.

From a governance perspective, fragmentation is an existential threat to the global internet. This threat puts global coordination and collaboration at the heart of this debate. 'Differences in the Internet across borders are predictive of international trade and military relations', according to research[13] undertaken as part of the University of California, Berkeley's Daylight Security Research Lab. In fact, according to some,[14] the debate about internet fragmentation is, in reality, a debate about sovereignty in the digital world. It is no longer just about the internet: it is about the global order and what role governments should have in it.

This is why discussions about fragmentation often lead to discussions about an open internet: if the internet is fragmented, then, de facto, it is not open.

Just like 'fragmentation', 'openness' is a term that is often used in an all-inclusive manner and, generally, it means different things to different people. At its most basic level, it refers to the ability of anyone to participate in the internet ecosystem. For the technical community, it refers to an 'architecture that creates common interoperable services, which deliver fast and permissionless innovation everywhere. The inclusive standardisation process and demand-driven adoption ensures that useful changes are

[10] Global Connectivity Report, International Telecommunications Union (2022), available at: https://www.itu.int/itu-d/reports/statistics/2022/05/29/gcr-chapter-1/

[11] Leslie Daigle, The Internet Invariants: The Properties Are Constant, Even as the Internet Is Changing (2019), available at: https://www.thinkingcat.com/wordpress/wp-content/uploads/2020/08/2019-InvariantsUpdated.pdf

[12] In the US, there is a renewed call for the banning of TikTok, which started during the Trump administration. Bethany Allen-Ebrahimian, 'FCC Commissioner says government should ban TikTok', Axios (2022), available at: https://www.axios.com/2022/11/01/interview-fcc-commissioner-says-government-should-ban-tiktok

[13] Nick Merrill and Steve Weber, 'Website blocking as a proxy of policy alignment' (2020), available at: https://daylight-lab.github.io/blocking-proxy-paper/writeup.html

[14] Milton Mueller, Will the Internet Fragment? Sovereignty, Globalization and Cyberspace (Cambridge: Polity Press, 2017).

adopted, while unnecessary ones disappear.'[15] On the other hand, from an economic perspective, it refers to the ability of users to access the internet and use it to advance their opportunities within digital markets. According to the Organisation for Economic Cooperation and Development (OECD), 'economic openness increases as broadband infrastructure grows, but it decreases when access providers lack competition and charge higher prices or provide poor service as a result'.[16] Finally, social openness is achieved when users are free to form communities and access information in non-preventative and non-limiting ways. Social openness is similar to empowerment.

It is the sum of all these aspects that makes openness such a crucial feature of the internet. Anything that constraints the openness of the internet – technical, economic and socio-political – is part of what we generally refer to as internet fragmentation. This is also one of the conclusions reached in a 2016 report[17] commissioned by the World Economic Forum (WEF). The report establishes the scope of fragmentation under three broad categories, which reflect how we tend to think of openness.

- *Technical* fragmentation refers to 'the conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points'.
- *Governmental* fragmentation refers to 'policies and actions that constrain or prevent certain uses of the Internet to create, distribute or access information resources'.
- *Commercial* fragmentation refers to 'business practices that constrain or prevent certain uses of the Internet to create, distribute or access information resources'.

When people connect to the internet, the expectation is that they connect to the global internet – not a restricted version. For example, policies that lead to filtering or blocking certain types of content, data localisation policy objectives and corporate control of large systems of content and messaging all constitute instances where fragmentation occurs, or the probability that it will occur increases.

On this basis, the impact of fragmentation differs depending on where exactly in the internet 'stack' it occurs and what type of fragmentation takes place each time. Imagine, for instance, that data flows were to be prohibited or that, due to governmental intervention, alternative root servers were to emerge. The impact would be felt widely across most – if not all – users, while processes and transactions would have to be re-evaluated to deal with the disruption. In the meantime, there might be instances where fragmentation was more focused, thus impacting only a certain number of actors and/or processes. For instance, the terms and conditions set by app stores and the way they 'lock' users within their 'walled gardens' should be considered as fragmentation, but its effect is limited to the users of these app stores.

Because of its multiple dimensions, it is generally difficult to measure the impact fragmentation has. The first problem is that fragmentation is not instantaneous; instead, it tends to become systemic over years as policies and processes create the conditions for it. The second problem is that it is users who will always feel fragmentation's true impact. A fragmented internet provides the means for better control over what users can see and access. This in turn can lead to disinformation, global separation and more

[15] 'The internet way of networking: defining the critical properties of the internet', Internet Society (2020), available at: https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/

[16] Economic and Social Benefits of Internet Openness (Paris: OECD, 2015), available at: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2015)17/FINAL&docLanguage=En. As of the writing of this report, a debate in Europe could lead directly to less economic openness. The Sending-Party-Network-Pays (SPNP) proposal, which is being considered in the European Union, will probably lead to a less open internet, resulting in some form of fragmentation.

[17] William J. Drake, Vinton G. Cerf and Wolfgang Kleinwächter, Internet Fragmentation: An Overview (Cologny: World Economic Forum, 2016), available at: https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

government control. For example, if one were to compare the internet experience of Chinese users with that of their European counterparts, the differences are substantial.

The loss of trust is another, significant parameter of fragmentation. Generally, much of the internet's day-to-day operation is based on trust. One of the sayings about the internet is that it is a reliable whole based on unreliable parts; in other words, it is fragile, but trust makes it resilient. In fact, the whole system that ensures that traffic is routed around the internet properly is based on trust, or an 'honour code'[18] of the internet. Fragmentation not only breaks this trust but it also capitalises on it by creating the necessary circumstances for more control over the way traffic flows. Fragmentation raises barriers to entry, exacerbating the costs of running a business and resulting in companies leaving digital markets.

There is also a security risk caused by internet fragmentation. The challenge with cybersecurity is that it is a so-called 'wicked problem'. Cybersecurity is 'transboundary in nature, occurs at multiple levels across sectors, between institutions, and impact[s] all actors, both public and private, in complex, interconnected, and often highly politicised ways'.[19] Wicked problems tend, in general, to be extremely complex and require collaboration, focus and, often, the crossing of boundaries to get resolved.[20] As a political problem, cybersecurity sits at the intersection of the evolution of the internet and its strategic and political use by state and non-state actors. A fragmented internet prevents any possible opportunity to address cybersecurity because it dismisses the many interdependent factors and closes down the venues for any potential collaboration.

**A fragmented internet prevents any possible opportunity to address cybersecurity because it dismisses the many interdependent factors and closes down the venues for any potential collaboration.**

People in countries where the internet is fragmented can become hostages to their governments' geopolitical aspirations as they determine what should or should not be available. In an internet that is less open, governments can 'lead' people to follow certain agendas, breaking the necessary levels of trust that are paramount for a functioning democracy.

## 3. Dimensions of fragmentation

It is generally difficult to sketch the exact dimensions of fragmentation. As state actors continue to retreat from globalsation, the threats against the open and global internet continuously change and evolve. However, over the years, a set of actions have been identified[21] that we know contribute to a fragmented internet ecosystem. These actions neither are conclusive nor should be seen as such; it is also impossible to place them concretely under the microscope without a proper examination of the legal framework they are part of. However, they are instructive as to how policymakers should be approaching internet openness.

[18] Craig Timberg, 'Net of insecurity: the long life of a quick fix', Washington Post (31 May 2015), available at: https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/

[19] Madeline Carr and Feja Lesniewska, 'Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance', *International Relations* 34 (3) (2020), 391–412.

[20] Leslie Daigle, Konstantinos Komaitis and Phil Roberts, 'Keys to successful collaboration and solving wicked problems', Internet Society (2016), available at: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-Collaboration-Behavior-20161122.pdf

[21] Jonah Force Hill, Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for US Policy Makers (Harvard, MA: John F. Kennedy School of Government, 2012), available at: https://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf

## 3.1 The threat to the Domain Name System (DNS)

The DNS is the glue that holds the global internet together and is responsible for translating internet protocol (IP) addresses to user-friendly alphanumeric domain names. Management and coordination functions of the DNS are performed by the Internet Corporation for Assigned Names and Numbers (ICANN). Any attempt by any actor to set up alternative root serves apart from ICANN will cause fragmentation; users, where such alternative root servers exist, will be severed from the global internet. For instance, a few years ago, the Digital Object Architecture (DOA) proposal emerged at the ITU and was seen as potentially threatening to the DNS.[22] Similarly, Europe's Network and Information Systems (NIS) 2 Directive is feared to undermine the functioning of the global DNS.[23]

## 3.2 The slow transition from IPv4 to IPv6 addresses

The IPv4 address space has been exhausted[24] for quite some time now.[25] If countries do not promote, and businesses do not proceed to, IPv6 deployment, there is a chance that users will not be able to access some new services and apps. We could have an 'IPv6 internet' that is fragmented from the legacy 'IPv4 internet'. Even though there is a steady increase in the adoption of IPv6 addresses, there is still a long way to go. 'Just 32 economies have IPv6 adoption rates above the global average of 30%. Regionally, the level of IPv6 adoption appears to be highest in South Asia, North America and Western Europe, and the lowest adoption rates are in Africa and the Pacific (Oceania).'[26] In the future, ensuring the global deployment of IPv6 addresses will be key for maintaining a global internet.

## 3.3 Internet content blocking and/or filtering

In the simplest case, some amount of internet fragmentation results from countries' inconsistent filtering of content based on their own definition of what constitutes permissible speech. Governments are deploying a variety of technical and legal tools to block websites and platforms and to remove online content. Using tools such as DNS filtering, IP blocking, distributed denial of service (DDoS) attacks and search result removals, governments are changing the way users connect to and participate in the global internet. China provides the most obvious example, with a sophisticated filtering system that can control which content users are exposed to. However, content blocking also occurs through other policy objectives, for example copyright or child sexual abuse material (CSAM), and it is widely deployed also in democracies.[27]

## 3.4 Breakdown of peering agreements and interconnection

As mentioned, the internet is a 'network of networks' that interconnects using open standards. Historically, in the internet, payments have been negotiated through bilateral peering agreements. There can be cases, however, where large internet service providers (ISPs) discriminate against competing services or prioritise certain types of data. This could limit the types of applications and

[22] Chip Sharp, 'Overview of the Digital Object Architecture (DOA)', Internet Society (2016), available at: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-DOA-Overview-20161025-A4-3_0.pdf

[23] 'ICANN org comments on the Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the EU, repealing Directive (EU) 2016/1148 (NIS 2 Directive)', available at: https://www.icann.org/en/system/files/files/icann-org-comments-proposed-nis2-directive-19mar21-en.pdf

[24] APNIC, 'IPv4 exhaustion details', available at: https://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details/

[25] RIPE NCC, 'The RIPE NCC has run out of IPv4 addresses', available at: https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses

[26] Geoff Huston, 'The transition to IPv6: Are we there yet?', APNIC (2022), available at: https://blog.apnic.net/2022/05/04/the-transition-to-ipv6-are-we-there-yet/

[27] Paul Bischoff, 'Internet censorship 2022: a global map of internet restrictions' (2022), available at: https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/; see also 'Internet Society perspectives on internet content blocking: an overview' (2017), available at: https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

services users see, based on the ISP to which they subscribe. This is a type of internet fragmentation. The renewed infrastructure and network fees debate, currently taking place in Europe, provides a clear example. The European Commission is considering ideas that will effectively change the interconnection market in Europe and will impose new obligations on the way peering agreements are negotiated.[28] Experience from South Korea indicates that such unwarranted changes create an internet ecosystem that tends to be burdensome, expensive and of low quality; ultimately, they create an internet that nobody wants to use.[29]

## 3.5 Data localisation practices

Whether motivated by concern for citizens' privacy, protection from foreign surveillance or their own access to data for law enforcement purposes, countries are increasingly placing geographic restrictions on domestic businesses' storage and transfer of data. While increased legal protections for personal data may be a necessary part of the solution to the online privacy problem, if many countries adopt their own unique privacy requirements, every company operating on the internet could potentially be subjected to a multiplicity of inconsistent laws. If companies are unable to meet each country's differing requirements, because those requirements conflict with one another or because of added costs associated with meeting multiple, disparate rules, businesses may pull out of particular markets, affecting user experience and contributing to a fragmented internet. Data localisation laws are particularly evident in China, Russia and India, with countries in Africa (e.g. Nigeria) and the Asia Pacific region (e.g. Indonesia, Brunei) also having strict data localisation polices. Europe's GAIAx[30] cloud initiative and its Data Governance Act and Data Act respectively[31], all point towards the localisation of data.[32]

## 3.6 'Walled gardens'

There is nothing new about the attempt to 'lock' users in a proprietary environment. In the United States, Prodigy, CompuServe and America Online did just that in the 1980s and 1990s, confining users to ecosystems that, unlike the internet, were not open. Over the years, however, there was a significant shift as companies started to realise the benefits of more open spaces. The walls fell and more services emerged. In recent years, this has again changed. Users increasingly accessing the internet via their mobile devices have generated app stores as a new frontier, where new walls have been erected. At the same time, economies of scale have made some companies the only gateways to the internet; these companies also offer a 'walled garden' experience. For example, according to Nobel Peace prize winner Maria Ressa, in the Philippines, 'Facebook is essentially the Internet'.[33]

## 3.7 Failure of internet standards processes

Over the past few years, governments have shown more interest in standard creation processes, placing the organisations that design the internet's technical standards under threat. Some governments,

[28] Konstantinos Komaitis, 'Europe's risky plan for the internet', Directions Cyber Digital Europe (2022), available at: https://directionsblog.eu/europes-risky-plan-for-the-internet/

[29] Kyung Sin Park and Michael R. Nelson, 'Korea's challenge to the standard internet interconnection model', Carnegie Endowment for International Peace (2021), available at: https://carnegieendowment.org/2021/08/17/afterword-korea-s-challenge-to-standard-internet-interconnection-model-pub-85166

[30] Olaf Kolkman and Andrei Robackevsky, 'Technical architecture of the GAIA-X project', Internet Society (2021), available at: https://www.internetsociety.org/resources/2021/internet-impact-brief-technical-architecture-of-the-gaia-x-project/

[31] Luca Bertuzzi, "Is data localization coming to Europe", The International Association for Privacy Professionals (23 August 2022), available at: https://iapp.org/news/a/is-data-localization-coming-to-europe/

[32] 'Internet way of networking use case: data localization', Internet Society (2020), available at: https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/

[33] Maria Ressa, 'Facebook let my government target me. Here's why I still work with them', Time (17 January 2019), available at: https://time.com/5505458/facebook-maria-ressa-philippines/

especially those of China[34] and Russia,[35] suggest that these organisations, which have been responsible for the internet's core standards and protocols since the 1980s, are unaccountable and discriminate against non-American companies; such suggestions, however, cannot stand the reality of the internet. In the internet, anyone can participate in the creation of standards and anyone can voluntarily adopt them. Recently, however, we have experienced some efforts to take the standards-making power out of the hands of (internet) institutions and place them into fora that are top-down and multilateral in nature. In recent years, China has been advancing on this front by creating native technologies that reflect its own national policies and politics.[36]

Some of these threats are more immediate than others, some are self-inflicted by governments and commercial actors and some are more existential. The fact, however, is that the idea of an open and global internet is progressively deteriorating and the internet itself is changing. Governments, in most cases without realising it, are making changes to the internet that contribute to its fragmentation. Some of these changes are driven by legitimate concerns such as privacy or competition and, normally, with time and through collaboration they tend to be of minimal impact. The General Data Protection Regulation (GDPR) is a good example: although in the beginning it created the conditions for many companies to stop showing their content to European users,[37] over time and, due to its widespread influence, they have managed to find ways to comply with the legislation. Other changes are more direct; South Korea's action on interconnection charges is a good example, especially considering the impact it has had already in the country's internet ecosystem.[38] Europe has a lot to lose from a fragmented internet.

The following section will identify what exactly fragmentation could mean for Europe and its internal market.

## 4. What does fragmentation mean for Europe?

When it comes to internet fragmentation, Europe finds itself at an inflection point. Its ambitious 2030 Digital Targets[39] insist on the ability for 'everyone [to] have access to the Internet'. Moreover, in 2015, the European Union enshrined into law[40] its commitment for an open internet by declaring that 'Internet traffic shall be treated without discrimination, blocking, throttling or prioritization'. Internationally, the European Commission has repeatedly stated its unyielding support for the open and global internet

[34] Luca Bertuzzi, 'China rebrands proposal on internet governance, targeting developing countries', Euractiv (6 June 2022), available at: https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/

[35] Ewen MacAskill, 'Putin calls internet a "CIA project" renewing fears of web breakup', The Guardian (24 April 2014), available at: https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia

[36] Stacie Hoffmann, Dominique Lazanski and Emily Taylor, 'Standardizing the splinternet: how China's technical standards could fragment the Internet', *Journal of Cyber Policy* 5 (2) (2020), 239–264.

[37] Konstantinos Komaitis 'GDPR: going beyond borders', Internet Society (2018), available at: https://www.internetsociety.org/blog/2018/05/gdpr-going-beyond-borders/

[38] Konstantinos Komaitis and K.S. Park, 'The global trend that could kill the Internet: the Sending-Party-Network-Pays', TechDirt (2022), available at: https://www.techdirt.com/2022/11/22/the-global-trend-that-could-kill-the-internet-sender-party-network-pays/

[39] European Commission, 'Europe's Digital Decade: digital targets for 2030', available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[40] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2015%3A310%3ATOC&uri=uriserv%3AOJ.L_.2015.310.01.0001.01.ENG

and, most recently, along with the United States and other international partners, it signed a declaration[41] for an internet future that is open, global and interoperable.

At the same time, however, the increasing number of legislative proposals on Europe's agenda seem to create conditions that contribute to a less global and less open internet. Some regulatory initiatives, such as the Digital Services Act (DSA) package or the GDPR, attempt to harmonise internet regulation across the EU and any fragmentation they cause should generally be regarded as unintentional, which makes it easier to address. There are some other proposals, though, mainly driven by Europe's 'digital sovereignty' rationale, where the threat of fragmentation is more tangible.

The DNS4EU initiative is one such example. As part of its cybersecurity agenda, the EU has recommended the creation of a public European DNS resolver service, which, if not implemented properly, could lead to a fractured DNS.[42] Another example is the proposal for a "fair share", which would require content providers to pay telecommunications operators for the traffic they carry on their behalf. If this proposal proceeds it is likely to lead to the breakdown[43] of peering agreements and reorder the entire interconnection market, as identified above. Finally, the Network Information Security (NIS 2) Directive may constitute the most glaring threat to fragmentation to date. The proposed directive has an overwhelmingly broad scope and an expansive territorial reach (extra-territorial effect). In essence, Europe is claiming jurisdiction over all network information services anywhere in the world, and this is a big bet that, at the minimum, could restructure the entire DNS[44] or, worse, encourage other governments to reciprocate, 'which would significantly complicate the operation of a fundamental component of the internet's global infrastructure – infrastructure that has been extremely resilient, reliable and secure throughout the history of its operation under current conditions'.[45]

> **Moving forward, Europe must make a choice as to what sort of internet it wants: an open, global, interoperable internet or one that is fragmented and limited in choice?**

Europe, therefore, is at a crossroads. It can be a catalyst for positive change, or it can create obstacles that contribute to a fragmented internet. Moving forward, Europe must make a choice as to what sort of internet it wants: an open, global, interoperable internet or one that is fragmented and limited in choice?

A recent study,[46] commissioned by the Panel for the Future of Science and Technology (STOA), identified three options for Europe. The first is maintaining the status quo. Under this option, Europe views both the internet and its own digital market as structures that are strong enough to resist fragmentation. The second option would see Europe embracing fragmentation. In this case, Europe could decide to align its own national 'digital sovereignty' agenda with a fragmented internet, in which case it would be easier to justify some of its own policy initiatives.

[41] U.S. Department of State, 'Declaration for the Future of the Internet', available at: https://www.state.gov/declaration-for-the-future-of-the-internet

[42] Geoff Huston, 'Some thoughts on DNS4EU – the European Commission's intention to support the development of a new European DNS resolver', CircleID (2022), available at: https://circleid.com/posts/20220213-some-thoughts-on-dns4eu-new-european-dns-resolver

[43] Komaitis and Park (see note 37 above).

[44] 'ICANN org comments' (see note 23 above).

[45] 'RIPE NCC Response to the European Commission's Proposed NIS 2 Directive', available at: https://www.ripe.net/participate/internet-governance/multi-stakeholder-engagement/ripe-ncc-response-to-nis-2-directive_march-2021.pdf

[46] Clément Perarnaud, Julien Rossi, Francesca Musiani and Lucien Castex, *Splinternets: Addressing the Renewed Debate on Internet Fragmentation* (Brussels: European Parliament, 2022), available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729530

Finally, in the third option, Europe would fight the entire fragmentation trend and proceed to rule-making through the lens of the global and open internet.

The three options have different levels of risks. The reality is that Europe does not have the option to stay active by merely supporting the current status quo. As the STOA study correctly mentions, 'Russian and Chinese initiatives, combined with a deteriorating international climate for upholding an open and global multi-stakeholder process, will inevitably place fragmentation on the agenda, either as an opportunity or as a risk.'[47] At the same time, its own wave of legislation demonstrates Europe's departure from the idea that the internet does not require state intervention. In the same vein, embracing fragmentation carries considerable tradeoffs that Europe might not be willing or ready to make. Fragmentation will certainly contribute to the deterioration of user experience in Europe and the disruption of its internal market, jeopardise its relationships with international trade partners and foster a potentially weak cybersecurity environment.[48]

Fighting fragmentation, therefore, appears to be the only *real* option for Europe. This option entails internal and external policies that are supportive of the open and global internet. Nevertheless, Europe faces the unique challenge of identifying ways to do that without compromising its own digital agenda.

## 5. Fighting fragmentation

Fragmentation is not an alternative. Europe should not opt for a top-down approach that could lead to an internet that is broken into smaller, unconnected and uncoordinated networks. For both security and economic reasons, building virtual walls is not the answer, while artificial regulation only adds to the pressure caused by fragmentation.

The first way to avoid fragmentation is by continuing to support and embrace the collaborative approach to internet governance, whereby stakeholders work together towards determining the internet's future. The ability of multiple actors to collaborate is at the core of how the internet works and can evolve. '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 that works is collaboration, both in exchanging and carrying traffic from other networks, and in solving problems that may have originated several hops away.'[49] The internet is transnational, and the processes Europe follows in creating internet regulation should reflect that. Europe has already set the global trend on regulation with the GDPR and the DSA package, but it has done so in isolation. As more jurisdictions begin to embrace the opportunity of regulating the internet extraterritorially, Europe has the opportunity to lead a collaborative effort that will ensure more streamlined policies. Creating policy hubs and processes that allow collaboration is very important in this case.

> **“**
>
> **The internet is transnational, and the processes Europe follows in creating internet regulation should reflect that. Europe has already set the global trend on regulation with the GDPR and the DSA package, but it has done so in isolation.**

An additional thing Europe can do is to become more mindful of how regulation may impact the internet. In order for any regulatory process to be effective, it needs to go through an impact

[47] Ibid.
[48] Ibid.
[49] Olaf Kolkman, 'Internet is all about collaboration, Internet Society (2015), available at: https://www.internetsociety.org/blog/2015/04/internet-is-all-about-collaboration/

assessment; it should be no different for the internet.[50] Impact assessments constitute a tested way to bring together the multitude of actors that are required in designing, implementing and monitoring any improvements in the regulatory system. Whether fragmentation is intentional or an unintended consequence, policies must be proportional, focused, consistent and predictable. To this end, there are some questions that Europe should ask when designing regulation, especially as EU institutions seek to find the balance between an open internet and regulation. Does the proposed new rule solve the problem? Does it balance problem reduction with fragmentation? Does it result in a fair distribution of the costs and benefits across all actors participating in the internet? Is it legitimate, credible and trustworthy? Does the regulation create any consequences for the open and global internet? For example, the European Commission should require that impact assessments are carried out as part of the regulatory process, with a focus on how the proposed legislation potentially undermines the open character of the internet.

International law, especially on human rights and trade, can provide another way to try to bridge the gap between the need to maintain an open internet and national regulation. International legal frameworks establish degrees of collaboration, which can be further advanced in the case of the internet. As mentioned above, the internet is a human technology; the ability to participate, express and create is integrated in the way it was designed and has evolved. Approaching internet fragmentation from a human rights perspective means that 'Internet unity derives from fundamental rights, such as freedom to access information, and asserts that any limitation to that right must be… necessary in a democratic society.'[51]Europe should ensure that all its proposed internet regulation is founded on human rights and the principle of proportionality. The EU should work with international organisations, and especially the Human Rights Council, to strengthen the human rights framework and the way it applies in the internet. The World Summit on the Information Society (WSIS) review in 2025 could also be used as an opportunity to solidify the open internet.

In a similar vein, a number of trade agreements[52] include language that points to a commitment to an open internet and negating any policies, such as data localisation, that could encourage fragmentation. Such agreements are predominantly bilateral or regional but they constitute a significant building block towards reaching global consensus for an open internet. As Europe negotiates free trade agreements, past ones can serve as a model and propose rules regarding the ban on tariffs and discrimination policies against foreign digital products, protection against unfair requirements to transfer source code to governments and policies against data localisation. Europe should also lead the open internet agenda and work through the World Trade Organization (WTO).

The final point is that Europe must reembrace interoperation and its benefits. This means commitment to the idea of open standards and their voluntary adoption. Since the early days of the internet, open standards have ensured that the internet continues to evolve in ways that are not necessarily restricted to any political or commercial interest:

> The Internet is the result of a market-based discipline that reflects consumer preference which itself guides the actions of producers of digital goods and services. Consumers may not necessarily want to avail themselves of every possible service all the time, but the aggregate of these consumer choices is for every service, and every service provider wants

[50] Konstantinos Komaitis, 'The silver lining of internet regulation: a regulatory impact assessment', TechDirt (2020), available at: https://www.techdirt.com/2020/08/11/silver-lining-internet-regulation-regulatory-impact-assessment/; the Internet Society has also produced an impact assessment toolkit that could help policymakers make better regulatory assessments. The toolkit is limited to addressing potential issues with technical fragmentation rather than covering its different variations. For more information, see: https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

[51] Ibid.

[52] For example, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTTP) and the United States–Mexico–Canada Agreement (USMCA) both include language for an open internet.

> to have their service accessible to every consumer. A coherent networking environment exhibits the same behaviors all the time, with consistent access to all servers and displaying the same service outcomes for all consumers. Both producers and consumers can assume universal access capabilities.[53]

The Digital Markets Act (DMA), which has interoperability at its core, is a good starting point for creating more competition, which is crucial for interoperation to work. Ensuring the proper implementation of the DMA, therefore, becomes important. Moreover, Europe should continue to support open standard processes, e.g. the Internet Engineering Task Force (IETF), and resist any attempts to move such discussions under the auspices of intergovernmental organisations, including the ITU.

**Europe must also adopt a more assertive foreign policy against other international players who challenge the open and global internet. As important as it is to have domestic policies and infrastructure that support the open internet, it is equally important to support other nations in their need to do the same.**

Finally, Europe must also adopt a more assertive foreign policy against other international players who challenge the open and global internet. As important as it is to have domestic policies and infrastructure that support the open internet, it is equally important to support other nations in their need to do the same. For instance, Europe should invest in infrastructure aid that facilitates internet connectivity in places where such connectivity continues to be scarce. Initiatives such as the EU-Africa Global Gateway Investment Package[54] should expand to other regions to help them with the prioritisation, programming and implementation processes related to infrastructure cooperative projects. Europe should form a much-needed digital foreign policy strategy, and an unfragmented internet should be at its core.

One of the key points about fragmentation is that it has multiple faces: it can occur through identifiable and not so identifiable threats; it keeps changing. The expectation, therefore, should not be that these recommendations will expunge internet fragmentation. Europe also must realise that, if it continues to advocate for an open internet, its policies must be reflective of this. The work should start at home, but internationally Europe should approach internet fragmentation as an important foreign policy issue.

## 6. Conclusion

In a recent report,[55] the Council on Foreign Relations (CFR) declared that 'the era of the global Internet is over' and that the United States should abandon its long-standing vision of an open and global internet. Driven by the geopolitical challenges posed by China and Russia, which use the open internet more as a weapon, the report argues, the United States should instead turn its attention to how to respond to these challenges.

Indeed, Russia's and China's behaviour creates the temptation for Europe to do the same and attempt a more controlled internet. The fact is, however, that there is no such thing as a 'controlled internet', at

[53] Geoff Huston, 'Reexamining internet fragmentation', CircleID (2022), available at: https://circleid.com/posts/20220926-reexamining-internet-fragmentation

[54] European Commission, 'EU-Africa: Global Gateway Investment Package', available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway/eu-africa-global-gateway-investment-package_en

[55] Nathaniel Fick, Jami Miscik, Adam Segal and Gordon M. Goldstein, Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet, Council of Foreign Relations (2022), available at: https://www.cfr.org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

least in the way China or Russia projects it. That is not the internet; it is just another form of networking. It is not where development, innovation and opportunities take place.

The tools to fight against fragmentation are already at Europe's disposal. It has generated a global conversation about internet regulation and, to this end, showing it can also achieve a balance between regulation and an open internet could give Europe a leading role. Moreover, Europe should create better processes for how to engage more substantively with different actors. The multi-stakeholder model is in place and Europe has the opportunity to shape it firmly in internet policy. Europe should also use and strengthen, where appropriate, the application of international law, especially human rights law, in cyberspace. And, finally, Europe must continue to support open standards development processes and recommit to interoperation. The alternative is isolation, as a fragmented internet effectively means seclusion.

The internet is resilient only insofar as its minimum set of norms are respected. Openness is one such norm. A fight for an open, unfragmented internet is a worthy one. Europe has shown again and again its commitment to its democratic values and its wish to foster environments that promote them. The internet is one such environment.

## About the author

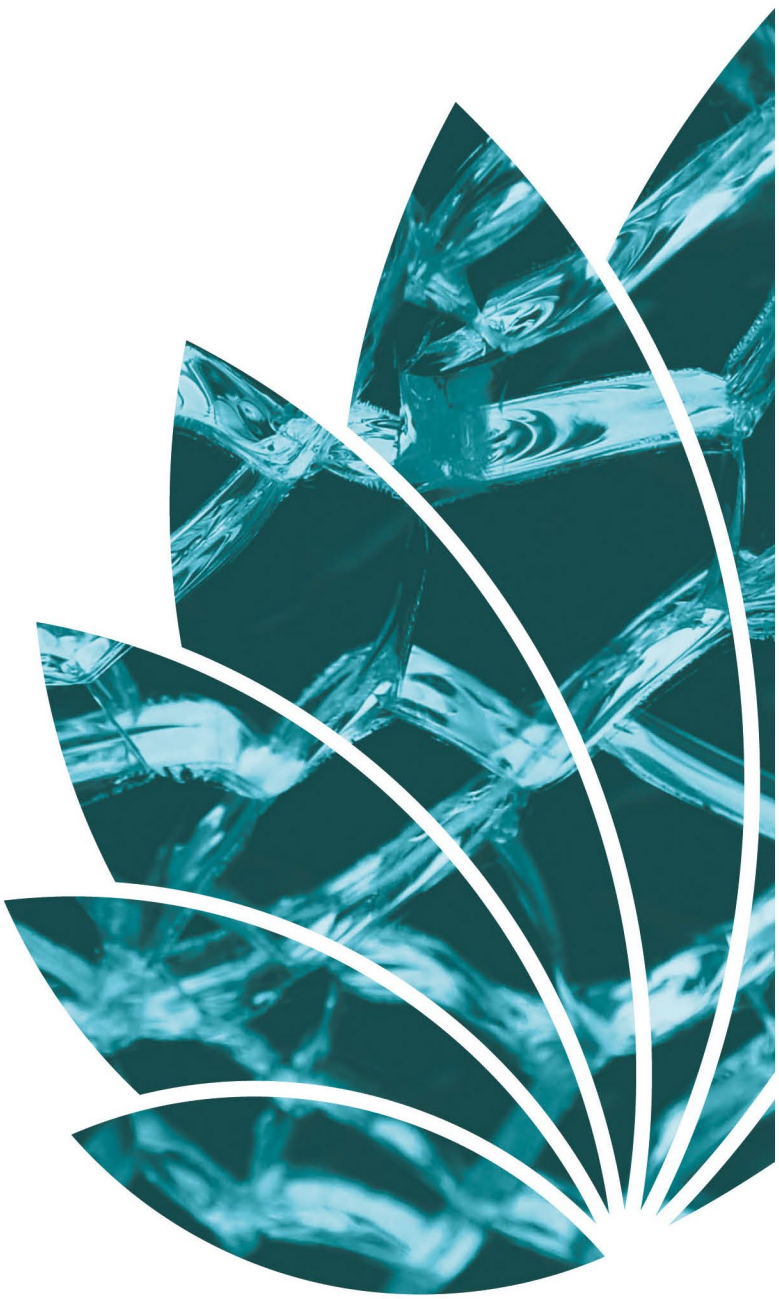
**Konstantinos Komaitis** is a veteran of developing and analysing Internet policy to ensure an open and global Internet. He worked in active policy development and strategy as a Senior Director at Internet Society and as a senior lecturer at the University of Strathclyde, UK, where he was researching and teaching Internet policy. Now, he is a non-resident fellow and a senior researcher at the Lisbon Council. He is also a non-resident fellow at Tallinn University of Technology.

## About EU Cyber Direct

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner counties and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.



EU CYBER DIRECT

This project is funded by the European Union.