CYBERDEFENSE REPORT

One, Two, or Two Hundred Internets?
The Politics of Future Internet Architectures

Kevin Kohler

Zürich, August 2022
Center for Security Studies (CSS), ETH Zürich

Available online at: css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Kevin Kohler

ETH-CSS project management: Stefan Soesanto, Project Lead Cyberdefense, Andrin Hauri, Head of the Risk and Resilience Team; Andreas Wenger, Director of the CSS.

Editor: Jakob Bund
Language editor: Taylor Grossman
Layout and graphics: Miriam Dahinden-Ganzoni

DOI: 10.3929/ethz-b-000563942

Table of Contents

Executive Summary

The political future of the Internet is often discussed in terms of three archetypes: 1) a single global Internet, 2) a bifurcated Internet, split into a Chinese-led and an US-led Internet, and 3) a fragmented Internet, split into many national segments. The primary purpose of this report is to enable informed discussion and decision-making on the topic of Internet fragmentation and bifurcation. The report aims to add value to the discussion in five ways:

First, the report provides a concept-dense introduction to how the Internet works. This ensures the necessary background for an informed discussion on future changes of the structure of the Internet.

Second, the report provides an overview of the Internet fragmentation and bifurcation discourse. It summarizes key literature and highlights the challenge of the diverse, evolving, and at times inconsistent understanding of fragmentation.

Third, the report provides a short overview of the Russian internet ("Runet") as a case study in Internet fragmentation. This makes the discourse more tangible and highlights how actions across different layers ranging from access to computer chips, to the domain name system, to censorship of social media are driven by similar underlying geopolitical concerns.

Fourth, the report examines Internet bifurcation in the context of the Chinese Digital Silk Road and the US Clean Network initiative. The distinction between fragmentation and bifurcation is examined because the incentives behind these trends are not the same. The long-standing approach of the US in global Internet governance has been to reduce barriers to local market entry (fragmentation). With the rise of the Chinese near-peer ICT-ecosystem the focus has shifted towards leveraging network effects of the US ICT-ecosystem to limit the global market access of specific companies (bifurcation).

Fifth, the report takes a deeper look at the politics of future Internet architectures, **with a particular focus on Huawei's New IP and the SCION project from ETH Zürich**. It highlights what problems next-generation Internet architectures aim to solve and why they are strongly incentivized to be backward compatible but also why a higher degree of freedom on naming systems and identifiers can create political concerns.

While this report is closer to a mini syllabus than a policy paper, the author still highlights a few policy ideas. Most notably, the idea of **a neutral public core of the Internet** that provides some basic services independently of geopolitical conflicts is presented as one potential avenue to maintain a global Internet in the long run.

Acknowledgements

This report has profited from feedback and answers to specific questions at multiple stages. The author would like to thank Professor Adrian Perrig (ETH Zürich), Olaf Kolkman (Internet Society), Maurice Eglin and Hans-Heinrich Aenishänslin (Swiss Federal Department of Defence, Civil Protection, and Sport), Jorge Cancio (Swiss Federal Office of Communications), as well as Jakob Bund, Taylor Grossman, and Andrin Hauri (Center for Security Studies). All opinions and mistakes are exclusively attributed to the author.

1 Introduction

The Internet has grown massively since it became commercialized and globalized in the 1990s. Yet, despite its success, the idea that the Internet may lose its global nature has high salience. It comes in two variants. In the first one, the Internet develops towards a "splinternet" consisting of **several national internets** due to intentional access and connectivity restrictions imposed by governments. For example, Eugene Kaspersky, the CEO and founder of the Russian cybersecurity company Kaspersky Lab, predicted in 2013 that "Internet fragmentation will bring about a paradoxical de-globalization of the world"[1]. In Russia, such a gradual detachment from the global Internet is now increasingly becoming a reality, due both to domestic legislation as well as Western tech sanctions in response to the Russian war of aggression against Ukraine. A second claim, which emerged with the start of the US-China "trade war" in 2018, is that we are moving towards **a bifurcation between a Western and a Chinese internet**. For example, the former CEO of Google Eric Schmidt has said that "the most likely scenario now is not a splintering, but rather a bifurcation into a Chinese-led internet and a non-Chinese-led internet, presumably led by America".[2]

The key issue underlying fragmentation is the mismatch between the highly globalized nature of the Internet and the clear borders that define sovereign governing structures. In the words of Milton Mueller, professor at the Georgia Institute of Technology School of Public Policy and author of the book *Will the Internet fragment?*, it is "a power struggle over the future of national sovereignty in the digital world".[3] The key driver of bifurcation is the global strategic competition between the US and China over power and values to shape and control important points of cyberspace.

Consequences

Internet fragmentation would enable more cyber sovereignty. However, on an economic level, a lack of interoperability between networking protocols and fragmented or bifurcated trust and namespaces would arguably also increase global online transaction costs and make it harder to maintain global brands.[4] Furthermore, networking protocols that give more power to intermediaries rather than the endpoints of communications would give Internet service providers (ISPs), which are closer aligned to nation states than key actors on the logic or content layer, more fine-grained control. Especially for second- and third-tier powers, this could enable easier Internet surveillance and censorship. A bifurcation between US-approved and Chinese-approved infrastructure and standards could also increase pressure on non-aligned states to choose one side of the electronic curtain. Therefore, Internet fragmentation and bifurcation are terms with mostly negative connotations in the West. Fragmentation has particularly gained traction in opposition to moves for stronger national control after the Snowden revelations.[5] In contrast, China sees more control over Internet infrastructure as a way to reduce its vulnerability in a conflict with the United States[6] and frames it as Internet decentralization[7].

Aims

One aim of this report is to provide an **overview of the discourse on Internet fragmentation and bifurcation**. Warnings about a fragmenting Internet are common. They have been voiced in many major news outlets including the Financial Times, Politico, the New York Times, the Huffington Post, Wired, and Slate. Similarly, there are several existing analyses by think tanks on the subject. Specifically, by the Belfer Center, the World Economic Forum, the Global Commission on Internet Governance, and the Stiftung Wissenschaft und Politik. Lastly, there are also a number of academic articles and books by Jack Goldsmith and Tim Wu, Scott Malcomson, and Milton Mueller on the subject.[8]

At the same time, the author, and presumably quite a few readers, can empathize with the former Singaporean diplomat and US-China analyst Kishore

---

[1] Kaspersky, Eugene (2013). What will happen if countries carve up the internet? theguardian.com

[2] Village Global. (2018). *Eric Schmidt & Tyler Cowen on The Future of Technology & Society*. youtube.com 35:20-35:35.

[3] Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization and cyberspace. John Wiley & Sons. p. 5

[4] Ibid. pp. 38-40.

[5] Ibid. pp. 13&14

[6] Binxing, F. (2018). *Cyberspace Sovereignty.* Springer: Singapore. pp. 326&327

[7] Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the Splinternet: How China's technical standards could fragment the internet. Journal of Cyber Policy, 5(2), 239-264.

[8] All articles and books mentioned here are listed in Annex E.

Mahbubani, who frankly admitted "I've been told by the experts that what is coming is a digital wall. I don't understand what a digital wall is".[9] The first challenge is that there can be a gap between the technical Internet community and policymakers. The second challenge is that high-level terms, such as Internet fragmentation, have not always been used consistently and can thus refer to a wide spectrum of Internet governance issues. Therefore, this report provides extensive background and a systematic review of the Internet fragmentation and bifurcation discourse.

Another aim of this report is to focus more specifically on the possibility of a split in Internet standards by providing an overview and a discussion of **proposals for clean-slate redesigns of the current Internet Protocol (IP) suite. Clean-slate Internet architectures could not just lead to competing internets existing in parallel but also have sociotechnical characteristics that may enable or counteract Internet fragmentation**. The particular focus is on Huawei's **New IP**, as it is closely related to a controversial proposal for standardization in the International Telecommunication Union (ITU), and **SCION**, as it is the most operationally advanced alternative IP suite and is developed at ETH Zürich. This report is one of the first to analyze their potential political implications, with a particular focus on Internet fragmentation and bifurcation. However, it is important to acknowledge that clean-slate protocols also have other security implications. SCION, in particular, could help to reduce several types of attacks that cause significant harm today.

Outline

To make sense of the policy implications, security contributions and potential concerns regarding clean-slate Internet designs, it is necessary to understand how the Internet functions today. To this end, the report provides a brief history of the Internet and its governance (section 2.1), as well as background information on the most relevant protocols that are part of it (section 2.2). Readers familiar with computer networks may skip this 15-page crash course. Subsequently, section 3 reviews Internet fragmentation (section 3.1) and bifurcation (section 3.2) claims from a wide array of sources. Section 4 explains the efforts to build clean-slate Internet architectures with a more in-depth treatment of New IP (section 4.3) and SCION (section 4.4). The discussion (section 5) aims to put these projects into the political context, analyzes some of the underlying factors, and highlights some specific points of relevance for Switzerland. Lastly, the conclusion (section 6) reiterates the findings of the report and highlights some actions that may help to strengthen trust in global Internet standards setting.

[9] Lee Kuan Yew School of Public Policy. (2019). *[Festival of Ideas 2019] Are the US and China Doomed to Enmity?* youtube.com, 44:00-48:30.

2 How the Internet Works

The Internet is a global public network that connects about 120,000 computer networks,[10] called autonomous systems (AS), consisting of billions of devices. The Internet has its roots in the US government networks ARPANET and NSFNET. It was privatized, commercialized, and globalized in the 1990s together with the rise of the World Wide Web. This history of the Internet (sections 2.1.1 and 2.1.2) is fundamental to understand its unique, path-dependent governance complex (section 2.1.3) and the longstanding conflict between the West, China, and Russia over Internet standards. At the same time, any discussion of the technical characteristics and political consequences of Internet standards requires a basic understanding of how these protocols and the Internet at large function. For this, it can be useful to conceptualize the Internet in several layers. Users generally interact with content and the companies that enable them to find, view or share text, pictures, or videos. These user-facing Internet services, in turn, are enabled by several underlying layers of protocols as well as physical infrastructure. In other words, the most basic representation of the Internet's structure is a stack consisting of an infrastructure layer (section 2.2.1) at the bottom, a logic layer (section 2.2.2) in the middle, and a content layer (section 2.2.3) on top.

2.1 History and Governance

2.1.1 Origins

The first computer networks were special-purpose and relied on existing telephone lines. The first large network, the **Semi-Automatic Ground Environment (SAGE)**, was researched by the US Air Force in the 1950s to get radar data to decision-makers in the event of a Soviet air attack. It became operational in 1958. The telecommunications company AT & T developed the first modem for SAGE and commercialized it.[11] This enabled the first civilian special-purpose computer networks, such as US airline reservation systems, in the 1960s. The first nationwide computer network that could be used by both the military and civilians was proposed in the Soviet Union in 1959 by Anatoly Kitov and called Economic Automatic Management. However, Kitov's supervisors felt that he had overstepped his authority and suspended him as director of Computation Center 1 of the Soviet military.[12] Renewed Soviet proposals in the early 1960s most notably included the All-State Automated System for the Management of the Economy (OGAS) by Victor Glushkov. OGAS was an ambitious project to create "electronic socialism" by making all relevant government documents electronic and allowing decentralized remote access for controlling and optimizing the information in those documents. It received some political support as early as 1963 but remained stuck in bureaucratic infighting for more than a decade and never materialized.[13] The first general-purpose computer network, the **Advanced Research Projects Agency Network (ARPANET)**, was only built in 1969 based on the visions of J.R.C. Licklider and funded by the US Department of Defense. ARPANET had a much smaller scope than OGAS and at first connected select US universities and corporate research institutions.[14] In the following two decades, other countries, corporations, as well as users created their own computer networks and networking protocols. **Annex A provides an overview of 21 general-purpose computer**

[10] Number Resource Organization. (2022, June 30). *Internet Number Resource Status Report Prepared by Regional Internet Registries AFRINIC, APNIC, ARIN, LACNIC, RIPE NCC*. nro.net. p. 21

[11] Kline, R. (2019). The Modem that Still Connects Us. In W. Aspray (Ed.) *Historical Studies in Computing, Information, and Society: Insights from the Flatiron Lectures* (pp. 29-50). Cham, Switzerland: Springer Nature. pp. 33 & 34

[12] Peters, B. (2016). *How not to network a nation: The uneasy history of the Soviet Internet*. MIT Press. pp. 87 & 88

[13] Ibid. pp. 107-109

[14] Leiner, B., Cerf, V., Clark, D. et al. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review, 39*(5), 22-31. p. 23

networks that were in operation between 1969 and 1989.

Protocol Wars

ARPANET, NPLNET, and CYCLADES were the first **packet-switched networks**. Packet-switching means that data packets are sent individually over the network and may take different routes during a communication session. In contrast, in a circuit-switched network, such as the telephone network, a fixed data path is established between the two parties for the duration of the communication session. Distributed networks without a fixed communication path do have the highest survivability in the case of physical network disruptions, e.g., in a nuclear attack.[15] However, the more general advantage of packet-switching is simply efficiency, as there is no bandwidth reserved for a circuit that is not fully used. The routing on the Internet is "best effort" and has no guaranteed quality of service (QoS). This means that unlike the transport of a physical packet by the postal service, there is no service-level agreement between a customer and an Internet provider that a data packet arrives at its destination within a specific time or at all.

Email was introduced to ARPANET in 1971 and became its first killer application. Furthermore, in the 1970s Bob Kahn and Vint Cerf worked out the principles behind the Transmission Control Protocol (TCP) and the **Internet Protocol (IP)**. Since the 1980s, the main organization that recognizes and develops standards for the ARPANET and then the Internet at large is the Internet Engineering Task Force (IETF). It publishes comments as well as standards in the series Request for Comments (RFC). RFC 791[16] from 1981 describes IP version 4 (IPv4), which has remained the dominant version of IP until today. In 1982, IP became the only approved protocol on ARPANET. In these early days, Jon Postel at the University of Southern California maintained a file that mapped names to IP addresses, which anyone could download as needed. To register a new name, one simply had to send an email to Jon. However, as this solution did not scale, RFC 882 and RFC 883[17] created the domain name system (DNS), which translates unique numbers into unique names.

In the 1970s and 80s, large computer manufacturers used their own **proprietary networking protocols**, such as DECnet and AppleTalk. At the same time, the number of computers started to grow rapidly with the introduction of personal computers in the 1980s. Agreeing on a common host protocol is more reliable and efficient than translation between several protocols. Hence, the UK presented the case for a global standard to the International Organization for Standardization (ISO) in 1977, which created the **Open Systems Interconnection (OSI)** model published in 1984. The adoption of OSI protocols was particularly supported by the European Economic Community. However, the US telecommunications and computer industry was already more familiar with the TCP/IP protocol from ARPANET. The IETF did discuss switching from IPv4 to an OSI-aligned protocol but eventually decided to keep working on the IP-protocol suite with IPv6.[18] The **explosive growth of the Internet in the 1990s meant that IP reached the critical mass so that its network effects established it as the common host protocol** and the winner of the so-called "protocol wars". Key developments included the creation of the National Science Foundation Network (NSFNET) Internet backbone in the US in 1986, the development of a hypertext standard – the **World Wide Web** – by Tim-Berners Lee at CERN in 1990, the first web browsers – such as Mosaic in 1993 – and the first search engines, such as AltaVista in 1995.

2.1.2 Privatization and Globalization

End of Export Control

With the end of the Cold War, there was pressure to loosen the multilateral export control regime that ensured that strategic Western technology was not traded with the Communist bloc. In the early 1990s the Coordinating Committee for Multilateral Export Controls (COCOM) was first weakened and then abolished and replaced with the Wassenaar Arrangement, a much weaker export control regime that focuses on rogue states.[19] Hence, even though China did not make any progress towards political

[15] Baran, P. (1964). *On Distributed Communications: I. Introduction to Distributed Communications Networks*. rand.org

[16] Postel, J. (1981). *RFC 791: Internet Protocol: DARPA Internet Program Protocol Specification*. datatracker.ietf.org

[17] Mockapetris, P. (1982). *RFC 882: Domain Names: Concepts and Facilities*. datatracker.ietf.org; Mockapetris, P. (1983). *RFC 883: Domain Names: Implementation and Specification*. datatracker.ietf.org

[18] Russell, A. (2006). 'Rough consensus and running code' and the Internet-OSI standards war. *IEEE Annals of the History of Computing, 28*(3), 48-61. p. 54

[19] Meijer, H. (2016). The Rise of China and the Collapse of COCOM. In *Trading with the Enemy: The Making of US Export Control Policy toward the People's Republic of China* (pp. 117-144). Oxford University Press

liberalization it suddenly had full access to Western information and telecommunications technology. China connected to the Internet in 1994, three weeks after the end of COCOM. In the subsequent years Western companies helped to build up the Chinese tech ecosystem through overt technology transfer for market access[20], management training[21], and a failure to stop industrial espionage[22].

Backbone Privatization

NSFNET offered high-speed connections between regional networks, which in turn connected to smaller local networks such as universities. It served as the free, public Internet backbone from 1986 onwards, and enabled the decommissioning of ARPANET in 1990. At the same time, there were discussions about the **privatization of the Internet backbone**.[23] In 1994, the National Science Foundation (NSF) awarded contracts to Sprint, MFS, Ameritech, and Pacific Bell to build network access points at which commercial backbones could intersect. In 1995, the NSFNET was retired. The publicly funded network access points had no performance requirements in their contracts, which is why they became congested and were eventually replaced by private Internet Exchange Points (IXPs).[24]

DNS Privatization

In 1985, the free registration of ".com", ".org", ".net", ".edu", ".mil", and ".arpa" addresses[25] was opened to organizations with access to ARPANET. For example, the computer manufacturer Symbolics registered "symbolics.com" as the first dotcom address. In 1991, the DNS contract awarded by the Department of Defense switched to the defense contractor Government Systems Inc., which outsourced it to Network Solutions Inc.[26] In 1995, Network Solutions Inc. got the right to charge individual applicants for domain name registrations 100 USD for the first two years and 50 USD per year thereafter. With the rise of the World Wide Web and the "dot-com boom" this was highly profitable. In 1999, Network Solutions Inc. collected more than 200 million USD in fees with very low operating expenses.

However, this government backed monopoly – and the general idea of too much government control over cyberspace – did not sit well with parts of the technical community of the Internet. They aimed to bring the registry and the policy authority over the domain name system to a global non-profit and organized a panel called the International Ad Hoc Committee[27] which published a memorandum of understanding in 1997.[28] This document foresaw the creation of new top-level domains that would be administered by an association located in neutral Switzerland called the International Council of Registrars (CORE). However, the US government communicated that it would not accept this. The conflict reached its climax on 28 January 1998. At 5 pm Pacific Time, Jon Postel organized a power demonstration when he ordered the colleagues maintaining the eight root servers that were not under direct control of the US government to follow the DNS root zone server B at the University of Southern California as the primary root server, rather than the server A operated by Network Solutions Inc. in Virginia. For a moment, this created a split DNS root. However, national security advisers soon woke up Clinton's Internet policy czar Ira Magaziner, who was in Davos for the World Economic Forum. Magaziner called Postel and his supervisor and informed them that this was illegal and that Postel and the University of Southern California would be held liable if he did not immediately restore the status quo.[29] Two days after the phone call, the US government published the so-called green paper[30], which suggested that it would gradually transfer existing Internet Assigned Numbers Authority (IANA) functions and the appropriate databases to a newly formed not-for-profit corporation. It eventually contracted the Internet Corporation for Assigned Names and Numbers (ICANN), a newly founded non-profit organization based in Cal-

[20] Fan, X. (1996). China Telecommunications: Constituencies and Challenges. pirp.harvard.edu pp. 146&147

[21] Murmann, J. P., Huang, C., & Xiaobo, W. (2018). *Constructing large multinational corporations from China: East meets West at Huawei, 1987-2017*.

[22] e.g., Motorola Inc. v. Lemko Corporation, Xiaohong Sheng, Shaowei Pan, Hanjuan Jin, Xiaohua Wu, Xuefeng Bai, Nicholas Labun, Bohdan Pyskir, Hechun Cai, Jinzhong Zhang, Angel Favila, Ankur Saxena, Raymond Howell, Faye Vorick, Nicholas Desai, and Huawei Technologies Co., LTD., a Chinese corporation. (2010). dig.abclocal.go.com; Chandler, M. (2012). Huawei and Cisco's Source Code: Correcting the Record. blogs.cisco.com

[23] Kahin, B. (1990). *RFC 1192: Commercialization of the Internet*. ietf.org

[24] Shah, R., & Kesan, J. (2007) The Privatization of the Internet's Backbone Network. *Journal of Broadcasting & Electronic Media, 51*(1), 93-109. pp. 100 & 101

[25] Postel, Jon & Joyce Reynolds (1984). *RFC 920: Domain Requirements*. datatracker.ietf.org

[26] Williamson, S. & L. Nobile. (1991). *RFC 1261: Transition of NIC Services*. datatracker.ietf.org

[27] Rony, Ellen & Peter Rony. (1998). *The Domain Name Handbook: High Stakes and Strategies in Cyberspace*. (Lawrence, KS: Miller Freeman). p. 524

[28] International Ad Hoc Committee (1997). "*Establishment of a Memorandum of Understanding on the generic Top Level Domain Name Space of the Internet Domain Name System (gTLD-MoU)*". web.archive.org; International Telecommunication Union. (1997). *80 organizations Sign MoU to Restructure the Internet*. itu.int

[29] Goldsmith, Jack and Tim Wu. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press. pp. 44-46

[30] National Telecommunications and Information Administration. (1998). *A Proposal to Improve Technical Management of Internet Names and Addresses: Discussion Draft 1/30/98*. web.archive.org

ifornia, with the IANA functions. However, it explicitly and indefinitely retained policy authority over the primary DNS root server.[31]

IANA Stewardship Transition

The commercialization of the Internet, the emergence of the World Wide Web, and the ability to connect to it over pre-existing telephone infrastructure also led to a rapid **globalization of the Internet**. In the late 1980s, the first countries established regular connections to the NSFNET.[32] In 1995, there were around 45 million Internet users globally and 25 million in the US, which still represented more than half of all Internet users. By 2016, the number of Internet users globally had climbed to about 3.4 billion and the share of those in the US dropped to 7 per cent.[33]

With this globalization, the US government's theoretical power to end its IANA contract with ICANN or to not implement ICANN's policy decisions in the primary root server became the subject of increasing scrutiny and criticism by other countries.[34] This criticism was aggravated by the revelations of Edward Snowden about the degree of worldwide surveillance by the US. In their 2013 Montevideo statement, the directors of ICANN, the Internet Society, the Internet Architecture Board, the IETF, and all regional Internet registries called upon the US government to accelerate the IANA stewardship transition.[35] In 2014, the US National Telecommunications and Information Administration announced its intent to **transition the stewardship of the IANA functions to the global multistakeholder community**.[36] As such, the US government relinquished its residual control and permanently transferred the IANA functions to ICANN starting from 1 October **2016**.

As countries such as Brazil, Russia, China, and France have pointed out,[37] ICANN and the IETF are non-profits headquartered in California and therefore still under **US jurisdiction**. As such, they can still be forced to follow US sanctions post-transition. However, in practice, any weaponization of this US structural power would incentivize the search and coordination for alternatives. Therefore, the US has not attempted to use its jurisdiction over ICANN and the IETF for political ends. This was highlighted in the case of Israeli victims of terror attacks that were awarded monetary compensation in US court judgements. Due to a lack of seizable assets they argued that ICANN should assign control of the country-code top-level domains (ccTLDs) for Iran (".ir"), Syria (".sy"), and North Korea (".kp") to them. This has been rejected twice by courts and the US government has written an amicus brief supporting that rejection:[38] "If a US court were to order the attachments the plaintiffs seek, it would not merely threaten disruption of the global Internet for millions who bear no fault for plaintiffs' injuries. It would also derail vital foreign policy efforts of the United States, destabilizing international confidence in ICANN and providing ammunition to foreign states who argue that the keys to the Internet belong in governmental hands."[39] Adding, that "it is not difficult to imagine that a court-ordered change to the authoritative root zone file at the behest of private plaintiffs would prompt members of the global Internet community to turn their backs on ICANN for good."[40]

2.1.3 Key Institutions

The current Internet governance regime is commonly referred to as **multistakeholder governance**, meaning it includes representatives from governments, the private sector, and civil society. The term multistakeholder governance has also been engrained by the US into the IANA Transition Agreement. The key organizations in this current model are two US-based non-profit organizations, ICANN and the IETF. The main alternative to this model would be to shift Internet governance to the United Nations and more specifically to the Geneva-based ITU.

[31] ICANN. (1999). *Fact Sheet on Tentative Agreements among ICANN, the U.S. Department of Commerce, and Network Solutions, Inc.* archive.icann.org

[32] Zakon, R. (1997). *RFC 2235: Hobbes' Internet Timeline*. ietf.org

[33] Roser, M., Ritchie, H., & Ortiz-Ospina, E. (2015). *Internet*. OurWorldInData.org.

[34] Working Group on Internet Governance. (2005). Report of the Working Group on Internet Governance. p. 12; World Conference on International Telecommunications 2012.

[35] Akplogan et al. (2013). *Montevideo Statement on the Future of Internet Cooperation.* icann.org

[36] National Telecommunications and Information Administration. (2014). *NTIA Announces Intent to Transition Key Internet Domain Name Functions*. ntia.doc.gov

[37] GAC (2017). Abu Dhabi – GAC discussion on Jurisdiction. static.sched.com

[38] United States Court of Appeals for the District of Columbia. (2015). Susan Weinstein, et al., Plaintiffs-Appellants, v. Islamic Republic of Iran, et al., Defendants-Appellees, Internet Corporation for Assigned Names and Numbers, Appellee-Garnishee. Brief for the United States as Amicus Curiae.

[39] Ibid. pp. 1 & 2

[40] Ibid. p. 13

ICANN is responsible for the DNS, IP numbers, and autonomous system numbers. In the DNS, ICANN assigns the top-level domains. The most common of these are ccTLDs, which are based on two-letter abbreviations for states[41], such as ".ch" for Switzerland, ".de" for Germany, or ".fr" for France. However, there is an increasing diversity of generic top-level domains (gTLDs), such as ".com", ".xyz", or ".zuerich". There is only one registry per top-level domain, which operates the file in which the IP addresses corresponding to email addresses or websites using this domain are listed. In the case of Switzerland, this is the foundation SWITCH. A registry can have contracts with multiple registrars. Registrars are platforms that sell domain names for many top-level domains to users and forward the registrations to the respective registries (see figure 1). The world's largest registrar is GoDaddy.

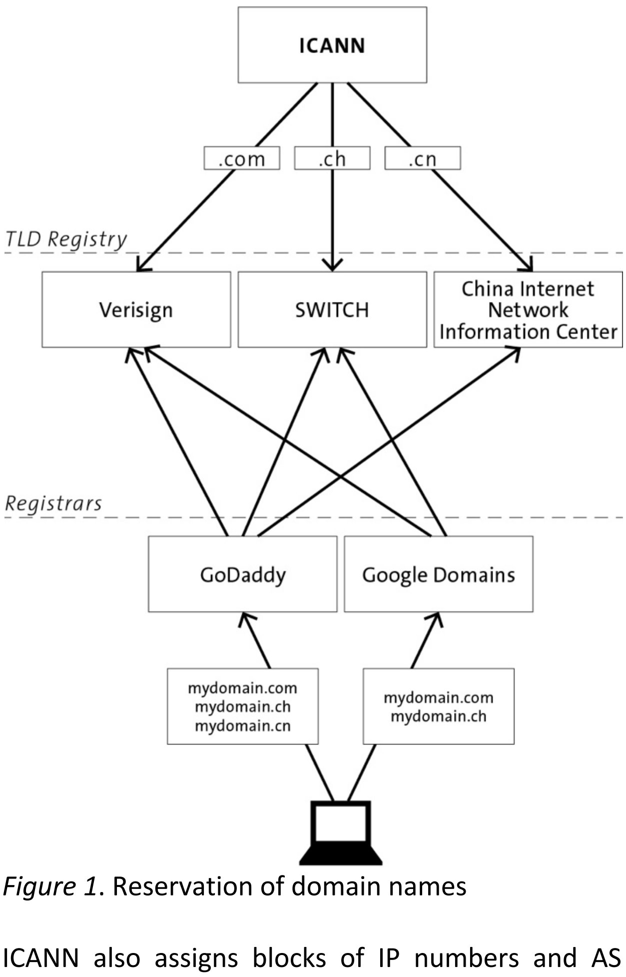


Figure 1. Reservation of domain names

ICANN also assigns blocks of IP numbers and AS numbers to one of five regional Internet registries: AfriNIC for Africa, ARIN for North America, APNIC for the Asia-Pacific, LACNIC for Latin America, and RIPE NCC for Europe. In turn, these regional registries assign IP-blocks and individual AS numbers to the operators of ASes (see figure 2).

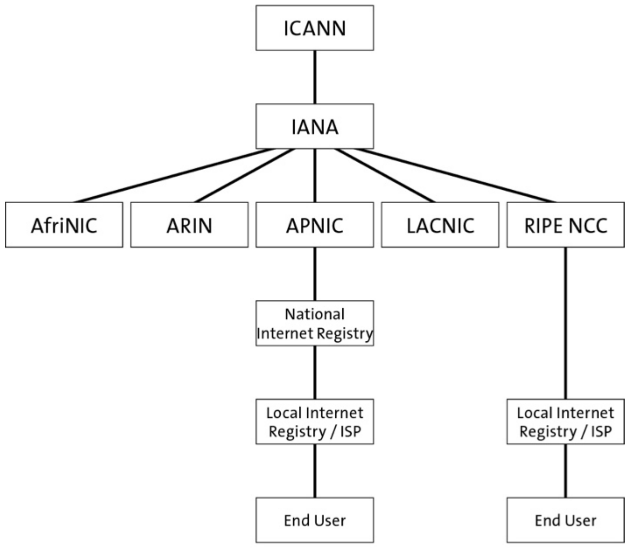


Figure 2. Assignment of IP-addresses

The **IETF** is a standards organization that defines protocols such as the Internet Protocol (section 2.2.2.2) and the Border Gateway Protocol (section 2.2.2.4). IETF-standards can be used free of charge and, theoretically, anyone can participate in the standards setting. Its unofficial motto was coined by David Clark in 1992: "We reject: kings, presidents and voting. We believe in: rough consensus and running code."[42] In line with this credo, participation in one of the over 100 working groups of the IETF is only possible as an individual, there are no representatives of states. Decisions are made by humming.[43]

The IETF is complemented by the Internet Research Task Force, which promotes research on the Internet's evolution. Both the IETF and the Internet Research Task Force are overseen by the 13-person Internet Architecture Board, which is selected by an IETF nomination committee[44]. This board provides long-range technical direction for Internet development, manages the RFC series, and reviews appeals. The IETF and the Internet Architecture Board are both a part of the non-profit organization Internet Society, which has offices in the US and Switzerland. These additional organizational structures provide

[41] ISO (n.d.). *ISO 3166-1 alpha-2*. iso.org

[42] Clark, David (1992). A Cloudy Crystal Ball – Visions of the Future. In Megan Davies, Cynthia Clark and Debra Legare (Eds.) *Proceedings of the Twenty-Fourth Internet Engineering Task Force*. ietf.org. p. 543

[43] Resnick, P. (2014). *RFC 7282: On Consensus and Humming in the IETF*. datatracker.ietf.org

[44] Kucherawy, M., Hinden, R. & Livingood, J. (2020). *RFC 8713: IAB, IESG, IETF Trust, and IETF LLC Selection, Confirmation, and Recall Process: Operation of the IETF Nominating and Recall Committees*. rfc-editor.org

continuity and give long-term insiders more weight in Internet standards setting.

The **ITU** is the specialized UN agency for ICT-governance. It originally started as the International Telegraph Union in 1865. It subsequently merged with the International Radiotelegraph Union and the Comité Consultatif International des Communications Téléphoniques à Grand Distance. After the Second World War, it was integrated into the United Nations. The ITU is a key player in standards setting for the transport of data over wires (e.g., DSL) and radio access networks (e.g., 5G). However, the ITU currently plays little to no role when it comes to higher protocol layers (IP, BGP, etc.).

2.2 Layers

There are several ways to conceptualize the Internet in layers. The most prominent ones amongst computer scientists are the seven layers of the OSI-model[45] and variations of TCP/IP layers.[46] Note that in this context the OSI model only refers to the categorization of layers that was developed by the ISO. It does not refer to an OSI protocol suite. Furthermore, note that both approaches are only concerned with logic. For example, the physical layer in the OSI-model is a category for communication protocols rather than for the cables and antennas that enable the communication and the ISPs that operate them. Furthermore, most Internet users have little interest in protocols. They interact with services provided to them and visualized content that they can view and share. Similarly, states generally regulate content, such as pornography or hate speech, and not the protocols used to distribute or view it. Hence, from a political perspective, it is useful to make an overarching **three-way partition between infrastructure, logic, and content**[47] in addition to the OSI and TCP/IP-layers.

The following sections are structured according to these three overarching layers and will introduce each of them. However, the primary focus of this report remains the logic layer and the specific components necessary for understanding subsequent claims and discussions. These include the Internet Protocol (IPv4, IPv6), the Domain Name System, the Border Gateway Protocol, and the Public Key Infrastructure.

Table 2: Overview of Internet Layers. Adapted from Voelsen (2019).[48]

		OSI-model layer	TCP/IP layer	Example	Authorative rule-setting	SDO
Content	User Web Services			Social media Text, photos, video	States: Laws & regulations	
	B2B Web Services			Cloud service, CDN, DDoS protection		
Logic		7 Application	Application	WWW/HTTP, SMTP HTML, JPEG	ICANN: DNS	IETF, W3C
		6 Presentation				
		5 Session				
		4 Transport	Transport	TCP, UDP, QUIC		IETF
		3 Network	Network	IPv4, IPv6		IETF
		2 Data Link	Network Access	MAC, LLC DSL, ISDN, Wi-Fi, 5G		ITU, IEEE, 3GPP
		1 Physical				
Infrastructure	Network			Operators: ISPs, IXPs Cables, antennas	States: Laws & regulations	
	User Devices			Laptop, smartphone		

[45] Zimmermann, H. (1980). OSI reference model-the ISO model of architecture for open systems interconnection. *IEEE Transactions on communications*, *28*(4), 425-432.

[46] Braden, R. (1989). *RFC 1122: Requirements for Internet Hosts -- Communication Layers*. datatracker.ietf.org

[47] See e.g., Kurbalija, J. (2016). *An Introduction to Internet Governance: 7th Edition*. DiploFoundation. p. 35

[48] Voelsen, D. (2019). *Risse im Fundament des Internets: Die Zukunft der Netz-Infrastruktur und die globale Internet Governance*. swp-berlin.org. p.11

2.2.1 Infrastructure

The hardware that is required to enable connectivity consists of both the end-user devices and the physical infrastructure for data transport. The former is often not included on the infrastructure layer, as smartphones and computers are mostly owned and operated by individuals and regularly change their location. However, as the suppliers for and manufacturers of smartphones, as well as their operating systems and software ecosystems, can be levers that some states may use to pursue their perceived national interests, they are still briefly presented here. Regarding the latter, there are three fundamental ways in which data is transported over distance on the Internet. First, there are electromagnetic waves that are transmitted through the air. Second, there is the transfer of electrons in cables. Third, there is the transfer of photons in cables. Rather than going into details of hardware, the report focuses on three aspects: Routers, ISPs, and IXPs.

2.2.1.1 User Devices

Devices: There are various types of devices, including desktop computers, laptops, smartphones, and tablets, that are connected to the Internet. All these devices have a screen and are intended for human interaction. However, there is an expectation that in the future a larger and larger share of Internet-connected devices will consist of independent sensors and effectors, called the Internet of Things. Lenovo (China, 25%), HP (US, 22%), Dell (US, 18%), and Apple (US, 8%) had the largest global market share of personal computers in 2021.[49] The largest vendors by numbers of smartphones are Samsung (South Korea, 20%), Apple (US, 17%), Xiaomi (China, 14%), Oppo (China, 10%), and Vivo (China, 10%).[50] User devices consist of hundreds of technical components, some of which are especially critical and hard-to-replace.

Chips: Computer chips are essential and their manufacturing is extremely complex, relying on global supply chains and specialized equipment. Key companies in manufacturing equipment include ASML (Netherlands), Applied Materials (US), Lam Research (US), and Tokyo Electron (Japan). Key companies in chip design include Arm (UK), Synopsys (US), Nvidia (US), AMD (US), and Intel (US). Key companies in the fabrication of chips include TSMC (Taiwan), Samsung (South Korea), and Intel (US).[51] Furthermore, in smartphones, baseband processors are required to turn digital information into radio signals. For 5G, the latest standard for radio access networks, the market for such mobile chips is dominated by Qualcomm (76%, US), followed by Mediatek (18%, Taiwan), and Samsung (4%, South Korea).[52] These baseband processors are the reason why Huawei smartphones were not able to offer 5G after US sanctions even though the company has often been described as the world's 5G leader.[53]

Operating system: At a stack above the device itself, there are dependencies on software, specifically on operating systems as well as the ecosystems of applications created for them. Most smartphones run on Google's Android operating system (US, 70%), the main exception is the iPhone, which runs on Apple's iOS (US, 29%).[54]

2.2.1.2 Network Infrastructure Manufacturers

Networking devices: Networking devices that receive and forward data packets between computer networks on the IP-layer are called **routers**. The most familiar type of routers are home routers. ISPs have larger routers that can forward more data. The largest vendors of service-provider and enterprise routers in the global market are Cisco (US, 35%), Huawei (China, 31%), and Juniper (US, 10%).[55] Networking devices that receive and forward data packets for communication using MAC-addresses for local communication in local area networks (OSI layer 2), such as offices or schools, are called **switches**. Devices that use more than one protocol to receive and forward data packets between multiple networks are called **gateways**.

Radio access network (RAN) infrastructure: The manufacturers of antennas for mobile network infrastructure sell their equipment to mobile network

[49] Gartner (2022). Gartner Says Worldwide PC Shipments Declined 5% in Fourth Quarter of 2021 but Grew Nearly 10% for the Year. gartner.com

[50] Yordan (2022). IDC numbers confirm global smartphone market growth in 2021. gsmarena.com

[51] Khan, Saif. (2021). Securing Semiconductor Supply Chains. cset.georgetown.edu p. 43

[52] Sharma, P. (2022). Qualcomm Gains Share in Smartphone AP/SoC Shipments in Q4 2021; MediaTek Continues to Lead. counterpointresearch.com

[53] Ting-Fang, C. & Li, L. (2021, August 9). Huawei drops 5G for new P50 phones as US sanctions grip. ft.com

[54] Statcounter (2022). Mobile Operating System Market Share Worldwide. gs.statcounter.com

[55] IDC. (2022). *IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Strong Growth in Fourth Quarter of 2021*. idc.com

operators (e.g., Swisscom, Sunrise, and Salt in Switzerland). RAN infrastructure has become particularly politicized with US campaigns to reduce the influence of Huawei (see section 3.2.2). The companies with the largest market share are Ericsson (27%, Sweden), Nokia (22%, Finland), Huawei (20%, China), ZTE (15%, China), and Samsung (8%, South Korea)[56].

Fiber optic cables: Fiber optic cables are the main source of Internet bandwidth. The market is fairly fragmented. Companies with a large market share include Corning (US), Yangtze Optical (China), Furukawa (Japan), Prymian (Italy), and Hengtong (China). Some key players in laying fiber optic cables on the sea floor, which is the main transmission channel for international data traffic, are Alcatel/Nokia (France/Finland), Subcom (US), Fujitsu (Japan), NEC Corporation (Japan), and HMN Tech (China).[57] Worldwide, there are about 60 ships that can lay and repair undersea cables[58] as well as a few specialized submarines that can cut or tap them.

2.2.1.3 Network Infrastructure Operators

Internet Service Providers: ISPs are organizations that offer Internet access as a service. These organizations have primarily emerged from the owners of telephone and cable TV networks, as early Internet traffic strongly relied on the use of their pre-existing communication infrastructure. For example, integrated services digital network (ISDN) and digital subscriber line (DSL) are standards that allow digital data to be transmitted over telephone lines with the help of a modulator-demodulator (modem) that can convert digital to analog signals and vice versa. Today, more and more Internet traffic goes over purposely built data lines, such as optical fiber. Telephone companies were mostly state-owned until the telecom liberalization of the 1990s. Hence, while ISPs are overwhelmingly private companies, they are usually still more closely aligned with states than the more globalized Internet content companies.

ISPs can be categorized into three tiers: Tier 3, or local ISPs, need to buy access from other ISPs. Tier 2, or national ISPs, have peering relationships with some networks but still need to pay for transit rights to some backbone providers. Lastly, there are tier 1, or international transit ISPs, which do not pay any other network for forwarding data traffic. The largest tier-1 ISPs ranked by the amount of fiber in kilometers are Lumen (US), Verizon (US), and Liberty Global (UK).

At the same time, the largest web content providers increasingly own their own fiber optic infrastructure. According to TeleGeography, content providers such as Amazon (US), Meta (US), Google (US), and Microsoft (US) own dozens of submarine fiber routes amounting to a majority of all international bandwidth.[59]

Internet Exchange Points: IXPs facilitate the data exchange between autonomous systems. These are hubs at which many autonomous systems intersect. As IXPs ensure that traffic between local senders and local recipients uses short paths rather than international links, new IXPs can generate significant cost savings for ISPs and improve access speeds for local content. According to Packet Clearing House, there are a bit more than 1,100 IXPs worldwide as of 2022.[60] Based on the average data traffic going through the IXP, the top three are the Deutscher Commercial Internet Exchange Frankfurt, the Amsterdam Internet Exchange, and the Ponto de Troca de Tráfego Metro São Paulo. In Switzerland, the largest IXPs are the SwissIX in Zurich, CERN IXP/ Equinix Geneva, and Equinix Zurich.

2.2.2 Logic

As highlighted in table 2, the logic layer in the TCP/IP-model consists of four layers itself: The network access layer[61], the network layer[62], the transport layer, and the application layer.

On the network access layer, we find various standards that are used to connect devices and exchange data within a computer network under the control of a single home, office, company, or mobile network provider. IP defines the network layer, which is also referred to as “layer 3” in the OSI-model. It is the element that ensures interoperability by defining **a header format for the data packets** sent over

[56] Kapko, M. (2022, January 26). Ericsson Dethrones Huawei as Global RAN Leader. sdxcentral.com

[57] TeleGeography (2022). ASN, Fujitsu, HMN Tech, NEC, Subcom: Submarine Cable Map. submarinecablemap.com

[58] International Cable Protection Committee. (2022). Cableships of the World. iscpc.org

[59] Mauldin, A. (2022, March). A Complete List of Content Providers' Submarine Cable Holdings. blog.telegeography.com

[60] Packet Clearing House. (2022). *Internet Exchange Directory*. pch.net

[61] Also called link, data link, or network interface layer

[62] Also called Internet layer

the network that includes **globally unique numbers** assigned to the sender and the receiver. While there are multiple ways and standards to physically transmit data over wires or electromagnetic waves, and several protocols to transport data and to build applications, the Internet Protocol is the only network layer protocol.[63] It is at the very heart of what makes the Internet the Internet.[64]

One aspect that is relevant for this report is that the Internet Protocol does *not* mandate how data packets are routed through the network. This is done based on **intra-domain routing protocols** within autonomous systems and based on the **Border Gateway Protocol** for data packets that are exchanged between autonomous systems. Furthermore, Internet users do not memorize the globally unique numbers (IP addresses) of servers but the globally unique names of websites. To translate these names into numbers for routing, there is a global, hierarchical system of assigning and storing the IP numbers that correspond to unique names. This is the **Domain Name System**. Lastly, to add security to the Internet and avoid man-in-the-middle attacks, in which someone pretends to be the operator of a website or an autonomous system, an authentication system based on **public key cryptography** has been added to several protocols.

These protocols are necessary to understand claims about fragmentation on the logic layer and clean-slate alternative designs of the Internet. However, please note that the following overview is far from comprehensive.[65]

2.2.2.1 Network Access Layer

MAC addresses: All devices that people use to access the Internet have been assigned an identifier by the device manufacturer. This is the media access control (MAC) address, sometimes also called hardware address or burned-in address. The standards for MAC addresses are set by the Institute of Electrical and Electronics Engineers (IEEE), a US-based professional association. The most used addresses are 48-bit long, which allows for 2^{48}, i.e., more than 281 trillion, possible MAC addresses. This unique device address is usually only shared for communication in local area networks and not shared as part of Internet traffic.

Local Area Networks (LANs): LANs are home and office networks that link laptops, desktop computers, smartphones, printers, and other devices to each other. For wired connections, these networks primarily use cables that follow the Ethernet standards of the IEEE. For wireless connections, the most common standard is Wi-Fi.

Radio Access Networks: This term is specifically used for the radio connection of mobile phones to antennas that are connected to the wired core network of mobile network operators and the Internet at large. RAN standards are ordered into generations (e.g., 3G, 4G, 5G) and set by the industrial partnership 3GPP and the ITU. The process is vision-driven in the sense that the ITU creates a list of key performance indicators under which a system must qualify to be part of such a generation (e.g., IMT 2000, IMT Advanced, IMT-2020). Several industry actors then aim to design systems that fulfill these criteria, which also means that a term such as 3G refers to multiple technical standards. On top of the above RAN generations, public safety organizations rely on separate private mobile radio standards that provide reliable and secure services. In Europe, these narrowband standards are TETRA and Tetrapol. These are essentially spin-offs of the commercial 2G that only allow for voice-traffic.

Wide Area Networks (WANs): Companies may think that the public packet-switched Internet is too unreliable, insecure, and path-agnostic for connecting their sites. Hence, they may use a layer 2 WAN to connect different locations of offices, production sites, and stores belonging to the same company.

One option for a WAN is for companies to lease a private communications circuit from an ISP, which reserves a specific amount of bandwidth for them. The downside of **leased lines** is that they are expensive.

An alternative is the use of **multiprotocol label switching (MPLS)**. This is a “layer 2.5” protocol that adds an additional label on IP-packets which contains a predetermined route. The routers within the AS then act like switches in a local network only

[63] Also known as the hourglass model of the Internet.

[64] Leiner, B., Cerf, V., Clark, D. et al. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review, 39*(5), 22-31. p. 30

[65] For a more in-depth introduction see Etter, K. (2022). *The Internet: explained from first principles*. explained-from-first-principles.com

reading the MPLS label. The label is dropped at the border router, which reads the IP address again. Because the ISP only creates a virtual circuit whenever a specific amount of bandwidth is actually needed, this is cheaper than a leased line.

A more recent alternative is the use of software-defined networking.[66] Its key feature is that the rules for how to forward data packets are computed in and then distributed from a central location to switches or routers in the entire network. In its terminology, the forwarding rules are the control plane, whereas the switches or routers that implement the forwarding are called the data plane. A **software-defined WAN (SD-WAN)** is generally cheaper than MPLS, and it can manage heterogeneous types of connections. To enable centralized routing policy, SD-WAN uses an overlay protocol to communicate between routers and the centralized software.

2.2.2.2 Network Layer

IPv4: The most important part of the IP-header are the two 32-bit fields for unique sender and receiver addresses. Note that the standard notation of IP addresses for humans is not in binary but in dotted decimal with four numbers between 0 and 255 (1 byte=8 bits =2^8=256) separated by points, for example, "192.168.1.3". Given that IPv4 addresses are 32-bit long, there are 2^{32} = about **4.3 billion unique IPv4-adresses**.

Another field that is worth mentioning is the **Differentiated Services (DiffServ) Code Point**. These six bits indicate different types of data traffic. The DiffServ architecture does not include predetermined judgments of what types of traffic should be given priority at routers; instead, it provides a framework for classification and differentiated treatment. As such, it allows for assured forwarding and expedited forwarding instead of the default best effort service. However, this refers to prioritization at a router and not an end-to-end guarantee as packets can go through multiple company environments before they reach their destination. DiffServ is mainly used to prioritize the forwarding of delay-sensitive types of data (voice-over-IP, video streaming). The full specification of the IPv4 header is listed in Annex B of this report.

IPv6: Due to the issue of IPv4 address exhaustion (section 3.1.3), a new version of IP was introduced in 1998. The main change from IPv4 to IPv6 is that there is now a 128-bit dedicated field for IP addresses in the header. This means that there are 2^{128} = 3.4 x 10^{38} = about **340 trillion trillion trillion unique IPv6 addresses**. Instead of sixteen numbers between 0 and 255, the standard notation of IPv6 addresses uses the hexadecimal (base 16) system, so that one byte can always be represented by two symbols from 0 to f. Secondary changes include that the DiffServ Code Point has been named Traffic Class and extended to eight bits. The full specification of the IPv6 header can be found in Annex C.

2.2.2.3 Transport Layer

Transmission Control Protocol: Routers only forward data packets towards the requested IP addresses. However, once a connection is established, they do not handle the logical overlay which ensures a reliable conversation. A communication protocol between the two end nodes is used to address issues such as data corruption, connection loss, and out-of-order delivery of data packets. On the Internet this is traditionally the TCP.

User Datagram Protocol (UDP): Sometimes the reliability provided by TCP is not desirable. In UDP the host just sends everything once and the users receives whatever arrives. This can be useful in time-sensitive applications, where the delayed retransmission of missing bits is not useful, such as voice calls, video calls, and video streaming.

QUIC: Google has created its own transport layer protocol called QUIC, which has been standardized by the IETF and is used for regular web traffic by several tech giants instead of TCP.

2.2.2.4 Routing

Autonomous systems: An AS is defined as "a connected group of one or more IP prefixes run by one or more network operators that has a single and clearly defined routing policy."[67] Each such network must request a globally unique AS number, which is issued by the regional Internet registries. These numbers were originally 16 bits long but were extended to 32 bits as it became clear that there would soon be more than 2^{16} (=65'536) ASes. Examples of the roughly 1,000 ASes in Switzerland include CERN

[66] Open Networking Foundation. (2022). OpenFlow. opennetworking.org

[67] Hawkinson, J. & Bates, T. (1996). *RFC 1930: Guidelines for creation, selection, and registration of an Autonomous System (AS)*. datatracker.ietf.org. p. 2.

(main AS number 513; 130,000 IPv4 addresses)[68], pharma company Roche (main AS number 2047, 200,000 IPv4 and 128,000 IPv6 addresses)[69], Swisscom (main AS number 3303; 8,350,584 IPv4 and $8*10^{30}$ = 8 nonillion IPv6 addresses)[70], and the Swiss National Bank (AS 196722; 1,800 IPv4 addresses).[71]

Routing within an AS: Different ASes use different routing protocols with different parameters, and they can update them independently. The Routing Information Protocol, the oldest widespread intra-domain routing protocol, aimed to minimize the number of routers through which data passes from source to destination. It is only suitable for smaller networks.[72] Today, intra-domain routing is mainly done through link-state protocols, such as Open Shortest Path First [73] and Intermediate System to Intermediate System.[74] These protocols calculate the route through a network based on a cost function that includes bandwidth, delay, and load on the links between routers. The relative weight of cost parameters can be set by the administrator. Every router maintains a network topology map, which is learned from routers advertising changes in the cost of their links to the network. Cisco has developed a proprietary intra-domain routing protocol which functions similarly.[75]

All the above are protocols in which the router that forwards the data packets is itself tasked to maintain an overview of the links in the network and decide on a forwarding path. However, there is an alternative approach in which the rules for forwarding are computed in and then distributed from a central location for the entire network. This is called **software-defined networking (SDN).[76]** Currently, SDN is mainly used for switching on layer 2 rather than for routing on the Internet.

Routing between ASes: On the Internet, inter-domain routing is exclusively carried out via the **Border Gateway Protocol.** Every autonomous system **advertises the IP address space which it administers** as well as paths that it has to reach other addresses to other autonomous systems through BGP. This information that links IP addresses and AS numbers propagates and after some convergence time, every AS should have learned how to reach any other address on the Internet. [77] As of January 2022, these are about 900,000 paths between ASes for IPv4 and about 140,000 paths for IPv6.[78]

This provides the routing options. However, it is the best-path selection algorithm that decides to where an AS forwards data packets.[79] Its first selection criterion is called “weight” (Cisco) or “PrefVal” (Huawei).[80] The value of this criterion can be manually assigned to neighboring ASes and is not communicated to BGP peers. Hence, there is a level of path control in that you have the possibility to always route packets for certain IP addresses or coming from a specific neighbor AS to another specific neighbor AS. However, it also means that an AS has no guarantees that a forwarded data packet will take the advertised AS path beyond its neighbor.

Geographical distance and political borders are not part of the algorithm. However, Cisco does offer a “cost community” feature that can be inserted at any step in the algorithm, including before the weight.[81] This local feature prefers forwarding data packets to ASes with a peering relationship (meaning traffic is exchanged for free) over those with a customer-provider relationship, where the AS must pay to forward the traffic. Whether implicitly through manual settings or explicitly through the cost community feature, economic considerations play a large role in routing decisions.

In general, this system works well. However, it **depends on trust and is vulnerable to misconfigurations and attacks**. Specifically, an AS can unintentionally or maliciously advertise IP addresses that it does not control to its neighbors and thereby attract traffic destined for another network.

[68] RIPEstat. (2022). AS 513. stat.ripe.net

[69] RIPEstat. (2022). AS 2047. stat.ripe.net

[70] RIPEstat. (2022). AS 3303. stat.ripe.net

[71] RIPEstat. (2022). AS 196722. stat.ripe.net

[72] Malkin, G. (1998). *RFC 2453: RIP Version 2*. datatracker.ietf.org

[73] Moy, J. (1998). *RFC 2328: OSPF Version 2*. datatracker.ietf.org

[74] International Organization for Standardization. (2002). *ISO/IEC 10589:2002*. iso.org

[75] Savage, D. et al. (2016). *RFC 7868: Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP).* datatracker.ietf.org

[76] Open Networking Foundation. (2022). OpenFlow. opennetworking.org

[77] Rekhter, Y., Li, T., & Hares, S. (2006). *RFC 4271: A Border Gateway Protocol 4 (BGP-4).* datatracker.ietf.org

[78] Huston, Geoff. (2022). *BGP in 2021 – The BGP Table.* blog.apnic.net

[79] Cisco. 2016. *BGP Best Path Selection Algorithm.* cisco.com

[80] These are vendor-specific, “proprietary” criteria. However, in practice they are pretty much the same as the first standardized criterion “local_pref”.

[81] Cisco. 2019. *Chapter: BGP Cost Community.* cisco.com

Based on BGP Stream, a free resource provided by Cisco for alerts about hijacks, leaks, and outages related to BGP, there are more than 10,000 minor BGP incidents per year.[82] Notable incidents of BGP prefix hijacking include Pakistan unintentionally taking down YouTube in 2008,[83] 15 per cent of all Internet traffic including for many US government websites being redirected to China in April 2010,[84] the routing of network traffic belonging to MasterCard, Visa, and other financial services providers through Rostelecom in April 2017,[85] and the routing of European mobile traffic through China Telecom in June 2019.[86]

2.2.2.5 Domain Name Resolution

Long unique numbers are more difficult to remember for humans than words. Hence, Internet queries usually start with a unique domain name that is then translated into a unique number (IP address). This process is called DNS resolution and its number of steps varies.

Recursive resolvers: If the web browser in which the name is typed or the operating system of the device has cached the domain, it will directly go to the saved IP address. If that is not the case, the computer sends the DNS query to a recursive DNS server. By default, this is usually a server of the ISP to which the device is connected. However, users can also change their settings to public recursive DNS servers by companies such as Cloudflare (1.1.1.1), Google (8.8.8.8), OpenDNS, or Quad9 (9.9.9.9), which might be faster. The recursive DNS server will first ask a root name server what the IP address for the requested top-level domain is. Then, it will go to the top-level domain servers to ask for the IP address of the requested page. Once it has the correct answer, the recursive DNS server reports it back to the device. As of January 2022, about 77 per cent of DNS resolutions in the EU are handled by the AS in which the request originates, whereas public resolvers have a market share of about 16 per cent.[87] The market share of public resolvers is growing. In 2019, it still stood at 10 per cent. Recursive DNS resolvers can be a political topic because countries may force local ISPs to not resolve requests for a list of banned websites due to issues such as malware, pornography, gambling, or media censorship. This DNS censorship is harder to implement when users rely on public DNS resolvers that have no legal seat in the country.

Root servers: There are only 13 IP addresses in the root zone entries for root name servers. Having more of them is not that easy because it would impact the DNS packet size. However, there are more than a thousand Anycast instances of these root servers. These servers mirror the content on the root name servers. If someone requests information from the IP address of one of the root name servers, the query is sent to the closest Anycast instance.[88] However, all Anycast instances automatically update their data file from one of the 13 root name servers, and 12 of these root name servers update their data file from the single primary root server located in Virginia in the United States and operated by Verisign. Root name servers are a political issue because the hierarchical set-up means that a deletion, addition, or reassignment of a top-level domain in the primary root server will quickly reverberate through the entire Internet.

2.2.2.6 Security

Security on the Internet's logic layer was added as an **afterthought** and relies on adding protocols that leverage **public key cryptography** on top of previously introduced protocols.

How public key cryptography works: In symmetric encryption, the same cryptographic algorithm is used to encrypt and decrypt data. Both the sender and the receiver must keep this cryptographic key secret. Hence, the key in any such system must be exchanged between the communicating parties in some secure manner *before* the system can be used. However, this requirement becomes difficult when the number of communicating parties increases. Therefore, the security of the Internet mainly relies on asymmetric encryption, in which two mathematically related but separate keys are used for encryption and decryption. The keys are based on mathematical one-way functions, which are easy to calculate but very difficult to reverse without prior knowledge. Multiplying two large prime numbers is

[82] Cisco. (2022). *BGP Stream*. bgpstream.com

[83] McCullagh, D. (2008). *How Pakistan knocked YouTube offline (and how to make sure it never happens again).* cnet.com

[84] Anderson, N. (2010). *How China swallowed 15% of 'Net traffic for 18 minutes.* arstechnica.com

[85] Goodin, D. (2017). *Russian-controlled telecom hijacks financial services' Internet traffic.* arstechnica.com

[86] Goodin, D. (2019). *BGP event sends European mobile traffic through China Telecom for 2 hours.* Arstechnica.com

[87] Huston, Geoff. (2022). Some Thoughts on DNS4EU – the European Commission's Intention to Support the Development of a New European DNS Resolver. circleid.com

[88] Internet Assigned Numbers Authority. (2022). *Root Servers*. root-servers.org

a one-way function and the basis of the best-known asymmetric encryption scheme. The product of two prime numbers can be used as a publicly shared instruction to build a mathematical lock whose key is held by only one person. If Alice wants to send a message to Bob, she can encrypt the message using Bob's public key and a mathematical operation. Conversely, only Bob, who knows the two original prime numbers used to create the public key, can easily decrypt the message with his private key. Due to increasing computing power, increasing key lengths are needed over time to ensure that the private key cannot be factorized from the public key.

Use of public key cryptography on the Internet: Public key infrastructure (PKI) refers to the set of processes and organizations that provide public key cryptography to enable **content encryption** and **party authentication**. Encryption ensures privacy with the caveat that metadata, such as the recipient and sender in the header of the IP packets, may remain readable. Authentication ensures that the requester is connected to the right server and that his or her traffic is not intercepted or modified by a party in between the two. This process usually involves trusted third parties in the form of **certificate authorities** that store, issue, and sign **digital certificates to bind public keys to specific users and organizations**. These certificates may be used to sign other certificates, meaning that there is a hierarchy of certificates. Importantly, the **PKI is a sociotechnical system**. You still have to trust another party (the certificate authority); the system just makes trust transitive.

Transport Layer Security (TLS)[89]: TLS is the main security protocol on the Internet. After a TCP session is initialized, the requester suggests a list of encryption suites that it supports from which the server choses one for content encryption. Further, the server sends a signed public-key certificate to the requester for party authentication. In theory, the user could also be authenticated through a public key certificate. In practice, this is usually organized on a higher layer through usernames and passwords.

In contrast to the DNS, in which all authority ultimately traces back to one root file, the TLS PKI has **multiple roots of trust**. This is possible because certificate authorities do not need to jointly verify the public key of an entity. One verification by one trusted organization is sufficient.

Users can manually accept certificates. However, this is the exception. The vast majority follow the default settings of their operating system and web browser, which contain a whitelist of trusted certificate authorities. This whitelist roughly consists of 150 to 250 root certificates issued by 50 to 100 organizations.[90] The largest certificate providers are IdenTrust, DigiCert, and Sectigo, which are all US firms and have a joint market share of a bit more than 75 per cent.

Certificate authorities can be compromised by intelligence services and similar actors. For example, the Dutch certificate authority DigiNotar was penetrated by one or multiple Iranian actor(s) who used it to issue false certificates for Google, Facebook, and other websites.[91] Similarly, the state-run Chinese root certificate authority has been caught issuing false certificates for Google.[92] In both cases, the goal may have been used to intercept and decrypt encrypted communications from citizens. One attempt to address this issue is certificate transparency. This means that certificate authorities publish public logs of the domain names and corresponding IP-addresses that they certify. This does not prevent a certificate authority from providing a false certification. However, others, including the website owner, can check if the binding is correct.

DNS Security Extensions (DNSSEC): While the use of caching makes the DNS resolution faster and more scalable, it introduces possibilities to poison the DNS cache and inject a false website. Additionally, DNS queries can still be subject to man-in-the-middle attacks. DNSSEC aims to bring authentication to this process through a hierarchical chain of certificates. The global trust root is operated by Verisign and ICANN and stored in two locations in the US. It is occasionally updated in a root signing ceremony.[93] DNSSEC is enabled for most top-level domains.[94]

89 Rescorla, E. (2018). *RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.*3. datatracker.ietf.org

90 See e.g., Apple. (2022). *Available trusted root certificates for Apple operating systems.* support.apple.com; Microsoft. (2022). *Included CA Certificate List*. ccadb-public.secure.force.com

91 Fox-IT. (2011). *DigiNotar Certificate Authority breach 'Operation Black Tulip'.* cryptome.wikileaks.org

92 Langley, A. (2015). *Maintaining digital certificate security*. security.googleblog.com

93 Cloudflare. (n.d.) *The DNSSEC Root Signing Ceremony*. cloudflare.com

94 Internet Society. (2021). *DNSSEC Deployment Maps.* internetsociety.org

However, it is only deployed for a minority of worldwide DNS resolutions (Finland, 91%; Switzerland, 64%; US, 39%; Russia, 38%; China, 1%).[95]

BGP security (BGPsec): From 2006 to 2018, the secure inter-domain routing group at the IETF has worked on making BGP secure. The result of this is the BGPsec protocol[96] and the corresponding Resource Public Key Infrastructure (RPKI). RPKI certificates link an IP address range with an autonomous system number. The five regional Internet registries issue these certificates to resource holders when IP ranges are assigned.

2.2.3 Content

The following is a brief and non-comprehensive list of some of the most important players on the content layer. As Internet users directly interact with the content layer, readers without a technical background will also be familiar with them, except for a few business-to-business services, such as content delivery networks.

Email: An interoperable standard for exchanging messages between computers that precedes the World Wide Web. The most common providers of email clients and addresses are Gmail (US), Microsoft Outlook (US), and Apple Mail (US).

Web browsers: An application for accessing and displaying websites. The most common web browsers on desktop computers are Google Chrome (US, 65%), Apple Safari (US, 10%), Microsoft Edge (US, 10%), and Mozilla Firefox (US, 10%).[97] The most common mobile browsers are Google Chrome (US, 62%), Apple Safari (US, 27%), and Samsung Internet (South Korea, 5%).[98]

Search engines: A software that searches the World Wide Web for relevant information based on a search query. The result is usually a list of websites, but it can also be images, videos, or infographics. The most common search engine is Google (US, 92%). Alternatives include Bing (US, 3%), Yahoo! (US, 2%), Baidu (China, 1%), Yandex (Russia, 1%), and DuckDuckGo (US, 1%).[99]

Social media: Services that allow users to share text, photos, and videos with their social networks. The largest social media platforms by number of active users are Facebook (US, 2.9 billion), YouTube (US, 2.3 billion), Instagram (US, 1.4 billion), TikTok (China, 1 billion) and Kuaishou (China, 1 billion).[100]

Private communication: Apps that enable the exchange of web-based private messages, as well as voice and video calling over IP. The largest private web-based communication providers are WhatsApp (US, 2 billion), Facebook Messenger (US, 1.3 billion), WeChat (China, 1.3 billion), and Telegram (UAE, 600 million).[101]

Cloud services: The on-demand remote availability of data storage, computing power, and many other services from centralized data centers. The largest providers of cloud services are Amazon Web Services (US, 33%), Microsoft Azure (US, 21%), Google Cloud (US, 10%) and Alibaba Cloud (China, 6%).[102]

Content delivery networks: Geographically distributed instances of web content that provide high availability and performance to end users. For example, Netflix has its own content delivery network consisting of about 10,000 server boxes, which has the storage capacity to host a large portion of the locally requested videos on them. The largest content delivery network providers are Akamai (US), Cloudflare (US), and Fastly (US).

e-Commerce: Online shops and marketplaces for digital and physical goods and services. The largest e-commerce companies include Alibaba (China), Amazon (US), JD.com (China), eBay (US), and Pinduoduo (China).

Payment processing: The largest global players for credit cards, which can be used for online and offline payments, are Visa (US, 50%) and MasterCard (US, 26%). The largest online payment processers are PayPal (US) and Stripe (US).

95 APNIC (n.d.). *DNSSEC World Map.* stats.labs.apnic.net

96 Lepinski, M. & Sriram, K. (2017). *RFC 8205: BGPsec Protocol Specification*. datatracker.ietf.org

97 Statcounter (2022). Desktop Browser Market Share Worldwide. gs.statcounter.com

98 Statcounter (2022). Mobile Browser Market Share Worldwide. gs.statcounter.com

99 Statcounter (2022). Search Engine Market Share Worldwide. gs.statcounter.com

100 Dixon, S. (2022). Most popular social networks worldwide as of January 2022, ranked by number of monthly active users. statista.com

101 Ibid.

102 Richter, Felix. (2022). Amazon Leads $180-Billion Cloud Market. statista.com

Cryptocurrencies: Cryptocurrencies offer a monetary exchange system based on public key cryptography, decentralized databases, and a transaction validation mechanism. Given all the talk about a decentralized Web3 based on the blockchain, it is worth highlighting that cryptocurrency transactions rely on the regular Internet infrastructure. Hence, security vulnerabilities, such as BGP hijacking[103], as well as political control levers, such as DNS censorship of cryptoexchanges at ISPs, also apply to it. The largest cryptocurrencies by market capitalization in early 2022 were Bitcoin and Ethereum. The largest exchanges are Binance (Cayman Islands), Coinbase (US), and FTX (Bahamas).

[103] Apostolaki, Maria, Aviv Zohar, and Laurent Vanbever. "Hijacking bitcoin: Routing attacks on cryptocurrencies." In 2017 IEEE symposium on security and privacy (SP), pp. 375-392. IEEE, 2017.

3 How the Internet Could Split

Both fragmentation and bifurcation can occur on different layers of the Internet. If selective local restrictions on the **content layer** count as fragmentation, then the Internet has always been fragmented. For example, China bans access for its citizens to most Western Internet companies. In contrast, the **logic layer** is what unifies and defines todays Internet. A fork in it would cut much deeper. In a sense it would be a return to the "protocol wars", in which multiple host protocols fought over market share from the 1970s to 1990s, with IP eventually gaining critical mass despite the international support for and standardization of the OSI) model. What makes today's situation substantially different is that we already start with a dominant protocol and that the cleavage would not so much be between private companies and nation states but between great powers. Lastly, we can also think of a split on the **infrastructure layer**. Telecommunications infrastructure has traditionally been fragmented in the sense that it was mostly operated by state monopolies until the late 1990s. For this reason, ISPs are still somewhat aligned with political borders. ICT-infrastructure has also become a field of US-China strategic competition, especially with regard to hardware manufacturers, which introduces a bifurcation dynamic.

3.1 Fragmentation

The process terms "Internet balkanization", "Internet fragmentation", and "Internet territorialization" as well as the static terms "bordered Internet", "splinternet", and "sovereign Internet" are used as synonyms or near-synonyms in Internet governance. Broadly speaking, the meaning of these terms is a trend towards, or the condition of non-universal Internet experiences based on the locations of users in sovereign territories. However, their exact meaning is often underspecified and/or inconsistently applied among journalists, think tankers, and scholars.

The term balkanization emerged in the context of the dissolution of the Ottoman Empire and has been used to describe the "parcelization of large and viable political units" with negative connotations as "a reversion to the tribal".[104] In the 1990s, the term regained salience in the context of the dissolution of Yugoslavia and the corresponding conflicts. Van Alstyne and Brynjolfsson (1996) coined the term "cyberbalkans" in contrast to Marshall McLuhan's idea of a global village, and to posit that the Internet will lead to interest-based subcommunities. Conversely, when Sagawa (1997) and Frieden (1998) used the term Internet balkanization they focused on pricing agreements among ISPs and an expected market consolidation. It was not until the mid-2000s that the term started to take on its modern meaning as "a collection of nation-state networks, still linked by the Internet Protocol, but for many purposes separate".[105] Jack Goldsmith and Tim Wu were the first to clearly outline the key issues around location, sovereignty, and the Internet in their book in 2006.[106] Then, in the early 2010s, there was a rhetoric shift away from balkanization to fragmentation to avoid stigmatizing people from the Balkans and possibly also to avoid legal precedent that says "economic balkanization" can only be solved if jurisdiction is transferred to a higher level.[107]

Jonah Hill's report on Internet fragmentation for the Belfer Center in 2012 was the first to clearly distinguish between fragmentation on different layers. The topic of Internet fragmentation really started to gain salience in the wake of Edward Snowden's revelations about the extent of worldwide Internet surveillance by the United States and the subsequent backlash. Specifically, the focus on Internet fragmentation as a threat can be seen as a rhetorical move to defend the multistakeholder model of Internet governance against the sovereigntist reaction.[108] These anti-fragmentation efforts culminated in the 2016 reports by the World Economic Forum and the Global Commission on Internet Governance. These reports helped to create increasingly long lists of actions or trends that conflict with the ideal that "the experience of every Internet user should be the same regardless of geographic location, computer

[104] Todorova, Maria. *Imagining the Balkans.* Oxford University Press, 2009. p.3

[105] Wu, Tim. (2004). *The Balkanization of the Internet.* archives.lessig.org

[106] Goldsmith, Jack and Tim Wu. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.

[107] Alves Jr, Sergio. (2014). *The Internet balkanization discourse backfires.* papers.ssrn.com

[108] Mueller, M. (2017). *Will the internet fragment?: Sovereignty, globalization and cyberspace.* John Wiley & Sons. pp. 13&14

type, or any other distinguishing characteristic of the user".[109]

In 2017, Milton Mueller helped to refocus the debate. He argued that the conception of Internet fragmentation as anything that violates the norm of a uniform Internet experience is too broad to be useful. Indeed, as Goldsmith and Wu had already pointed out there are good reasons why such a universal experience would not be desirable.[110] For example, if you search for "weather", you are more interested in your local weather than that on the other end of the world. According to Mueller, the fragmentation discourse should focus on intentional, permanent, and third-party enforced restrictions of connectivity.[111] At the same time, Mueller remains skeptical that the Internet would ever lose global interoperability on the logic layer.[112] His main argument is that the economic network effects of IP and the DNS are so large that no clean-slate Internet architecture or alternate DNS root can challenge it.

This report generally uses the term Internet fragmentation in the narrow sense. There are many forms of very local technical Internet fragmentation that we are not particularly interested in because they have limited political implications, such as NAT (section 2.2.2). In contrast, it is also worth highlighting that some actions that do not strictly qualify as fragmentation are still of interest as they are part of Internet "territorialization", "sovereignization", "borderization", or "nationalization". **On a global scale, an increasing national control of the Internet amounts to a deglobalization and decentralization. However, from a country perspective, Internet territorialization will generally imply the opposite,** namely, more centralized control over data flows. For example, there are currently about 100,000 ASes with independent routing policies. If states legally mandate routing policies, this number would go down to about 200. In a similar vein, Russia has reduced the number of IXPs on its territory to exert greater state control over the Internet. All Internet connections between China and the world go through one of three government monitored IXPs in Beijing, Shanghai, and Guangzhou, whereas HongKong alone has 10 different IXPs. Lastly, it is worth highlighting that the trend towards fragmentation or bifurcation is not uniform. There are some subsections of the Internet that are still becoming more global (e.g., recursive DNS resolution, section 2.2.2.5).

The author has reviewed a total of **36 articles on Internet fragmentation published by academic journals, think tanks, and major news outlets, which are summarized in Annex E**. In this literature, the term Internet fragmentation has been used to refer to a **wide variety of Internet governance issues**. Furthermore, Internet fragmentation is a **Western-dominated discourse**, and, with very few exceptions, the term is used with **negative connotations.** The implicit or explicit assumption in most publications is that the current Internet is global and that it should stay this way.

As highlighted in figure 3, the most frequently mentioned topic is state censorship. However, with respect to the logic layer, which is the focus of this report, the three leading issues identified in the reviewed articles are a **fragmented namespace**, **competing standardization bodies and standards**, as well as the **IPv6 transition**. These three issues are explained in more detail in the following subsections. Finally, to make fragmentation more tangible, section 3.1.4 goes through the specific **case study of the separation dynamics between the Russian and the global Internet**.

[109] Hill, Jonah. (2012). *Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers.* belfercenter.org p. 12

[110] Goldsmith, Jack and Tim Wu. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press. p. 51

[111] Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization and cyberspace. John Wiley & Sons. p. 32

[112] Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization and cyberspace. John Wiley & Sons. pp. 42-70.

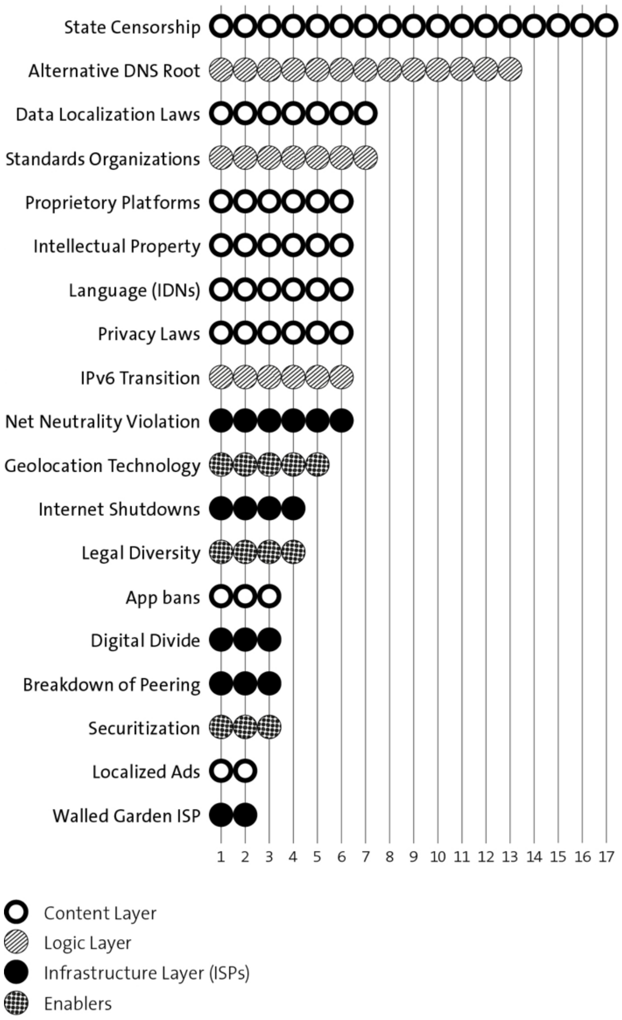


Figure 3. Frequency of concrete issues mentioned multiple times in 36 publications on Internet fragmentation.

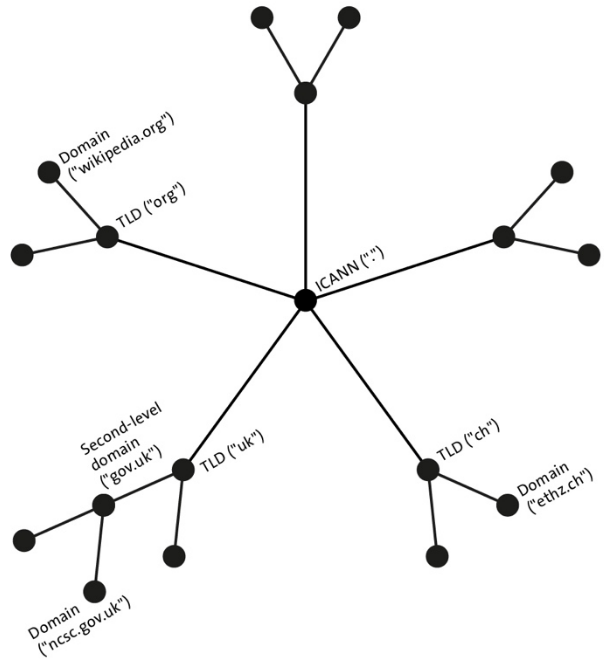


Figure 4. Visualization of a hierarchical DNS.

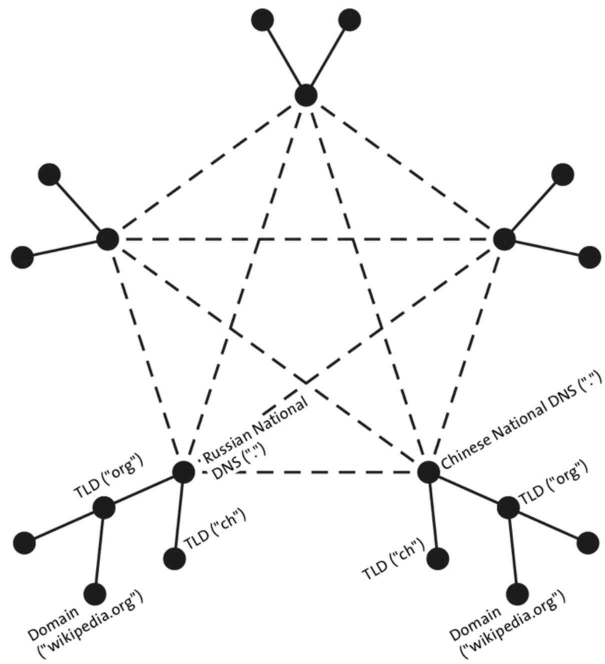


Figure 5. Visualization of a federated DNS.

3.1.1 Alternative DNS root

What makes the DNS root (section 2.2.2.5) a frequent center of contention is that it is a centralized point of control on the logic layer. The current DNS ensures that there is one namespace with globally unique names through a hierarchical structure. Maintaining the current DNS at ICANN is a fundamental position of Western and "like-minded states" that support multistakeholder Internet governance. In contrast, the geopolitical rivals of the US would prefer more national control over the DNS in a federated structure that is closer to how telephone numbers are assigned and resolved.[113]

Proposals for a federated DNS have no support at ICANN and, so far, have not been successful at the ITU. Hence, Russia has been the first and only country to unilaterally create a national DNS root. If other countries choose to follow Russia in developing national root alternatives, such a group might coordinate through the ITU or another standards organization, leading to a split in global standards (section 3.1.2).

[113] See e.g., Diao, Yuping, Yongping Diao, & Ming Liao. (2012). *DNS Extension for Autonomous Internet (AIP)*. datatracker.ietf.org

Alternate DNS-roots have existed in various forms and for various reasons. Yet so far none of them has gained sustained and widespread support. The split that reached the largest part of the Internet was arguably the one ordered by Jon Postel in 1998 (section 2.1.2.2). However, that did not last for long.

There are three main motivations for creating alternate DNS roots. The first is namespace expansion, as an alternate DNS root can provide more freedom in choosing generic top-level domains and to earn money from alternate domain name registrations. This was the main motivation for the creation of AlterNIC and OpenNIC. However, the case for namespace expansion has become a lot weaker as ICANN has decided to liberalize the creation of new gTLD in 2011.[114] Since then, the number of gTLDs listed in the ICANN root file has expanded from 22 to more than 1,300.[115]

The second reason why actors might pursue an alternate DNS root is a desire for more autonomy from ICANN and the US government. This was the main motivation for the creation of the Open Root Server Network and the Russian national DNS. However, there is obviously a qualitative difference between the privately maintained Open Root Server Network and the Russian national DNS, whose use is legally mandated for all Russian ISPs. The concern of autonomy from the US can also be extended to DNSSEC, because it depends on a centralized trust root that is located in the United States.

Finally, actors might adopt an alternate DNS root to create a more decentralized and censorship-resistant Internet. This includes a desire for more autonomy on the individual level from any state or large tech company. Blockchain-based DNS roots have decentralized rather than federated structures and may provide additional functionalities that support decentralization.

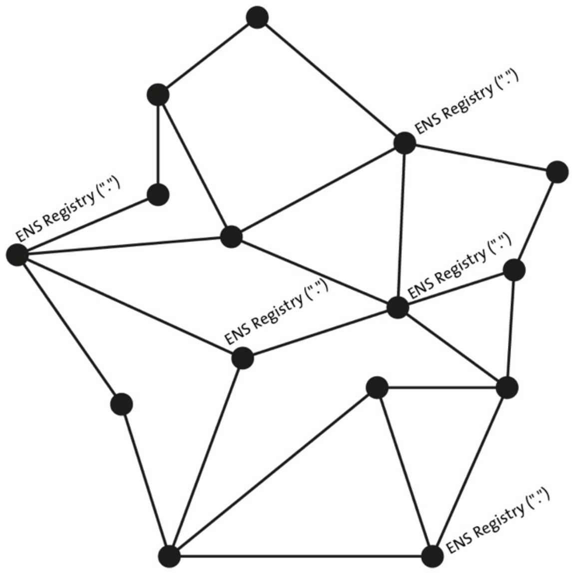


Figure 6. Visualization of a distributed DNS.

Western technologists, such as the "father of the Internet", Vint Cerf, have framed government-backed alternate DNS roots as the "mother of all fragmentations".[116] In a similar vein, the Internet Architecture Board is very critical of any namespace fragmentation.[117] Even Yeti DNS, which is only a testbed for DNS changes, has been criticized for providing technical assistance to countries (most notably China) that might want to set up their own national or regional DNS.[118] Unauthorized name space expansion amounts to squatting. However, its effects are relatively benign. A root that purposefully does not link to officially recognized domains is of more concern. This would amount to censorship and undermine the global reach of Internet brands. Lastly, confrontational roots that assign different IP addresses to the same name would lead to confusion and misdirected traffic.[119]

[114] ICANN. (2011). *ICANN Approves Historic Change to Internet's Domain Name System | Board Votes to Launch New Generic Top-Level Domains*. icann.org

[115] ICANN. (2022). *Delegated Strings*. newgtlds.icann.org

[116] Drake, W., Cerf, V. & Kleinwächter, W. (2016). Internet fragmentation: An overview. weforum.org p. 28

[117] Internet Architecture Board. (2000). *RFC 2826: IAB Technical Comment on the Unique DNS Root*. datatracker.ietf.org

[118] Kuerbis, Brenden & Milton Mueller. (2016). *Alternate DNS roots and the abominable snowman of sovereignty*. internetgovernance.org

[119] Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization and cyberspace. John Wiley & Sons. pp. 37-41; Bertola, Vittorio.(n.d.) *Oversight and multiple root server systems*. wgig.org

Name	Status	Description
AlterNIC	Defunct	AlterNIC was an alternative domain name registry launched in 1995 to challenge the monopoly of Network Solutions. It offered many new gTLDs such as ".alt", ".biz", ".usa", ".xxx", & ".wired".
Blockchain-based DNS	Active	There are several start-ups that aim to provide blockchain-based registries for domain names, usually coupled with the goal of being censorship-resistant. The oldest project is Namecoin, which allows the registry for the alternate ".bit" top-level domain. Other blockchain-based registries include Handshake and Blockstack. Given their permissionless design, blockchain-based registries have raised concerns about allowing the spread of malware and child pornography.
Decentralized Internet Resource Trust Infrastructure[120]	Experimental	This is not an alternate DNS but an alternate security protocol for DNS. Huawei and CNNIC experiment with a permissioned ledger on Ethereum on which IP addresses can be requested and mapped to an AS based on smart contracts. The experimenters proposed to use this to replace the trust roots in DNSSEC and PKI.
Ethereum Name Service (ENS)	Active	ENS is a naming protocol that uses smart contracts on the Ethereum blockchain to perform the registry, registrar, and resolver function. ENS is developed by the Singapore-based True Names Ltd., but it has also issued a governance-token that enables holders of the token to suggest and vote on protocol changes. The primary purpose of ENS is to bind human-readable names to the public key of cryptocurrency wallets. For example, if you wanted to send Ether to Vitalik Buterin, the founder of Ethereum, you could send it to "vitalik.eth" through a browser with native support (e.g., Brave) or with a plug-in (e.g., Metamask for Chrome). However, the ENS has additional functionality: it can also include content, text records, and DNS records. For example, it can also serve as a decentral registry of ".onion" addresses and enables decentralized websites.
OpenNIC	Active	OpenNIC is a user-owned and -controlled alternative TLD registry. For example, it links to alternative two-letter ccTLD for internationally unrecognized nations, such as Tibet or Kurdistan. At the same time, it does recognize all existing TLDs by ICANN.
Open Root Server Confederation	Defunct	The Open Root Server Confederation is a non-profit founded in 1998 that aimed to compete with ICANN for the US government contract to fulfill the IANA function.
Open Root Server Network	Defunct	The ORSN operated from 2002 to 2008 and again from 2013 to 2019 as a system of 13 root servers located in Europe and India that synchronize daily or manually with the DNS root servers by ICANN except for TLDs that are removed. As such, it was meant to provide an independent back-up to mitigate unilateral deletions or reassignments of TLDs.
RealNames	Defunct	RealNames was a keyword-based alternate domain registry that did not follow the hierarchical name structure of the DNS but simply translated words into IP numbers (e.g., "pizza" rather than "pizza.com"). It was integrated into Microsoft's Internet Explorer from 1997 to 2002. Thereafter Microsoft decided to resolve words typed into the browser address bar into the MSN search engine.
RHINE	Active	RHINE is the clean-slate DNS redesign by SCION. RHINE is a flexible naming protocol in the sense that it can be used to point to the global ICANN root but also to any alternative DNS root (see section 4.4.1).
Russian National DNS	Active	In 2019, Russia introduced a series of amendments, informally referred to as "Sovereign Internet Law", which include the creation of a national DNS. Implemented in 2021, all Russian ISPs are forced to rely on root servers under the control of Roskomnadzor. Roskomnadzor is the federal agency responsible for monitoring, controlling, and censoring mass media and also has policy authority over the namespace (see section 3.1.4.2).
Yeti DNS	Experimental	Yeti DNS is an experimental root server testbed that provides an environment where experiments such as IPv6-only operation or key signing key rollovers can be performed without risk to the operational root server infrastructure. Its primary research partner is the Beijing Internet Institute.
.chn	Active	.chn is a top-level domain with its own root DNS server for the Internet of Things in China.

[120] Bingyang Liu, Fei Yang, Marcelo Bagnulo, Zhiwei Yan, Qiong Sun. 2018. Decentralized Internet Resource Trust Infrastructure. 2018. datatracker.ietf.org

Special-use domain names: There are certain forms of namespace fragmentation that are sanctioned by the IETF. Specifically, the IETF has reserved certain domain names for local use, and it tolerates or even promotes the use of alternative namespaces that are used to evade censorship and control by states.

Name	Status	Description
.local	active	Not intended to be used in the global DNS, reserved for hostnames in local area networks.
.test	active	Not intended to be used in the global DNS, reserved for use in the testing of software.
.onion	active	The Onion Router Project (Tor) provides free software originally developed by the US military in the 1990s. Its more than two million users use it for services in which both the provider and the user are anonymous and difficult to trace. Onion addresses are opaque strings of base32 characters generated from public keys (e.g., 27m3p2uv7igmj6kvd4ql3cct5h3sdwrsa-jovkkndeufumzyfhlfev4qd.onion). In 2015, ICANN and the IETF formally accepted ".onion" as a special use domain of which there is no central registry.

Pseudo top-level-domains: The namespace of non-IP computer networks. Specifically, some of the networks that co-existed with Arpanet during the "protocol wars" and sites accessible through the invisible internet protocol.

Name	Status	Description
Historic networks	defunct	Used to forward emails to addresses in non-Internet networks, such as BITNET, CSNET, or UUCP.
Not formally accepted anonymous networks.	active	Most notably, the Invisible Internet Project (I2P), which uses the ".i2p" top-level domain. It is designed to provide access to "eepsites", which are the sites hosted within the I2P intranet.

3.1.2 Standards Organizations

The institutional location of Internet standards development is a central and longstanding issue in Internet governance. Most Western states, tech giants, and civil society prefer the current **multistakeholder model of Internet governance centered around ICANN and the IETF**. In contrast, China, Russia and a number of other states have long been pushing for **multilateral Internet governance centered at the ITU**. These views have clashed at venues such as the World Summit on the Information Society (2003 and 2005) and the World Conference on International Telecommunications (2012). Theoretically, they could lead to a bifurcation of Internet standards at some point.[121] The relation to Internet fragmentation is the assumption that an Internet governed by states would subsequently lead to policy changes that enable more intelligence in the network, as well as more national control of the DNS, IP addresses, and autonomous system numbers.

Multistakeholderism vs. Multilateralism

Despite its name, the multistakeholder model can be close to private global governance in practice, as Mueller highlights.[122] Specifically, the IETF does not allow any representatives of governments and representatives of civil society play a very marginal role. In contrast, ICANN does have a Governmental Advisory Committee (GAC). However, the GAC is a consultative body that is only represented with one non-voting seat in the ICANN Board. The element of the multistakeholder Internet governance complex that really includes governments, the private sector, and civil society to a significant degree is the Internet Governance Forum. However, the Internet Governance Forum is a place for exchange and does not have any decision-making capacity.

Western states and US-tech giants argue that the Internet can only remain nimble if it is run by technical experts, and that the ITU would be a too political and slow decision-body. Furthermore, US tech giants are the principal economic winners of a globalized

[121] Klimburg, Alexander. (2013). "*The Internet Yalta*" cnas.org.

[122] Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization and cyberspace. John Wiley & Sons. pp. 116&117

online market and liberal forces do not want to give authoritarian states, such as China, Russia or Saudi Arabia, more influence over the development of the Internet. In contrast, these states argue that the ITU should govern the Internet[123] as states have more legitimacy than non-state actors and as developing countries find it difficult to follow and meaningfully participate in the decentralized Internet governance complex. However, the main concern of China and Russia arguably remains that the United States has disproportionate influence in the current multi-stakeholder model, which they view as "a front for maintaining Western-centric dominance" of the Internet.[124]

3.1.3 IPv6 Transition

The transition from IPv4 to IPv6 as a response to IPv4 address exhaustion has theoretically split the Internet in two. Furthermore, the transition went slowly, and organizations used network address translation (NAT) as a mitigation measure rather than switching to IPv6, which has created Internet fragmentation albeit at the level of local area networks rather than at the level of nation states. Overall, the **IPv6 transition is not a politically contested issue** because it is about two versions of IP that have been standardized by the IETF and that follow the same "smart endpoints and dumb pipes" design principles.

IPv4 address exhaustion: The IPv4 address space was large when it was standardized in 1981, as ARPANET only connected a bit more than 200 computers at that time. However, with the establishment of IP as the global internetworking standard in the early 1990s it became clear that the 4.3 billion unique IPv4 addresses would eventually be exhausted. The solution on which the IETF agreed in 1998 was to increase the size of the IP-address field to extend the amount of available globally unique IP numbers. However, the resulting new standard **IPv6 fails to be backwards compatible with IPv4**, which means that strictly speaking there have been two internets ever since. This incompatibility has meant that service providers have had to implement dual-stack solutions to connect IPv6 addresses to the rest of the Internet and were generally not economically incentivized to do so. Instead, they have relied on mitigation strategies, most notably network address translation, which is explained below. However, as the problem of IPv4-exhaustion has gotten more pronounced, IPv6 adoption has finally taken off in recent years. The last available block of IPv4 addresses was assigned by ICANN to regional Internet registries in 2011. The regional Internet registries themselves all ran out of new addresses between 2011 and 2020. IPv4 addresses that are no longer needed can still be recycled but for all practical purposes, the IPv4 number space is exhausted.

Network Address Translation (NAT): NAT is a local label-switching process to conserve IP addresses. The basic principle is that multiple devices behind a NAT box share a common public IP address towards the outside world. When a computer behind a NAT box sends a packet, the NAT box rewrites the source address of the packet with its own address but remembers the internal IP address and port number of the packet. When an incoming packet arrives for a stored port number, the NAT box rewrites the destination address of the incoming packet with the correct local address. For incoming packets without a prior outgoing packet, such as when hosting some content behind a NAT box, finding a good solution is more complicated, or it may just revert to a manual static configuration. In specific terms, this means that the wireless local area networks (WLAN) networks deployed at home are usually private networks using internal IP addresses within specified number ranges for their devices that are only locally unique. These ranges are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. **NAT is a violation of the principle of a global address space**. However, it is different from telephone number prefixes in the sense that its governance does not follow political borders and that the **fragmentation mostly happens at the level of local area networks**.

A number of countries ranging from Germany[125] to China[126] have encouraged the public administration

[123] e.g., President of Russia (2022, February 4). Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development. en.kremlin.ru section 3, para. 23

[124] Lantis, J., & Bloomberg, D. (2018). Changing the Code? Norm Contestation and US Antipreneurism in Cyberspace. *International Relations 32*(2), 149–172. p. 156

[125] Der Beauftragte der Bundesregierung für Informationstechnik. (2019). IPv6-Masterplan für die Bundesverwaltung. frag-den-staat.de

[126] Cyberspace Administration of China. (2021). 关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知［Notice on Accelerating the Large-scale Deployment and Application of Internet Protocol Version 6 (IPv6)]. cac.gov.cn

and business community to switch to IPv6. Switzerland could also consider if it wants to provide technical guidance and support to government agencies or SMEs in their the IPv6 transition. This also involves some security considerations, as highlighted in the IPv6 guidance issued by the US Cybersecurity and Infrastructure Security Agency (CISA).[127]

3.1.4 Case Study: Russia

Publications about Internet fragmentation focus on a range of case studies reflecting the variety in how the term is understood. For example, there are closed-off autocracies with a high demand for control over domestic information flows, such as North Korea and Iran. However, there are also actors that aim to partially balance US dominance with strong privacy regulations, such as the European Union. Still, Russia is arguably the main poster child of Internet fragmentation because of how systematic and persistent its efforts to create an independent national segment in the global Internet are, and because it is a major military and energy power that opposes the US-led international order but lacks the ICT industry or market size to strongly shape the Internet beyond its borders. The applied example of Russia highlights several issues mentioned in the Internet fragmentation discourse, including state censorship, a national DNS root, and a breakdown of peering. Further, it also highlights the issue of national encryption, which has mostly been overlooked in the discourse.

3.1.4.1 Domestic Surveillance and Censorship

Asserting strong state control over communications networks has a long tradition in Russia.[128] The System for Operative Investigative Activities (SORM) hardware-devices by the FSB, Russia's domestic intelligence service, are middle boxes that are installed at ISPs and allow the domestic intelligence service to surveil data traffic without any consent from ISPs or a court order. The first generation of SORM was deployed in the 1990s. The current third generation of SORM started to be deployed in 2014 and includes some deep-packet inspection capability.[129] Additionally, in 2016, the so-called "Yarovaya package" forced all Russian ISPs to retain data, including video, phone calls, and text messages, for six months. The metadata must be kept for three years.[130] In terms of censorship, Russia passed a law in 2012 requiring the establishment of an Internet blacklist. ISPs are forced to block requests to IP addresses associated with these websites.[131]

3.1.4.2 Runet

Runet is a term describing the Russian national segment of the Internet. Over the years, Russia conducted various tests in implementing a national DNS. Similarly, Russia has prepared to replace TLS certificates issued by Western companies through a government-issued certificate since at least 2016. The company which was foreseen to implement the certificates on behalf of the Russian government has links to the Russian domestic intelligence service.[132] Given this and the example of the misuse of government-issued certificates by the former Soviet Republic Kazakhstan,[133] outside observers may view this as a tool for domestic surveillance.

In 2019, Russia passed the so-called "Sovereign Internet Law" or "Sovereign Runet Law", a series of amendments aimed at more centralized management of network by the government.[134] The most important aspect of the law is that it requires the creation of a national DNS, and that ISPs are required to use this for domain name resolution. Other aspects include that IXPs must disconnect non-compliant ISPs and, vice versa, ISPs are forbidden from connecting to IXPs that are not approved in a registry of Roskomnazdor, the Federal Service for Supervision of Communications, Information Technology and Mass Media. In the same year, Russia also intro-

[127] CISA. (2022). Internet Protocol Version 6 Considerations for Trusted Internet Connections 3.0. cisa.gov

[128] ITU. (1875). Convention télégraphique internationale de Saint-Pétersbourg et Règlement et tarifs y annexés. search.itu.int

[129] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. Media and Communication, 5(1), 29-41.

[130] Duma. (2016). О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности [On Amendments to the Federal Law "On Combating Terrorism" and Certain Legislative Acts of the Russian Federation in Part of Establishing Additional Measures to Counter Terrorism and Ensuring Public Security]. pravo.gov.ru. Art. 13

[131] Duma. (2012). О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации [On Amendments to the Federal Law "On the Protection of Children from Information Harmful to Their Health and Development" and Certain Legislative Acts of the Russian Federation]. publication.pravo.gov.ru

[132] Kolomychenko, M. (2016, February 15). Рунет прикроют сертификатом [Runet will be covered with a certificate]. kommersant.ru

[133] Raman, Ram Sundara, Leonid Evdokimov, Eric Wustrow, Alex Halderman, Roya Ensafi (2019). Kazakhstan's HTTPS Interception. censoredplanet.org

[134] Duma. (2019). О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации" [On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection"]. publication.pravo.gov.ru

duced a law that required the preinstallation of Russian apps and a Russian search engine on newly sold smartphones in a bid to boost local alternatives to global products.[135]

3.1.4.3 Russian Invasion of Ukraine

The full-scale Russian invasion of Ukraine in February 2022 has led to a significant speed-up in the separation of Russia's national segment of the Internet from the global Internet. The drivers of this trend are stricter Russian domestic censorship as well as Ukrainian and other Western efforts to isolate Russia internationally as a punishment for its war of aggression. The 31-year-old Minister of Digital Transformation and Vice Prime Minister of Ukraine Mykhailo Fedorov has shown particular resourcefulness in leveraging social media for public diplomacy to that end.[136]

Infrastructure layer

Hardware sanctions and market exits:
About 1,000 multinational companies have suspended their business activities in Russia or at least suspended orders for new products or services.[137] This notably includes some Chinese tech firms that could be hit by secondary sanctions from the US.[138] The list includes key device manufacturers such as Apple, Dell, HP, LG, Lenovo, Samsung, and Xiaomi. It includes key semiconductor manufacturers, such as AMD, ARM, Intel, Micron, Nvidia, Qualcomm, Samsung, and TSMC. It includes networking device manufacturers Juniper and Huawei, as well as fiber companies Corning, NEC, and Fujitsu. Lastly, it includes the RAN equipment manufacturers Nokia, Ericsson, and Huawei. Nokia was also a key supplier for SORM.[139]

Short-term mitigation efforts by Russia include a temporary export ban on many goods, including all electronics that are not produced within Russia, intended to stop foreign companies from relocating assets,[140] buying out or confiscating computer infrastructure from the private sector,[141] suspending some of the "Yarovaya" requirements to store videos for domestic surveillance,[142] and legalizing imports of many goods, including semiconductors, without the permission of the copyright holder from its list of "unfriendly" countries.[143]

ISP connectivity: Two of the largest transit ISPs, Lumen and Cogent, have announced that they are ceasing to deliver packets to or from Russia. Lumen stated that their "physical network is disconnected in Russia – all the way down to the hardware". However, they still do "provide services to ISPs outside Russia who are routing traffic into the country."[144] This clarification is quite important. According to Cisco, many packets exchanged between Western and Russian computers still go through Lumen and Cogent with one additional intermediary before going into Russia, thus the overall backbone Internet connectivity has not been significantly affected.[145]

---

[135] Duma. (2019). О внесении изменения в статью 4 Закона Российской Федерации "О защите прав потребителей" [On Amending Article 4 of the Law of the Russian Federation "On Protection of Consumer Rights"]. publication.pravo.gov.ru

[136] Fedorov, M. [@FedorovMykhailo]. (2022). I've contacted @tim_cook, Apple's CEO, to block the Apple Store for citizens of the Russian Federation, and to support the package of US government sanctions! If you agree to have the president-killer, then you will have to be satisfied with the only available site Russia 24.; I've addressed the @Google to stop supplying Google services and products to Russian Federation. Including blocking access to Google market and Google Pay. We are sure this will motivate proactive youth to stop this war!; We've also asked @Netflix for the support. We appealed to them to block the Russian Federation's access to Netflix and shut off Russian content. We believe you do care. Let's stop this disgraceful bloody war!; We are constantly working on development of aggressor's isolation! I've contacted the CEO of Rakuten (@Viber) and @PayPal on blocking their services in russia. Youth and thinking russians, you better wake up!; Russia started a disgraceful war in my country! In 2022 cruise missiles target residential neighborhoods, kindergartens and hospitals. I address @Visa and @Mastercard to block their services on all cards issued within the Russian Federation @VisaNews @Mas; More sanctions imposed — faster peace restored in Ukraine! I've addressed to @SAP and @Oracle for support! twitter.com

[137] Sonnenfeld, J. and the Yale Research Team (2022). Almost 1,000 Companies Have Curtailed Operations in Russia—But Some Remain. som.yale.edu

[138] Fischer, S. (2022). Quiet Compliance: China's Dilemma Over Western Sanctions Against Russia. isnblog.ethz.ch

[139] Satariano, A., Mozur, P., Krolik, A. (2022, March 28). When Nokia Pulled Out of Russia, a Vast Surveillance System Remained. nytimes.com

[140] Government of the Russian Federation. (2022, March 9). О мерах по реализации Указа Президента Российской Федерации от 8 марта 2022 г. № 100 [On measures to implement the Decree of the President of the Russian Federation of March 8, 2022 No. 100] static.government.ru

[141] Korolev, Nikita & Julia Tisina (2022, March 15). Цодразверстка. kommersant.ru

[142] Government of the Russian Federation. (2022, March 28). О внесении изменений в Правила хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи, приостановлении действия отдельного положения указ [On Amendments to the Rules for the Storage by Telecom Operators of Text Messages of Users of Communication Services, Voice Information, Images, Sounds, Video and Other Messages of Users of Communication Services, Suspension of a Separate Provision of the Said Rules and Recognition of the Decree of the Government of the Russian Federation dated June 16, 2021 as invalid. No. 914]. static.government.ru

[143] Ministry of Industry and Trade (2022, April 19). Об утверждении перечня товаров (групп товаров), в отношении которых не применяются положения подпункта 6 статьи 1359 и статьи 1487 Гражданского кодекса Российской Федерации при условии введения указанных товаров (групп товаров) в оборот за пределами терри. [On approval of the list of goods (groups of goods) in respect of which the provisions of subparagraph 6 of Article 1359 and Article 1487 of the Civil Code of the Russian Federation do not apply, subject to the introduction of these goods (groups of goods) into turnover outside the territory of the Russian Federation by right holders (patent holders), as well as with their consent]. publication.pravo.gov.ru

[144] Lumen. (2022). Lumen's Readiness to Meet Global Events. news.lumen.com

[145] Internet Research Team. (2022, March 11). *Russia and the Global Internet.* thousandeyes.com

IXPs: The London Internet Exchange has disconnected the Russian ISPs Rostelecom and Megafon.[146] However, the impact of this remains very limited as both are still present at other IXPs, such as DE-CIX in Frankfurt.[147]

Logic layer

DNS: The Ukrainian Ministry of Digital Transformation has asked ICANN[148] and the Regional Internet Registry for Europe, RIPE NCC, to remove Russian TLDs from the DNS root file and to deregister IP numbers that had been assigned to Russian ASes. Both organizations rejected these requests, highlighting that "the DNS must remain neutral"[149] and that this neutrality acts "in support of the global Internet".[150] If ICANN were to restrict access to segments of the Internet as a punitive action, this "would have devastating and permanent effects on the trust and utility of this global system".[151] This sentiment was echoed by the Internet Society[152] and other civil society organizations.[153]

However, both ICANN and regional Internet registries still need to comply with sanctions of countries in whose jurisdiction they are registered. Specifically, EU sanctions prohibit RIPE NCC from assigning new blocks of IP addresses to sanctioned Russian entities.[154]

TLS certificates: Ukraine's campaign to disconnect Russia from the global Internet was more successful with regard to certificate authorities. On 15 March, the Ukrainian Minister of Digital Transformation announced that "at the initiative of the Ministry of Finance, the main companies that issue SSL and TLS security certificates for websites, namely GeoTrust, Sectigo, DigiCert, Thawte, Rapid, have stopped working in Russia and Belarus."[155] At least for the world's second largest certificate provider, DigiCert, this can be independently confirmed on their website.[156]

Russia has subsequently started to offer its own free substitute certificate to businesses[157] and has mandated banks and a total of 198 websites to switch to it. However, since this certificate authority is not whitelisted on Western devices or browsers, users have to manually confirm that they trust this certificate. Therefore, Russia advises its citizens to use Russian-made browsers Yandex and Atom, which have whitelisted the governmental certificate. Privacy-focused organizations, such as the Electronic Frontier Foundation, warn that Russian government-mandated certificates could be misused for surveillance and should not be trusted.[158]

Content layer

Domestic narrative control: Russia took steps to assert control over its domestic media prior to the invasion. In December 2021, Gazprom, which is majority-owned by the Russian government, has acquired a majority of VK, the country's largest social network.[159] Several platforms have also reported a noticeable uptick in pro-Kremlin troll accounts prior to the invasion.

Domestic censorship: On 4 March, the Russian parliament criminalized the "public dissemination under the guise of reliable messages of knowingly false information containing data on the use of the Armed Forces of the Russian Federation in order to protect the interests of the Russian Federation and its citizens, maintain international peace and security", with a fine of up to 1.5 million rubles or up to three years in jail. If the "disinformation" causes "grave consequences" the prison term is up to 15 years.[160] As a consequence, critical Russian media outlets, such as Echo of Moscow and Dozdh, were forced to end their operations.[161] On 22 March, the Duma introduced amendments that expanded the ban on

[146] Moss, S. (2022). London Internet Exchange disconnects Megafon and Rostelecom. datacenterdynamics.com

[147] DE-CIX. (2022). Angeschlossene Netzwerke in Frankfurt. de-cix.net

[148] Nabko, A. (2022, March 1). *Ukraine urgently need ICANN's support.* atlarge-lists.icann.org

[149] Holen, H. (2022, March 10). RE: Official Request from Ukrainian Government to Help Stop Russian War. ripe.net

[150] Marby, G. (2022, March 2). Letter to Mykhailo Fedorov. icann.org

[151] Ibid.

[152] Sullivan, A. (2022, March 2). *Why the World Must Resist Calls to Undermine the Internet*. internetsociety.org

[153] Access Now et al. (2022, March 10). Civil society letter to Biden Admin re Russia sanctions and internet access. accessnow.org

[154] Fragkouli, A. (2022, March 18). EU Sanctions and Our Russian Membership. labs.ripe.net

[155] Fedorov, M. (2022, March 15). https://t.me/zedigital/1364

[156] DigiCert. (2022). Embargoed Countries & Regions. knowledge.digicert.com

[157] Public Services Portal of the Russian Federation (2022). Получите электронный сертификат безопасности [Get an electronic security certificate]. gosuslugi.ru

[158] Hancock, Alexis. (2022). You Should Not Trust Russia's New "Trusted Root CA". eff.org

[159] Marrow, A. (2021, December 3). *CEO of Russia's VK resigns as state assumes control of internet firm.* reuters.com

[160] Duma. (2022, March 4). Вводится ответственность за распространение фейков о действиях ВС РФ [Responsibility is introduced for spreading fakes about the actions of the RF Armed Forces]. duma.gov.ru

[161] Human Rights Watch (2022, March 4). Russia: With War, Censorship Reaches New Heights. hrw.org

criticizing the armed forces to banning criticism of all Russian government actions abroad.[162]

Blocking Western media: Russia has withdrawn press accreditation of some foreign journalists, including the entire staff of Deutsche Welle.[163] Furthermore, many Western media outlets, such as Bloomberg,[164] suspended their in-country reporting after Russia's censorship law was introduced. Furthermore, Roskomnazdor has instructed Russian ISPs to block access to Facebook, Twitter, and the open-source intelligence website Bellingcat in March 2022**.**

Restrictions on Russian media abroad: Ukraine has campaigned to remove Russian media from Western Internet platforms. The EU has banned Russia Today and Sputnik, both Russian state outlets aimed at foreign audiences.[165]

Market exits: Encouraged by Ukrainian social media campaigns, many Western B2B web services have suspended some or all of their services on the territory of Russia. This includes cloud giants Amazon, Microsoft, and Google. Additional companies include financial service providers Visa, Mastercard, and Paypal, as well as content delivery platform Akamai.

Russian substitutes: In order to deal with the fallout from sanctions, exits, and bans of popular Western software, apps, and platforms, Russia uses compulsory licensing and promotes national clone versions of popular apps and platforms, such as RuTube (YouTube), Rossgram (Instagram), and RuStore (PlayStore).[166] However, so far, all of them suffer from major issues.

In summary, the Russian internet is becoming more insulated on all layers, but it remains interoperable as evidenced by the use of Russian online sources in this section. The largest threat to interoperability likely comes from Russian websites that are forced to use certificates that need to be manually deemed trustworthy or may be blocked by most browsers, so that they will become inaccessible from outside of Russia. While Russia may succeed at its goal of asserting more control over the domestic Internet discourse, it has not managed to convince a group of countries to follow suit in nationalizing their Internet segment, and its involuntary cut-off from Western technology as punishment for its invasion means that the costs of the growing insulation vastly exceed any perceived benefits. Only China has an ICT-ecosystem that is a near-peer rival to the US.

3.2 Bifurcation

The US and China are in a global strategic competition over power and values.[167] This competition is particularly intense in high technology and is sometimes also referred to as a "tech war" or "tech Cold War".[168] However, the US and Chinese economies and tech sectors are much more intertwined than that of rivaling states in previous examples of great power competition. Hence, scholars discuss this competition in terms of weaponized interdependence and intentions on both sides to reduce vulnerabilities and to decouple supply chains. This decoupling may remain limited to specific key areas while the cooperation in many other sectors remains intact. This is also framed as the "small yard, high fence" model or the "porous curtain".[169] However, it may not stop there. In his speech to the 74th UN General Assembly in 2019, UN Secretary General António Guterres warned about "the possibility of a Great Fracture: the world splitting in two, with the two largest economies on earth creating two separate and competing worlds, each with their own dominant currency, trade and financial rules, their own internet and artificial intelligence capacities, and their own zero sum geopolitical and military strategies."[170] Along these lines, Internet bifurcation is to be understood as a subtrend of US-China decoupling and denotes the development towards separate Chinese and American Internet ecosystems

[162] Duma. (2022, March 22). Приняты поправки об ответственности за фейки о работе госорганов РФ за рубежом [Amendments on liability for fakes about the work of state bodies of the Russian Federation abroad have been adopted]. duma.gov.ru

[163] DW (2022, March 2). Russia shuts DW's Moscow bureau, withdraws staff credentials. dw.com

[164] Gregori, R. (2022, March 4). Bloomberg to Temporarily Halt Work of Its Journalists in Russia. bloomberg.com

[165] Council of the European Union. (2022, March 2). Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions. eur-lex.europa.eu. Art. 1

[166] Reuters. (2022). Russia's VK launches RuStore for apps after exit of Western alternatives. Reuters.com

[167] See e.g., Pillsbury, Michael. *The hundred-year marathon: China's secret strategy to replace America as the global superpower*. Henry Holt and Company, 2015. Doshi, Rush. *The Long Game: China's Grand Strategy to Displace American Order,* 2021.

[168] See e.g., Segal, Adam (2020). The Coming Tech Cold War With China. foreignaffairs.com

[169] Laskai, Lorand & Samm Sacks. (2018). The Right Way to Protect America's Innovation Advantage. foreignaffairs.com

[170] Guterres, António. (2019). *Address to the 74th Session of the UN General Assembly*. un.org

and supply chains. In line with the "tech cold war" analogy, this has also been framed as a "digital iron curtain". 5G standards and Internet architecture are the most frequently cited areas of contestation. However, it may ultimately divide the entire technology stack. Furthermore, it also includes attempts to shape and control strategic points of cyberspace that include third parties, such as standardization forums.

On the infrastructure layer, key areas of competition include the manufacturers of computer chips, antennas, routers, smartphones and their operating systems, IXPs, undersea cables, and the handful of ISPs that operate this infrastructure in each country. On the logic layer, key areas include numbering and naming resources, DNS root servers, certificate authorities, as well as the bodies governing them, such as the IETF, ICANN, ITU, and the IEEE. On the content layer, key areas include cloud services, content delivery networks, payment processors, search engines, anti-virus software, as well as commerce and media platforms.

Internet bifurcation and fragmentation are related and not entirely mutually exclusive developments. If fragmentation is a move towards 193 "national internets", bifurcation is simply the extension of Internet nationalism to the two superpowers. However, there are two crucial distinctions between them. First, only the US and China can engage in full-stack competition (see sections 2.2.1-2.2.3). The two countries have the most economic and technological leverage to shape the Internet globally and may be able to force many countries to choose sides. Second, the incentives for supporting or opposing these development patterns may not be the same. China is one of the main champions of national Internet sovereignty and supports the concept in other countries as this may lessen dependence on the US and particularly enables authoritarian regimes to exert greater domestic control. By contrast, the US generally opposes the erection of digital borders. It has arguably also been the main winner of a free, open, and global Internet, given the global success of many dominant service platforms that are headquartered in the US. As such, a bifurcated Internet would probably be more fragmented on the Chinese side.

However, when it comes to bifurcation itself the calculus is somewhat different. China's Internet technology stack has become globally competitive and is gaining ground on the US in many areas. At the same time, the logic of network effects indicates that it is the largest network that may gain from non-interoperability with other networks. These network effects clearly favor the US tech ecosystem in the foreseeable future. Hence, US sanctions and campaigns against Chinese products are discussed as often as drivers of bifurcation as Chinese initiatives to export its infrastructure and standards.

A review of publications on Internet bifurcation underlines several key points. First, the discourse on Internet bifurcation has only emerged recently and there are fewer publications that address this phenomenon compared to Internet fragmentation. The first discussion of the possibility of Internet bifurcation that the author could find was in 2016. However, what really started the conversation were the remarks of former Google CEO Eric Schmidt in 2018 and the US sanctions of Huawei. Overall, Internet bifurcation is largely subsumed into the broader discourse on technological decoupling. Second, the two specific initiatives that are mentioned most often as drivers of bifurcation are the Digital Silk Road on the Chinese side and the Clean Network initiative on the US side (figure 7). These are briefly introduced in the subsections 3.2.1 & 3.2.2. Third, the concrete levers in and beyond these initiatives to influence other countries include export controls, targeted sanctions on companies, bans, limits on intelligence sharing, and subsidies. Fourth, whereas fragmentation mostly happens at the content and logic layers, bifurcation focuses more on logic and infrastructure. Concrete areas of bifurcation include future Internet architectures (section 4), 5G/6G standards, and chips. Fifth, the discourse contains individual references to a wide variety of additional technologies in which a split might emerge. This is not due to conceptual ambiguity, as it is the case for Internet fragmentation. Rather it boils down to many systems that would sooner or later be affected if the decoupling of tech ecosystems were to continue. A summary of the reviewed documents can be found in Annex F.[171]

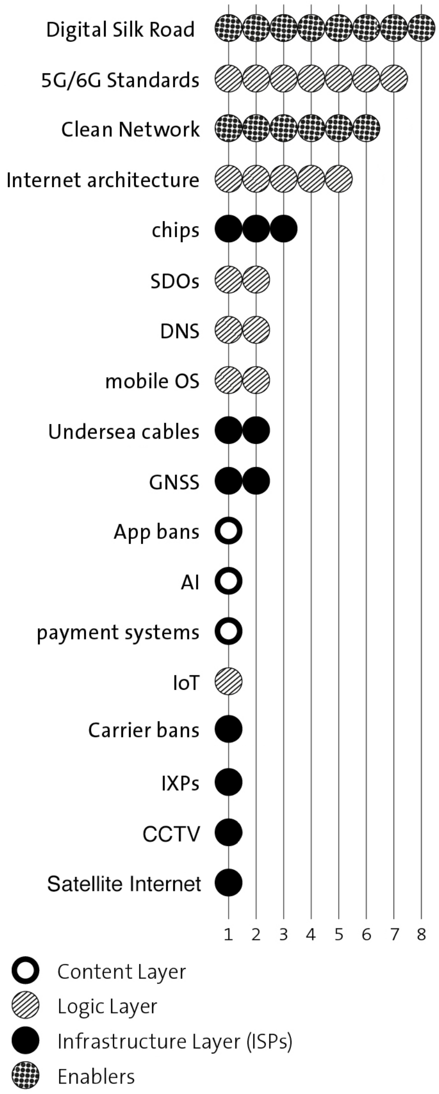


Figure 7. Frequency of concrete issues mentioned in 12 publications on Internet bifurcation.

3.2.1 Digital Silk Road

Digital Silk Road is the name of the **technology dimension of China's Belt and Road Initiative** (BRI). BRI is a global infrastructure development strategy that was launched in 2013.[172] While it is sometimes unclear what is part of it and what not, it is probably the world's largest infrastructure development program with about 840 billion USD committed to construction and investment projects from 2013 to 2021.[173] While the original BRI concept was centered around reviving the old Silk Road connecting Europe and China over land, it has morphed into a global initiative engaging 138 countries in some way.

There is widespread agreement among economists that many low- and middle-income countries have an infrastructure investment gap.[174] Consequently, the construction of more roads, railroads, ports, and telecommunications infrastructure in these countries is generally expected to have a positive impact on their GDP. Still, the BRI has also raised concerns. The US has accused China of "debt diplomacy", meaning the use of oversized megaprojects to create dependence, which is then traded for political influence.[175] Furthermore, China uses different standards for infrastructure investments than the West. The loans from China are used almost exclusively to pay Chinese companies, which bring in Chinese workers rather than locals. Furthermore, large construction projects can be a good vehicle for political bribes, and China has been accused of looking the other way. Bribery makes projects less efficient for the countries in which they are built; however, it allows China to accrue more political influence.[176]

Given the perceived threat from China's BRI, Western states have launched several initiatives to provide countries with alternatives to Chinese-backed infrastructure development. The **Blue Dot Network** initiated by the US, Japan, and Australia provides assessment and certification of infrastructure development projects. The **Partnership for Global Infrastructure and Investment** infrastructure development program was announced by the G7. Lastly, the EU announced the **Global Gateway**, essentially a plan to support infrastructure development around the world.

Telecommunications and standards

The Digital Silk Road was first mentioned in 2015[177] and its main goals are to promote the construction of new communication infrastructure by Chinese

[171] This review focuses on Internet bifurcation specifically and does not include a lot of the general literature on US-China decoupling. However, the delineation between the two can admittedly be quite arbitrary.

[172] Jinping, Xi. (2013). *Promote Friendship Between Our People and Work Together to Build a Bright Future.* fmprc.gov.cn

[173] American Enterprise Institute. (2022). *China Global Investment Tracker.* aei.org

[174] OECD. (2018). *China's Belt and Road Initiative in the Global Trade, Investment and Finance Landscape*. oecd.org. p.5

[175] Note that Western-led development projects have faced similar accusations in the past. Perkins, John. *Confessions of an Economic Hit Man*. Berrett-Koehler Publishers, 2004.

[176] Pompeo, Mike. (2018). *Interview With Hugh Hewitt of the Hugh Hewitt Show.* 2017-2021.state.gov

[177] National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce of the People's Republic of China. (2015). *Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road*. web.archive.org

companies with a particular focus on **cross-border optical cables**, the internationalization of the **Beidou satellite navigation system,**[178] and the adoption of **Chinese standards**. Note that while the attention with regard to radio access networks is mostly on 5G, in low-income countries this may also still refer to the spread of China's homegrown 4G standard TD-LTE.[179] TD-LTE was one of the few ICT-standards explicitly mentioned in the first Belt and Road action plan on standardization.[180] Standards cooperation with Belt and Road countries is also discussed in the action plan 2018-2020[181] and mentioned in China's Standards 2035 Strategy.[182]

The long-term fear on the Western side is that due to the Digital Silk Road "the Internet will be less global and less open. A major part of it will run Chinese applications over Chinese-made hardware. And Beijing will reap the economic, diplomatic, national security, and intelligence benefits that once flowed to Washington."[183]

3.2.2 Clean Network

The Clean Network initiative is an umbrella term for the efforts of the Trump administration to lead and build an alliance of democracies and companies to compete with China. Using 5G as a "beachhead", the initiative wants to leverage network effects to remove Chinese companies from the technology stack. In May 2019, the US government put Huawei on its Entity List, which prohibits any US company from collaborating with them.[184] This collapsed Huawei's smartphone business due to a lack of access to chips, to mobile 5G baseband processors, and to the US app ecosystem. In April 2020, the US State Department announced that the 2019 National Defense Authorization Act will require a "Clean Path" for all standalone 5G network traffic entering and exiting US diplomatic facilities. In May 2020, the US government announced the "5G Trifecta" consisting of onshoring of TSMC's semiconductor fabrication, making it harder for Huawei to acquire advanced semiconductors and the global rollout of the Clean Path strategy. On 5 August 2020, US Secretary of State Mike Pompeo announced that the Clean Network initiative will be expanded to the following components:

- **Clean carrier:** Ensuring that Chinese carriers are not connected with US telecommunications networks. In 2021 and 2022, the Federal Communications Commission revoked the telecom licenses of China Telecom and China Unicom.[185]
- **Clean store:** Removing untrusted Chinese applications from US mobile app stores. On 6 August 2020, then US President Donald Trump signed Executive Orders that banned US transactions with TikTok and WeChat.[186] In January 2021 an executive order on Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay, and WPS Office followed.[187]
- **Clean apps:** Preventing trusted apps to be preinstalled or made available for download on smartphones of untrusted Chinese manufacturers. As the US government placed Huawei on its Entity List, all its devices produced after May 2019 cannot pre-load or download apps such as Gmail, Google Maps, or the Google Play Store.
- **Clean cloud:** Preventing sensitive personal information of US citizens and valuable intellectual property of US businesses from being stored and processed on cloud-based systems accessible to Chinese companies, such as Alibaba, Baidu, China Mobile, China Telecom, and Tencent.
- **Clean cable:** Ensuring that the undersea cables are not used for intelligence gathering by China.

[178] The State Council Information Office of the People's Republic of China. (2016). *Full Text: China's BeiDou Navigation Satellite System*. web.archive.org

[179] China Mobile Communications Corporation. (2017). *Briefing on China Mobile's Participation in Jointly Building "the Belt and Road".* web.archive.org. section 3

[180] 标准联通, 一带一路'行动计划（2015—2017） [Action Plan to Connect One Road, One Belt through Standardization (2015-2017)]. yidaiyilu.gov.cn p. 5

[181] 标准联通共建"一带一路"行动计划（2018-2020年）[Standards Connectivity Action Plan on Jointly Building the Belt and Road (2018-2020)]. yidaiyilu.gov.cn

[182] Central Committee of the Communist Party of China. (2021). 国家标准化发展纲要 [National Standardization Development Outline]. gov.cn 6.22

[183] Segal, Adam. (2018). *When China Rules the Web*. foreignaffairs.com

[184] A Rule by the Industry and Security Bureau on ay 21, 2019, "*Addition of Entities to the Entity List*". federalregister.gov

[185] FCC (2021). *FCC Revokes China Telecom America's Telecom Services Authority*. fcc.gov; FCC. (2022). *FCC Revokes China Unicom Americas' Telecom Services Authority*. fcc.gov

[186] Executive Order 13942 of August 6, 2020, "Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain". Executive Order 13943 of August 6, 2020, "Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain"

[187] Executive Order 13971 of January 5, 2021, "Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies"

- **Clean path:** The US Department of State requires an end-to-end communication path that does not use any equipment from untrusted vendors, such as Huawei and ZTE, for all 5G network traffic entering and exiting US diplomatic facilities.

While there is no "clean standards" item on this list, the US sanctions have impeded the participation of Huawei and other Chinese firms in standardization bodies.[188] Only in June 2020 the US Bureau of Industry and Security within the Department of Commerce exempted standards organizations from US sanctions on Huawei, thereby avoiding a forced bifurcation of standards.[189]

By November 2020, the Trump administration had collaborations with 53 countries for its Clean Network initiative.[190] Under the Biden administration the branding "Clean Network" was retired and the three executive orders banning specific apps, such as TikTok, were revoked in June 2021.[191] However, this mainly reflects a change of rhetoric and tactics, not a change of strategy. Biden's tech advisor Tim Wu has publicly defended the decision to ban TikTok.[192] Trump's decision was not embedded in a clear process and did not hold up in court. The Biden administration aims to create a principles-based national security review of apps.

The "**Alliance for the Future of the Internet**" proposed by the Biden administration in 2021 used softer rhetoric; however, in terms of content it echoed the Clean Network initiative. The alliance was supposed to be launched on the margins of the 111-country Summit for Democracy in December 2021. A leaked non-paper published by Politico in November 2021 outlined that it aimed to "advance democratic values and the rule of law by offering the benefits of an open Internet for those who adhere to basic principles and protections, while declining those benefits to non-adherent nations".[193] In terms of concrete actions, this included "a commitment to use only trustworthy providers for core information and communications technologies network infrastructure".[194] While the term "trustworthy" may be ambiguous, Huawei was the specific example used by Ruth Berry, the Director for Digital Technology Policy, International Economics and Competitiveness on Biden's National Security Council.[195] However, the initiative was criticized for being self-contradictory. On the one hand, it echoed the traditional US criticism of cyber sovereignty and multilateral Internet governance arguing that some states have "defected" from "the Internet's original vision, and now regard the network primarily as a tool of state power."[196] On the other hand, it itself was a multilateral initiative aimed at bifurcation.[197]

After some back and forth, the US, the EU, and 32 additional states launched "**A Declaration on the Future of the Internet"** in April 2022. This declaration is meant to be a more affirmative vision of what like-minded states support, rather than an alliance against digital authoritarianism. The text still includes a line on promoting and using "trustworthy network infrastructure and services suppliers, relying on risk-based assessments that include technical and non-technical factors for network security".[198] However, it also includes an explicit commitment to a global Internet, which was framed as abstaining from Internet shutdowns, following net neutrality, and promoting the "benefits of data free flows with trust based on our shared values as like-minded, democratic, open and outward looking partners".[199]

Regardless of specific initiatives, the focus of US digital foreign policy has shifted from dealing with pressures to (inter-)nationalize Internet governance towards strategic competition with China. With this, the emphasis in statements of the US government and US think tanks is increasingly on trust and democracy.[200] In 2011, the US International Strategy for Cyberspace argued that "the alternative to global

[188] Schwartz, Ari. (2020). Standards Bodies Are Under Friendly Fire in the War on Huawei. lawfareblog.com

[189] Bureau of Industry and Security. (2020). Release of "Technology" to Certain Entities on the Entity List in the Context of Standards Organizations. federalregister.gov

[190] Pompeo, Mike. (2020*). "Three more countries are now members of the Clean Network: Brazil, Ecuador, and the Dominican Republic. 53 Clean Countries, 180 Clean Telcos, and dozens of leading companies—representing 2/3 of the world's GDP—have already joined the tide toward trusted "* twitter.com

[191] Executive Order 14034 of June 9, 2021, "Protecting Americans' Sensitive Data From Foreign Adversaries"

[192] Wu, Tim. (2020). *A TikTok Ban Is Overdue*. nytimes.com

[193] *Non-Paper//Discussion Purposes Only: The Alliance for the Future of the Internet. (*2021). politico.com p.3

[194] ibid. p.1

[195] USTelecom. (2022). *Transatlantic Tech Partnerships*. ustelecom.org. 6:00-8:35

[196] *Non-Paper//Discussion Purposes Only: The Alliance for the Future of the Internet. (*2021). politico.com p.3

[197] Lapowsky, Issie. (2021). *Inside the scramble to fix Biden's plan for the future of the internet.* protocol.com

[198] US, EU, & 32 states (2022). *A Declaration on the Future of the Internet.* whitehouse.gov p. 1

[199] Ibid. p.1

[200] Webster, Graham, and Justin Sherman. (2021). *The Fall and Rise of Techno-Globalism: Democracies Should Not Let the Dream of the Open Internet Die*. foreignaffairs.com

openness and interoperability is a fragmented Internet, where large swaths of the world's population would be denied access to sophisticated applications and rich content because of a few nations' political interests".[201] In contrast, the 2021 Quad Principles on Technology Design, Governance, and Use reflect a commitment to "fostering an open, accessible, and secure technology ecosystem, based on mutual trust and confidence".[202] Similarly, in 2013 the Council on Foreign Relations wrote that "a global Internet increasingly fragmented into national Internets is not in the interest of the United States".[203] In contrast, in 2020, Robert Knake from the Council on Foreign Relations argued that "the United States should shift its diplomatic efforts from promoting a global, open Internet to preserving an open Internet that connects the digital economies of democratic countries".[204] In 2022, a task force by the same think tank stated no less than four times that "the era of the global internet is over".[205] Instead, the US should gather "a coalition of allies and partners around a vision of the internet that preserves a trusted, protected international communication platform".[206]

Similarly, in the words of a recent report by the Carnegie Endowment for International Peace by Jon Bateman with a foreword by Eric Schmidt, "The U.S. government has been a principal driver of recent technological decoupling with China and remains uniquely able to adjust this global trend up or down".[207] Those who defend a global Internet, such as the Internet Society and the World Wide Web Foundation, are framed as "cooperationists".[208]

[201] White House. (2011). ***International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.*** obamawhitehouse.archives.gov p. 8

[202] White House. (2021). *Quad Principles on Technology Design, Development, Governance, and Use*. whitehouse.gov

[203] Negroponte, John, Samuel Palmisano, and Adam Segal. (2013). *Defending an Open, Global, Secure, and Resilient Internet*. cdn.cfr.org p. 13

[204] Knake, Robert. (2020) *Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity.* cdn.cfr.org. p.1

[205] Fick, N., Miscik, J., Segal, A., & Goldstein, G. (2022). Confronting Reality in Cyberspace Foreign Policy for a Fragmented Internet. cfr.org pp. vii, 3, 7, 15

[206] Ibid. pp. vii

[207] Bateman, J. (2022). *U.S.-China Technological "Decoupling": A Strategy and Policy Framework.* carnegieendowment.org p. 10

[208] Ibid. p. 39

4 Future Internet Architectures

Future Internet architectures have a twofold relevance to the fragmentation and bifurcation discourse. First, there is simply the possibility that in the future there could be two or more competing Internet architectures with significant market share that are developed by separate SDOs. Second, there is the possibility that a future Internet architecture contains design choices that enable or counteract Internet fragmentation. Aside from these considerations, there is also a general technical discourse on the desired qualities of an Internet architecture and the question of whether the current Internet architecture should continue to evolve incrementally or if a clean-slate redesign is needed for the future.

This section first presents the key arguments on whether the Internet would profit from a clean-slate redesign. It then provides an overview of projects for clean-slate Internet architectures. Lastly, it takes a specific look at the most controversial future Internet architecture, New IP, as well as the one that is the furthest developed in terms of operational deployment, SCION, and discusses them in the context of Internet fragmentation and bifurcation.

4.1 Do We Need a New Internet?

The TCP/IP protocol suite has evolved gradually through standardization at the IETF. This process can be time-consuming, and it often requires that a standard has already been deployed and proven in the field. This stands in sharp contrast to the definition of transmission standards for mobile data networks, which is more vision-based and has distinct generations of clean-slate designs (e.g., 3G, 4G, 5G). **The IETF generally prefers an incremental evolution of the TCP/IP suite.** However, a part of the technical community maintains that a clean-slate Internet architecture is desirable or even required to make the Internet future-proof. The following represents three key arguments brought forward by advocates and opponents of clean-slate Internet designs.

Arguments in favor of clean-slate redesigns

Security-by-design: The TCP/IP suite was not designed with security in mind. In the 1970s, when the main protocols were designed, access to ARPANET was limited to trusted parties, such as the military, as well as selected universities and companies in the US. Hence, in 1988, security was still not even an evaluation criterion for network protocols in the IETF.[209] Most of today's security was added as an afterthought through the addition of PKI. However, key parts of the Internet such as BGP still mostly depend on trust between autonomous systems. A clean-slate design could use security-by-design.

Technological change since the 1970s: The TCP/IP suite was designed in the technological environment of the 1970s, which is starkly different from that of the 2020s. Specifically, in the 1970s the network was not yet able to perform complicated per-hop behaviors that enable QoS due to the cost of memory and computing. Furthermore, the IP number serves both as an identifier as well as a locator. This dual function did not make any difference originally as computers were not mobile. However, today one can make an argument that the end-node-ID and the location identifier should be separated.

Integration of additional technologies: There are existing computer networks that are not using IP, in particular operational technology in industrial contexts. Furthermore, there is an expectation that a large share of future computer network traffic could be generated by the Internet of Things. Lastly, there are visions for future Internet use cases such as holographic communication. There are arguments that the Internet can only enable such services or connect to these areas if it gets a new protocol suite that can guarantee QoS.[210]

Arguments in favor of incremental evolution

Network effects: The main benefit of IP is that it is common. The network effects of IP already gained critical mass in the 1990s. Today they are over-

[209] Clark, David. "The design philosophy of the DARPA Internet protocols." In Symposium proceedings on Communications architectures and protocols, pp. 106-114. 1988.

[210] Li, Richard. (2018). *Towards a New Internet for the Year 2030 and Beyond*. researchgate.net

whelming. As highlighted in the decade-long transition from IPv4 to IPv6, any next-generation protocol would have to be able to overcome the massive momentum of IP in terms of infrastructure, training, etc.

Generality: There is an argument in favor of keeping the network layer as application-agnostic as possible. There would be small efficiency gains if the network protocols were optimized more strongly for the prevalent type of content or service (e.g., packet size). However, this optimization would create technological momentum that locks in the currently prevalent type of Internet use. In the 1980s, the Internet consisted almost exclusively of email. In the 1990s it became dominated by websites. Today, most of the Internet traffic is video streaming. These changes may have occurred more slowly if the TCP/IP suite had been less general.[211]

Minimality: The minimality argument says that the network layer should remain a platform with stable interfaces and services to enable innovation at higher layers. Whenever the lower layer changes, this creates adaptation costs for the complementary systems built on top of it. Hence, whenever possible, problems should be solved on higher layers. Previous claims that voice-over-IP and video streaming could not become a reality on the Internet without switching from best-effort delivery to QoS turned out to be wrong. These applications are widespread and work reasonably well today.

Another way to approach the question of Internet architecture is by looking at desired design principles. There is a lot of agreement on **resilience, security, support for a variety of networks and devices, economic efficiency, backward compatibility, and extensibility as desired properties**. However, there can be differences in operationalization. For example, resilience in Clark (1988) means “smart endpoints and dumb pipes”, whereas in the ITU’s Network 2030 group it means a smart network.[212] There can also be tensions between some principles, such as between the idea that it is easier to accommodate network diversity if most services are provided on a higher layer and the desire to add additional network services. An overview of Internet design principles can be found in Annex G.

4.2 Overview

The first state-sponsored exploration of clean-slate Internet designs was the NewArch Project funded by DARPA (2000-2003).[213] In 2006, the NSF initiated the Future Internet Design project and funded more than 50 research projects on all kinds of design aspects of the future Internet.[214] Its successor project, the **NSF Future Internet Architecture program,** was initiated in 2010. The four selected projects were MobilityFirst, Named Data Network, Nebula, and eXpressive Internet Architecture. In May 2014, the NSF announced awards for Future Internet Architectures - Next Phase in which each project was expected to demonstrate working full-scale prototype systems for testing and evaluation. Furthermore, the projects would continue to consider societal, economic, and legal issues. The three project that made it into this phase are MobilityFirst, Named Data Network, and eXpressive Internet Architecture.[215]

The EU Commission also funded a variety of future Internet architecture activities in its **Seventh Framework Programme** (2007-2013), with names such as Future Internet Research and Experimentation and Evolving Future Internet for European Leadership.[216]

Overall, the **US and the EU have been the biggest sponsors of research on clean-slate Internet architectures**. This has resulted in many proposals. However, in terms of **implementation and adoption**, the results of two decades of research **remain modest**.

This section first provides an overview of alternative network architectures based on chapter seven of David Clark’s *Designing an Internet*.[217] Huawei’s proposal of a New IP (section 4.2) and the ETH Zürich

[211] Clark, David. (2018). Designing an Internet. MIT Press. p. 29

[212] Clark, D. (1988). The design philosophy of the DARPA Internet protocols. In *Symposium proceedings on Communications architectures and protocols.* pp. 107&108; Focus Group on Technologies for Network 2030 (2020) Network 2030 Architecture Framework. itu.int pp. 27&28

[213] Clark, David, Robert Braden, Karen Sollins, John Wroclawski, and Dina Katabi. *New Arch: Future Generation Internet Architecture*. apps.dtic.mil. 2004.

[214] Fisher, Darleen. "US National Science Foundation and the future Internet design." ACM SIGCOMM Computer Communication Review 37, no. 3 (2007): 85-87.

[215] Fisher, Darleen. "A look behind the future internet architectures efforts." ACM SIGCOMM Computer Communication Review 44, no. 3 (2014): 45-49.

[216] The BLED Declaration: Towards a European approach to the Future Internet web.archive.org, 2008.; Domingue, John, Alex Galis, Anastasius Gavras, Theodore Zahariadis, Dave Lambert, Frances Cleary, Petros Daras et al. *The Future Internet: Future Internet Assembly 2011: Achievements and Technological Promises.* Springer Nature, 2011.

[217] Clark, David. (2018). Designing an Internet. MIT Press.

project SCION (section 4.3) are discussed more extensively in the subsequent subsections. An alphabetic list of 27 future Internet architecture proposals and their key papers are in Annex H.

Protocols for a fragmented Internet

The first type of clean-slate Internet architecture proposals originated from the "protocol wars" and the assumption that the competing architectures would coexist in the future. Therefore, these proposals intended to **enable interoperability between network regions that run different protocols.**

The Metanet[218] proposal did not suggest a specific architecture. However, it laid out requirements for a network that connects heterogeneous regions. The Sirpent[219] proposal still assumed a single global name space and gave users more control over the route that a packet takes. However, regions would have access control in the sense that authorization tokens were needed to confirm the right of the sender to use the selected route. In the Plutarch[220] proposal the Internet is also divided into regions that assign addresses that are not globally unique to entities. At interconnection entities, the addresses are rewritten to be meaningful for the region to which a packet is forwarded.

The anticipated need for a protocol that connects a fragmented Internet did not materialize. However, the Framework for Internet Innovation[221] proposal still aimed to enable fragmentation as it argued that it has beneficial properties. It is an attempt at an overarching minimal design, which various future regional Internet architectures could take into account to maintain connectivity. They suggest routing through pathlets, and a standard to mitigate the specific challenge of DDoS attacks in the form of a "shut up message".

Information-centric Networking

The second type of clean-slate architecture is called information-centric or content-centric networking. Its main idea is that today's networking protocols focus on *where* something can be found. However, users are primarily interested in *what* content a site contains and content can be replicated at many locations across the network. Hence, the primary focus of information-centric networking is the **introduction of a new set of identifiers for services and pieces of information**. One key difference between information-centric protocols is the logic of how these identifiers are assigned and how the name resolution system that links content IDs with locations is organized.

TRIAD[222] aims to create a DNS-style lookup for pieces of data. The user sends a data lookup packet, which is forwarded by routers toward a location where the data is stored. The content IDs follow a hierarchical logic. The routing between ASes is organized in a similar fashion as BGP, with ASes advertising ranges of content IDs hosted in their network to others. Because the same content can be hosted in several places, there is no issue if several ASes advertise the same content. Once a server with the requested data is reached, the data is exchanged through a slightly modified TCP.

The Data-Oriented Network Architecture[223] is similar to TRIAD. However, the content IDs are not hierarchical but derived from hashes of the data and its creator. This requires a lot more individual entries in the BGP-like advertising of content that is hosted within an AS. The way it attempts to deal with this is by assuming that only large networks keep comprehensive name-based forwarding tables and that smaller ASes just forward requests to them.

The Network of information[224] was funded by the European Commission's future Internet research program. NetInf uses flat, globally unique content IDs. In the case of NetInf, the name of the object is the hash of its contents.

The Publish / subscribe Internet routing paradigm[225] was also funded by the future Internet research program of the European Commission. It is similar to the proposals above, except that the content IDs are not

---

[218] Wroclawski, J. (1997). The Metanet: White Paper - Workshop on Research Directions for the Next Generation Internet. archive.cra.org

[219] Cheriton, David "Sirpent: A high-performance internetworking approach." In *Symposium proceedings on Communications architectures & protocols*, pp. 158-169. 1989.

[220] Crowcroft, J., Hand, S., Mortier, R. et al. (2003). Plutarch: An Argument for Network Pluralism. acm.org

[221] Koponen, Teemu, Scott Shenker, Hari Balakrishnan, Nick Feamster, Igor Ganichev, Ali Ghodsi, P. Brighten Godfrey et al. "Architecting for innovation." ACM SIGCOMM Computer Communication Review 41, no. 3 (2011): 24-36.

[222] Cheriton, David, and Mark Gritter. "*TRIAD: A new next-generation Internet architecture*." (2000). citeseerx.ist.psu.edu

[223] Koponen, Teemu, Mohit Chawla, Byung-Gon Chun, Andrey Ermolinskiy, Kye Hyun Kim, Scott Shenker, and Ion Stoica. "*A data-oriented (and beyond) network architecture.*" In *Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 181-192. 2007.

[224] Dannewitz, Christian, Dirk Kutscher, Börje Ohlman, Stephen Farrell, Bengt Ahlgren, and Holger Karl. "Network of information (NetInf) – an information-centric networking architecture." *Computer Communications* 36, 7 (2013): 721-735.

[225] Trossen et al. 2008, Trossen and Parisis, 2012

necessarily globally unique. Rather they are only valid within a region.

Lastly, Named Data Networking[226] is funded by the NSF's Future Internet Architecture program. A user can broadcast his or her interest in a named piece of data through the network. When this interest package reaches a node with a cache of the requested data, it forwards it back to the user. Intermediary nodes can save a local cache of frequently requested content. Importantly, named data networking is the only proposal that completely replaces traditional location-based addresses. In all other projects location addresses are still used once the requested content has been found.

The key question that information-centric networking protocols face is **whether it is necessary to integrate the content ID into the network layer**, as there are many existing solutions on higher layers. This includes content delivery networks, search engines directly embedded into the top-bar of web browsers, as well as multiple naming systems that bind names and location, such as digital object identifiers (DOI), and international standard book numbers, serial numbers, audiovisual numbers, recording codes, text codes, and musical work codes. The main advantage of integrating content ID into the network layer would be efficiency gains from routers in the network caching short-term popular content. Those approaches that use hashes of the data itself as identifiers would also add a bit of additional security through self-certification.

Other Architectures

MobilityFirst[227] is funded by the NSF. Its main goal is to better incorporate mobile devices that can move from one network to another. A key part of this is the separation of location from the identity of end-nodes. It foresees an additional globally unique identifier with a flat structure that can be assigned to a host, service, sensor, data, or context. The header of the data packets includes both the last known network address as well as the end-node identifier. If the network address is not current anymore, routers can look up in a global name service where a mobile host, service, sensor, data, or context is currently registered and re-route it to that location.

The eXpressive Internet Architecture[228] is also funded by the NSF. Its emphasis is on allowing many ways of delivering a packet to its destination and for the network to provide a range of services. For example, it allows four types of identifiers: the location of a host, the content, a service hosting data, and an administrative domain in which a desired content ID is known. This expressiveness also allows it to use the SCION routing protocol.

Nebula[229] is yet another Internet architecture that uses cryptographic proof of paths and proof of consent to ensure that routes are authorized and followed. Lastly, the Recursive Internetwork Architecture[230] aims to reduce the number of Internet layers.

4.3 New IP

In the context of future Internet architectures, the terms "new IP" and "big IP" have been used in a generic sense to talk about a next generation IP and an extension of IP respectively. The capitalized term "New IP" is a placeholder name for a future Internet architecture on which Huawei works as well as a related but separate effort to define what criteria a new IP standard should fulfill in the ITU. Both efforts are led by Richard Li. He is the chief scientist of Huawei-subsidiary Futurewei, chaired the focus group "Network 2030" in the ITU, and served as vice-chair of the Industry Specification Group on Next Generation Protocols of the independent European Telecommunications Standards Institute (ETSI).

[226] Zhang, Lixia, Alexander Afanasyev, Jeffrey Burke, Van Jacobson, K. C. Claffy, Patrick Crowley, Christos Papadopoulos, Lan Wang, and Beichuan Zhang. "Named data networking." *ACM SIGCOMM Computer Communication Review* 44, no. 3 (2014): 66-73.

[227] Raychaudhuri, Dipankar, Kiran Nagaraja, and Arun Venkataramani. "Mobilityfirst: a robust and trustworthy mobility-centric architecture for the future internet." ACM SIGMOBILE Mobile Computing and Communications Review 16, no. 3 (2012): 2-13.

[228] Anand, A., Dogar, F., Han, D., Li, B., Lim, H., Machado, M., Wu, W., Akella, A., Andersen, D.G., Byers, J.W. and Seshan, S., 2011, November. XIA: An architecture for an evolvable and trustworthy Internet. In Proceedings of the 10th ACM Workshop on Hot Topics in Networks (pp. 1-6).

[229] Anderson, Tom, Ken Birman, Robert Broberg, Matthew Caesar, Douglas Comer, Chase Cotton, Michael J. Freedman et al. "A brief overview of the NEBULA future internet architecture." ACM SIGCOMM Computer Communication Review 44, no. 3 (2014): 81-86.

[230] Day, John, Ibrahim Matta, and Karim Mattar. "Networking is IPC: a guiding principle to a better internet." In Proceedings of the 2008 ACM CoNEXT Conference, pp. 1-6. 2008.

4.3.1 How New IP Works

The goal of Huawei's New IP is to enable better than best-effort routing which in turn enables future Internet services relevant for application areas such as the Industrial Internet, smart agriculture, cloud driving, holographic communication, and IP mobile backhaul transport in 5G and beyond 5G networks.[231] Li acknowledges that the current architecture already allows for some QoS. This includes the DiffServ field in the IP-header (section 2.2.2.1), which allows routers to prioritize voice and video traffic, as well as the use of MPLS within a wide area network (section 2.2.2.4) to send packets through pre-determined paths. However, the current Internet architecture has no mechanism to provide **end-to-end guarantees of throughput, maximum latency (in-time), and precise latency (on-time, no "jitter")**.

Contract field: The main mechanism through which New IP wants to enable such guarantees is through **a new contract field** that is inserted between the header and the payload of data packets. In this field, the packet delivery conditions can be specified. Categories include *BoundedLatency*, *OnTimeDelivery*, *NoPacketLoss*, and *PreferredPath*. Routers that get such packets may then prioritize their forwarding based on the agreed latency and the preferred path. The contract clause also contains fields for tracing and monitoring the packet to understand its path and the latency between two routers. Finally, there is the field *ReportInsuringParty* to report failures to meet the service conditions in the contract.[232]

Flexible, end-host addressing: Another motivation of Futurewei that is of relevance to this report is that it sees the need for an addressing scheme that can tie together heterogeneous regions: "Observations about shrinking transits and maximal data residing in public clouds, have led us to believe that the public Internet of today will be just one of the 'Internets' as new public access Internets begin to emerge. We call this phenomenon as 'ManyNets' and the current public Internet as 'OneNet'. Thus, ManyNets will be a group of Internets (network of networks) with their regulations, structure, and business objectives. OneNet will be one such Internet in this collection."[233]

To enable communication between heterogeneous networks, New IP contains a flexible addressing scheme. Specifically, it changes the data packet header to newly include a field called *AddrType.* This field signals which type of networking protocol is used to be backwards compatible with IPv4 and IPv6 as well as other networking means, such as a user identity ID, or a content ID. It also enables variable length addresses instead of the fixed address length of IPv6 to minimize the size of the header for small IoT devices.[234]

Huawei has not published a full specification of New IP. This puts uncertainty on the degree of operational readiness of the protocol. However, the domestic standardization efforts indicate that Huawei is getting closer to deploying New IP, particularly to connect industrial networks to the Internet and for backhaul traffic in 5G and beyond 5G networks.[235]

4.3.2 Adoption and Standardization

International standardization: In 2018, Huawei, together with ETRI (South Korea) and Verizon (US), suggested creating a new focus group in the standardization sector of the ITU to perform pre-standardization research and investigate novel ideas on future networks. This "Network 2030" group has inter alia identified holographic communications, the tactile Internet, and digital twins as relevant future use cases and defined required performance indicators for them.[236] For the study period after the World Telecommunication Standardization Assembly (WTSA) 2020, which was postponed to 2022 due to the COVID-19 pandemic, contributions by Huawei had suggested turning these requirements into questions for standardizing a new IP. These suggestions were submitted in near-identical form to two ITU-T Study Groups. Presumably, Huawei planned to submit its New IP protocol as fulfilling this standard

[231] Li, R. (2020). Some Notes on "An Analysis of the "New IP" Proposal to the ITU-T". Wordpress.

[232] Li, Richard, Kiran Makhijani, and Lijun Dong. "New IP: A data packet framework to evolve the internet." In *2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR)*, pp. 1-8. IEEE, 2020. pp. 5&6

[233] ibid. p. 2

[234] Ibid. p. 4

[235] Li, R. (2020). Some Notes on "An Analysis of the "New IP" Proposal to the ITU-T". Wordpress.

[236] Focus Group on Technologies for Network 2030. (2020). *Network 2030 - Gap Analysis of Network 2030: New Services, Capabilities and Use cases.* itu.int

as a next step.[237] After critical Western media articles came out, Huawei explained that New IP is only intended to integrate IP-networking with networking protocols used in industry rather than to fully replace IP. It also replaced the term “New IP” with “**Future Vertical Communication Networks**” in contributions without substantially changing the content otherwise.

In **December 2020**, the ITU-T Study Groups 11 and 13 discussed these proposals. The only countries to explicitly support the proposal were India, Russia, and Zambia. In contrast, the EU and a group of countries consisting of Australia, Austria, Belgium, Bulgaria, Burundi, Canada, Czechia, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Japan, Latvia, Lithuania, Malta, Norway, Poland, Portugal, Slovenia, Spain, Sweden, the United Kingdom, and the United States has objected to them. Regular decisions within the ITU require a consensus. Hence, these objections have stopped the standardization. Member states can request a vote among member states in a physical meeting. However, the path that China and Huawei seem to have chosen is one of whack-a-mole, with further attempts to introduce similar proposals under new names and in new forms at the ITU.

This includes the March 2021 proposals for “Polymorphic Networking”[238] and “Immersive real-time communications” in Study Group 13, a discussion on forming a focus group on “6G Networking Technologies” based on outcomes of “Network 2030” at the Study Group 13 workshop for Africa, and a proposal for a new work item on “Security guidelines of deterministic communication services for IMT-2020 networks and beyond” in Study Group 17.

Domestic standardization: The China Communications Standards Association is working on nine New IP standards under the name “**deterministic IP**”. This work takes place in “Technical Committee 3: Network and Service Capability”, “Technical Committee 10: The Internet of Things”, and “Special Task Group 8: Industrial Internet” and it involves various Chinese companies.[239]

Adoption: In 2020, Huawei published a report on its tests of “deterministic IP” on the recently inaugurated Internet test-bed of the Chinese government that connects Beijing to Nanjing, the China Environment Network Infrastructure.[240] In 2021, Huawei has started to promote its New IP technology as “deterministic IP” to business clients. At the Future Network Development Conference in Nanjing, Huawei has also released a white paper on deterministic networking technologies together with industry partners, including the government-backed Purple Mountain Lab in Nanjing, Beijing University of Posts and Telecommunications, 5G Deterministic Networking Alliance, Jiangsu Hengtong Optic-Electric Co., Ltd., and Jiangsu Future Networks Innovation Institute.[241] The white paper states the primary goal of the project as “occupying the commanding heights of the new generation of network technology development”.[242] “Commanding heights” is a term for strategically important private industry in Marxist economics that is also referenced in Chinese military strategy.[243]

4.3.3 Discourse and Impact

RIPE (the regional Internet registry for Europe)[244], the IETF[245], the Internet Society[246], ICANN[247], and the European Telecommunications Network Operators (ETNO)[248] have raised a number of concerns about New IP.

237 As with IMT-requirements for RAN generations, it is conceivable that multiple standards could fulfill these criteria. SCION argues that “SCION not only satisfies Huawei’s requirements but exceeds them, New IP can build on SCION to achieve additional properties”. Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., & Perrig, A. (2022). *The Complete Guide to SCION: From Design Principles to Formal Verification*. Springer Cham. p. 580

238 Note that this term also overlaps with a paper on trials of a new protocol with a flexible addressing by the PLA Strategic Support Information Engineering University. Hu, Yuxiang, Dan Li, Penghao Sun, Peng Yi, and Jiangxing Wu. "Polymorphic smart network: An open, flexible and universal architecture for future heterogeneous networks." IEEE Transactions on Network Science and Engineering 7, 4 (2020): 2515-2525.

239 Organizing Committee of the 5th Future Network Development Conference. (2021). 未来网络白皮书 [Future Network White Paper]. file.huawei.com pp. 71&72

240 Wang, S., Wu, B., Zhang, C., Huang, Y., Huang, T., & Liu, Y. (2021, May). Large-scale deterministic IP networks on CENI. In *IEEE INFOCOM WKSHPS: CNERT 2021: Computer and Networking Experimental Research using Testbeds*. (pp. 1-6).

241 Huawei (2022). Huawei and Purple Mountain Laboratories Release the Future Network White Paper on Deterministic Networking Technologies. huawei.com

242 Organizing Committee of the 5th Future Network Development Conference. (2021). 未来网络白皮书 [Future Network White Paper]. file.huawei.com p. 5

243 The State Council Information Office of the People's Republic of China. (2015). China's Military Strategy. china.usc.edu section 1, para. 6

244 RIPE NCC. (2020). *Response to “New IP, Shaping Future Network” proposal*. ripe.net

245 IETF. (2020). *Liaison statement: Response to "LS on New IP, Shaping Future Network".* datatracker.ietf.org

246 Sharp, Hascall, and Olaf Kolkman. (2020). *Discussion Paper: An analysis of the "New IP" proposal to the ITU-T*. internetsociety.org

247 Durand, Alain. (2020). *New IP*. icann.org

248 ETNO. (2020). *ETNO position paper on the New IP proposal.* etno.eu

Distrust towards Huawei and China: Before delving into specific concerns, it is worth highlighting that any major Internet standards initiative from Huawei will face increased scrutiny from advocates of the multistakeholder model considering China's repeated efforts to shift Internet governance to the UN and its preference for paternalistic oversight. While Huawei is not China, Chinese firms differ from Western firms in their relationship with the government and their ability to distance themselves from it. Even billionaires disappear if they criticize the Communist Party of China (CPC) and companies are required by law to enable an internal CPC organization.[249] Huawei's founder Ren Zhengfei worked on military communications systems for the People's Liberation Army from 1974 to 1982 before founding the company in 1987.[250] Until 2018, Huawei had received 75 billion USD of indirect subsidies from the Chinese government.[251] It has a unique ownership structure that has been reported to go back to the Chinese government and means that it does not need to comply with financial reporting standards.[252] Furthermore, it has been reported to have a management culture that almost exclusively hires Chinese, prohibits them from having relations with non-Chinese, and extensively uses military metaphors.[253] The US designates Huawei as a military-backed company.[254]

Gap analysis: RIPE, the IETF, the Internet Society, ICANN, and ETNO disagree with the gap analysis by the Network 2030 group at the ITU and highlight the track record of IP. For example, the IETF writes, "we expect the existing protocol stack to continue to evolve to meet the needs of new networks and applications, just as it has for more than 50 years".[255]

ITU vs. IETF: Another point of contention is that many believe that the ITU is the wrong forum for Internet standards. The first argument against New IP standardization in the ITU is that would **duplicate efforts** of working groups at the IETF, such as the deterministic networking group.[256] The second argument is that all Internet standards should be developed in an **open, multistakeholder, and bottom-up** fashion.[257] The IETF also highlights that it "maintains copyright and change control for the IP specifications in the interests of global interoperability".[258] Richard Li has rejected this criticism as a catch-22, because the IETF has ruled out changes to the network layer in its deterministic forwarding group: "If the IETF is not interested in it, then the IETF should not seek to prevent other SDOs from addressing this topic".[259]

Premature standardization: The vision-based model of standardization used for radio access networks is viewed skeptically in the IETF, as there are often unforeseen challenges that only become apparent in operational deployment. For example, the ICANN report states, "due to the lack of specification, it is worth noting that it is difficult to see New IP as a candidate for a protocol standard. Rather, it appears to be a list of perceived issues about the current Internet architecture and a list of desired features."[260] Li counters that an approach that primarily acknowledges existing standards with a proven track record means that it is only large tech companies, such as Google (which just went forward with QUIC unilaterally), that can change Internet standards.[261]

Contractual complexity: Today ISPs only need to have peering or transit agreements with neighboring ISPs. QoS would significantly complicate agreements between ISPs as it adds more types of service agreements as well as a requirement for them to cover

[249] Company Law of the People's Republic of China (2018 Revision), Article 19: "The Communist Party of China may, according to the Constitution of the Communist Party of China, establish its branches in companies to carry out activities of the Communist Party of China. The company shall provide necessary conditions to facilitate the activities of the Party." Constitution of the Communist Party of China (2017 Revision), Article 30: "A primary-level Party organization shall be formed in any enterprise, villagers' committee, government organ, school, research institute, subdistrict and community, social organization, company of the People's Liberation Army, and any other primary-level danwei [an organization where people work] where there are three or more full Party members."

[250] Hongwen, Li (2017). *Ren Zhengfei & Huawei: A Business and Life Biography.* London, United Kingdom: LID publishing. chapter 2

[251] Yap, Chuin-Wei. (2019). *State Support Helped Fuel Huawei's Global Rise*. wsj.com

[252] Balding, Christopher, and Donald C. Clarke. "Who Owns Huawei?." *Available at SSRN 3372669* (2019).

[253] Gruhnwald, Sylke. (2021). *Inside Huawei*. republik.ch

[254] Department of Defense. (2021). *Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (PUBLIC LAW 116-283)*. media.defense.gov

[255] IETF. (2020). *Liaison statement: Response to "LS on New IP, Shaping Future Network".* datatracker.ietf.org. section 2

[256] IETF. (2022). *Deterministic Networking (detnet).* datatracker.ietf.org

[257] ETNO. (2020). *ETNO position paper on the New IP proposal.* etno.eu

[258] IETF. (2020). *Liaison statement: Response to "LS on New IP, Shaping Future Network".* datatracker.ietf.org. section13

[259] Li, R. (2020). Some Notes on "An Analysis of the "New IP" Proposal to the ITU-T". internet4future.wordpress.com

[260] Durand, Alain. (2020). *New IP*. icann.org. p. 28

[261] Li, R. (2020). Some Notes on "An Analysis of the "New IP" Proposal to the ITU-T". internet4future.wordpress.com

several ISPs end-to-end. Li does not deny this point but argues that there is no alternative.

Protocol fragmentation: New IP has flexible addressing, which means New IP routers could handle IPv4, IPv6, and a variety of other traffic. However, existing routers would still not be able to handle variable length addresses. Therefore, the Internet Society argues that "introducing a new protocol system (…) would require the need for yet another decades-long migration, requiring tens of billions of IP-enabled nodes to interwork and interconnect with the new system. Merely providing a variable-length address does not solve the problem. Creating a new protocol system to 'solve' a perceived interoperability problem adds another interoperability problem and because of increased complexity likely adds security and resiliency issues as well."[262] Huawei's New IP paper references Ammar's notion of ManyNets, which frames Internet fragmentation in terms of network protocols as something normatively desirable that enables innovation.[263]

Intelligence in the network: New IP could arguably shift power by adding more intelligence to the network. This would give ISPs, which are more state-aligned than companies providing content platforms to users, more fine-grained control measures. Furthermore, there are fears that flexible addressing would make it possible to introduce additional IDs by law that create strong binding between Internet users and thus would increase the surveillance capacity of ISPs and nation states.[264]

4.4 SCION

SCION is a clean-slate inter-domain routing architecture focused on security and high availability developed by the Network Security Group of Professor Adrian Perrig at ETH Zürich and commercialized through the spin-off Anapaya Systems AG. SCION is an acronym of "**s**calability, **c**ontrol, and **i**solation **o**n **n**ext-generation networks". The following is a high-level summary of SCION features with potential relevance to Internet fragmentation and bifurcation, for a comprehensive technical description please consult the official guide to SCION, which is more than 600 pages long.[265]

4.4.1 How SCION Works

The most important feature of SCION is the switch from governance mechanisms with global scope to clusters of autonomous systems with shared local governance institutions. It calls these clusters, isolation domains (ISDs). Each ISD has two classes of ASes, core and non-core. The core ASes have a number of special functions as they handle trust roots, the distribution of intra-ISD paths and the connection to other ISDs. **ISDs can but do not have to correspond to the political borders of states**: "Some ISDs may evolve from existing tier-1 ISPs (…) On the other hand, jurisdictions may insist on sovereign authority (…) in these jurisdictions, only the national ISD would be available".[266] In the latter case, "a sovereign authority ISD would be created by an internationally recognized sovereign power. Interconnections between sovereign authorities would be governed by bilateral or multilateral treaty. A multilateral SCION Internet treaty could be overseen by an existing international body, for example a United Nations agency such as the ITU."[267]

Local path information: Rather than having a global BGP routing table (see section 2.2.2.4)most AS-level path information is only collected and stored locally within an ISD. The SCION process for this is called intra-ISD beaconing. The second form of beaconing is core beaconing, which explores the routes between the core ASes of different ISDs. This hierarchy of path information would decrease the size of inter-domain routing tables compared to today, as all BGP routers maintain a table of routes for the entire Internet (ca. 100,000 ASes that advertise ca. 900'000 IPv4- and 150'000 IPv6-prefix ranges[268]). In contrast, a connection between two computers in non-core ASes in different ISDs relies on the combination of **three separate inter-domain path services.** The sender obtains path segments from the local path service that highlight the options on how to get to a core AS in its ISD, from the core path service of its

262 Sharp, Hascall, and Olaf Kolkman. (2020). *Discussion Paper: An analysis of the "New IP" proposal to the ITU-T*. internetsociety.org

263 Ammar, Mostafa. "ex uno pluria: The Service-Infrastructure Cycle, Ossification, and the Fragmentation of the Internet." *ACM SIGCOMM Computer Communication Review 48*, no. 1 (2018): 56-63.

264 Durand, Alain. (2020). *New IP*. icann.org. p. 26

265 Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., & Perrig, A. (2022). *The Complete Guide to SCION: From Design Principles to Formal Verification*. Springer Cham. doi.org/10.1007/978-3-031-05288-0

266 Perrig, A., Szalachowski, P., Reischuk, R. M., & Chuat, L. (2017). SCION: A Secure Internet Architecture. Heidelberg: Springer. p. 51

267 Ibid. p. 51

268 Huston, Geoff. (2022). BGP in 2021 – The BGP Table. blog.apnic.net

local ISD for how to get to the target ISD, and from the core path service of the target ISD for how to get to the target AS. Through a combination of these path segments, end-to-end paths are created that can be embedded in the packet header.[269] This **may be viewed as a natural response to the challenge of scaling which then goes from local IP (NAT) to global IP to AS to ISD**. Put simply, the Internet is turned from a network of networks into a network of networks of networks. The vision of SCION is that ISD numbers could be assigned in the future by ICANN and regional Internet registries similar to how it works for AS numbers (see section 2.1.3).[270]

Flexible, end-host addressing: The idea of SCION is that inter-domain routing newly relies on a pairing of ISD numbers and AS numbers rather than on a pairing of AS numbers and IP-addresses. As the SCION team writes, "only the border router at the destination AS needs to inspect the destination address to forward it to the appropriate local end host. An interesting aspect of this forwarding is enabled by the split of locator (the path towards the destination AS) and identifier (the destination address). In other words, an AS can select an arbitrary addressing format for its hosts, e.g., a 4-byte IPv4, 6-byte media access control (MAC) address, 16-byte IPv6, or any other up to 16-byte addressing scheme".[271] It would also mean that "**end-host addresses do not need to be globally unique—they can be assigned independently by each AS** including private address space."[272]

Path-based, authenticated, inter-domain routing: The second key innovation of SCION aside from adding a logical grouping above ASes is that the inter-domain routing is path-based. SCION uses the same distinction between a data plane and a control plane that SD-WAN has established for large corporate networks (see section 2.2.2.1). Specifically, **the entire path from source AS to target AS is selected by the source and the routers on the path only execute this decision**. Consequently, there is no need to look at a routing table to decide where to forward the packet at every router. However, **the choice for the sender is limited to path segments that are offered in conformity with the policies of ASes in its path**. The source AS can only combine paths based on the available path segments that it can look up from three different path services (source AS to core-AS within same ISD; core-AS to core-AS of target ISD; core-AS to target AS in target ISD). The beaconing that creates paths for these path services uses cryptographic authentication at every router, meaning it does not just depend on gossip or trust. Each AS can, among other things, specify a set of minimum and maximum allowable values for paths involving them as well as blacklist ASes that must not appear in downstream paths from them.[273]

In many cases, the source will be able to choose from multiple possible paths. This multi-pathing feature would allow the source to optimize for different criteria such as cost, borders, speed, and environmental impact.

SCION packet header: The SCION header is composed out of three subheaders. First, there is a common header (12 bytes) that fulfils several administrative functions similar to those contained in the IPv6 header. Second, there is an address header (24 to 48 bytes) that contains the ISD-number, AS-number, and end-host address (e.g., IPv6) of the source and the destination. While the end-host address is not read by SCION routers, it still must be transported for the intra-domain routing in the target AS. Third, there is a path header (32 to 796 bytes). This **header contains the sequence of ASes through which the path traverses as well as an expiry time and per-AS cryptographic authentication** for every single router-to-router transmission.

Overall, **the SCION header is significantly larger than current headers** because it needs to contain path information. This protocol overhead requires slightly higher bandwidth from the communication infrastructure. On the other hand, it releases routers from compute intensive route calculation. The full specification of the SCION header is in Annex D.

Local trust roots: The third key point of SCION is that it increases local control over trust roots. SCION's creators criticize the trust roots in today's Internet as either monopolistic with a single root of trust (DNSSEC, BGPsec) or as oligopolistic (TLS) (see section 2.2.2.6). The basic idea of SCION is that "**authentication relies on local trust roots, limiting the scope of [certificate] authorities and offering local**

[269] Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., & Perrig, A. (2022). *The Complete Guide to SCION: From Design Principles to Formal Verification*. Springer Cham. doi.org/10.1007/978-3-031-05288-0 p. 81

[270] ibid. pp. 32&33

[271] Ibid. p. 28

[272] Ibid. p. 326

[273] Ibid. p. 65-92

sovereignty".[274] In its first version SCION used the rust root configuration in an ISD for the authentication of everything: the control plane in inter-domain routing (BGPsec equivalent), the name system (DNSSEC equivalent), and end-entities (TLS PKI equivalent).[275] **In its newest iteration SCION only uses the trust root configuration for AS authentication for inter-domain routing**, and its approach for the web PKI and the DNS has been changed. The trust root configuration of an ISD inter alia defines core ASes and a list of root certificates that are used to sign AS certificates, which use public key cryptography to sign routing messages in the control plane. SCION offers a new key derivation system called Dynamically Recreatable Key to enable efficient authentication of messages in the forwarding plane.

Additional systems outside of the SCION core

Levels of trust in web PKI: In the current Internet there is only one intermediary that affirms that a public key belongs to a certain domain name and trust in this intermediary is binary. You either trust it or you don't. SCION works on a new TLS PKI called flexible PKI (F-PKI) in which every client can set up a validation policy that includes three levels of trust in different CAs: untrusted, trusted, and highly trusted.[276] Initially, browser vendors may set the default trust levels but users can freely modify them. This ability of clients to express trust preferences more granularly should create incentives that penalize misbehaving or vulnerable CAs, while favouring those with strong security measures. It might also incentives domain owners to offer more than one certificate.

A clean-slate DNS that enables local control: The need for changes in the naming service is a consequence of the abandonment of IP for inter-domain routing, as in today's DNS website names are only translated into IP numbers. SCION would like existing name servers to add a new type of resource record to their files that links ISD number, AS number, and IP address to a domain name.[277] At the same time, SCION also attempts to create **an alternative DNS that rivals the existing DNS and enables a more federated structure.** In the words of its creators, this system will "co-exist with DNS for an extended period of time, in a similar way to the transition from IPv4 to IPv6".[278] **This system is still in a dynamic design phase and not deployed yet** in operational SCION infrastructure. However, it is still discussed here because it is one of the politically more sensitive aspects. Originally, it was called RAINS; in the newest iteration it has been renamed to RHINE.

As the SCION team highlighted in its first book, "there is an inherent tension between SCION's architectural principle of isolation and the need for a globally consistent namespace".[279] Hence, "within SCION, publicly available names within an ISD exist within that ISD's native isolation context. The use of context explicitly separates global usage of the DNS from local usage thereof". Concretely, per default the ownership of all domain names using a dot (e.g., example.com) are cryptographically validated in the DNS of the local ISD, which may or may not correspond to national borders. In contrast to the current DNS, there are no globally valid domain names in this system anymore.[280] However, RAINS offered naming isolation transparency, meaning it is possible to see how a domain name is cryptographically validated in another ISD through the special command "isd--r-", where "r" represents the ISD number. RAINS further offered a naming consistency observer that highlighted how different ISDs link domain names with different end-host addresses.[281]

In its second book, the SCION team has changed its clean-slate DNS in a way that is hybrid with both a global and a local context, resulting in the RHINE system, specifically acknowledging that "a radical change of security infrastructure at the root level will surely raise tremendous concerns and resistance from the existing DNS ecosystem".[282] Hence, SCION now accepts and even defaults to the ICANN root. At the same time, RHINE introduces a field called "assertion context" which allows for alternative roots or locally used names. Each RHINE Certificate "must be associated with one and only one context of either global or local type".[283] In other words, while RHINE is more backwards compatible than RAINS because the global ICANN root is one possible context, the

[274] Ibid. p. 36

[275] Perrig, A., Szalachowski, P., Reischuk, R. M., & Chuat, L. (2017). SCION: A Secure Internet Architecture. Heidelberg: Springer. p. 63

[276] Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., & Perrig, A. (2022). *The Complete Guide to SCION: From Design Principles to Formal Verification*. Springer Cham. doi.org/10.1007/978-3-031-05288-0 pp. 419-430

[277] Ibid. p. 459

[278] Ibid. p. 457

[279] Perrig, A., Szalachowski, P., Reischuk, R. M., & Chuat, L. (2017). SCION: A Secure Internet Architecture. Heidelberg: Springer. p. 105

[280]. Ibid. p. 110

[281] Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., & Perrig, A. (2022). *The Complete Guide to SCION: From Design Principles to Formal Verification*. Springer Cham. doi.org/10.1007/978-3-031-05288-0 p. 116

[282] Ibid. p. 447

[283] Ibid. p. 452

context field in SCION is the highest logical naming layer in RHINE and therefore the only layer which needs to be globally unique. Below that, RHINE allows the use of locally valid and multiple globally valid namespaces. This is not by accident. Perrig views the global ICANN root negatively as a potential kill switch, citing the recent Ukrainian attempt to remove Russian TLDs from the DNS root file (section 3.1.4.3).[284] As the SCION team explicitly notes, as a side effect, RHINE also makes it easier and cheaper for governments to create a national DNS: "With the effective use of context, RHINE makes naming data inconsistency transparent to everyone on the Internet. Regardless of social or political issues, **governments can implement their virtual boundaries at lower costs without building new infrastructures from scratch**. End users can make more informed decisions on what they (dis)trust".[285] If a domain wishes "to operate in multiple global namespaces", it must obtain a certificate in each context.[286]

4.4.2 Adoption and Standardization

What makes SCION different from almost any other clean-slate Internet architectures is that it is already operationally deployed and that its creators pay explicit attention to the economic incentives needed for organic adoption despite the network effects of IP. While key security benefits such as a better protection from BGP hijacking and DDoS attacks only become tangible with widespread adoption, the path control guarantees can be a substitute for leased lines for communication within industries with high compliance requirements, such as finance or healthcare.

In 2016, the first SCION routers were deployed in the networks of two Swiss ISPs, Swisscom and SWITCH. In 2021, the Swiss National Bank and SIX, the main provider of infrastructure for interbank settlements in Switzerland, launched the Secure Swiss Finance Network, which connects Swiss banks through SCION routers.[287] SWITCH, the data network operator for Swiss universities, has started to offer SCION to all universities in Switzerland,[288] whereas Swisscom has started to offer SCION services to business customers.[289] Lastly, SCION is experimenting and working on implementation with various (primarily Swiss) institutions. This includes the Secure Swiss Health Network, the network of representation sites of the Swiss Federal Department of Foreign Affairs, Swiss critical infrastructure, and the International Committee of the Red Cross.

International standardization: SCION aims to replace the current Internet architecture, referring to it as the "legacy Internet".[290] The ambition to establish SCION as a global standard has been echoed among others by the Swiss Federal Cyber Security Delegate[291] and it includes standards recognition by the IETF, the ITU, and ENISA.[292] Perrig has contributed to the "Network 2030" group in the ITU (section 4.3.2).[293] However, SCION has mainly been active in the IETF working group on Path Aware Networking.[294] As mentioned in section 4.1, the IETF generally prefers an incremental approach to standardization and there is no avenue to standardize an entire clean-slate architecture in a working group. A major reform of Internet architecture would have to be initiated or at least supported by the Internet Architecture Board (section 2.1.3). Such support remains unlikely without architectural changes, considering the Internet Architecture Board's stance that "to remain a global network, the Internet requires the existence of a globally unique public name space".[295] Instead, the favored approach seems to be splitting SCION into individual components for standardization.[296]

SCION Association: The SCION association will independently publish SCION standard documents that allow enterprises to create SCION-compatible products and services. The association is also building a

[284] Perrig, A. (2022). Swiss Cyber Security Days 2022. anapaya.net 10:47-11:47

[285] Ibid. p. 452

[286] Ibid. p. 452

[287] Swiss National Bank. (2021). *SNB and SIX launch the communication network Secure Swiss Finance Network*. snb.ch

[288] Bertolo, D. (2021). *A quantum leap in cybersecurity*. switch.ch

[289] Swisscom. (2021). *The secure, high-speed Internet under your control.* swisscom.ch

[290] Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., & Perrig, A. (2022). *The Complete Guide to SCION: From Design Principles to Formal Verification*. Springer Cham. pp. 35, 201, 311, 318, 332, 333, 338, 345, 346, 350, 382 & 458.

[291] Schütz, Florian. (2022). Swiss Cyber Security Days 2022. anapaya.net. 45:30-46:00.

[292] SCiON Internet (2022). SCiON Association - Prof. Vanessa Wood & Patrick Naef. 4:15-6:15. youtube.com

[293] Focus Group on Technologies for Network 2030. (2020). *Network 2030 - Architecture Framework.* itu.int p. ii

[294] IETF. (2022). Path Aware Networking RG (panrg). datatracker.ietf.org

[295] Internet Architecture Board. (2000). RFC 2826: IAB Technical Comment on the Unique DNS Root. datatracker.ietf.org

[296] Perrig, Adrian, Juan Garcia Pardo, David Hausheer, Nicola Rustignoli, & Corine de Kater. (2022). SCION Inter-domain Routing Architecture: A Side Meeting at IETF 113. cloud.inf.ethz.ch p. 36; Tramell, Brian. (2022). [PANRG] PANRG June 2022 interim minutes and next steps for SCION mailarchive.ietf.org

certification institute to certify devices, ISPs, and IXPs for their compatibility with SCION.[297]

4.4.3 Discourse and Impact

SCION has several features that gives it security advantages over the current IP suite. This includes authentication, the ability of the source to choose a path for the packet, and local control over encryption.

BGP hijacking: BGP is not authenticated, which makes it vulnerable to path hijacking, and BGPSec has not been widely adopted (see section 2.2.2.4). SCION is authenticated and scalable.[298]

DDoS attacks: SCION's defense against DoS is to enable inter-domain traffic management and resource allocation. This includes source authentication, which is currently not the case for the Internet Control Message Protocol.

Path control: This feature is particularly relevant for businesses that want, or are legally forced, to keep data within certain borders. This can, for example, be the case for sensitive medical data. Furthermore, path control would enable more exact measurements of the carbon cost of forwarding, thereby enabling a movement towards greener routing.[299] Lastly, it could potentially allow states in the future to route cyberattacks around neutral countries.[300]

Availability: Path control allows a sender to select multiple possible paths that can carry packets towards the destination. If one path is blocked, the other(s) can subsequently still be used. Multipathing can be useful in time-sensitive applications, such as voice-over-IP or video streaming, as the quality will not degrade even if some packets are dropped.

Resilience: It can take minutes for routers to converge on new routes after BGP updates. Thanks to the separation of the data and the control plane, SCION aims to bring this down to a few seconds, thereby allowing the network to route around damages faster.

Privacy: In today's Internet, it is not possible to encrypt end-host addresses because they are needed for forwarding packets. This metadata is collected in large swaths by intelligence services and other actors. In a path-based routing system, the routers arguably do not need to be able to read source and destination addresses. They still get metadata to confirm compliance with routing policies; however, this is on the level of ISD or AS numbers, rather than IP numbers.

[297] SCION Association (2022). *About the Association*. scion.org

[298] Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., & Perrig, A. (2022). *The Complete Guide to SCION: From Design Principles to Formal Verification*. Springer Cham. pp. 148-156

[299] Ibid. pp. 399-404

[300] Cordey, Sean & Kevin Kohler. (2021). The Law of Neutrality in Cyberspace. css.ethz.ch p. 44

5 Protocol Politics

The discussion starts by highlighting why and how the technical standards-setting process can be of relevance to politics (section 5.1). Second, it offers a lens for analyzing and understanding the political positions of various actors in the Internet fragmentation debate (section 5.2). Third, it aims to right-size specific challenges, hopes, and fears with regard to New IP (section 5.3) and SCION (section 5.4). Fourth, it analyzes political trade-offs with regard to flexible addressing (section 5.5) and interoperability (section 5.6). Lastly, it highlights a few points specific to Switzerland (section 5.7).

5.1 Why Standards Matter

Standards-setting can be framed as an entirely technical, apolitical process. However, standards have multiple dimensions, some of which are relevant to politics:

Interoperability: The adoption of common standards lowers non-tariff barriers and creates more integrated markets, as well as inertia.

Change control: Who decides on the evolution of standards?

(Un)intended political effects: Standards can (de)centralize and shift power. For example, the issue of address number exhaustion that was resolved with longer IP addresses (IPv6) could have also been addressed by reusing IP numbers locally, as is done for frequencies in cellular networks. However, this would have nationalized the authority to assign them. Similarly, there were discussions about including the hardware serial number (MAC address) within IPv6. However, this was dismissed due to privacy concerns.

Technical limitations: For example, maximum data transmission speed.

Patents: For example, Qualcomm earns billions of dollars from smartphone makers for 5G intellectual property licenses.

Patents are not the key issue of disagreement on the network layer as IP is an open standard. Similarly, there is a principal agreement that technical limitations should be small, and interoperability is good, even though in practice there can be disagreements and mishaps – most notably the fact that IPv6 is not backwards compatible with IPv4, which means technically speaking there are already two internets. However, users do not notice this due to multiplexing. Furthermore, the key limitation that IPv6 solves has not been extremely pronounced yet due to alternative mitigation strategies, such as network address translation. The reasons the existence of these two Internets is not a hot political issue is because the same institutions have **change control** and they are very similar in terms of their **political effects**. These two intertwined issues are at the heart of the Internet governance conflict.

Standards have always had a political component. However, it is a recent phenomenon that some governments also adopt explicit political standardization strategies. Most notably, China has a standards strategy that provides monetary incentives for Chinese companies to be more active in international standard-setting. The goal is to be more aligned between domestic and global standards[301] while also shaping global standard setting more actively. In 2022, the EU has for the first time published a strategy on standardization. Among other things, the European Commission plans to set up a coordination mechanism with EU Member States to strengthen the European approach to international standardisation (e.g., ITU), to establish an EU Excellence Hub on Standards, to establish an EU Internet standards monitoring website, and to fund standardisation projects in selected African countries as part of its development cooperation policy and the Global Gateway.[302]

The US and the EU also collaborate on standards through their joint Trade and Technology Council

[301] The goal is to align 85 per cent of domestic standards with international standards by 2025. Central Committee of the Communist Party of China. (2021). 国家标准化发展纲要[National Standardization Development Outline]. gov.cn section 1.2

[302] European Commission. (2022). An EU Strategy on Standardisation: Setting global standards in support of a resilient, green and digital EU single market. ec.europa.eu

and the US-EU strategic standardisation information-sharing mechanism established by it.[303] Goals include to "foster participation in international standardization organizations for civil society organizations, start-ups, small and medium sized enterprises, and to protect our joint interests in international standardization activities underpinned by core World Trade Organization ('WTO') principles".[304]

5.2 Ideologies and Polities

The largest and most consequential disagreements about Internet standards are about change control underpinned by different ideologies. Specifically, the history of Internet standards can be framed as a power struggle between **four ideologies: libertarianism, Americanism, internationalism, and nationalism.** The OSI vs. IP "protocol wars" from the 1980s to the mid-1990s primarily pitted internationalists against Americanists. The DNS "privatization wars" in the 1990s primarily pitted libertarians against Americanists. The ongoing "multistakeholder vs. multilateral" governance conflict primarily pits Americanists and libertarians against nationalists.

Libertarianism

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather".[305]

- John Perry Barlow, Davos, 8 February 1996

In the 1990s, during the early years of the privatization and globalization of the Internet, most states took a hands-off approach. At the same time, the technical community was influenced by the **cyber- and cypherpunk movements, which advocated for a self-sovereign or even anarchic Internet**. Even in the mainstream, most believed that the Internet contains a degree of liberal or libertarian determinism. For example, Nicholas Negroponte, the co-founder and director of the MIT Media Lab stated that, "the Internet cannot be regulated", explaining that "cyberlaw is by nature, global, and we're not very good at global law".[306] Similarly, US President Clinton quipped: "Now there's no question China has been trying to crack down on the Internet. [Chuckles.] Good luck! [Laughter.] That's sort of like trying to nail jello to the wall. [Laughter.]".[307]

Americanism

"Jon, you don't have the legal right to conduct a test [changing the DNS Root server]. You cannot conduct a test without DARPA's approval. You will be in trouble if you continue this; both you and USC will be liable".[308]

- Ira Magaziner, Davos, 29 January 1998

Americanism is just another term for US nationalism. However, because the Internet is a globalization of a **US network** and matured during the Pax Americana, it is worth highlighting separately. The US finished the IANA transition that handed over policy control for the DNS to the multistakeholder community in 2016.

Internationalism

"The idea is to produce a global text so there cannot be 'digital havens' or 'Internet havens"' where anyone planning some shady business could find facilities to do it".[309]

- Jean-Pierre Chevenement, 2000

The internationalists accept that the Internet needs to be regulated; however, they contend that global problems require global solutions. Hence, they frame cyberspace as a **global commons** like international waters, outer space, or Antarctica with joint management and no territorial sovereignty. Governments maintain some control insofar as they can influence international organizations.

Nationalism

"Countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing".[310]

- Chinese International Strategy of Cooperation on Cyberspace, 2017

[303] U.S.-EU Trade and Technology Council. (2022). U.S.-EU Joint Statement of the Trade and Technology Council. whitehouse.gov p. 4

[304] Ibid. p. 2

[305] Barlow, John Perry. (1996). A Declaration of the Independence of Cyberspace. eff.org

[306] Higgins, Andrew & Azeem Azhar (1996, February 5). China begins to erect a second Great Wall – in cyberspace. In *The Guardian*. p. 9

[307] Clinton, Bill (2000). *Full Text of Clinton's Speech on China Trade Bill*. iatp.org

[308] Goldsmith, Jack and Tim Wu. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press p. 46

[309] Goldsmith, Jack and Tim Wu. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press p. 26

[310] Ministry of Foreign Affairs of the People's Republic of China. (2017). International Strategy of Cooperation on Cyberspace. fmprc.gov.cn section 2.2

As the political and economic importance of the Internet grew, states increasingly formed a consensus that territorial sovereignty principally applies to the Internet. While China and Russia have been the most prominent advocates of **cyber sovereignty** in the sense of exerting a high degree of national control over Internet infrastructure and content, the general applicability of sovereignty and therefore jurisdiction over ICT-infrastructure located within a state's territory is supported by almost all actors today. This includes the United Nations Group of Governmental Experts,[311] as well as the international group of experts of the Tallinn Manual, the most comprehensive Western handbook on international cyberlaw.[312] Despite this consensus, it remains difficult for states to assert full sovereignty in practice.

Counterfactual Internets

Information and communication technologies have differed in their level of state-control across time and jurisdictions. However, in general, it would be fair to say that the first 150 years of modern telecommunications, from around 1840 to 1990, have been characterized by a high degree of state-control. In contrast, today's Internet is associated with open networks, flat hierarchies, and a culture of cooperation. Indeed, not few would argue that computer networks inherently favor decentralization and liberalism. However, most historic claims about the exclusive compatibility of certain technologies with certain polities have not materialized. Hence, it remains debatable to what degree this is a misattribution based on the geopolitical context in which the Internet globalized. **The Internet not only emerged from the most liberal great power in all of history, including with regard to information and communication technologies, but also globalized, commercialized, and matured during the 1990s, the peak years of "strategic holiday" and liberal triumphalism**.[313] Furthermore, the early technical community of the Internet that disproportionately shaped norms, standards, and the public discourse was a clear outlier with regard to libertarian beliefs even within the United States. As such, the level of freedom on the Internet that we currently enjoy is not just an outlier based on the history of our technological development, but it is arguably also exceptional across counterfactual human societies at the same level of technological development. For example, the Internet could have been developed by other types of polities. The British and French Empires were eager adopters of communication technology in part because their colonial empires were so geographically dispersed. In the words of a former British finance minister, the submarine telegraph lines were "the true nerves of the Empire".[314] If colonial empires had not been massively weakened through two World Wars, they might have been logical early adopters of computer networks. Similarly, there are counterfactual scenarios in which socialist[315] or communist[316] centrally planned economies would have shown more persistent interest in computer networks. Even today, it is worth noting that China is building a planned smart city destined to become its new capital and showcase the superiority of a planned economy over a market economy.[317]

A return to the mean?

All this background serves to highlight that **Internet fragmentation in the form of more national control and more censorship is a return towards the historic mean of telecommunications governance**. The headwinds against Internet exceptionalism include its increasing importance, unequal national competitiveness, a geopolitical environment defined by renewed strategic competition, and the Internet's increasing legibility to policymakers. A historical analogy that some have suggested is the open era of radio communications. In the analysis of Tim Wu, there is a historical life cycle of telecommunications technologies that begins with a period of openness, but eventually progresses towards monopoly, centralization, and a closed approach.[318]

Today, the technological determinist arguments that the Internet will inevitably lead to liberal democracy seem naive. Internet history and the diversity of suggested future Internet architectures highlight that there are very often multiple socio-technical configurations that can address the same problem. As Tim Wu stated, "**if the Internet is exceptional in a lasting**

311 UN General Assembly (2013). *Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/68/98).* documents-dds-ny.un.org art. 20

312 Schmitt, Michael (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. rule 1/ pp. 11-13

313 Fukuyama, F. (1992). *The End of History and the Last Man*. Free Press.

314 House of Commons. (1900, May 22). Imperial Telegraphic Communication. hansard.parliament.uk column 1009

315 Medina, E. (2011). Cybernetic Revolutionaries: Technology and Politics in Allende's Chile. MIT Press.

316 Peters, B. (2016). *How not to network a nation: The uneasy history of the Soviet Internet*. MIT Press.

317 Jia, Y., Wildau, G. (2018). China's 'digital city' showcases Xi's grand ambition. ft.com

318 Wu, T. (2011). The Master Switch: The Rise and Fall of Information Empires. Vintage

way, it must be for its ideology as expressed in its technology".[319]

5.3 Keeping New IP in Perspective

The ideology behind New IP and its expected political effects have raised a number of public concerns (section 4.3.3). This section adds several qualifications that help to contextualize this discussion.

First, there is still uncertainty with regard to **how developed Huawei's New IP efforts are**. Huawei has not shared the full specification of a New IP header.

Second, China has not openly campaigned for New IP in the ITU. While it expressed its support in the December meeting, only Huawei and Russia have released full statements to that end. Hence, at least based on public documents, there is no proof that New IP is part of a top-down political campaign[320] or that Huawei gets large-scale subsidies specifically for this project. However, there are several reasons to think that the project has a minimum level of **support from the Chinese government** and is aligned with its agenda. All ITU-contributions from Chinese firms are preapproved by the Chinese Ministry of Industry and Information Technology, which has also cosigned Huawei's proposals. Furthermore, New IP is aligned with the Internet Plus and Standards 2035 strategies, as well as the objective of more ITU- and state-control over the Internet.

Third, advocates of New IP are incentivized to overemphasize the degree to which technical shortcomings of IP cannot be solved on other layers, whereas its critics are inclined to overstate the political effects of New IP. The IP suite has managed to adapt to new services, such as voice-over-IP in the past, without changing the network layer. Vice versa, the "pipes" of the Internet have already gotten a lot smarter through means such as deep packet inspection, which allows (de-)prioritizing some types of traffic. Furthermore, the IETF is also working on deterministic networking, just without the flexible addressing.

Fourth, both Huawei and China are **unlikely to intentionally push for non-interoperability** with IPv4 and IPv6 as it would not make any strategic sense. The Internet is very different from the World Bank, where China was simply able to set up an alternative institution. The logic of network effects means that only the largest network may be incentivized to be intentionally non-interoperable (section 5.5).

Fifth, companies do not like technological, market, and policy uncertainties. **Based on market forces New IP adoption is unlikely to go beyond specific use cases in the foreseeable future**. If New IP were meant to replace IP, this would realistically represent a **multidecade effort that requires a non-market strategy** with backing by the Chinese government. The closest historical analogy may be mobile communications standards, where the Chinese government has massively subsidized and supported the development of a largely indigenous 3G standard developed in partnership with Siemens, named **TD-SCDMA**.[321] This standard was accepted by the ITU as one of the 3G-standards. However, it has not been adopted beyond the network of China Mobile. Hence, several Chinese scholars, such as Kaili Kan, Professor at the Beijing University of Post and Telecommunications, view TD-SCDMA as an expensive failure.[322] For 4G, China again promoted its own national standard **TD-LTE** with China Mobile as the main user. However, this time the Chinese standard closely matched other international standards, except that the domestically developed encryption algorithm ZUC was required.

Sixth, the fate of TD-SCDMA and the fact that IP won out over OSI should be reminders that the success of standards is ultimately decided based on action "on the ground", meaning adoption amongst network device manufacturers, ISPs, IXPs, etc. Huawei has started to **advertise New IP as a protocol for the industrial Internet, independent of international standardization bodies**.

[319] Wu, Tim. (2010). Is Internet Exceptionalism Dead? In Berin Szoka & Adam Marcus (Eds.) T*he Next Digital Decade: Essays on the Future of the Internet*, 179-188. p. 183

[320] Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the Splinternet: How China's technical standards could fragment the internet. Journal of Cyber Policy, 5(2), 239-264.

[321] Gao, P., Gao, X., & Liu, G. (2020). Government-controlled enterprises in standardization in the catching-up context: case of TD-SCDMA in China. *IEEE Transactions on Engineering Management, 68*(1), 45-58.

[322] Kan, Keili. (2014). *TD式创新" 祸国殃民 [TD-style innovation is a disaster for the country and the people]*. techsir.com

Seventh, one key advantage that standardization nevertheless has is that it does provide **legitimacy, particularly in developing countries**, which are standards takers and do not have much existing network infrastructure. Moreover, **international standards set in the ISO, the International Electrotechnical Commission, and the ITU are protected in the Technical Barriers to Trade Agreement in the WTO**[323], which limits the possibilities for countries to oppose their use. An instructive example for this is the case of China's indigenous standard for WLANs called **WAPI**, which relies on proprietary encryption. In 2003, the Chinese government announced that wireless devices sold in China must include WAPI support and foreign companies wanting access to the Chinese market could produce WAPI-compliant products independently or partner with select Chinese firms to which the standard was disclosed. In 2006, China submitted WAPI for standardization in the ISO, where it was blocked by the US and the UK. In 2009, when smartphones increasingly used WLAN, China mandated that devices using the internationally accepted WiFi standard would only be approved if they also supported the WAPI standard. The United States challenged this as a technical barrier to trade in the WTO[324] and the Chinese government eventually withdrew the requirement.

5.4 SCION: Promises and Challenges

The SCION suite has several attractive security characteristics. The most important one and the one that is most often highlighted by the development team is that **SCION offers a solution to the widely accepted problem of BGP's reliance of trust**. BGPSec, which is the result of the deliberations on BGP security within the IETF, has not managed to get a lot of adoption so far in part due to the concerns that root certificates could be misused as centralized kill switches and that the additional required traffic slows down the convergence of BGP routing tables.[325]

At the same time, framing SCION as a BGP replacement can be misleading. On one hand, it is underselling SCION because it highlights the one point on which most people agree that the current architecture is broken. SCION attempts to change the entire Internet architecture, ranging from authentication, to IP addresses, to DNS. On the other hand, for early adopters, the product with which SCION competes is not necessarily BGP. The benefits of an authenticated and scalable inter-domain protocol grow in lockstep with its level of global adoption. Hence, **the early adoption of SCION also depends on its competition with layer 2 solutions for WANs**, more specifically leased lines, MPLS, and SD-WAN. Thus, the key question for organic adoption of SCION will be if it can convince enough groups of institutions to choose it over these more traditional solutions. In Switzerland, this is the case. However, it remains to be seen if this will also work in other contexts. The main commercial advantage that SCION offers is that it does not require a lot of hardware to be deployed and is provider-agnostic.

On the political stage, SCION is currently not a topic as the project is still in an early stage, initiated by a trusted party, and illegible to policymakers and journalists. However, if SCION succeeds in terms of its global business appeal and scales to replace large parts of the existing Internet architecture as it plans, it will face increasing scrutiny. SCION has already mitigated some of the most politically sensitive issues in its newest iteration. Still, the spotlight will likely bring forward a few residual political questions, particularly from the libertarian and Americanist Internet communities:

First, the fact that **RHINE is designed to be able to operate with multiple competing DNS roots** is not merely adding transparency about alternative DNS roots. It adds interoperability and thereby makes it easier to implement national DNS roots. The long-run effect of this would likely be a less global namespace.

Second, a decrease in compliance cost with **data localization laws** might lead to induced political demand and even enable new types of laws that would

[323] World Standards Cooperation. (n.d.) International standards & trade agreements. iso.org

[324] World Trade Organization. (2009). *G/TBT/W/324: Transitional Review Mechanism Pursuant to Section 18 of the Protocol on the Accession of the People's Republic of China: Questions and Comments from the United States to China.* docs.wto.org

[325] Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., & Perrig, A. (2022). *The Complete Guide to SCION: From Design Principles to Formal Verification*. Springer Cham. pp. 3-6

route data away from geopolitical fault lines and essentially create a whitelist or blacklist of countries and regions.

Third, making **end-host addressing more flexible** (see section 5.5) can enable more privacy in liberal countries. However, it could also make it easier for states to implement laws that strongly bind Internet users to their real-world identity, thereby enabling domestic surveillance and censorship.

Facing some reservations is unavoidable simply because of the heterogeneity of global preferences. For example, while data localization laws may draw criticism from some, there is a robust case for storing and transferring certain types of sensitive data only within a jurisdiction. Furthermore, it is difficult to accurately foresee political effects of future Internet architectures deployed at a global scale. At the same time, it is also much easier to make changes to a technical artifact, protocol, or sociotechnical system, while it is in an early stage. This basic tension is also known as Collingridge Dilemma[326] and it cannot be fully resolved. The best that can be done is to have an open conversation about the social and political effects of future Internet architectures, to test things, and to remain as nimble as possible.

If unintended political consequences are identified, both technical and political mitigation efforts may be considered. SCION's removal of local trust roots for the web PKI is a concrete example highlighting that architecture changes that anticipate and reduce undesired political obstacles and consequences are possible. The biggest known incidents of forged certificates have been perpetrated by authoritarian states aiming to intercept and spy on traffic on Western websites from their own population. Localizing trust roots for the web PKI would arguably not improve this problem. The potential forcible use of the local government as the trusted intermediary in web PKI that also has jurisdiction over local ISPs and a stronger motive to surveil local users than other actors could have been problematic.

A second example is SCION's switch from RAINS to RHINE (section 4.4.1). A technical option that would go even further in aligning the architecture with the Western political consensus that multiple global roots would be harmful would be to only accept a global scope for ICANN's root in RHINE. A political option that could mitigate the political and public relations risk around enabling a national DNS and national encryption is an implicit or explicit export moratorium to governments with a clear track record of censorship and surveillance (e.g., Russia, Iran).

Either way, stresstesting future Internet architectures should not be confused with IP-maximalism, a principal refusal to explore extensions to the IP header or non-IP networking. Nor should they be taken as an assertion of political primacy. The goal is to solve technical issues whilst also considering change control as well as (un-)intended political effects. The first part should remain the primary focus, otherwise Internet consolidation and ossification are real prospects.

5.5 Flexible Addressing

A flexible addressing scheme like New IP really tries to shift the narrow waist of the Internet hourglass up to a new "**layer 3.5**", that can handle multiple types of addressing. This does create protocol fragmentation in the sense that not everyone would use this new layer and that it would enable a much greater variety of layer 3 protocols if established. However, it does not create protocol fragmentation in the sense of non-interoperable protocols. Indeed, **both New IP and SCION would arguably counteract one form of logical Internet fragmentation by being able to handle both IPv4 and IPv6 addresses**.

However, it remains unclear to the author why end-host address flexibility would require a New IP or ISDs as an additional hierarchical numbering level. Whereas ISD numbers are currently self-assigned with hope of a future governance mechanism that ensure global uniqueness, AS numbers are already globally unique. Theoretically, the IP addresses of end-nodes are not required to be globally unique; they only need to be globally routable. For this, only the highest layer of identifiers really needs to be globally unique. Hence, in theory, it already would be possible to have routers only read the AS address and forward packets to the destination AS. The border router at the destination AS could then read the next part of the packet, which could be any locally unique address in any locally accepted addressing

[326] Collingridge, David. (1982). The Social Control of Technology. London, United Kingdom: Pinter.

format. In practice, the DNS is an obstacle to ASN-routing, more specifically the fact that the DNS binds names with IP numbers rather than AS numbers. The consequences of this (over-)precision are longest-prefix matching on IP addresses and lookup of IP-AS pairing at every router, which is repetitive and requires expensive hardware, and the need to use IP for end-host addressing.

The question of whether the overall benefits of end-host address flexibility outweigh its downsides remains debatable. This flexibility has advantages in the sense that it will not only allow IPv4 and IPv6 addresses but all desired formats. However, it also has a trade-off, at least with regards to ASN-routing and information-centric networking, in the sense that you first must go to a destination AS before looking at a content ID, even if the same content may also be hosted in a closer AS.

The flexible addressing in SCION and New IP differ in one important way. New IP adds a field to handle multiple end-host addresses but still uses them in routing. In contrast, SCION removes the need for any end-host addresses to be part of unencrypted metadata in routing. As such, **SCION can be privacy-enhancing in liberal contexts**. However, a **key question for both is whether end-host address flexibility will create a loss of online privacy for users in authoritarian states**.

Consider the following example: The fictional country "Mustelus" creates a law that the MAC numbers of all Internet-enabled devices must be registered to the buyer at the point of sales. Furthermore, it instructs its ISPs to implement MAC-numbers as unique identifiers in Internet communication. Today, such a scheme would be very challenging to implement as the rest of the global Internet is using IP numbers. Under the conditions of end-host address flexibility, it would be easier to implement and hence induce political demand.

The trade-off for the flexible naming structure that RHINE offers is similar. RHINE arguably improves the interoperability of naming systems by adding an additional logical layer on top in the form of a globally unique "assertion context". At the same time, it is not very clear if that interoperability is desirable, as it may induce more states to implement their own national DNS and increasingly hamper the development of global Internet brands.

5.6 Interoperability and Network Effects

Standard-setting has political relevance, and this report has highlighted some considerations for select future Internet architectures. However, **fears that future Internet architectures would be intentionally built to be technically non-interoperable with the IP suite are unfounded**. As Mueller[327] argues, the benefits of connecting to the large existing IP-networks are simply too overwhelming. Indeed, the "Network 2030" group in the ITU explicitly affirmed backward compatibility as a "very important practical principle" for a new IP.[328]

However, while new entrants are strongly incentivized to be interoperable, **the largest existing network has rational incentives to intentionally refuse interoperability with competitors.** A great example of the strategic use of non-interoperability is the British-German competition in radiotelegraphy at the beginning of the 20th century. The British Marconi Company had a head start and subsequently aimed to leverage its network effects and defend its quasi-monopoly on ship communication by refusing to "intercommunicate" with German Telefunken devices.[329] In fact, the Marconi company initially claimed technical non-interoperability as a justification for its policy of non-intercommunication; however, this was objectively not true.

This brings us to the essence of today's tech competition. The US aims to maintain its globally dominant position on the infrastructure, logic, and content layers through the **legal non-interoperability** of bottlenecks of the tech stack with key Chinese companies. This does work as highlighted by Huawei's sale of its smartphone and submarine divisions, as well as its setback in RAN equipment. The main reason why it works is not network effects in the narrow sense but the **vertical network effects of the entire US-ICT**

[327] Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization and cyberspace. John Wiley & Sons. pp. 42-70.

[328] Focus Group on Technologies for Network 2030. (2020). *Network 2030 - Architecture Framework*. itu.int p. 13

[329] Brunnermeier, M., Doshi, R., & James, H. (2018). Beijing's Bismarckian ghosts: How great powers compete economically. The Washington Quarterly, 41(3), 161-176.

stack. Everyday ICT-functions that end-users consume today have networks effects but rely on a complex set of infrastructure, logic, and services (see section 2.2). Not all these subfunctions are equally technologically complex and concentrated; however, the US is dominant across enough bottlenecks that it can leverage legal non-interoperability with secondary sanctions on them against any competitor that produces leading technology on a specific subfunction.

At the same time, **using this leverage with US tech sanctions reinforces incentives for increasingly bifurcated supply chains and tech ecosystems**. Ultimately, the goal seems to be to build an alliance of democracies whose combined network effects and capacity to innovate sustainably exceed those of China. Such an alliance could use as combination of industrial policy and multilateral export controls for strategic technology to ensure that the 21st century is safe for democracies and to defend the liberal rules-based order.

Europe may support the US on this due to shared values. However, it also has its own agenda of increasing its autonomy by gaining a larger share of the digital economy. As a market entrant, this follows the reverse logic of **legally forced technical interoperability**. For example, email is an interoperable standard because people can communicate with each other independent of their email provider. This is very much not the case for private messaging apps. Hence, even though it is not very difficult to build a private web-based messaging apps, it is currently very hard to break the network effects of the largest providers in the West, such as WhatsApp. Legally forced interoperability through some shared identifier and protocol would allow European companies to compete on a more even the playing field. This is why the EU Digital Markets Act will most likely force interoperability for "number-independent interpersonal communication services".[330] Of course, an even playing field on one aspect by itself does not guarantee an overall even playing field. Email services are notably still heavily concentrated in the US and the few companies that can preinstall them on their operating systems.

5.7 Switzerland

This last discussion section highlights two issues of particular relevance to Switzerland. First, it highlights the idea of a neutral public core as a potential antidote to Internet fragmentation. Second, it explores the consequences of different SCION adoption scenarios for Switzerland.

Neutral public core: The fear that centralized Internet resources could be weaponized against them in the context of an international armed conflict has been a key driver for Russia, China, and others to explore a national DNS. However, more national control over the DNS and the corresponding encryption can also be abused for surveillance and censorship, and it would make it more difficult and costly to maintain global Internet brands. Hence, if the exceptionalism of the last 30 years of the Internet in the history of telecommunications (section 5.2) is deemed worth protecting, we should consider the libertarian and internationalist case for making global Internet institutions more credibly neutral to address security concerns of nation states without handing more control tools to them.

Both ICANN and RIPE explicitly refer to their neutrality in their negative responses to the Ukrainian request to revoke Russian TLD's and IP-numbers (section 3.1.4.3). This corresponds well with the more general idea proposed by the Netherlands Scientific Council for Government Policy to designate the Internet's public core as a global public good that should be protected from unwarranted State interference.[331] This would make DNS root servers an illegitimate target for belligerents while also prohibiting their weaponization against a belligerent. The concept of a public core of the Internet was supported by the Netherlands, Finland, Slovenia, Germany, the UK, and the Global Commission on the Stability in Cyberspace in the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG).[332] However, a challenge to this concept is that neutrality is a legal concept for sovereign states. As long as the non-neutral Dutch Ministry of Foreign Affairs can put sanctions

330 Secretariat of the European Council (2022). Proposal for regulation on contestable and fair markets in the digital sector (Digital Markets Act). consilium.europa.eu Art. 64 / p. 54

331 Broeders, Dennis. (2016). The public core of the Internet: an international agenda for Internet governance. Amsterdam University Press.

332 Markovski, Veni, & Alexey Trepykhalin. (2021). UN Update: Cyber-Related Developments. itp.cdn.icann.org pp. 3-6

on IP numbers RIPE cannot be credibly neutral. Similarly, as ICANN itself acknowledges, "there is a tension between ICANN's goal of administering the Internet as a neutral global resource and the imposition of sanctions by the U.S. on other countries."[333]

One potential solution to the jurisdiction challenge would be shifting the legal headquarters of key multistakeholder institutions, such as ICANN, to a permanently neutral country, such as Switzerland.[334] Permanently neutral countries can enact sanctions on belligerents; however, in contrast to other countries they cannot choose to ignore the law of neutrality as non-belligerents. If one applies the law of neutrality to cyberspace, one can very reasonably view the decision of a state to remove a belligerent from the DNS as a violation of the neutral impartiality duty in Art. 9 of the Hague Convention V with regard to access to communication infrastructure described in Art. 8 of the same convention.[335] A state that is permanently neutral and has this permanent neutrality enshrined in its constitution would not be legally allowed to enact sanctions that disconnect a belligerent from the DNS without changing its constitution. However, so far, no state has explicitly declared that it would view a decision to disconnect a belligerent from the DNS as a violation of the Hague Convention V.

Instead, an organization tasked with the private global governance of Internet resources could also aim for a host state agreement like that between Switzerland and the International Committee of the Red Cross (ICRC), which would grant ICANN immunity within the scope of its mission from local jurisdiction. In their submissions to the ICANN jurisdiction working group, Brazil[336] and the Just Net Coalition[337] both explicitly pointed to the ICRC and the option of a host state agreement as the "best and most sustainable"[338] solution of jurisdiction issues. ICANN is not a regular NGO and granting legal immunity to it would somewhat insulate the public core of the Internet from geopolitics and provide a solid, long-term fundament for a global Internet governed by the multistakeholder community. In principle, any potential host state (e.g., US, Switzerland, Netherlands) can offer such a host state agreement.

In practice, the US has opposed an agreement or shift of headquarters that would hand over full control to the multistakeholder community, even though it also insists that it has no intention of ever weaponizing its jurisdiction over the DNS. A change in ICANN headquarters would also require an amendment of standard bylaws, which requires a qualified majority of the ICANN Board of Directors.[339] Specifically, article 24.1 of the ICANN bylaws states that "the principal office for the transaction of the business of ICANN shall be in the County of Los Angeles, State of California, United States of America".[340] Hence, for the foreseeable future, ICANN remains as neutral as the current US president allows it to be.

SCION and Switzerland: As the country of origin of SCION, Switzerland profits from special access to its core development team. This report can hopefully make SCION more legible to policymakers and help to highlight specific political considerations. However, discussions and evaluations of if and how to implement SCION on additional specific networks, such as the closed networks of the Swiss military or for connecting Swiss critical infrastructure, should be led at the technical level.

Either way, as the first country with significant adoption of SCION, Switzerland has an interest in the further spread of its use. First, further adoption would increase its network effects and its corresponding usability as a BGP replacement. Second, there is the commercial interest of having a Swiss company (Anapaya) playing an important role in the Internet ecosystem. A simple way to think about adoption scenarios is to differentiate between local and global use, as well as specific and general use. As argued in section 5.4, the chances for international adoption are higher if the Internet architecture is designed to be politically compatible with the key multistakeholder institutions of the Internet (ICANN, IETF) as well as like-minded states.

[333] ICANN. (2018). Annex 4.1 – Jurisdiction Final Report and Recommendations – CCWG-Accountability WS – March 2018. icann.org p. 15

[334] This was a discussed option back in the late 1990s with the attempt to bring the DNS to the Internet Council of Registrars (CORE) in Geneva.

[335] Cordey, Sean & Kevin Kohler. (2021). The Law of Neutrality in Cyberspace. css.ethz.ch pp. 18&19, 38&39, 58, I.

[336] ICANN (2017). CCWG-Accountability WS2 Jurisdiction Sub-group Recommendations. icann.org. Annex E – pp. 5 & 6

[337] Ibid. p. 76

[338] Ibid. p. 76

[339] ICANN. (2022). Bylaws for Internet Corporation for Assigned Names and Numbers. icann.org Art. 25.1

[340] Ibid. Art. 24.1

Scenario 1: If SCION adoption will turn out to be as global and broad as its development team optimistically predicts, Switzerland would profit from its special relationship to the project.

Scenario 2: International adoption remains low but adoption in Switzerland becomes pervasive. Perhaps, the closest analogy among developed, democratic, market economies would be South Korea. The Korean "third way" in digital standards includes the establishment of a national-level authentication infrastructure that has a superior technical security to many other certificates called the National Public Key Infrastructure-based Authorized Certificate. The government mandated its use for online banking, payments over 300,000 Korean won (ca. 230 CHF), and e-government-related services. However, over time two major issues emerged. First, the set-up gave the Korean certificate authority theoretical surveillance opportunities over companies. Second, the lock-in into an idiosyncratic standard created interoperability challenges as it did not work with new international technological components such as mobile operation systems and web browsers. Ultimately, the public and civic groups turned against the mandated use of the National Public Key Infrastructure and the government withdrew it in 2017.[341] The analogy has its flaws. However, it cautions that the network effects of the Western tech ecosystem are powerful and that an idiosyncratic standard is not guaranteed to succeed even if most experts would agree that it has some superior technical security characteristics.

Scenario 3: SCION is adopted in like-minded states but mostly in specific sectors that have high data protection and localization requirements, such as banking and the health sector. This would bring SCION's security benefits to the sectors that need it the most, while avoiding the politically much more problematic notion of nation state ISDs. Hence, advertising SCION as a tool for specific sectors might be a more strategic framing in discussions with like-minded states.

[341] Gyehyun, Jang, & Lim Jong-In. (2021) Technologies of Trust: Online Authentication and Data Access Control in Korea. In Evan Feigenbaum and Michael Nelson (Eds.), *The Korean Way With Data: How the World's Most Wired Country Is Forging a Third Way*. carnegieendowment.org pp. 24-29

6 Conclusion

In this report we have examined how the Internet works, what the concrete concerns around Internet fragmentation and bifurcation are, and what role next-generation Internet protocols might play in this regard. Internet history and the diversity of suggested future Internet architectures highlights that there are multiple socio-technical configurations that can address the same problem. Hence, it is worth highlighting that a return towards the historic mean of telecommunications governance would imply more national control and more censorship.

One potential point of tension for future Internet architectures is that increased local control over the logic layer is attractive from a technical security point of view. However, many political entities also lack respect for human rights and the rule of law. Giving such entities more control over their segment of the Internet can impede the political freedom and security of individuals living in these areas. For example, while it is unambiguously positive to deploy SCION in specific contexts with increased security needs, its global and broad deployment might at least raise questions from libertarian and Americanist perspectives.

Having said that, there is a crucial difference between a clean-slate architecture spreading through organic adoption and a potential use of national legislation or international standardization by an authoritarian state to promote a new protocol suite without being transparent about its specification. **European states and like-minded democracies should uphold the current Internet governance arrangements.** As such, they should continue to monitor the international New IP standardization attempts and oppose an IP replacement in the ITU, as this would fall under the scope of the IETF.

Global standards require compromise

While individual projects such as New IP may raise justified concerns, this report has also highlighted that the principal driver of Internet bifurcation is not as much inherent technical non-interoperability as it is a geopolitical desire to be less interoperable. One potential point of tension here is that the national security sphere in Washington is pursuing a technological decoupling, which may be at odds with the support for a global Internet in the libertarian-adjacent technical Internet community. The idea of **a neutral public core of the Internet could be a complementary vision to the drive towards decoupling ICT-ecosystems**, in the sense that it highlights that some core elements, such as the DNS, should remain globally connected in the long-run, even if there is a trend towards infrastructure bifurcation.

Switzerland's historical policy of extracting small but meaningful reciprocal concessions from key stakeholders to align them step-by-step was successful in unifying telegraph networks.[342] Aiming to apply the same spirit of constructive incrementalism to Internet governance, the author thinks that the following concessions could help to strengthen mutual trust in global standard setting:

ITU: The ITU could make its discussions publicly available. Whereas all IETF drafts and meeting protocols are publicly available, many if not most relevant ITU documents are often only available to paying members. This limits the ability of civil society and academia to serve as friendly "watchdogs" and thereby undermines trust.

IETF: Even though the IETF is open to anyone, the capacities to contribute are unevenly distributed. To strengthen its global legitimacy, the IETF could support capacity-building through training and grants to ensure that more members of demographic groups and key stakeholders of the Internet that are underrepresented (e.g., civil society, women) are able to contribute to Internet standards. Further, the Internet Architecture Board should at least be open to discuss the merits of a vision-based versus an incremental approach. There are serious arguments on both sides. However, if the set-up of the IETF with many small working groups is not suited for next-generation protocol suites, projects are incentivized to look at other venues.

ICANN: The concept of a neutral public core could be a solution to keep the Internet global in the long run. To make its neutrality in future conflicts more credible, ICANN could explore the possibilities for a host state agreement that exempts it from sanctions.

342 Balbi, G., Fari, S., Richeri, G., Calvo, S. (2014). Network Neutrality: Switzerland's role in the Genesis of the International Telecommunication Union. Peter Lang. pp. 82-83

Huawei: The company could be more transparent on the specification and implementation of New IP, similar to how other future Internet architectures such as SCION do it. This would help to create more trust than re-naming exercises.

SCION: Any clean-slate redesign of the Internet architecture unavoidably has a political component. Hence, SCION should continue to work on tests and technical options to ensure architectural alignment with the Western consensus on Internet governance on select issues.

As a final note, it is worth citing the 2013 testimony to Congress on international proposals for multilateral control of the IANA function by FCC Commissioner Robert McDowell: "Merely saying 'no' to any changes is – quite obviously – a losing proposition".[343] This statement on the IANA transition might be extended by analogy to Internet architecture. The fact that some future Internet architectures, such as SCION, have tangible security and quality-of-service advantages over the current TCP/IP-suite puts pressure on the dominant design to integrate new innovations or to risk disruption.

[343] *Fighting for Internet Freedom: Dubai and Beyond: Joint Hearing before the Subcommittee on Communications and Technology of the Committee on Energy and Commerce and the Subcommittee on Terrorism, Nonproliferation, and Trade, and the Subcommittee on Africa, Global Health, Global Human Rights, and Intenational Orgnizations of the Committee on Foreign Affairs*, House of Representatives, 113th Cong. 1 (2013). p. 17

List of Abbreviations

ARPANET	Advanced Research Projects Agency Network
AS	Autonomous System
BGP	Border Gateway Protocol
BGPsec	Border Gateway Protocol Security
BRI	Belt and Road Initiative
ccTLD	country code Top-Level Domain
DARPA	Defense Advanced Research Projects Agency (US)
DDoS	Distributed Denial-of-Service
DiffServ	Differentiated Services (IP)
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DSL	Digital Subscriber Line
ETSI	European Telecommunications Standards Institute
GAC	Government Advisory Council (ICANN)
gTLD	generic Top-Level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IS-IS	Intermediate System to Intermediate System
ISD	Isolation Domain (SCION)
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization (UN)
ISP	Internet Service Provider
ITU	International Telecommunication Union (UN)
IXP	Internet Exchange Point
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
NAT	Network address translation
NSF	National Science Foundation (US)
NSFNET	National Science Foundation Network
OGAS	All-State Automated System for the Management of the Economy
OSI	Open Systems Interconnection
PKI	Public Key Infrastructure
QoS	Quality of Service
RAN	Radio Access Network
RFC	Request for Comments (IETF)
RIP	Routing Information Protocol
RPKI	Resource Public Key Infrastructure
SAGE	Semi-Automatic Ground Environment
SD-WAN	Software-Defined Wide Area Network
SDO	Standards Developing Organization
SORM	System for Operative Investigative Activities (Russia)
TCP	Transmission Control Protocol
TD-LTE	Time Division – Long Term Evolution (4G standard)
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access (3G standard)
TLD	Top-Level Domain
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAN	Wide Area Network
WAPI	WLAN Authentication and Privacy Infrastructure
WLAN	Wireless Local Area Network
WTO	World Trade Organization
WTSA	World Telecommunication Standardization Assembly

Appendix

A General-Purpose Computer Networks (1969-1989)

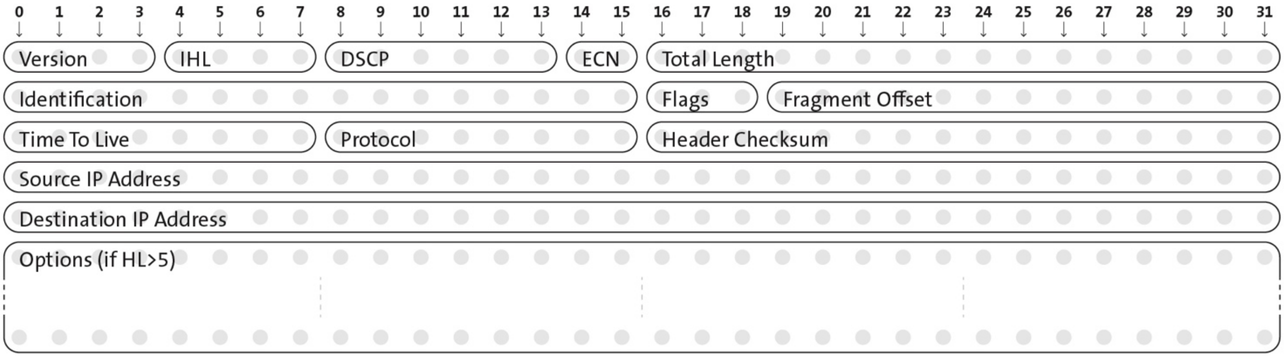
This list is non-comprehensive and has been adapted from Quarterman and Hoskins (1986)[344], as well as Townes (2012).[345]

Creation	Network Name	Protocol	Adopters	Type of Use
1969	ARPANET	TCP/IP	US (ARPA)	research, government
	NPLNET	Some form of packet-switching	UK	research
1973	CYCLADES	Some form of packet-switching	France	research
1975	SATNET	TCP/IP	US	research
1976	Xerox Research Internet	XNS	Xerox	research, commercial
1978	Easynet	DECnet	Digital Equipment Corporation	commercial
1979	USENET	UUCP	Users (US)	public
	ACSnet	MHSnet	Australia	academic
1981	CSNET	TCP/IP, X.25	US (NSF)	academic
	BITNET	IBM protocol	Users (US)	academic
1982	EUnet	X.25, later TCP/IP	Users (Europe)	academic
	SDN	UUCP, TCP/IP, X.25	South Korea	academic
1984	FIDONET	Fido protocols	Users (US)	public
	EARN	UUCP	Users (Europe)	academic, research
	JUNET	UUCP	Corporations (Japan)	academic
1985	Xerox Corporate Internet	XNS	Xerox	commercial
1986	NSFNET	TCP/IP	US (NSF)	academic
	SPEARNET	X.25	Australia & New Zealand	academic
1987	UUNET	UUCP	commercial	commercial
1988	WIDE	TCP/IP	Japan	academic, research
1989	NORDUNET	X.25, TCP/IP	Nordic countries	academic

[344] Quarterman, J., & Hoskins, J. (1986). Notable computer networks. *Communications of the ACM*, *29*(10), 932-971.

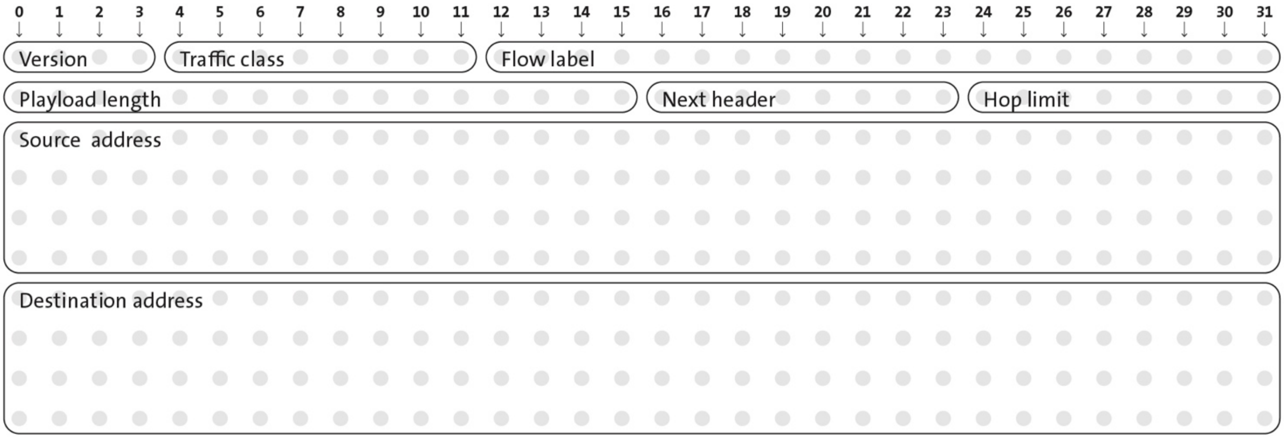
[345] Townes, M. (2012). The spread of TCP/IP: How the Internet became the Internet. *Millennium: Journal of International Studies, 41*(1), 43-64.

B IPv4 Header Specification



1) **Version:** Always equal to 4 (0100) in IPv4.
2) **Internet Header Length (IHL)**: The length of the IPv4 header in increments of 4 bytes. The minimum field value is 5*4 bytes = 20 bytes = 160 bits, the maximum field value is 15.
3) **Differentiated Services Code Point (DCSP):** Indicates different types of data traffic. The differentiated services (DiffServ) architecture does not include predetermined judgments of what types of traffic should be given priority at routers, instead it provides a framework to allow traffic classification and differentiated treatment. Specifically, it allows for assured forwarding and expedited forwarding instead of the default best effort service. However, this refers to prioritization at a router and not an end-to-end guarantee as packets can go through multiple company environments before they reach their destination. DiffServ is mainly used to prioritize the forwarding of delay-sensitive types of data (voice-over-IP, video streaming).
4) **Explicit Congestion Notification (ECN):** A way to signal network congestion without dropping the data packet.
5) **Total Length:** Describes the packet size in bytes. As the field has 16-bits, this limits the maximum data packet size to 2^{16} bytes, which is 65'535 bytes.
6) **Identification:** Data packets may be fragmented into smaller packets during their journey. This is because the maximum transmission unit (MTU) on the network can be lower than the maximum IP-packet size. Specifically, anything travelling on an Ethernet cable has an MTU of 1500 bytes. The identification field allows to signal to which packet a fragment originally belonged to, so that it can be reassembled by the host.
7) **Flags:** Control bits for packet fragmentation. The first bit is not in use. A value of 1 in the second bit indicates that a packet should not be fragmented. A value of 0 in the third bit indicates that the packet is unfragmented or that this is the last fragment of a packet.
8) **Fragment Offset:** This field indicates the position of a fragment within the original, unfragmented IP packet. This is important because the fragments may arrive at their destination out of order.
9) **Time To Live:** This counter function is used to prevent accidental infinite loops between routers. The value is set by the sender with a maximum value of 255 (8-bits field) and a recommended value of 64. Every router through which a data packet goes reduces this number by 1. If it reaches 0 the router deletes the data packet and send an error message to the sender IP-address.
10) **Protocol:** This field signals which layer 4 protocol is used. Most notably TCP at a value of 6 and UDP at a value of 17. Other relevant values are ICMP at 1, and OSPF at 89.
11) **Header Checksum:** Used to check for error in the IPv4 header. If the checksum calculated by the router based on the values in the header doesn't match the one placed here by the previous router it drops the packet.
12) **Source IP-address:** 32-bit unique sender address
13) **Destination IP-address:** 32-bit unique destination address
14) **Options:** This field is optional (0-320 bits) and rarely used.

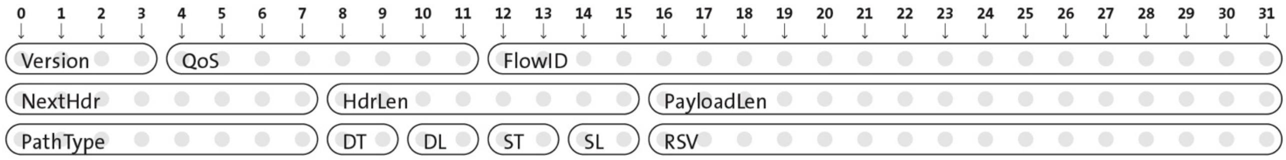
C IPv6 Header Specification



1) **Version:** Always equal to 6 (0110) in IPv6.
2) **Traffic Class:** Equivalent to DCSP field in IPv4. Except that it has been extended from 6 bits to 8 bits.
3) **Flow Label:** This new 20-bit field allows the identification of specific types of communications between a specific source and destination.
4) **Payload Length:** Describes the payload size in bytes. Meaning in contrast to IPv4 this length does not include the IPv6 header which is always 40 bytes. As the field has 16-bits, this limits the maximum data packet size to 2^{16} bytes plus 40 bytes, which is 65’575 bytes.
5) **Next header:** This field signals which layer 4 protocol is used and is equivalent to “protocol” in IPv4.
6) **Hop limit:** This field is used to prevent accidental infinite loops between routers. Every router through which a data packet goes reduces this number by 1. It is the same as the time to live field in IPv4.
7) **Source IP-address:** 128-bit unique sender address
8) **Destination IP-address:** 128-bit unique destination address

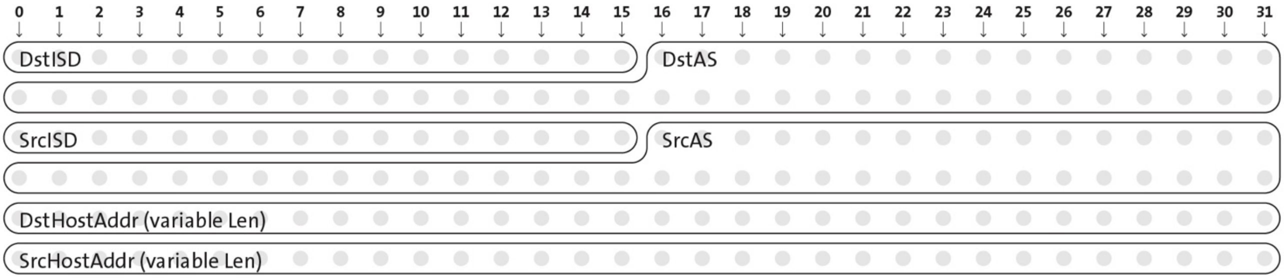
D SCION Header Specifications

D.1 Common Header



1) **Version:** Always equal to 0 for the moment.
2) **QoS:** Equivalent to Traffic Class in IPv6.
3) **FlowID:** Equivalent to the FlowLabel in IPv6.
4) **NextHdr:** Equivalent to Next Header (IPv6) and Protocol (IPv4). Except that the next header can be either a SCION extension or a layer-4 protocol.
5) **HdrLen:** The length of the SCION header (sum of the lengths of the common header, the address header, and the path header) in increments of 4 bytes. Same as IHL (IPv4), except that maximum length is longer in SCION (60 bytes vs. 1024 bytes).
6) **PayloadLen:** Equivalent to Payload Length in IPv6. Describes the payload size in bytes. This includes extension headers and the L4 payload. Maximum payload size of 65’535 bytes.
7) **PathType:** Specifies the SCION path type with up to 256 different types. The initially proposed SCION path types are Empty (0), SCION (1), OneHopPath (2), EPIC (3) and COLIBRI (4).
8) **DT/DL/ST/SL:** Type and length of destination host address (DstHostAddr in SCION Address Header). Type and length of source host address (SrcHostAddr in SCION Address Header). The length fields are two-bits long and support multiples of 4 bytes. Similarly, there is room for 4 different types of addresses.
9) **RSV:** Reserved for future use.

D.2 Address Header

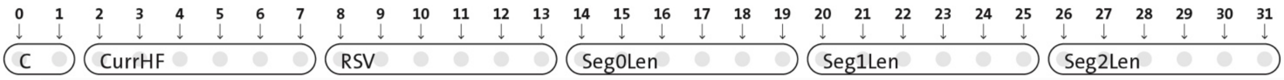


1) **DstISD:** 16-bit identifier of destination ISD
2) **DstAS:** 48-bit identifier of the destination AS
3) **SrcISD:** 16-bit identifier of the source ISD
4) **SrcAS:** 48-bit identifier of the source AS
5) **DstHostAddr:** Variable length host address (32, 64, 96, or 128 bit). Most commonly this will either be an IPv4 adress (32-bit) or an IPv6 address (128-bit)
6) **SrcHostAddr:** Variable length source address (32, 64, 96, or 128 bit). Most commonly this will either be an IPv4 adress (32-bit) or an IPv6 address (128-bit)

D.3 Path Header

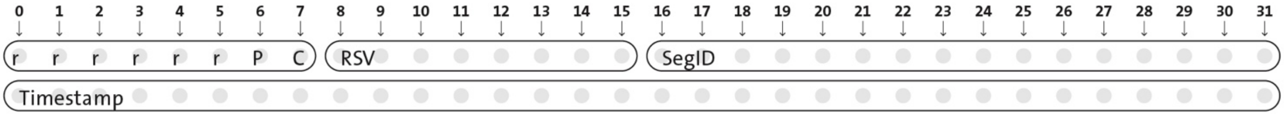
The Path Header consists of a one path meta header, up to three info fields (one per path segment), and up to 64 hop fields.

D.3.1 PathMeta Header



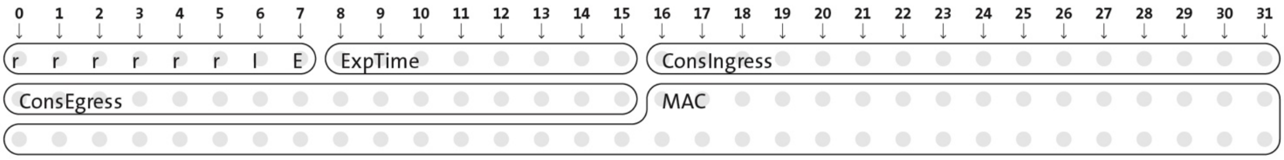
1) **C:** 2-bits updated field that points to the info field to is applicable to the current path segement (max. 3)
2) **CurrHF:** 6-bits updated field pointing to the current hop field (max. 64).
3) **Seg{0,1,2}Len:** The number of hop fields in a given segment. If the segement length is set to zero the path segment does not exist and hence there is no corresponding info field.

D.3.2 Info Fields



1) **r:** Reserved for future use.
2) **P:** Peering flag. If set to true, then the forwarding path is built as a peering path.
3) **C:** Construction direction flag. If set to true then the hop fields are arranged in the direction they have been constructed during beaconing.
4) **RSV:** Reserved for future use.
5) **SegID:** SegID is an updatable field that is required for the MAC-chaining mechanism.
6) **Timestamp:** Timestamp created by the initiator of the path segment on the control plane. The timestamp is expressed in Unix time with 1-second time granularity (0=Jan. 1, 1970, max value in 4 bytes = ca. year 2106). Enables the validation of the expiration time of paths and authentication (MAC).

D.3.3 Hop Fields



1) **r:** Reserved for future use.
2) **I:** If the ConsIngress Router flag is set, the ingress router will process the L4 payload in the packet.
3) **E:** If the ConsEgress Router flag is set, the egress router will process the L4 payload in the packet.
4) **ExpTime:** The expiration time of the hop field. The values range from 0 to 256 and are combined with the timestamp in the info field. The minimum expiry time is timestamp + 5 min and 37.5 seconds. The maximum expiry time is timestamp + 1 day, 5 min and 37.5 seconds.
5) **CongsIngress:** 16-bits ingress interface IDs in construction direction. This identifies the destination router of this hop.
6) **ConsEgress:** 16-bits egress interface IDs in construction direction. This identifies the source router of this hop.
7) **MAC:** 6-byte Message Authentication Code to authenticate the hop field.

E Literature Review of Internet Fragmentation

Source	Term(s)	Definition	Topics [categorization in fig. 1]
Van Alstyne, M., & Brynjolfsson, E. (1996). *Electronic Communities: Global Village or Cyberbalkans?* web.mit.edu	cyber-balkanization	Virtual separation based on people selecting their acquaintances by non-geographic criteria such as common interests, status, economic class, academic discipline, or ethnic group.	1. The use of private mailing lists, personalized news feeds and targeted advertisements. 2. Increased out-of-country co-authorships in academic papers.
Sagawa, Paul (1997). The Balkanization of the Internet. *The McKinsey Quarterly, 1*, 126-139.	Internet balkanization	The evolution to an Internet composed of interconnected but specialized network families that offer differentiated quality of service.	1. Shift from flat price Internet access to market pricing, which will lead to the disappearance of smaller ISPs. 2. Market competition between different Internet standards with the IETF as a standard acknowledging body rather than a standard-setting body. “Middleware” software standards critical to maintain inter-network connectivity. [SDO]
Frieden, R. (1998). Without Public Peer: The Potential Regulatory and Universal Service Consequences of Internet Balkanization. *Virginia Journal of Law and Technology*, 3(8).	Internet balkanization	The disaggregation of the Internet into an amalgam of networks with varying quality of service.	Larger ISPs require more compensation from smaller ISPs due to network congestion, asymmetric traffic, and the absence of a legal common carrier requirement. The expected result is reduced and more expensive service to rural areas based on economic incentives rather than universal Internet service as a public utility. [peering]
Earle, Beverley and Gerald Madek, "International Cyberspace: From Borderless to Balkanized," Georgia Journal of International and Comparative Law 31, 2 (2003): 225-264.	Internet balkanization	Legal demarcations of crossing into a different zone with different rules.	1. Geolocation technology that enables differentiated service. 2. Content filtering, such as in Saudi Arabia. 3. Differences in national laws on hate speech, gambling, pornography, and libel. [geolocation, censorship, legal diversity]
Wu, Tim. (2004). The Balkanization of the Internet. archives.lessig.org	Internet balkanization	A collection of nation-state networks, still linked by the Internet Protocol, but for many purposes separate.	1. China’s use of censorship and the fact that most of its data traffic remains within its borders. 2. Geolocation software allows big websites like Google to cater to various national interests. 3. Australia’s consideration of a country-wide government filter for porn. 4. European lawmakers are considering hosting separate web services for Europe. 5. US enforcement of intellectual property creates incentives for shielding content from the U.S. markets. 6. International bandwidth differences coupled with websites that are optimized for either broadband or narrowband. [censorship, geolocation, intellectual property, digital divide]
Goldsmith, Jack and Tim Wu. (2006). Who Controls the Internet? Illusions of a	bordered Internet		1. Geolocation technology (IP-based, WiFi-based, GPS-based) 2. Consumer demand for the location-based differentiation of web content (local language, local

Borderless World. Oxford: Oxford University Press.			weather, local news, ads for local services and goods) 3. Government's ability to enforce local laws through a limited number of intermediaries between producers and consumers of illicit content (ISPs, financial services, search engines, and domain name registrars) [geolocation, ads, legal diversity]
Foroohar, R. (2006). The Internet Splits Up. newsweek.com	Internet balkanization, split, fragmentation [censorship, DNS,	A quagmire of special interests, competing political agendas and international bureaucracy.	1. Online censorship in China, Iran, North Korea, and Vietnam. 2. Alternative DNS roots, such as the Open Root Server Network. 3. Countries subsidizing national champions, such as France and Germany funding the creation of Quaero as an "Euro-Google". 4. Telecoms wanting to charge content companies extra for the reliable delivery of video-rich content. 5. Countries pushing for internationalized domain names with a non-latin alphabet. [censorship, DNS, net neutrality, language]
Werbach, K. (2008). The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart. UC Davis L. Rev., 42, 343.	Internet balkanization, fragmentation	Dissolution into distinct and potentially hostile sub-units.	1. Expansion of instant messaging services, VoIP (Skype), and social networks (MySpace, Facebook), on which users are only reachable through private, application-specific addresses rather than a universal email address. 2. Internationalized domain names. 3. Alternative DNS roots, such as the the Open Root Server Network. 4. The Great Firewall of China **"Service balkanization":** 5. Internet backbone providers failing to agree on peering **"Application balkanization":** 6. Incumbent broadband providers discriminating against unaffiliated providers of Internet applications and content. **"Information balkanization":** 7. More stringent interpretation and enforcement of copyright protection vis-à-vis search engines and ISPs. [proprietary platforms, language, DNS, censorship, peering, net neutrality, intellectual property]
The Economist. (2010). *A virtual counter-revolution*. economist.com	balkanization, fragmentation	A shift from one global network where the same rules applied to everyone, everywhere, to a collection of more or less connected islands.	1. Law enforcement demands access to data 2. Big IT companies are building their own digital territories (e.g., Facebook) 3. Violations of net neutrality 4. Chinese censorship 5. National DNS 6. Internationalized domain names 7. Geoblocked content (Intellectual property) [proprietary platforms, net neutrality, censorship, DNS, language, intellectual property]
White House. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness*	Internet fragmentation	An Internet, where large swaths of the world's population would be denied access to sophisticated applications and rich content because of a	1. Actions that go against the principles of free flow of information and end-to-end interoperability.

in a Networked World. obamawhitehouse.archives.gov		few nations' political interests.	
Hill, Jonah. (2012). "A Balkanized Internet?: The Uncertain Future of Global Internet Standards." Georgetown Journal of International Affairs (2012): 49-58.	Internet balkanization	Dynamic changes in the Internet ecosystem that pull the global network apart into various distinct, idiosyncratic "internets".	1. A large country or a coalition of countries deciding to withdraw from the current Internet standards process. **Remedies:** a) The US and the EU should persuade companies that profit from their patents being included in current Internet standards to accept reduced royalty payments from poorer countries. b) The US should engage in capacity building and train engineers from underrepresented countries to enable participation in standard-setting in the IETF. [SDO]
Hill, Jonah. (2012). *Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers.* belfercenter.org	Internet fragmentation, balkanization		**"Fragmentation at the Logical Layer":** 1. National DNS root servers apart from the ICANN-approved root 2. Piecemeal Transition from IPv4 to IPv6 3. The Collapse of the Internet Standards Process. A concerted effort to take the standards-making power out of the hands of the IETF, and to give ultimate authority for standards to the United Nations and the ITU **"Fragmentation at the Information Layer":** 4. Internet Censorship, Blocking and Filtering **"Fragmentation at the People and Physical Layer":** 5. The Breakdown of Peering and Transit Agreements/Net Neutrality **"Fragmentation at the People Layer":** 6. Local Privacy Regimes [DNS, IPv6, SDO, censorship, privacy]
Meinrath, S. (2013). *We Can't Let the Internet Become Balkanized*. slate.com	Internet balkanization	An Internet with a complex array of different jurisdictions imposing conflicting mandates and conferring conflicting rights.	Countries that challenge U.S. Internet hegemony after the Snowden revelations and call for a more "democratic" global system of Internet regulation.
Leahy, Joe. (2013). *Brazil sparks furore over internet privacy bill*. ft.com	Balkanization of the web	-	1. Data localization laws (Brazil) [data localization]
Akplogan et al. (2013). *Montevideo Statement on the Future of Internet Cooperation.* icann.org	Internet fragmentation at a national level	-	**Remedies:** a) Global multistakeholder Internet cooperation. b) Acceleration of the globalization of ICANN and IANA functions c) IPv6 transition [IPv6]
Patrick, Stewart. (2014). The Obama Administration Must Act Fast to Prevent the Internet's Fragmentation. cfr.org	Internet fragmentation	-	1. Shifting Internet governance from ICANN to the ITU 2. A surge in cybercrime 3. The growing specter of cyberconflict [SDO]
Drake, W., Cerf, V. & Kleinwächter, W. (2016). Internet fragmentation: An overview. weforum.org	Technical Fragmentation	Conditions in the underlying infrastructure that impede the ability of systems to fully interoperate	1. Network Address Translation 2. IPv4 and IPv6 incompatibility and the dual-stack requirement 3. Routing corruption

		and exchange data packets and of the Internet to function consistently at all end points.	4. Firewall protections 5. Virtual private network isolation and blocking 6. TOR "onion space" and the "dark web" 7. Internationalized Domain Name technical errors 8. Blocking of new gTLDs 9. Private name servers and the split-horizon DNS 10. Segmented Wi-Fi services in hotels, restaurants, etc. 11. Possibility of significant alternate DNS roots 12. Certificate authorities producing false certificates [IPv6, language, DNS]
	Governmental Fragmentation	Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources.	1. Filtering and blocking websites, social networks or other resources offering undesired contents 2. Attacks on information resources offering undesired contents 3. Digital protectionism blocking users' access to and use of key platforms and tools for electronic commerce 4. Centralizing and terminating international interconnection 5. Attacks on national networks and key assets 6. Local data processing and/or retention requirements 7. Architectural or routing changes to keep data flows within a territory 8. Prohibitions on the transborder movement of certain categories of data 9. Strategies to construct "national Internet segments" or "cybersovereignty" 10. International frameworks intended to legitimize restrictive practices [censorship, data localization, securitization]
	Commercial Fragmentation	Business practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources.	1. Potential changes in interconnection agreements 2. Potential proprietary technical standards impeding interoperability in the IoT 3. Blocking, throttling, or other discriminatory departures from network neutrality 4. Walled gardens (e.g., Facebook) 5. Geo-blocking of content 6. Potential use of naming and numbering to block content for the purpose of intellectual property protection [peering, net neutrality, proprietary platforms, intellectual property]
De Nardis, Laura. (2016). *One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation*. cigionline.org	Internet Fragmentation	The Internet develops into disjointed segments based on geographical borders or proprietary ecosystems.	**"Physical Infrastructure Layer"** 1. Lack of Internet access for half of the world. 2. Lower bandwidth in developing countries. 3. Fewer IXP's in developing countries **"Logical Layer"** 4. IPv4 to IPv6 transition **"Application and Content Layer"** 5. Language fragmentation 6. Censorship 7. Restriction of content based on intellectual property 8. Non-interoperable messaging apps **"Legal Layer"** 9. Diverging national laws

			[digital divide, IPv6, language, censorship, intellectual property, proprietary platforms, legal diversity]
Global Commission on Internet Governance. (2016). One Internet. cigionline.org	Internet Fragmentation	-	**Existing fragmentation:** 1. A lack of basic Internet technologies, such as IXPs (“infrastructure layer”) 2. Incomplete transition from IPv4 to IPv6 (“logic layer”) 3. Censorship practices of repressive regimes (“content layer”) 4. Different legal regimes and regulatory environments (“institutional layer”) **New trends:** 5. Companies developing propriety platforms that limit the traditional openness of the Internet. 6. Governments asserting the right to impose significant constraints on the free flow of information on the Internet. [digital divide, IPv6, censorship, legal diversity, proprietory platforms]
Malcomson, S. (2016). Splinternet: How geopolitics and commerce are fragmenting the World Wide Web. OR Books.	Splinternet	A permanent division of the Internet into discrete, national or regional Internets.	1. Commercial logic of market segmentation (marketing etc.) 2. Parallel but secured networks built by defense departments (e.g., DoD Cloud) and financial institutions (e.g., Symphony). 3. Securitization and militarization of the Internet [ads, securitization]
Scott, M. (2017). Goodbye internet: How regional divides upended the world wide web. politico.eu	Internet balkanization, splinternet	A world wide web in which your user experience is determined by local regulation.	1. European privacy regulations and hate speech laws 2. US abandonment of net neutrality 3. Data localization laws [privacy, net neutrality, data localization]
Mueller, M. (2017). Will the internet fragment?: Sovereignty, globalization and cyberspace. John Wiley & Sons.	Internet fragmentation	Intentional, permanent, and third-party enforced restrictions of connectivity.	1. North Korean national intranet 2. Split DNS root 3. Incompatible protocols (IPv6 transition) 4. Walled garden ISP (AoL) [DNS, IPv6, walled garden ISP]
Editorial Board. (2018). There May Soon Be Three Internets. America’s Won’t Necessarily Be the Best. nytimes.com	Splintered Internet, Internet balkanization	Sets of rules, regulations and norms that are rubbing up against one another.	1. The Great Firewall of China and Internet censorship 2. EU GDPR [censorship, privacy]
Ammar, Mostafa. "ex uno pluria: The Service-Infrastructure Cycle, Ossification, and the Fragmentation of the Internet." *ACM SIGCOMM Computer Communication Review 48*, no. 1 (2018): 56-63.	ManyNets, Internet fragmentation	-	1. Competing network protocols 2. Dominance of content providers, which host content within access networks through CDN 3. Commercial bypass networks (High-Frequency Trading, Google WAN, IPTV) Enablers 4. Ossification of Internet governance 5. Demand for new services, such as low-latency gaming or IoT [SDO]

Voelsen, Daniel. (2019). Cracks in the Internet's Foundation. swp-berlin.org	Internet fragmentation	-	1. China's largely closed off intranet 2. Russia's "Sovereign Internet law" and its national DNS 3. Browser-based DNS encryption coupled with default-use of public DNS resolvers (Google Chrome, 8.8.8.8; Mozilla Firefox, 1.1.1.1) [censorship, DNS]
Lambach, D. (2020). The territorialization of cyberspace. International Studies Review, 22(3), 482-506.	(Re-) Territorialization of Cyberspace	Practices aimed at creating, delimitating and controlling a space: 1. Treating territory as a material fact on maps and as administrative categories. 2. Communication of territorial boundaries through symbols and boundary Markers. 3. Display of power through laws, taxation, surveillance, and policing.	**"State territory":** 1. Geolocation technologies 2. National firewalls, such as the Great Firewall of China and the Kwangmyong intranet in North Korea. 3. Internet shutdowns 4. Data localization laws 5. Notions of cyberwar, cyberdefense, and cyber deterrence, including the framing of cyberspace as fifth domain of warfare. 6. ccTLD 7. Nationalized DNS system **"Corporate territory":** 8. Historical walled gardens by AOL and CompuServe 9. Corporate ecosystems that are only partially interoperable, such as Apple products. 10. Facebook's "free basics" Internet access program [geolocation, censorship, shutdown, data localization, securitization, DNS, walled garden ISP, proprietary platforms]
Munn, Luke. "Porous Territories: the Internet beyond Borderless versus Balkanized." Glocalism: Journal of culture, politics and innovation 1 (2020): 1-25.	Internet territorialization, balkanization, fragmentation	Splintering of the Internet into nationalized fragments that are regulated and actively shaped.	1. Data localization laws 2. Internet shutdowns 3. Content filtering [data localization, shutdown, censorship]
Hoffmann, Stacie, Dominique Lazanski & Emily Taylor (2020) Standardising the splinternet: how China's technical standards could fragment the internet, *Journal of Cyber Policy, 5(*2), 239-264.	Splinternet, fragmentation	Breaking the global, free, and interoperable Internet into two or 200 distinct intranets.	
Weyrauch, David & Thomas Winzen. (2021). Internet Fragmentation, Political Structuring, and Organizational Concentration in Transnational Engineering Networks. *Global Policy 12*(1), 51-65.	Internet fragmentation	Fractionation dynamics in transnational engineering networks that govern the global Internet (particularly the IETF).	1. Network size decline in transnational engineering networks. 2. Collaboration decline in transnational engineering networks. **Further relevant dynamics** 1. Governmental pressure on engineers to align technical contributions with political interests (e.g., China). 2. Organizational concentration (e.g., Google) due to the scale and logic of standards negotiations in the IETF. [SDO]

Lemley, Mark A. "The Splinternet." Duke Law Journal 70 (2021): 1397-1427.	Splinternet, balkanization nationalization	Walled gardens created by private companies or by drawing national boundaries around the Internet.	**“Nationalizing software”** 1. Nations with locally successful content companies rather than US Internet giants 2. Geoblocking to protect intellectual property 3. European privacy protection 4. Censorship in China and Russia 5. Internet shutdowns **“Nationalizing hardware”** 6. US Sanctions on Huawei 7. Ban of Chinese apps (eg TikTok) 8. Incompatible 5G standards **“Nationalizing the network”** 9. DNS filtering of malicious websites at ISPs 10. Federated or split DNS [intellectual property, privacy, censorship, shutdown, app bans, DNS]
Van Raemdonck, Nathalie. (2021). What If … the Internet is No Longer Open? In Florence Gaub (Ed.) What If … Not? The Cost of Inaction. *Chaillot Papers, 163*. iss.europa.eu	Internet fragmentation, decoupling	-	1. National digital app ecosystems that include bans and subsidies based on national security considerations (China: Ban of all Western apps, US: TikTok ban, India: Ban of Chinese apps). [app bans]
O'Hara, Kieron, and Wendy Hall. (2021). *Four Internets: Data, Geopolitics, and the Governance of Cyberspace.* Oxford University Press	Internet fragmentation, balkanization, splinternet, splinternet of things	Incompatibility of technical standards across different parts of the Internet	1. Enough large nations adopting Russian Internet policies (national DNS) 2. Chinese use of DOA in IoT 3. Competing visions for the Internet as an enabler of fragmentation in the long run (“Silicon Valley Open Internet, Brussels Bourgeouis Internet, DC Commercial Internet, Beijing Paternal Internet, Moscow Spoiler Internet”) [DNS]
Seiler, Jake. (2021). TikTok, CFIUS, and the Splinternet. *University of Miami International and Comparative Law Review*, *29* (1), 36-61.	splinternet, balkanization	Dividing the internet based on various factors, such as by nation, political ideology, religion, and other interests.	1. Tik Tok ban by the Trump administration 2. Censorship (e.g., China) [app bans, censorship]
Laurent, Sébastien-Yves. (2021). The United States, States and the False Claims of the End of the Global Internet. In S. Laurent (ed.) *Conflicts, Crimes, and Regulations in Cyberspace (vol. 2)* (pp. 1-42). John Wiley & Sons	fragmentation, balkanization	Attempts by states arriving into the sociotechnical system created by the United States to control their own networks	1. Non-English Internet content 2. Censorship and other content controls 3. EU GDPR and privacy regulations 4. Russian National DNS [language, censorship, privacy, DNS]
Fick, N., Miscik, J., Segal, A., & Goldstein, G. (2022). Confronting Reality in Cyberspace Foreign Policy for a Fragmented Internet. cfr.org	fragmented Internet	-	1. Geolocation technology 2. EU privacy protection 3. Data localization 4. Russian National DNS 5. Content filtering / censorship 6. Internet shutdowns [geolocation, privacy, data localization, DNS, censorship, shutdown]

Perarnaud, Clément, Julien Rossi, Francesca Musiani, and Lucien Castex. (2022). 'Splinternets': Addressing the renewed debate on internet fragmentation. europarl.europa.eu	splinternet, Internet fragmentation, balkanization	Technical fragmentation is the result of choices that intentionally or unintentionally break, restrict or suspend technical connectivity between a part of the internet and the rest of the network	**“Technological factors”** 1. IPv6 transition 2. Competition between security protocols for the transport layer (TLS 1.3 vs. ETS) 3. The *lack of universal acceptance* for internationalised domain names **“Commercial factors”** 1. QUIC 2. Concentration of the DNS resolver market 3. The plans of Google and Apple to end support to third-party cookies in their respective web browsers **China** 1. Belt and Road 2. New IP **Russia** 1. Control over IXPs 2. National DNS 3. Import substitution of ICT products 4. Data localization requirements **EU** 1. imposing intermediary services obligations to DNS services extra-territorially [IPv6, SDO, DNS, data localization]

F Literature Review of Internet Bifurcation

Source	Term(s)	Definition	Topics [categorization in fig. 2]
Dickow, Marcel. (2016). EurasiaNet – How They Split the Internet. In Sabine Fischer & Margarete Klein (Eds.) *Conceivable surprises: eleven possible turns in Russia's foreign policy*, 43-46. Berlin: Stiftung Wissenschaft und Politik.	Split in the Internet	The Internet breaks into two parts, with different technical and legal standards and correspondingly different political coordinates.	1. Large states make a coordinated move to only accept the ITU as Internet standard-setting body and leave the Government Advisory Council of ICANN 2. There is a split with regards to transfer protocols and encryption standards 3. Use of Chinese hardware in these states 4. Fewer IXPs connecting the West with these states. [SDO, Internet Architecture, IXP]
Village Global. (2018). *Eric Schmidt & Tyler Cowen on The Future of Technology & Society*. youtube.com	Bifurcation	-	1. Competitiveness of Chinese Internet ecosystem vis-à-vis US ecosystem 2. The Digital Silk Road aimed to connect developing countries with Chinese digital infrastructure [Digital Silk Road]
Chin, Josh. (2019). *The Internet, Divided Between the U.S. and China, Has Become a Battleground.* wsj.com	Divided, splitting in two, divergence	-	1. China exporting Internet censorship to its client states 2. Digital Silk Road 3. Incompatible 5G standards [Digital Silk Road, 5G/6G]
Triolo, Paul. (2020). *The Telecommunications Industry in US-China Context: Evolving toward Near-Complete Bifurcation.* apps.dtic.mil	Bifurcation	The US-China decoupling of technology stacks, supply chains, and markets.	**US-specific:** 1. US sanctions against Huawei, ZTE and other Chinese companies 2. Five Eyes coordination, Clean Network Initiative and other attempts to get allies to not rely on Chinese digital infrastructure **China-specific:** 3. Made in China 2025 and similar actions aimed to make the technology stack independent from the US 4. The Digital Silk Road aimed to connect developing countries with Chinese digital infrastructure **General** 5. Ban of apps and Internet services from the other country 6. Ban of carriers from the other country 7. Restricting licenses for undersea cables 8. Separate next-generation mobile communications standards 9. Separate next-generation Internet architecture [Clean Network, Made in China 2025, Digital Silk Road, apps, carriers, undersea cables, 5G/6G, Internet architecture]
Kleinwächter, Wolfgang. (2020). *Internet Bifurcation: Will the US-China Digital Arm-Twisting Splinter the Open and Free Internet?* circleid.com	Internet bifurcation	A “digital iron curtain” which will split the global Internet space into two cyberworlds.	1. US “Clean Network” Initiative and the Chinese response to it [Clean Network]
Walia, Apjit. (2020). *The coming Tech Wall and the covid dilemma.* dbresearch.com	Tech wall	Splits the world into two parallel tech regimes, a	1. Separate next-generation Internet architecture 2. Separate next generation mobile communications standards (US-based 6G vs. Huawei 6G) 3. Separate chip architecture (X-86/ARM vs. C-Sky)

		US centric one and a Chinese centric one, with little or no inter-operability.	4. Separate mobile operating systems (iOS/Android vs. HarmonyOS) 5. Separation between GPS and Beidou 6. Separation in IoT 7. Separate payment systems (Fedwire vs. Yuan Wire) [Internet Architecture, 5G/6G, chips, GNSS, IoT, payment]
Houser, Kimberley. "*The Innovation Winter Is Coming: How the U.S.-China Trade War Endangers the World*," *San Diego Law Review 57*, 3 (2020): 549-608	Bifurcated Internet	Highly divergent standards, and technology with non-interchangeable components, forcing the rest of the world to pick a side.	1. Separate 5G standards 2. Separate Internet protocols 3. Separate domain name systems 4. Separate data pools on which AI systems are trained 5. Separate mobile operating systems 6. Separate semiconductor supply [5G/6G, Internet Architecture, DNS, AI, mobile OS, chips]
Hoffmann, Stacie, Dominique Lazanski & Emily Taylor (2020) Standardising the splinternet: how China's technical standards could fragment the internet, *Journal of Cyber Policy, 5(*2), 239-264.	Splinternet, fragmentation	Breaking the global, free, and interoperable Internet into two or 200 distinct intranets.	**Driver** 1. A three-pronged Chinese "decentralized Internet infrastructure" campaign in the ITU 1a) Promotion of DOA as alternative to DNS 1b) Blockchain-based DNS 1c) New IP 2. Digital Silk Road **Result** 3. Split DNS 4. Split in standard-setting organizations with the the Western camp using IETF-standards and the "Eastern" camp using ITU-standards. [DNS, Internet Architecture, SDO]
Van Raemdonck, Nathalie. (2021). What If … the Internet is No Longer Open? In Florence Gaub (Ed.) What If … Not? The Cost of Inaction. *Chaillot Papers, 163*. iss.europa.eu	Internet fragmentation, decoupling	-	1) US clean network initative and clean path policy 2) China's Belt and Road Initative. **More specifically:** 1a) Exports controls from US prohibit use of US hardware with Belt and Road Software or the use of US software if it is run on Belt and Road hardware in third countries. 1b) Exports from third countries to US tech ecosystem cannot contain Belt & Road technology 1c) Third country embassies and intelligence services can only send and receive classified information from US if they have a "clean path". 1d) The app stores in the US tech ecosystem are subject to a national security review. 2a) Third party exports to Belt & Road countries cannot contain American technology 2b) Embassies and intelligence services with clean path infrastructure cannot send or receive intelligence with Belt & Road countries. 2c) Chinese export controls on emerging technology [Clean Network, Digital Silk Road]
O'Hara, Kieron, and Wendy Hall. (2021). *Four Internets: Data, Geopolitics, and the*	technological Iron Curtain, giant virtual firewall	Two separate information ecosystems with different regulations.	1. Separate 5G standards (US & China) 2. Digital Silk Road (China) 3. Clean Network Initative (US)

Governance of Cyberspace. Oxford University Press		Even if there are connections across the rift, it would still be complex, difficult, and slow to transfer data.	[5G/6G, Digital Silk Road, Clean Network]
Hillman, J. (2021). The Digital Silk Road. HarperCollins.	network wars	The United States and China are fighting for control over the networks of tomorrow.	1. Digital Silk Road 2. Clean Network 3. China's Great Firewall 4. 5G/6G 5. Smart cities / surveillance cameras 6. Undersea cables 7. GNSS 8. Satellite Internet access [digital silk road, clean network, 5G/6G, CCTV, undersea cables, GNSS, satellite Internet]
Bateman, J. (2022). *U.S.-China Technological "Decoupling": A Strategy and Policy Framework*. carnegieendowment.org	technological decoupling, split	In its strongest form, it can mean a total technological divorce between the United States and China. In its weaker form, it refers to the marginal reduction of tech interdependence.	1. 5G 2. Semiconductors 3. Clean Network 4. Digital Silk Road [5G/6G, semiconductors, clean network, digital silk road]

G Design Principles for Internet Architectures

The following table is not comprehensive, various groups have referred to their own principles for future Internet architectures. At the same time, the author is not aware of any high-level political effort to systematically work towards shared Internet architecture design principles similar to what has happened in AI since 2017, even though it would seem easier to apply design principles to a single, global, sociotechnical system, such as the Internet, rather than to a broad field of research and application. The numbers in the table indicate the order in which the authors of design principles have listed them. The order within the table aims to group similar principles together to make it easier to compare them.

Clark (1988)[346]	Clark (2009)[347]	Network 2030 (2020)[348]	Chuat et al. (2022)[349]
1) Internet communication must continue despite loss of networks or gateways: The state information which describes the on-going conversation (e.g. number of packets transmitted) must be stored at the endpoints of the net.	**2) Availability and resilience:** While the Internet of today deals with specific sorts of faults and component failures (lost packets, links and routers that fail), it does not have an overall architecture for availability.	**7) Resilience:** Networked systems need to be able to continue to offer a satisfactory QoS no matter what challenge they experience. Resilience needs to be stronger because an increasing amount of rcritical services (SCADA, ICS) will run on future networks.	**1) Availability in the presence of adversaries:** As long as an attacker-free path between end hosts exists, it should be discovered and provide some guaranteed amount of bandwidth between hosts.
2) Support for multiple types of communications service: The architecture must be able to tolerate simultaneously transports protocols which	**7) Support for tomorrow's computing:** Take the wide spectrum of computation from the IoT to cloud computing into account.	**4) Heterogeneity in communication, compute, storage, service and their integration.** Meet the needs of mobile Internet, IoT, Cloud, Big Data, and	

[346] Clark, D. (1988). The design philosophy of the DARPA Internet protocols. In *Symposium proceedings on Communications architectures and protocols.* pp. 106-114
[347] Clark, D. (2009) Toward the Design of a Future Internet (ECIR Working Paper No. 2009-3). dspace.mit.edu pp. 6&7
[348] Focus Group on Technologies for Network 2030 (2020) Network 2030 Architecture Framework. itu.int pp. 23-28
[349] Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., & Perrig, A. (2022). The Complete Guide to SCION: From Design Principles to Formal Verification. link.springer.com pp. 9-13

wish to constrain reliability, delay, or bandwidth. at a minimum.	**9) Support for tomorrow's applications:** Includes a range of security requirements, support for highly available applications, new sorts of naming, etc.	Satellite. Multiple types of multiple network devices, network and /or service nodes, multiple protocols, multiple network and virtual network functions, multiple services, will exist.	
3) Accommodation of a variety of networks: The Internet architecture operates over a wide variety of networks, including long haul nets, local area nets, broadcast satellite nets and packet radio networks. There are a number of services which are explicitly not assumed from the network to enable this.	**8) Utilize tomorrow's networking:** Wireless (and mobility) implies new sorts of routing, intermittent connectivity, and dealing with losses. Advanced optical networks can offer rapid reconfiguration of the network connectivity graph.		
4) Permission of distributed management of Internet resources: There are several different management centers within the deployed Internet, each operating a subset of the gateways, and there is a two-tiered routing algorithm which permits gateways from dilferent administrations to exchange routing tables, even though they do not completely trust each other.			
5) Cost effectiveness: Limit inefficiencies such as header overhead and the need for retransmissions of lost packets.	**4) Economic viability:** There is a tension between the open Internet, and the desire of investors to capture the benefits of their investment. A future architecture favors vertical integration and a closed Internet if additional functions are bundled with basic forwarding.		**3) Efficiency and Scalability:** We seek improved scalability compared to the current Internet, in particular with respect to BGP and the size of forwarding tables. An approach to achieving efficiency and scalability is to avoid storing forwarding state on routers wherever possible. We thus aim to encode state into packet headers.
6) The Internet architecture must permit host attachment with a low level of effort.		**3) Backward Compatibility** It is impractical and enormously costly to deploy at large a new architecture if it does not inherently support existing network operation.	**5) Deployability:** Early adopters must already obtain benefits without disrupting current services. Migration should be cheap, only requiring a few border routers and limited personnel training.
7) The resources used in the Intemet architecture must be accountable: The Internet architecture contains few tools for accounting for packet flows.	**3) Better manageability:** Effective management is a challenge today, both for large ISPs (who must hire highly-skilled and trained employees) and for individual users (who have few tools and little recourse if their home networks fail).		

	1) Security: A Future Internet must have a coherent security architecture, which makes clear what role the network, the application, the end node, etc. each has in improving security.	**6) Intrinsic Anonymity and security support for all network operations:** The security fabric of Network 2030 builds on an end-to-end security system including identity authentication, network security, platform security, data security and business security with guarantees for trustworthiness.	**2) Transparency and Control:** Taking transparency of network paths as a first property, we aim to additionally achieve path control‹, a stronger property that enables ASes to control the incoming path segments‹ through which they are reachable and allows senders to then create and select end-to-end paths. **6) Formal Verification:** Current engineering approaches based on reviews and testing are insufficient to ensure the security of advanced distributed protocols.
	5) Suitable for the needs of society: Standards, tends to work the same everywhere. It will be necessary, as part of the design process, to think about how to avoid "baking in" unnecessary cultural norms. The network will be expected to work differently in different contexts.		
	6) Longevity: The network must have the adaptability and flexibility to deal with changing requirements, while remaining architecturally coherent. The goal of evolution is closely linked to the goal of operating in different ways in different regions, in response to regional requirements such as security. On the other hand, a factor that can contribute to longevity is the stability of the system: providing a platform that does not change in disruptive ways.	**1) Simplicity:** Large numbers of virtualized and non-virtualized components make Network 2030 complex. One way to increase reliability or flexibility would be to reduce the number of components in a service delivery path. **2) Native Programmability and Soft Re-architecting** Network 2030, architecture is expected to be extremely flexible and highly programmable with native softwarization infrastructures.	**4) Extensibility and Algorithm Agility:** Core architecture and codebase are designed to be extensible, such that additional functionality can be easily built and deployed. Algorithm agility allows a protocol to easily migrate from one algorithm to another. It is especially important in the context of cryptographic algorithms, which only become weaker over time.
		4) Native Slicing: A network slice is a managed group of subsets of resources, network functions at the data, control, management and service planes at any given time. Slices may offer single uniform capability interfaces to entities and network functions.	
		5) Unambiguous naming network functions and services.: Enable future users to access specific content, function or service rather than a specific server (information-centric networking).	
		8) Network Determinism: Guaranteed latency to meet end-to-	

		end of new business applications such as industrial control, telemedicine, robotics and vehicle networking	

H List of Clean-Slate Internet Architectures

Name	Reference
Application Layer Framing (ALF)	Clark, David D., and David L. Tennenhouse. "Architectural considerations for a new generation of protocols." ACM SIGCOMM Computer Communication Review 20, no. 4 (1990): 200-208.
ANTS	Wetherall, David J., John V. Guttag, and David L. Tennenhouse. "ANTS: A toolkit for building and dynamically deploying network protocols." In 1998 IEEE Open Architectures and Network Programming, pp. 117-129. IEEE, 1998.
ChoiceNet	Wolf, Tilman, James Griffioen, Kenneth L. Calvert, Rudra Dutta, George N. Rouskas, Ilya Baldin, and Anna Nagurney. "ChoiceNet: toward an economy plane for the Internet." ACM SIGCOMM Computer Communication Review 44, no. 3 (2014): 58-65.
Data-Oriented Network Architecture (DONA)	Koponen, Teemu, Mohit Chawla, Byung-Gon Chun, Andrey Ermolinskiy, Kye Hyun Kim, Scott Shenker, and Ion Stoica. "A data-oriented (and beyond) network architecture." In Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 181-192. 2007.
Delegation-oriented architecture	Walfish, Michael, Jeremy Stribling, Maxwell N. Krohn, Hari Balakrishnan, Robert Tappan Morris, and Scott Shenker. "Middleboxes No Longer Considered Harmful." In OSDI, vol. 4, pp. 15-15. 2004.
Delay/disruption tolerant network (DTN)	Fall, Kevin. "A delay-tolerant network architecture for challenged internets." In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 27-34. 2003.
eXpressive Internet Architecture (XIA)	Anand, A., Dogar, F., Han, D., Li, B., Lim, H., Machado, M., Wu, W., Akel-la, A., Andersen, D.G., Byers, J.W. and Seshan, S., 2011, November. XIA: An architecture for an evolvable and trustworthy Internet. In Proceedings of the 10th ACM Workshop on Hot Topics in Networks (pp. 1-6).
Framework for Internet Innovation (FII)	Koponen, Teemu, Scott Shenker, Hari Balakrishnan, Nick Feamster, Igor Ganichev, Ali Ghodsi, P. Brighten Godfrey et al. "Architecting for innova-tion." ACM SIGCOMM Computer Communication Review 41, no. 3 (2011): 24-36.
HLP	Subramanian, Lakshminarayanan, Matthew Caesar, Cheng Tien Ee, Mark Handley, Morley Mao, Scott Shenker, and Ion Stoica. "HLP: A next generation inter-domain routing protocol." ACM SIGCOMM Computer Communication Review 35, no. 4 (2005): 13-24.
Internet indirection infrastructure (i3)	Stoica, Ion, Daniel Adkins, Shelley Zhuang, Scott Shenker, and Sonesh Surana. "Internet indirection infrastructure." In Proceedings of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp. 73-86. 2002.
Metanet	Wroclawski, J. (1997). The Metanet: White Paper - Workshop on Research Directions for the Next Generation Internet. archive.cra.org
MobilityFirst	Raychaudhuri, Dipankar, Kiran Nagaraja, and Arun Venkataramani. "Mobilityfirst: a robust and trustworthy mobility-centric architecture for the future internet." ACM SIGMOBILE Mobile Computing and Communications Re-view 16, no. 3 (2012): 2-13.
Named Data Networking (NDN)	Zhang, Lixia, Alexander Afanasyev, Jeffrey Burke, Van Jacobson, K. C. Claffy, Patrick Crowley, Christos Papadopoulos, Lan Wang, and Beichuan Zhang. "Named data networking." ACM SIGCOMM Computer Communication Re-view 44, no. 3 (2014): 66-73.
Nebula	Anderson, Tom, Ken Birman, Robert Broberg, Matthew Caesar, Douglas Comer, Chase Cotton, Michael J. Freedman et al. "The nebula future internet architecture." In The Future Internet Assembly, pp. 16-26. Springer, Berlin, Heidelberg, 2013.
Network of information (NetInf)	Dannewitz, Christian, Dirk Kutscher, Börje Ohlman, Stephen Farrell, Bengt Ahlgren, and Holger Karl. "Network of information (NetInf) – an information-centric networking architecture." Computer Communications 36, 7 (2013): 721-735.
New IP	Li, Richard, Kiran Makhijani, and Lijun Dong. "New IP: A data packet framework to evolve the internet." In 2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR), pp. 1-8. IEEE, 2020.
NewArch	Clark, David, Robert Braden, Karen Sollins, John Wroclawski, and Dina Kat-abi. New Arch: Future Generation Internet Architecture. apps.dtic.mil. 2004.
Nimrod	Castineyra, Isidro, Noel Chiappa, and Martha Steenstrup. The Nimrod routing architecture. RFC 1992, August, 1996.

New Internet Routing Architecture (NIRA)	Yang, Xiaowei, David Clark, and Arthur W. Berger. "NIRA: a new inter-domain routing architecture." IEEE/ACM transactions on networking 15, no. 4 (2007): 775-788.
Plutarch	Crowcroft, J., Hand, S., Mortier, R. et al. (2003). Plutarch: An Argument for Network Pluralism. acm.org
Postmodern internetwork architecture	Bhattacharjee, Bobby, Ken Calvert, Jim Griffioen, Neil Spring, and James PG Sterbenz. "Postmodern internetwork architecture." NSF Nets FIND Initiative (2006): 1-18.
Publish / subscribe Internet routing paradigm (PSIRP)	Tarkoma, Sasu, Mark Ain, and Kari Visala. "The Publish/Subscribe Internet Routing Paradigm (PSIRP): Designing the Future Internet Architecture." In Future Internet Assembly, pp. 102-111. 2009.
PURSUIT	Fotiou, Nikos, Pekka Nikander, Dirk Trossen, and George C. Polyzos. "Developing information networking further: From PSIRP to PURSUIT." In International Conference on Broadband Communications, Networks and Systems, pp. 1-13. Springer, Berlin, Heidelberg, 2010.
Recursive Internetwork Architecture (RINA)	Day, John, Ibrahim Matta, and Karim Mattar. "Networking is IPC: a guiding principle to a better internet." In Proceedings of the 2008 ACM CoNEXT Conference, pp. 1-6. 2008.
Recursive Network Architecture (RNA)	Touch, Joe, Yu-Shun Wang, and Venkata Pingali. "A recursive network architecture." ISI, Tech. Rep 626 (2006).
SCION	Chuat, Laurent, Markus Legner, David Basin, David Hausheer, Samuel Hitz, Peter Müller, and Adrian Perrig. (2022). The Complete Guide to SCION: From Design Principles to Formal Verification. Springer Cham.
Sirpent	Cheriton, David "Sirpent: A high-performance internetworking approach." In Symposium proceedings on Communications architectures & protocols, pp. 158-169. 1989.
TRIAD	Cheriton, David, and Mark Gritter. "TRIAD: A new next-generation Internet architecture." (2000). citeseerx.ist.psu.edu

About the Author

Kevin Kohler is a Senior Researcher in the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zürich. His research interests include the long-term trajectory and politics of digital technologies, strategic foresight, and the use of information and communication technologies in disaster risk management.

…

CSS
ETH Zürich

The **Center for Security Studies (CSS)** at ETH Zürich is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.