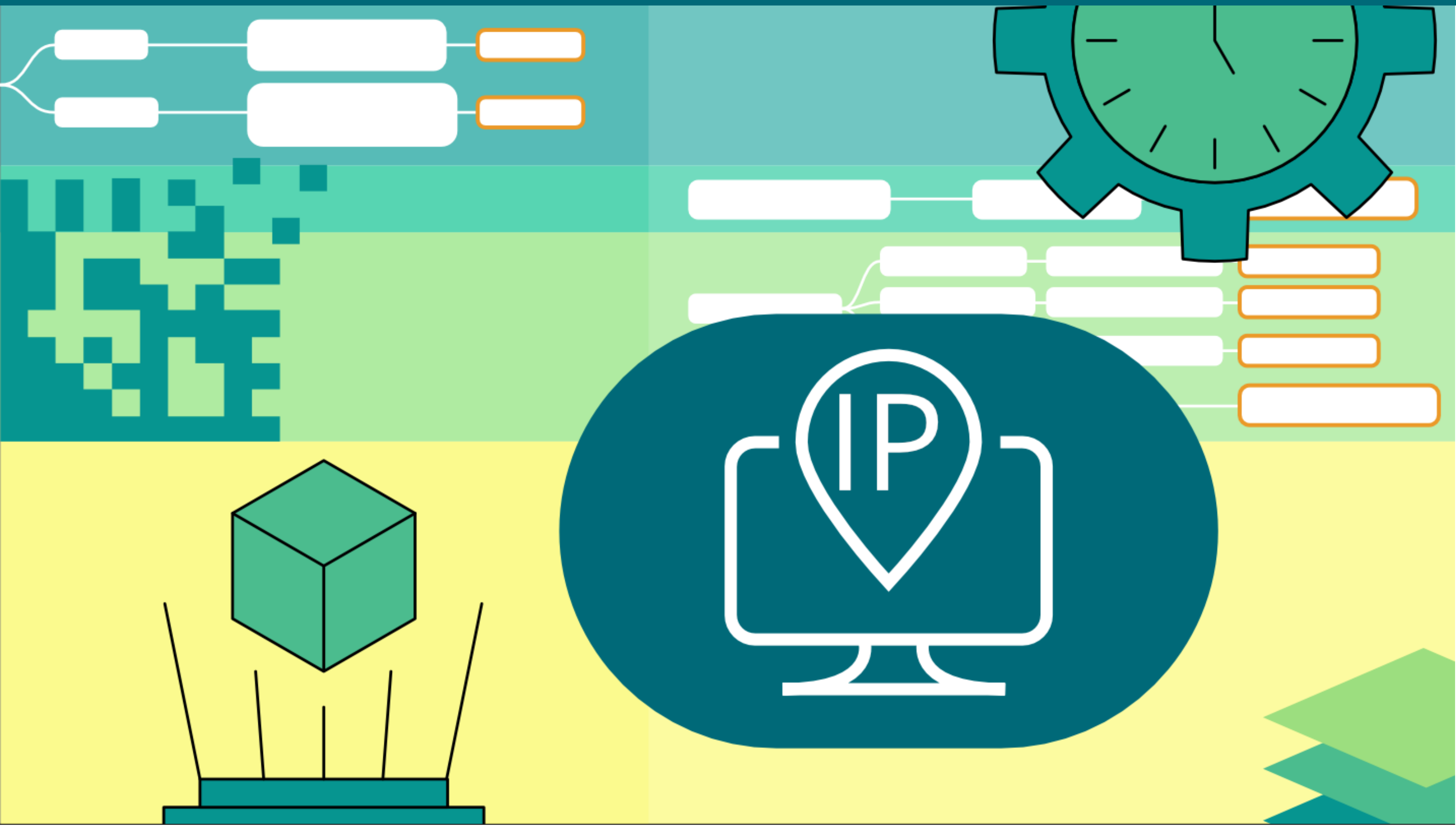
Standards: the new frontier for the free and open Internet

Introducing a taxonomy for New IP



DNS Research Federation DNSRF.org

About the DNS Research Federation

The DNS Research Federation is a centre of excellence incubated by Oxford Information Labs and dedicated to advancing the understanding of the domain name system and its connections with cybersecurity, Internet policy, emerging technology and digital standards.

About this document

This paper is a companion piece to a roundtable held in London on 7 September 2022.

Authors: Carolina Caeiro, Mark McFadden, Emily Taylor

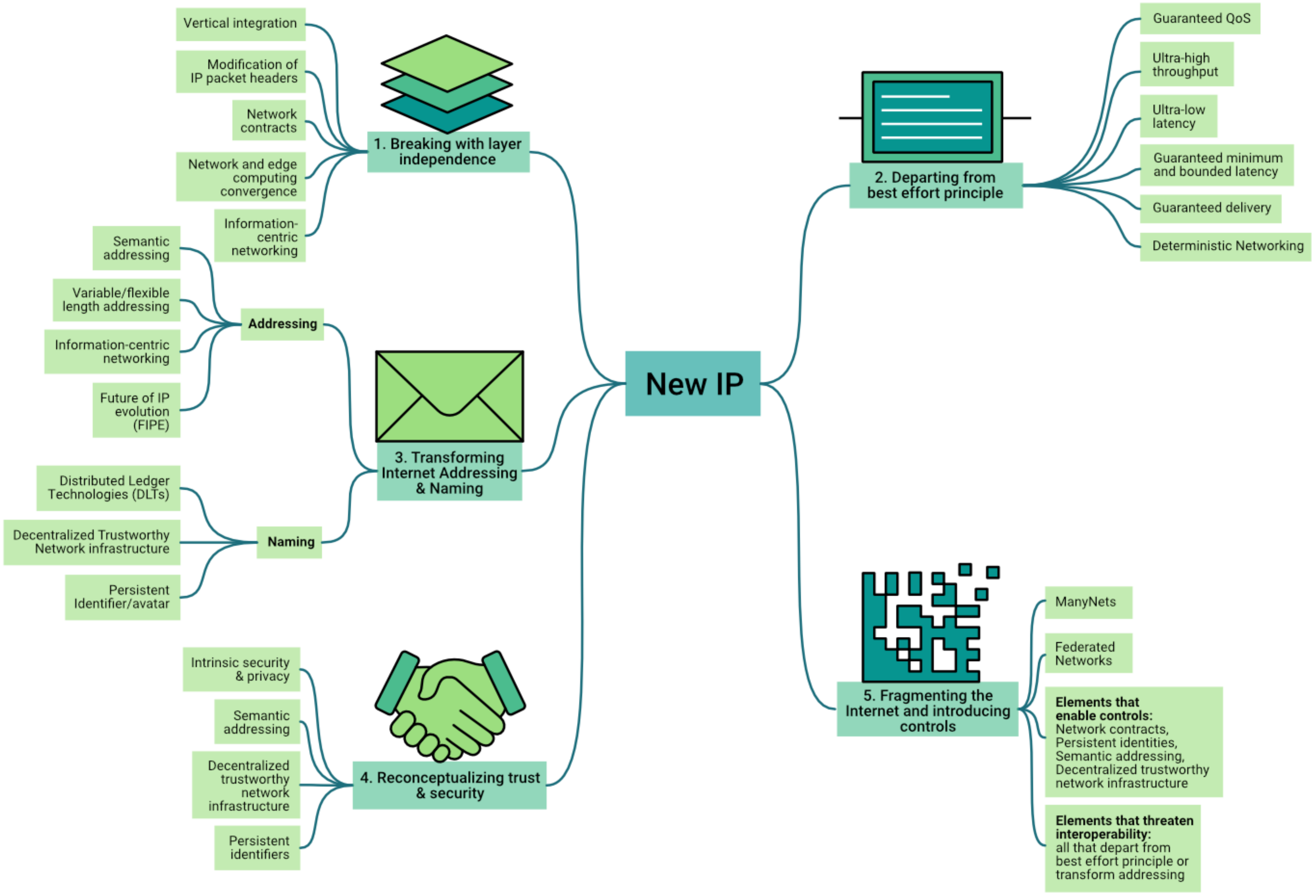
Carolina Caeiro is Senior Policy and Governance Specialist at Oxford Information Labs and Queen Elizabeth II Leadership Academy Associate at Chatham House. She specialises in Internet policy with a focus on the role of the technical community in the governance landscape and regional perspectives from the Global South. Prior to joining OXIL, she worked for the Internet and media industry including the Regional Internet Registry for Latin America and the Caribbean (LACNIC) where she spearheaded regional initiatives to promote internet security, stability and access in Latin America and the Caribbean. She co-authored the book chapter "Technical Standards and Human Rights: The Case of New IP" in the forthcoming volume Human Rights in a Changing World by Chatham House and Brookings Institution Press.

Mark McFadden is the Principal Consultant on Internet Infrastructure and Governance for internet policy advisors, llc. He works on projects related to Internet infrastructure and security for Fortune 500 companies, government and standards organizations. Mark is a Distinguished Associate of Oxil Information Labs and a regular collaborator on projects related to the core of the current and future Internet. Previously he was the Director for Internet Governance, Infrastructure and Cybersecurity at InterConnect Communications in the United Kingdom. Since 2012, Mark has been a member of the UK delegation to the ITU's Study Groups on Security and Future Networks and has been the UK lead on Cloud Computing Security.

Emily Taylor is CEO of Oxford Information Labs and a founder of the DNS Research Federation. A lawyer by training, Emily has worked in Internet policy for more than 20 years. Emily is an associate fellow at Chatham House and editor of the Journal of Cyber Policy; a research associate at the Oxford Internet Institute and an affiliate professor at the Dirpolis Institute, Sant'Anna School of Advanced Studies, Pisa. Emily has written on geopolitics, standards and emerging technologies and is a regular commentator on cybersecurity for news and broadcast media. Emily is a graduate of Cambridge University, and has an MBA from Open University. Twitter @etaylaw

DNS Research Federation
Lincoln House
4 Pony Road
Oxford
OX4 2EZ

www.dnsrf.org



New IP

1. Breaking with layer independence

- Vertical integration
- Modification of IP packet headers
- Network contracts
- Network and edge computing convergence
- Information-centric networking

2. Departing from best effort principle

- Guaranteed QoS
- Ultra-high throughput
- Ultra-low latency
- Guaranteed minimum and bounded latency
- Guaranteed delivery
- Deterministic Networking

3. Transforming Internet Addressing & Naming

Addressing

- Semantic addressing
- Variable/flexible length addressing
- Information-centric networking
- Future of IP evolution (FIPE)

Naming

- Distributed Ledger Technologies (DLTs)
- Decentralized Trustworthy Network infrastructure
- Persistent Identifier/avatar

4. Reconceptualizing trust & security

- Intrinsic security & privacy
- Semantic addressing
- Decentralized trustworthy network infrastructure
- Persistent identifiers

5. Fragmenting the Internet and introducing controls

- ManyNets
- Federated Networks
- **Elements that enable controls:** Network contracts, Persistent identities, Semantic addressing, Decentralized trustworthy network infrastructure
- **Elements that threaten interoperability:** all that depart from best effort principle or transform addressing

Contents

1 Executive Summary

The term ‘New IP’ originally described a set of proposals put forward by Chinese proponents in 2018-2020 that would have created the technical underpinnings for an alternative internet. Those original proposals were rejected, leading many to assume that New IP had gone away – it hasn’t. The original New IP proposals have been rebranded, broken into smaller parts, and re-presented across numerous standards organisations. Even as recently as July 2022, New IP-inspired proposals were being submitted at ITU study group 13 and the IETF.

As well as posing risks to the continued viability of a single, global Internet, implementing New IP proposals would also threaten human rights and create unpredictable consequences for cybersecurity, for economies and societies.

The ever-changing strategy to standardize New IP makes it extremely challenging to track. This paper aims to assist policy makers and standards attendees in tracking New IP proposals in three ways:

- An explanation on how New IP would undermine essential elements of the Internet,
- A taxonomy for New IP, and
- A toolkit to enable standards watchers to critically evaluate New IP or indeed any proposal to create new Internet standards.

New IP undermines the principles and protocols that make the Internet the Internet. These principles been identified by the Internet Society and Regional Internet Registries and others as factors that have underpinned the Internet’s success as a global communications network. These are: the principle of **layer independence**, the **best effort principle**, the system of **global identifiers (domain names and IP addresses)** and a common transport protocol, the **absence of centralised control**, and the Internet’s status as a **network of networks**.

The Internet, in the last 50 years, has evolved to meet new needs and deliver new services. In some cases, that evolution has required implementing services and protocols that do not seem consistent with those defining principles described above. But New IP proposals are different. Instead of proposing an occasional adaptation of principles, it mandates an entire overhaul of the way networking works on the Internet (revolution over evolution). Transformations would enable new forms to control and fragment the Internet both from a user and architectural design perspective. New IP breaks those key aspects – threatening the future interoperability of the Internet as a global network, and creating direct risks to human rights and multistakeholder Internet governance.

There is a lot at stake, and this makes it important to be able to identify New IP proposals, and track them. This paper proposed a five-stage taxonomy, which highlights ways in which New IP undermines those defining Internet principles and uses seemingly favourable terminology to garner support. These are:

- **Breaking with layer independence**, by proposing the vertical integration of Internet layers and introducing cross-layer intelligence sharing. This would happen primarily through the modification of packet headers in the network layer that would carry greater information about the content and identity of users, enabling new forms of control.
- **Departing from the best effort principle**, to allegedly deliver greater quality of service, which would in practice generate new protocol complexity and hinder interoperability and connectivity.

- **Transforming Internet naming and addressing**, through the remodelling of unique identifiers and application of blockchain in ways that would introduce online tracing and permanent identifiers.
- **Reconceptualizing trust and security** by baking into the network intrinsic ways to verify users identity and sources of information online.
- **Fragmenting the Internet and introducing controls**, by putting forth a vision for a splintered Internet made up heterogenous networks with different sets of identifiers and address-user binding that would enable the tracing of individuals and their browsing habits.

For each of the taxonomy levels, the paper gives examples of use cases that are being used to justify making fundamental changes to the Internet's architecture through New IP. These can be summarized as:

- **Industrial applications and supply chain management,** such as industrial IoT with Cloudification, industrial control systems, network and computing convergence
- **Real time applications and holography,** such as audio / video streaming and virtual reality, holographic type communications including the Metaverse, digital twins, and tactile Internet for remote participation
- **Network efficiency,** such as intelligent operation network, space terrestrial integrated network, and fixed networks in 5G and 6G.

There is no doubt that the use cases do reflect real challenges, but New IP is not the answer. Groups within IETF, IEEE, 3GPP or W3C are actively working on solutions in ways that remain interoperable with today's Internet. This is the preferred approach – for standards to both support emerging technologies, and retain interoperability. Evolution rather than revolution.

While technical experts clearly have a leading role to play in the evolution of future digital standards, the best technical solution does not always win in standards wars. New IP is not simply a collection of technical proposals, but is politically and ideologically backed, supported with significant human resources. Currently, industry-led standards organisations are poorly adapted to handle the politicization and geopolitical contention. The solution cannot be to pretend the problem doesn't exist.

The loss of interoperability implied by the New IP proposals would fragment the global Internet, and requires vigilance on the part of those who value a single, interoperable, open network that supports the free flow of information and supports democratic values.

This paper aims to raise awareness of the persistence of New IP-like proposals, enable people to identify them as they change name, or are presented across different standards organisations. It also seeks to bring communities of interest together to oppose the creation of new standards that would undermine interoperability, or pose threats to the fundamental values and principles that have characterised the global Internet.

The case of New IP highlights the multi-faceted nature of standards: far from being the exclusive domain of technical experts, standards carry implications for geopolitics, societies, economies, and human rights. As new generations of emerging technologies come to be standardized, it is essential that those who support democratic values and human rights engage the right people at the right time – a far more diverse set of stakeholders than have traditionally been associated with standards development. This implies coordination across siloes, as the task is too challenging for a single stakeholder group or state to manage alone. Shared taxonomies, shared resources and new, sustained coalitions will be essential to ensure that emerging standards reflect economic interests, respect human rights and democratic values.

2 New IP – What It is and Why the Fuss?

The term 'New IP' originally described a **set of proposals for an alternative networking infrastructure**, put forward at the United Nations' International Telecommunication Union (ITU) and at a side session at the Internet Engineering Task Force (IETF) by Huawei in 2018-2020.[1] The proposals set out a vision for an alternative Internet, seeking to introduce transformations that would amount to a reinvention of the Internet's core architecture.

While the original proposals did not manage to move forward, New IP did not go away. Instead proposing broad architectural changes to the Internet, Its proponents **readjusted their strategy to introduce New IP in smaller pieces**. This is done across multiple fora, with a focus on multilateral standards development organizations (SDOs) --as opposed to in multistakeholder organizations that have historically dealt with Internet standards and protocols.

New IP proponents have made a concerted effort to **link their vision for an alternative networking model with potential use cases** -- that is, examples of requirements that would allegedly benefit from the standardization and subsequent deployment of New IP. Specifically, they claim that the current Internet has been "facing increasing challenges to support new use cases beyond connectivity"[2] and that increased digitisation will generate new network requirements which cannot be met with the current Internet Protocol. These requirements draw heavily on the work of Network 2030, a focus group set up by ITU's SG 13 to study future network architecture requirements for emerging technologies, and provided grounds to anchor the initial introduction of New IP at ITU.[3]

Originally presented as a private sector initiative, **New IP is a product of China's roadmap for the future of the internet and other emerging technologies** set out in several published documents including the Made in China 2025 strategy,[4] the Standards 2035[5] report and the Belt & Road initiative.[6] As part of the recent change in strategy, government agencies and universities have taken the lead in putting proposals forward.

New IP proposals raised concerns among the internet community and advanced democracies that support the open and free Internet, as they proposed to **break fundamental aspects** that have enabled the Internet to consolidate as a global network of networks.

The transformation envisioned under New IP poses three concrete risks which render the monitoring of proposals at standards development organizations especially crucial:

Threat to interoperability. New IP proposals seek to introduce greater network complexity that would potentially fragment the Internet's shared, ubiquitous architecture. If adopted and deployed, New IP would be 'deployed in parallel with the current Internet infrastructure, interconnecting via gateways.'[7] In other words, it is proposed to replace, or at best, run in parallel with the existing Internet.

Challenges to human rights. As well as posing risks to the continued viability of a single, global Internet, through the introduction of new network capabilities for online tracing, New IP also threatens human rights[8] and would create unpredictable complexities for an already challenging area–cybersecurity.

Transformation of standardization and internet governance. By transforming the nature of naming and addressing, and pursuing standardisation at multilateral rather than multistakeholder fora, New IP set out to transform standardization and Internet governance

China, as one of the world's largest economies, is bound to have a significant role to play in defining the shape of future technologies. New IP served as a wakeup call, reminding some of the world's most advanced democracies of the **strategic role that technical standards can play in the political, economic and social spheres.** These spheres involve industry, governments, policy makers, the academic community and NGOs. Failing to include these communities in the development of standards risks unwelcome results in each of the spheres. Complacency in addressing technical standards can even **risk undermining democratic values and human rights.**

The detail of New IP, what it would do to the existing global Internet, throws into sharp relief the extraordinary achievement of the Internet's original design, based as it is on interoperable building blocks, the use of a common transport protocol and open standards.

3 What's So Good About the Internet?

The Internet is a collection of people, nodes, networks and content. Often it is described as a cloud made up of connections between devices, but this is misleading because there are rarely direct connections over the Internet. In fact, **the Internet is completely decentralised with many nodes and combinations of direct and indirect connections between them**. Its design principles, which focused on bringing together many diverse computers and networks, led to rapid global uptake, unbounded innovation and extraordinary flexibility in the applications that use the network.

In the early days of the Internet, people used computers to construct and send requests to other computers that serviced those requests. This request and response model, over a collection of decentralised networks served the Internet very well in its early decades. **Today's Internet is far more complex**, as it connects things, services, mobile devices, cars and much more.

This section highlights **five essential Internet properties that are specifically challenged by New IP's vision** for an alternative Internet: the principle of layer independence; the best effort principle; the use of global identifiers and a common transport protocol; the absence of centralised control; and the ability to become a network of networks.

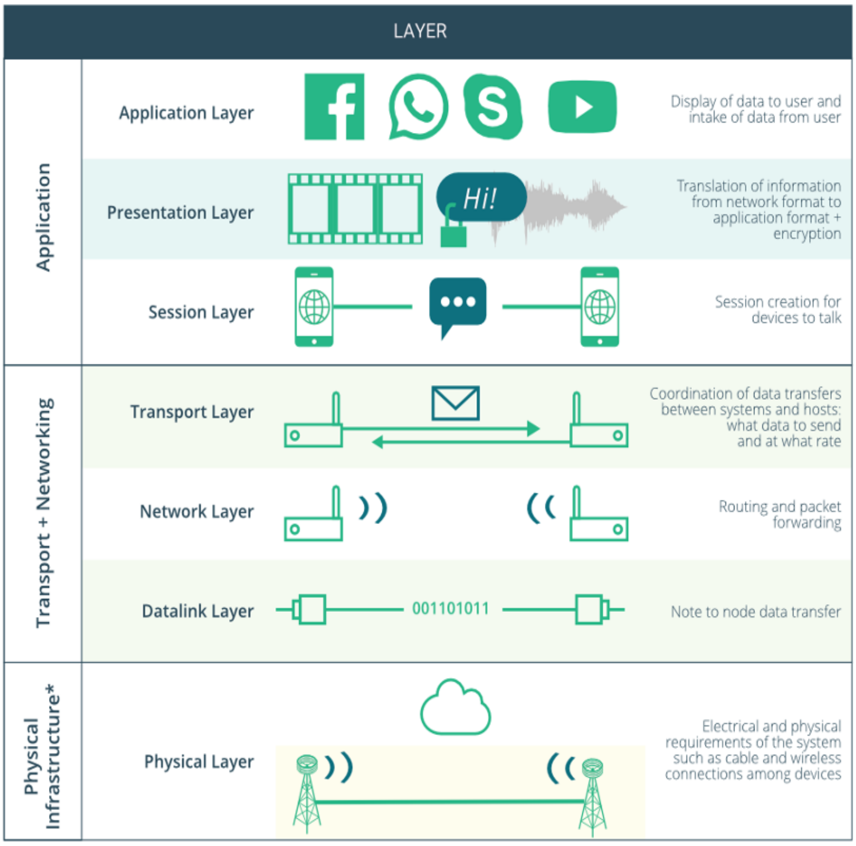

LAYER
Application
Transport + Networking
Physical Infrastructure*
Application Layer
Display of data to user and intake of data from user
Presentation Layer
Hi!
Translation of information from network format to application format + encryption
Session Layer
Session creation for devices to talk
Transport Layer
Coordination of data transfers between systems and hosts: what data to send and at what rate
Network Layer
Routing and packet forwarding
Datalink Layer
001101011
Note to node data transfer
Physical Layer
Electrical and physical requirements of the system such as cable and wireless connections among devices

Figure 1, The Internet's layers.

3.1 Principle of Layer Independence.

The Internet's original design foresaw a model where **layers operate independently and largely unaware of one another**. Layer independence allows for 'permissionless innovation,' meaning that innovation and improvements at one layer do not need the replacement or updating of other layers. As a result, innovation on a layered Internet takes place at a faster pace than traditional, integrated, networks. Often referred to as the "dumb pipes" of the Internet, the network layer is solely concerned with the transport of packets. Unlike the application layer—which is the user-facing layer dealing with content creation and consumption—**the network layer is unaware of the content it transports and has been regarded as largely apolitical**.

3.2 Best Effort Principle

Best effort networking means that, on the Internet, **the transport of packets has no guaranteed data delivery or quality of service**. When your video streaming feed becomes pixelated for a couple of seconds, that is usually due to **packet loss** - an example of the best effort principle in practice. Life goes on and generally the service adapts and corrects itself. Perhaps counterintuitively, the best effort principle has helped keep Internet infrastructure interoperable and comparatively lightweight. At its most basic level, the Internet is a **packet switching** network. Whether a communication is an email, a video, a sensor-to-sensor communication, details of a drone's flight path, a multiplayer game or an immersive environment – that communication is made up of many individual packets. **Each packet contains the bare minimum of information needed for delivery of the packet** (the "header") along with the information being communicated (the "payload").

3.3 Global Identifiers and a Common Transport Protocol

Global identifiers – primarily, domain names (for instance www.example.com) and IP addresses (for example 192.28.203.10) – **play a critical role in maintaining the unity of the Internet as a network**, enabling packets to reach their intended destination and providing the interface between the network's physical layer and the application layers. Information and services rely on the ability to transport information in packets across the Internet. The Transmission Control Protocol (TCP) is responsible for packet ordering, error checking and packet assembly. The Internet Protocol (IP) provides the addressing and packet-forming system. Together – abbreviated as TCP/IP – the protocols provide much of the glue that holds the Internet together. While the unique, global identifiers deliver consistency across the entire network –without fragmentation– **the common Internet transport protocol enables unrestricted access and has allowed the Internet to grow and adapt to new requirements**. Another fundamental principle associated to the existence of a common transport protocol is the end-to-end principle which means that "information pushed into one end of the Internet should come out the other without modification.[9]" While nowadays, the end-to-end principle has been limited by, for example, firewalls, in practice it still holds, marking a central feature of what renders the internet a global network.

3.4 No Centralised Control

There are two important features of the Internet when discussing the absence of centralised control: **decentralisation and security**. The Internet's decentralised and distributed design avoids single points of control and of failure. This principle has rendered the uniform deployment of policy or security enhancements across the network challenging.

Still, the benefits of a **decentralised network** are evident. The combination of swift and unfettered transport of packets at the core of the network, and intelligence at the edges, **have made it easy for the Internet to scale,** for new services to be deployed and for new users to join.

Internet security is another aspect where the Internet has avoided centralised controls. When building the initial versions of what has become the Internet, its creators did not consider security as a central area of concern. Instead, the Internet's design focused on keeping protocols simple, and creating a network that was decentralised and open. As time went on, and security threats became more evident, others added new features to address these challenges. Today, encryption-based technologies are the preferred strategy for securing the Internet, while avoiding centralised trust mechanisms.

3.5 Network of networks

The history and evolution of the **Internet used a model that allowed diverse networks**, using different devices for different purposes, **all to be connected**. The protocol rules that made this possible not only allowed users from remote networks to have access to local data and services, but it also allowed for computers to connect across many heterogeneous networks -- a "network of networks."

3.6 Evolution Versus Revolution

The Internet, in the last 50 years, has evolved to meet new needs and deliver new services. In some cases, that evolution has required implementing services and protocols that do not seem consistent with the defining principles described above. For example, video streaming relies on placing intelligence and information at the core of the network. New IP is different. Instead of proposing an occasional adaptation or evolution of principles, it mandates an entire overhaul of the way networking works on the Internet (revolution over evolution).

4 Where is New IP Today?

After its initial rejection at ITU and IETF, organisations continue to bring New IP proposals to standards bodies. This is part of a broader strategy to bring New IP proposals in smaller broken down pieces that are much harder to recognise.

Proponents of New IP rebranded the New IP vision as **Future IP Evolution** (FIPE). **Rebranding has been an essential strategy to reintroduce New IP** in standards-setting organisations. The FIPE proposals concentrated on use cases that justified IP addressing and forwarding transformation. These use cases include heterogeneous networking technologies, such as space-terrestrial networks, Internet of Things (IoT) networks, and industrial networks. Most notably, organisers of the FIPE side event at IETF 109, held in November 2020, claimed that the group would tackle issues that are not "better covered by other IRTF RG" and proposed the creation of a new research group on the subject and IETF[10].

4.1 Recent Proposals in the IETF

At IETF 114, held in Philadelphia in July of 2022, **the trend toward proposing standards for components of New IP** – rather than an overall architecture – continued. Proponents of New IP held informal side meetings to discuss proposals for **changes to the way addressing works** on the Internet and to discuss use cases where networks generate physical and mechanical changes to their environments.[11] In addition, **ManyNets** was raised again in the context of Internet services deployed by satellites in low Earth orbit. Proponents of this activity claimed that:

> *"due to the fast and special moving pattern of LEO satellite network, there are many challenges to the current IETF technologies, such as addressing, routing, multi-path, mobility, traffic engineering, security, etc."*[12]

Participants in the COIN research group discussed the intersection of namespaces, security and addressing. DETNET, the deterministic networking working group, discussed various proposals to support low-latency, high-reliability services in large networks. In most cases, the discussion was limited to supporting those requirements in a single provider's network.

4.2 Recent Work at the ITU-T

ITU-T has been and continues to be the favoured home for New IP proposals in 2022. Study Groups with the most critical volume of New IP-related proposals include SG13 on Future Networks, SG17 on Security and SG11 on Protocols and test specifications. Most recently, New IP is also beginning to crop up in SG16 on Multimedia, tied to Chinese's visions for the Metaverse.

Study Group 13 offers interesting insights into the latest attempts to standardise New IP. The group's July 2022 meeting saw the re-emergence of **decentralised, trustworthy network infrastructure** with proposals to initiate new work items on the subject.[13] Perhaps most importantly, SG13 has seen an increased focus on **network and edge computing convergence** and **fixed, mobile and satellite network convergence** to justify the rollout of New IP.[14] As part of these proposals, new terms are constantly introduced to describe the central tenets of New IP –in what may be interpreted as an effort to rebrand and possibly inhibit proposal tracking. For example, in the SG13 July meeting, multiple proposals introduced the concept of **information-centric networking**, which at its heart advocates for vertical integration and the merging of intelligence into the networking layer –that is, taxonomies element #1 and #2 introduced later in this report. Lastly, the introduction of New IP-related proposals has shifted from being an endeavour pushed forth by private sector companies –as was the case with Huawei when New IP was first introduced– to **becoming an effort directly**

spearheaded by Chinese ministries, state-run firms and national universities. New IP proponents continue to work through **proxies** through academic communities, networks of consultants and other supporting country delegations.

4.3 Forum Shopping and the Future

Forum shopping has also continued to feature in renewed strategies to promote New IP's alternative vision for the Internet, even venturing beyond standards setting. The China Internet Network Information Center, for instance, has filed a US patent application for decentralised blockchain DNS.[15]

In recent months academic, commercial and governmental groups in China have continued the approach of moving away from proposing broad, architectural changes to the Internet. Instead, they have continued to break New IP into component building blocks which meet specific requirements. As an example, very low latency (the speed at which information can be moved through a network) is an important goal of New IP. However, low latency is an important feature for many use cases, beyond the ones envisioned for New IP. By breaking New IP into component parts, proponents can attempt to get broader support for individual parts of the overall New IP strategy. It is likely that this strategy will continue into the near future.

5 A Taxonomy for New IP

The original New IP proposals imply a vision for an alternative Internet. To understand how this vision differs from that of today's Internet, this taxonomy identifies transformations that are **unlike the Internet** or that would deliver a non-Internet-like experience. The taxonomy classifies these proposed changes into five categories:

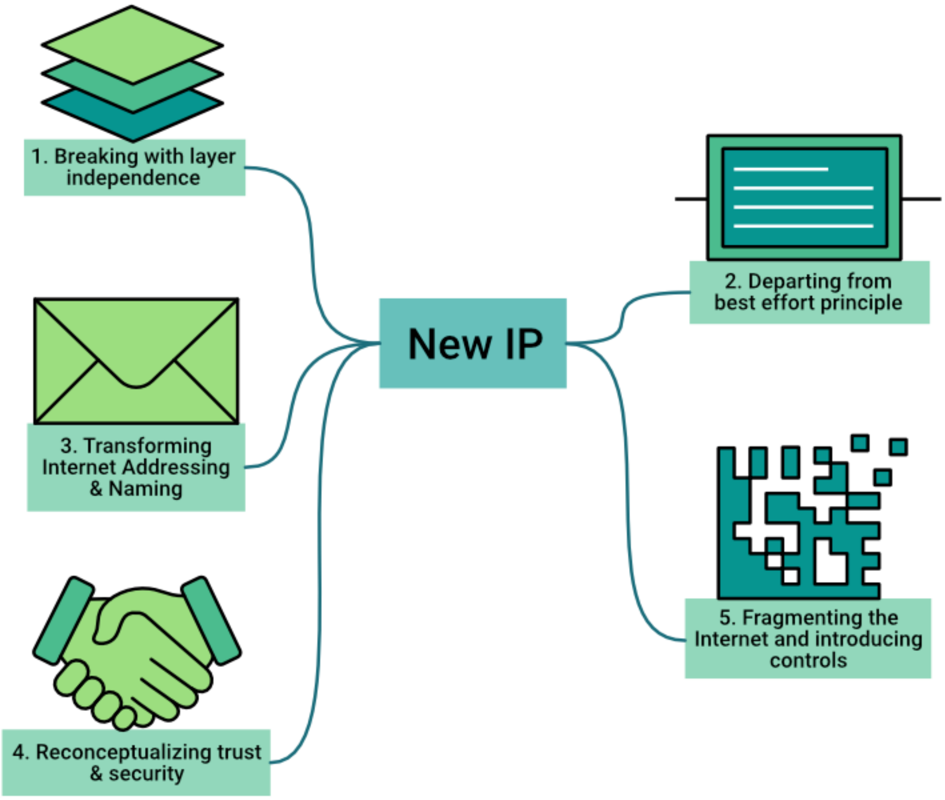

1. Breaking with layer independence
2. Departing from best effort principle
New IP
3. Transforming Internet Addressing & Naming
4. Reconceptualizing trust & security
5. Fragmenting the Internet and introducing controls

Figure 2, A taxonomy for New IP

5.1 Taxonomy element #1: Breaking with layer independence

A first feature of New IP proposals is the notion of **vertical layer integration**, which proposes to do away with the principle of layer independence.

Justifications to advance vertical integration leverage network needs of **vertical industries** as a central use case. Vertical industries are described as those that require integrated information sharing across the network, the ability to communicate among heterogeneous networks and that are likely to need high-precision networking. Breaking with layer independence is also invoked as benefit for **supply chain integration networks**, another industrial use case for New IP. The vertical integration model of New IP allows for information to be integrated along the networking process, therefore generating enhanced opportunities for control and management of supply-chain networks.

5.1.1 What is it?

Under New IP, the **network layer is the most severely transformed**. Intelligence would be moved from the application layer – such as information pertaining to content or the identity of users– down to the network level or even below.[16] Vertical integration and Intelligence sharing can also happen the other way round, with the lower transport layers signalling information back to the application layer.

The primary way in which vertical integration is delivered under New IP is through the **modification of IP Packet headers**.[17] Under this alternative networking model, IP headers would be modified to also include a description of the contents and information about users.[18] Revealing this amount of information at the network layer would turn this previously apolitical layer into a new proxy for control.

The **introduction of network contracts** is another way through which vertical integration is put forth under New IP. A contract is a specification of what the packet expects from the network, such as guaranteed delivery, a specific packet discard rate or network delay guarantees. This concept is closely associated with that of active networks, where end-user applications can embed code within packets to be executed by routers and switches. The use of contracts could lend itself to abuse. Failing to meet requirements may result in the packet not being accepted or transported by the network. This would break another fundamental principle in Internet networking, the end-to-end principle, by which information pushed into one end of the network, should come out the other end unaffected.[19]

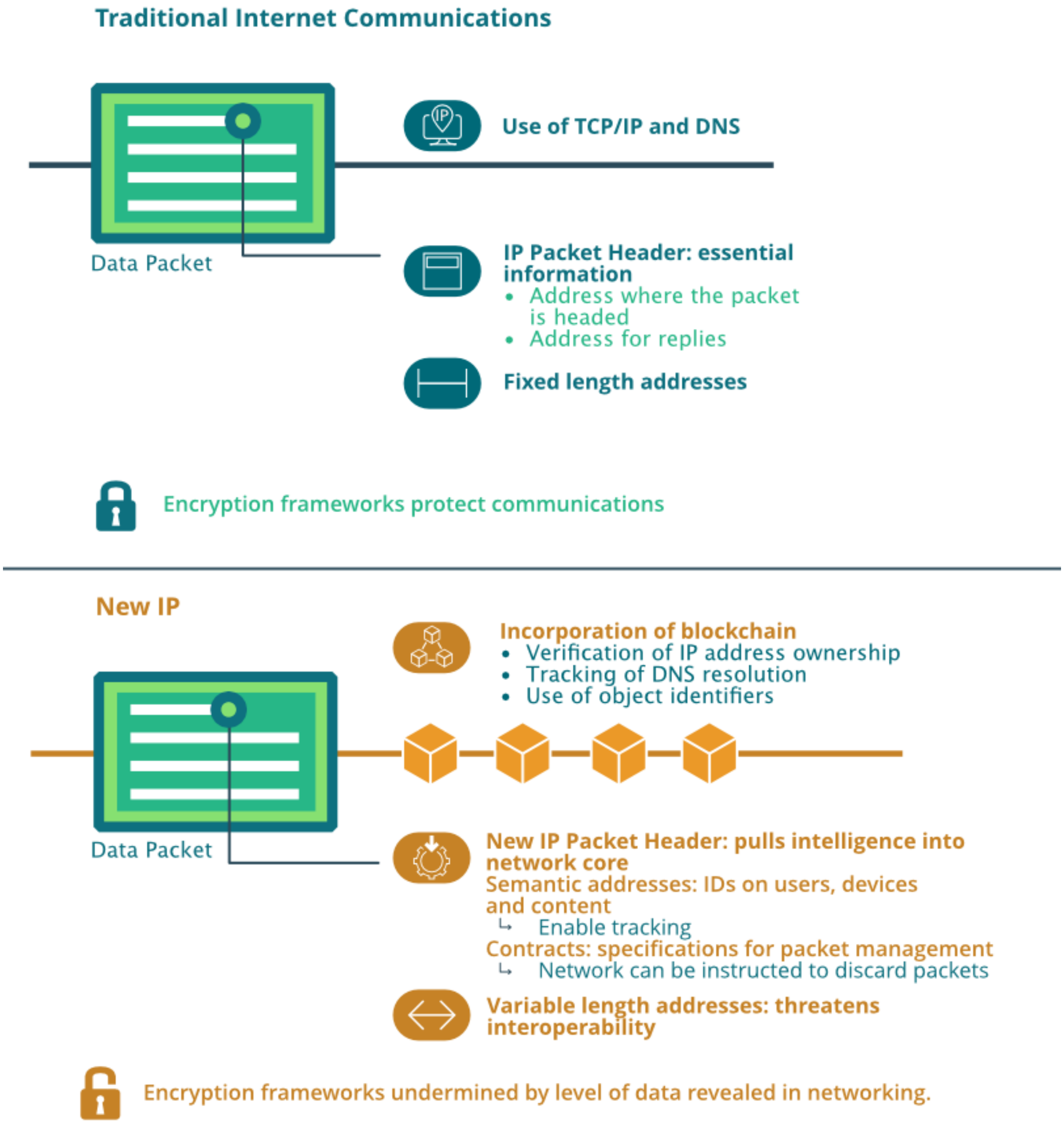

Traditional Internet Communications
Use of TCP/IP and DNS
Data Packet
IP Packet Header: essential information
• Address where the packet is headed
• Address for replies
Fixed length addresses
Encryption frameworks protect communications
New IP
Incorporation of blockchain
• Verification of IP address ownership
• Tracking of DNS resolution
• Use of object identifiers
Data Packet
New IP Packet Header: pulls intelligence into network core
Semantic addresses: IDs on users, devices and content
↳ Enable tracking
Contracts: specifications for packet management
↳ Network can be instructed to discard packets
Variable length addresses: threatens interoperability
Encryption frameworks undermined by level of data revealed in networking.

Figure 3, Transformation of packets under New IP

5.1.2 Why does it matter?

If visions for an alternative networking infrastructure were to be realised, having an intelligent network layer would severely **affect how information on users and content is handled online**.

Infrastructure providers that supply networking equipment, and **Internet Service Providers** (ISPs) that provide access to the networks, **would become key players in handling the political aspects of Internet policy**. In China, and in several nations across the Global South, ISPs are state-owned or licensed and regulated by the state. Hence, vertical integration would place such controls in the hands of the government.

The introduction of network contracts would be especially concerning, as these could be used to control or prevent the connection of specific devices, individuals, or content to the network.

While some of the proposed features that address vertical integration are acceptable in private networks, New IP seeks to expand these requirements to the whole of the Internet. Proposed use cases associated with vertical integration would drive dramatic changes to fundamental protocols; and it would introduce protocol complexity that would threaten both performance and interoperability. These are discussed in detail in the descriptions of elements 2 and 3 below.

5.2 Taxonomy element #2 - Departure from best effort principle

A second feature of New IP is the proposal to move away from the best effort principle.

Justifications to depart from the best effort principle draw primarily on use cases associated with **real-time applications** that require transmission to be as immediate as possible. Most common examples include video games, augmented and virtual reality, as well as holographic communications. Industrial cases associated with **high-precision equipment**—such as robotic arms and manufacturing equipment—are also cited as requiring highly precise packet delivery and network performance. **Network improvements** for 5G and 6G networks, as well as integrated networks that combine low-orbit satellites and on-earth infrastructure, are also cited as purported use cases to justify departure from the best effort principle.

5.2.1 What is it?

New IP's vision for an alternative Internet places great focus on **quality of service**, challenging the Internet's existing best effort principle. New-IP related proposals associated with this taxonomy element claim the ability to deliver **ultra-high throughput** and **ultra-low latency**. Throughput refers to the number of packets or information that can be processed in a specific period of time, while latency is the time it takes for a packet to travel from source to destination.[20]

5.2.2 Why does it matter?

Proposals to adopt better than best effort networking risks driving dramatic changes to fundamental protocols and expanding specialised requirements to the apply across the Internet's architecture as whole. Such transformation would introduce **new protocol complexity.**

Keeping standards lightweight and interoperable has allowed the Internet to gain scale and remain resilient. While better than best-effort-networking is a reasonable requirement for special purpose networks, what appears to set New IP proposals apart from other ongoing efforts to work on deterministic networking, latency requirements and improve QoS, is the **intent to enable these features to operate over the Internet by default**.[21] This is driven by New IP's proposed use cases for which it is claimed the required performance improvements could not be properly supported by the Internet's current suite of protocols.

Introducing greater protocol complexity by default could severely affect the proper functioning of the Internet globally.[22] From the information available, it is unclear how some of the proposed solutions could achieve scalability, hinting at a general disregard among New IP proponents for protecting and ensuring interoperability and connectivity.

5.2.3 Example Uses

Proponents claim that future networks will demand that there are upper bounds to how long it takes a packet to be delivered from source to destination and suggest that **guaranteed delivery** will become a must. Performance improvements above best-effort are also associated with the notion of **deterministic networking**. While traditional packet-switched networking (non-deterministic networks) are more likely to experience variable degrees packet loss, latency issues and jitter, deterministic networking seeks to provide network services of higher reliability and predictability for specific applications, such as high-speed trains and drones.[23] New IP networks, purportedly, intend to offer full-scale deterministic networking, using bounded latency and delivering near zero packet loss.

Whether and how the proposed changes envisioned by New IP would truly be able to deliver these performance improvements is uncertain.

5.3 Taxonomy element #3 - Transformation of Internet addressing and naming

A third feature of the New IP proposals is the introduction of radical reforms in Internet addressing and naming.

Purported use cases include for transforming addressing include those associated with **network efficiency improvements**, particularly in the context of network and computing convergence, and networks that integrate low earth orbit (LEO) satellites and on-earth Internet infrastructure. Changes to addressing and naming that introduce permanent identifiers and online tracking feature in association to use cases related to **real time applications, holography and the metaverse**, where persistent identifiers are linked to the introduction of avatars or digital. These permanent IDs are also presented as a **security feature** in association to both real-time applications and industrial use cases for New IP.

5.3.1 Transformation of Addressing

5.3.1.1 What is it?

New IP, as the name indicates, challenges the adequacy of the existing IP and proposes the adoption of a **hierarchical system** based on variable length and semantic addressing[24] to achieve greater network efficiency.

Variable length addressing is the idea that IP addresses should adopt a flexible length, as opposed to having a fixed length – like IPv4 and IPv6 do. Network and computing convergence is the flagship use case where flexible addressing is presented as a requirement to address local computing needs and optimise network resources. New IP proponents argue that the overhead associated with the use of fixed addresses is not suitable for networks which have limited resources (for example, sensors in IoT). It is unclear, however, how or whether using variable length addressing solves the questions of overhead, interoperability or connectivity.

New IP packet headers can reportedly **carry different address families** – using either an IPv4, IPv6 or variable length address.[25] However, requiring complex translators between different protocols hinders interoperability, and generates potential security, quality of service, and resiliency issues.[26]

In **semantic addressing**, the order of certain bits in a network address are assigned a semantic meaning.[27] In New IP presentations, semantic addresses are presented as IDs: resource ID, service ID, content ID, device ID, and so forth.[28] Using IP addresses to map out Internet services and resources is not new,[29] and it is also unclear how New IP's IDs would provide added-value in doing so.[30]

Overall, hierarchical models for IP address allocation have been often considered by the Internet community across SDOs, and the current IP addressing model has always been favoured over other alternative approaches.

5.3.1.2 Why does it matter?

The introduction of variable length addressing would **threaten Internet interoperability**, the property that allows different machines and devices to talk to one another, as long as they use the same open protocols such as TCP/IP.[31] New IP's proposal to carry multiple address families would render the core of the network more complex, generating new security vulnerabilities and increasing chances of malfunctioning. Transforming fundamental protocols in ways that threaten interoperability is disproportionate to any value gained by adding new functions to the IP layer.

The incorporation of identifiers through semantic addressing could **enable new forms of control**. In today's Internet, the IP address indicates not just "what" is connected but "where" it is connected. **New IP wants to add information "about" what is connected.** This is dangerous because exposing information "about" what is connected, allows those who control the networks to make policy decisions about what a connected device can do and what information it can receive. Similarly, networks could be instructed to shut off specific devices, users, or even content. While the use of identifiers to express information about devices, content and services is a reasonable means to address specific network needs, adopting it as a default standard for the entire Internet is likely to lend itself to abuse.

Lastly, transforming addressing would also **threaten the existing governance model** for number resources on the Internet, effectively challenging the community-led work of the world's five regional Internet registries and IANA.

5.3.2 Transformation of Naming, the Domain Name System

5.3.2.1 What is it?

The vision put forward through the New IP proposals for an alternative Internet proposes to transform the Domain Name System (DNS) through the use of **distributed ledger technologies (DLTs)** --also known for their most common application, blockchain.

Two arguments are used to justify the incorporation of blockchain into the DNS. First, New IP leveraged legitimate concerns that the DNS has become increasingly centralised to call for a renewed form of **decentralisation**.[32] While concentration is a valid concern, the DNS system is already a distributed service and has largely proven to be resilient to attacks.

Second, the incorporation of blockchain into the DNS is presented as a **security feature to enhance trust**. The perceived centralisation of the DNS is cited as the source of current system vulnerabilities like DDoS attacks. New IP claims to solve DNS security issues by using blockchain for the verification of IP address ownership and tracking of DNS resolution which, in practice, would introduce unparalleled tracing over the Internet.[33]

5.3.2.2 Why does it matter?

Applying blockchain to the DNS as proposed under New IP would transform the Internet's architecture and **introduce new forms of traceability and control**. Its deployment would normalise packet inspection and the generation of data logs on users and online activity. In addition, features such as persistent identifiers could further reinforce the erosion of anonymity online and have important **privacy and security implications**. Despite claims of decentralisation, those controlling forwarding and access to the network could block particular data flows –this might include governments if ISPs are state-controlled or blockchain is publicly managed. These controls could enable governments to block specific users or content, and introduce micro-targeted shutdowns to replace the unpopular, complete network shutdowns that are commonplace today.

Transforming the DNS through blockchain would potentially **undermine the governance models** of current Internet identifiers. By placing decision-making in the hands of those who control the blockchain, multi-stakeholder organisations such as ICANN (Internet Corporation for Assigned Names and Numbers) would see their influence curtailed at best, eliminated at worst.

Lastly, embedding blockchain into the Internet architecture is also far from a proven concept. Applying the technology would create a more heavyweight core and **challenge interoperability,** including issues spanning from higher energy use --and therefore climate impact-- to the very performance challenges that New IP claims to solve, such as maintaining low latency.

5.3.2.3 Example Uses

New IP's vision for a transformed DNS has primarily been introduced in standards proposals as **'Decentralised Trustworthy Network Infrastructure.'** Described as a decentralised management scheme for network resources, this type of networks would be designed to determine whether applications –and by extension, devices, users and content — are deemed acceptable and trustworthy enough to access the network.

New IP visions to transform the DNS also seek to introduce **persistent identifiers**. These are naming systems that provide a way to associate an identifier with any object, concept or "thing." Persistent identifiers and avatars are emerging as important features in Chinese proposals for standardisation of the metaverse.

Primary use cases include industrial networks and real-time applications where blockchain can be used to establish trust and assign permanent identifiers to digital and physical objects.

5.4 Taxonomy element #4 - The reconceptualisation of trust and security

A fourth feature of the New IP proposals is the reconceptualization of trust and security. Having trust turned into intrinsic network is presented as a benefit for use cases related to **Industrial networks and real-time applications** explored under sections 5.3.

5.4.1 What is it?

New IP proposes to reconceptualise how trust and security are dealt with for the Internet. The argument put forth is that existing security and trust mechanisms based on encryption –such as public key infrastructure or the use of Certificate Authorities– are ineffective.

New IP's reliance on blockchain and proposed transformation of Internet identifiers seek to **shift away from Western notions of security that focus on encrypted communications**. As an alternative, **New IP proposes to build trust directly into the network**, in what has been described as 'intrinsic' trust and privacy. [34] While this may appear to be a reasonable solution, in practice, it would lead to the creation of immutable data logs on users' online activity and normalise packet inspection. Either or both could easily lead to surveillance and censorship.

5.4.2 Why does it matter?

The alternative Internet envisioned by New IP seeks to merge the data link and network layers into a new "blockchain" layer. **Network operators would be able to exercise more control over flows of data traffic.** This control could be subject to government intervention, such as through a national authority asserting direct control over data traffic.

Having security and trust be “intrinsic” to the network will require core layers to carry metadata about the users, applications and services being transported. If users need to register in order to have packets sent to their destination, the result is that **network operators, and those who license the operators, can remove individual users’ access at any time**.

New IP’s security model is inspired by the STRIDE framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege)[35]. The New IP approach to repudiation stresses that the source of specific attacks can be traced back to their origin. By making the data “trusted,” the model incorporates information that goes beyond identifying sources of attack. Instead, New IP makes **policy and connectivity decisions based on data about the user, source, device, and other metadata** –as opposed to basing such decisions on the performance or operation of the network. This enables forms of social control over who has access to what and would undermine the user’s privacy that New IP claims to reinforce.

New IP suggests that there is a need for protocol layers that provide complete protection from spoofing and denial of service attacks, solving these problems from the ground up. However, there are many existing, well-established and commercially implemented solutions for these issues running on the current Internet. In addition, building robust or mandatory authentication into the networking process would likely make it more difficult for users to connect and use the Internet.

5.5 Taxonomy element #5 - Fragmenting the Internet and introducing controls

A fifth feature of New IP is fragmentation and the introduction of controls.

New IP’s vision for an alternative networking model would inherently splinter, if not entirely replace, the existing Internet. As a means to justify the radical transformation of internet way of networking, New IP proposals argue that the Internet is unfit to connect **heterogenous networks**, pointing to a range of industrial use cases as well as space-terrestrial or IoT networks. The introduction of network capabilities for online tracing will also contribute to fragment the Internet and introduce controls. The adoption of these features is justified to allegedly **guarantee trust and facilitate persistent identifications** particularly in industrial, real time and holographic use cases.

5.5.1 What is it?

Several elements of the New IP threaten interoperability, but the vision for a normalised fragmentation is best crystallised in the concept of *ManyNets*.[36] **Manynets** refers to the idea that future networks will need to connect heterogeneous network infrastructures,[37] ‘potentially using different sets of unique identifiers and addresses.’ [38] The concept **seeks to normalise the emergence of a fragmented Internet composed of islands of communication.** New IP proponents claim that the capacity for flexible length addresses to hold different address families would ensure interoperability. However, an analysis of available specifications by ICANN’s Office of the CTO concludes that **New IP’s ability “to carry IPv4, IPv6, or mix and match types, does not guarantee interoperability**.”[39]

Beyond this level of fragmentation, what is concerning is the vision for how these communication islands, or **‘federated networks’**, as they are also referred to in New IP documentation, would operate. New IP proposes to have this set of diverse federated networks rely on **permanently binding addresses with users’ identities**. As explained by ICANN’s analysis, this means that:

> *"any intermediary system on the Internet could have access to anyone's real identity and browsing habits simply by observing the New IP addresses of their traffic as it passes through intermediary networks."*[40]

This binding appears to run contrary to New IP's claims to protect privacy and could easily open the door for surveillance and censorship.

5.5.2 Why does it matter?

The emergence of an alternative networking model that enables the introduction of systematised controls would **fragment the Internet by generating a radically different experience for its users.**

Fragmentation would also manifest at the very level of networking infrastructure, through the introduction of greater network complexity that would challenge interoperability. New IP's proposed transformations to Internet addressing will mean that not all networks will be able to communicate among themselves. That would lead to a situation where there were **islands of connectivity rather than the Internet's network of networks.**

To solve that challenge, New IP proposes that gateways between the islands be introduced to "translate" the local network flows into ones that could traverse remote networks. However, gateways introduce delay and new faults into a network, and generate administrative, business and legal hurdles that are likely to hinder interconnection.

6 The Problems New IP Claims to Solve and How are Others Solving them

Technical standards development usually starts with use cases– descriptions of new requirements, services and applications. The New IP taxonomy described use cases that New IP claims to solve. These can be summarized as following into three main categories, illustrated with accompanying examples that have featured in New IP-related proposals:

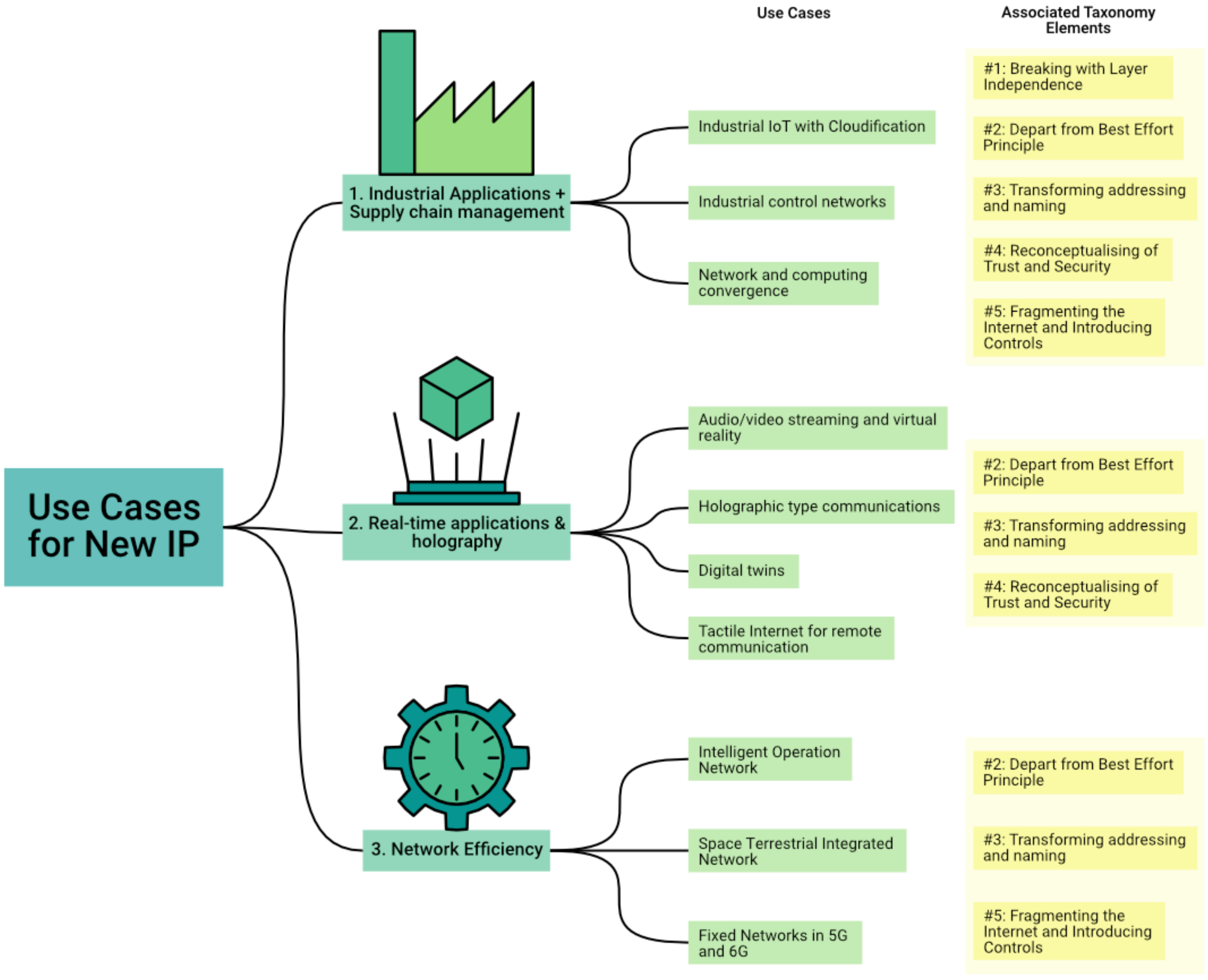

Use Cases
Associated Taxonomy Elements
Use Cases for New IP
1. Industrial Applications + Supply chain management
Industrial IoT with Cloudification
Industrial control networks
Network and computing convergence
#1: Breaking with Layer Independence
#2: Depart from Best Effort Principle
#3: Transforming addressing and naming
#4: Reconceptualising of Trust and Security
#5: Fragmenting the Internet and Introducing Controls
2. Real-time applications & holography
Audio/video streaming and virtual reality
Holographic type communications
Digital twins
Tactile Internet for remote communication
#2: Depart from Best Effort Principle
#3: Transforming addressing and naming
#4: Reconceptualising of Trust and Security
3. Network Efficiency
Intelligent Operation Network
Space Terrestrial Integrated Network
Fixed Networks in 5G and 6G
#2: Depart from Best Effort Principle
#3: Transforming addressing and naming
#5: Fragmenting the Internet and Introducing Controls

Figure 4, New IP use cases

Several of the requirements that New IP proposals claim to solve are currently under consideration across multiple SDOs. This is important because those SDOs often have the expertise and experience to directly address the evolution of protocols for new uses. It is important to have the conversation about protocol development in the organizations that have the background and capability to do the work and where a variety of stakeholders can provide input to the process.

Aspects related to **improving network's security and performance** –from increasing throughput, reducing latency or providing guaranteed delivery– are being actively worked on across IETF, IEEE, 3GPP, ETSI and W3C.

While TCP is the most widely used transport protocol, **the current Internet uses other protocols in the layered model to deliver performance improvements,** such as ensuring that information successfully moves from one place to another.[41] The IETF, for example, has developed the real-time transport protocol (RTP) which is used for multimedia applications. There is ongoing work to improve RTP at IETF in collaboration with W3C.[42] The User Datagram Protocol (UDP)-based QUIC Protocol has also focused on delivering performance improvements and is another example of a transport protocol that is seeking to tackle these issues while becoming widely deployed. Additionally, the **IETF has a dedicated Transport area** (tsv) focused on transport protocols. Ensuring interoperability is a key goal of tsv, in contrast to proposing alternative infrastructures like New IP that may fragment the Internet.[43] The work of IETF's tsv area includes low latency, low loss, scalable throughput (L4S) Internet service and active queue management.

Beyond work on transport architecture, there is **extensive work on deterministic networking**.[44] New IP networks, purportedly, will offer full-scale deterministic networking. There are several groups within SDOs working to deliver options for networks with specific quality of service requirements; however, these do not propose to replace the entire Internet architecture or apply deterministic networking principles to all networks across the Internet.

Similar developments are observed in connection to the need to evolve Internet addressing. SDOs have developed **complementary mechanisms to deal with invariable address length without transforming the IP layer stack**. For example, the IEEE has developed what is known as Media Access Control (MAC) addresses which are commonly used for ethernet, Bluetooth and Wi-Fi technologies; these MAC addresses can vary in length and integrate identifiers in lower-levels of the stack without modifying the IP layer and forwarding systems.[45] Likewise, **IETF is considering proposals related to semantic addressing** such as segment routing without seeking to embed this feature across the entire public Internet.[46]

7 A Framework for Evaluating New Standards Proposals

Evaluating standards proposals is a complex task. This section offers some guidelines to facilitate the work of practitioners on the ground engaging in the evaluation of Internet-related standards.

Proposals that contain New IP taxonomy elements pose potential risks to the open, free Internet. Beyond searching for those elements in standards proposals, practitioners evaluating standards proposals may consider the following steps.

7.1 Does a proposal meet best practice principles for Internet standards making?

Assessing proposals for standardisation should be done against a background of common principles for standardisation. There are a variety of sources for best practice principles for protocol development. These include the NCSC protocol design principles[47], the Internet Society's 'critical properties of the Internet[48]', and APNIC/LACNIC's 'Internet Success Factors[49].' Using those sources, this report identifies **four guiding principles**. These cover the standardisation process (openness, multi-stakeholder model) and essential qualities for any outputs that emerge from that process (general purpose and interoperability).

7.1.1 Four Essential Principles

Principles for the standards **process**:

- **Openness:** *Standards should be open and made available to the general public.*
- **Multi-stakeholder process**: *Any new protocol development be industry-led, inclusive and enable diverse participation.*

Principles for standards outputs:

- **General purpose:** *standards should be general purpose, scalable and have multiple implementations to avoid single points of failure.*

- **Interoperability.** *A proposed standard should ensure interoperability and mechanisms of coexistence that render the Internet flexible to different types of underlying networks and adaptable to new applications*.

7.2 Do existing standards and protocols satisfy the use case?

An essential question for any new standards proposal is: "Can existing technology, and the protocols that support those technologies, already address this need?". In other words, the approach is one of evolution rather than revolution - confining changes to fundamental protocols to what is the minimum necessary to achieve the intended goals.

Look out for study proposals

In the case of New IP, many proposals for standards work are simply research studies. Research regarding New IP roughly falls into two categories:

● Research on future use cases as preparation for future standardisation. This type of research is mainly descriptive and intended to inform future work on standardisation. A risk is that **research on an out-of-scope topic can establish a foothold to legitimise future standardisation work**.

● Research on protocol requirements based on existing, defined use cases.

There is no need for standardisation activity in either case. Instead, each SDO provides a separate vehicle for publishing research that is at a pre-standardisation state (for instance, the ITU has Technical Reports and the IETF has informational RFCs).

7.3 Is the proposal in the appropriate SDO venue?

The SDO venue is the standards organisation in which the proposal appears (for instance, IETF or ISO). **Industry-led, multi-stakeholder SDOs are preferred SDO venues**.

Duplication of work taking place in another standards organisation should be avoided. Duplication comes with the cost of tracking and engaging in the work in various organisations. Almost all SDOs have a policy of not duplicating standards work.

Proposals for standards work should be **appropriate to the abilities and remit of the proposed SDO**. This can be a risk in standards bodies that attempt to extend their area of influence. They do so by starting work that is either beyond their established remit or beyond the capabilities of the participants in the SDO.

If the use case is well-defined and has the potential for global impact, the next step is to decide the appropriate venue for possible standardisation. One size does not fit all. For example:

- radio aspects of networking standards components have a natural home in the ITU-R;
- aspects of mobility have a natural home in 3GPP; and,
- the primary standards organisation for the Internet is the IETF[50].

Forum shopping between SDOs, with the goal of quicker progress or a more favourable outcome, should be discouraged.

8 Standards: the new frontier for defending the free and open Internet

The Internet is evolving, and with it, are its technical standards and protocols. Standards development organisations are currently holding important conversations about how the Internet should change to meet the needs of future networks and emerging technologies. However, as shown in this document, **some of the proposals under consideration are seeking to radically transform the Internet's building blocks** and, in some cases, move Internet standards and protocol development to multilateral SDOs. This transition would conflict with the long standing multistakeholder approach to the development of standards for the Internet.

These developments call for serious conversations about how supporters of the multistakeholder model envision the Internet of the future, what Internet values and design principles the community expects to uphold and what proactive engagement strategies are required to address identified challenges including fragmentation of the global Internet.

As standards development emerges as a new frontier for defending the free and open Internet, **new forms of close cooperation** between the Internet´s technical community, public policy advocates, and country delegations and like-minded stakeholders are ever more urgently needed. Building those bridges between islands of expertise will require commitment from the diverse stakeholders that make up the Internet community, and an effort to engage in knowledge sharing and translation between technical and policy communities.

It is critical that these communities work together toward a common goal: **Internet evolution that does not break what we already have and depend upon.** This evolution needs to meet future needs while not increasing the risk of human rights abuses and continuing to reflect shared values. The future of the Internet is dependent on the standards that act as its foundation. The evolution of that foundation is a task for a far broader group than simply the technical community and is a key reason why we need multistakeholder engagement in standards development organizations.

Notes

[1] Stacie Hoffmann, 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, DOI: 10.1080/23738871.2020.1805482

[2] Asia-Pacific Telecommunity, Preparatory Group for WTSA-20 (2020), 'Proposed New Resolution on Enhancing the Study and Standardisation Activities in the ITU Telecommunications Standardisation Sector for the Future Network Evolution Supporting Vertical Applications.'

[3] The work streams of Focus Group Network 2030 and New IP are closely linked. Several of the network requirements identified as necessary for future networks in Focus Group Network 2030 went on to become the basis of New IP. Network 2030 also provided detailed information on potential use cases for New IP. The group concluded its work in June 2020. Chinese delegates conducted a live demonstration of New IP at ITU as part of the concluding activities of the focus group. See ITU-T (2020), 'Technical Report: Network 2030 - Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day, 13 January 2020,' www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Description_of_Demonstrations.pdf?csf=1&e=D7M69p.

[4] For reference, see Max J. Zenglein and Anna Holzmann, "Evolving Made in China 2025: China's industrial policy in the quest for global tech leadership," Mercator Institute for China Studies, July 2, 2019, https://merics.org/en/report/evolving-made-china-2025.

[5] "Original CSET Translation of 'Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035,'" Center for Security and Emerging Technology, Georgetown University, May 13, 2020, https://cset.georgetown.edu/publication/china-14th-five-year-plan/.

[6] For reference, see "The digital side of the Belt and Road Initiative is growing," The Economist, February 6, 2020, www.economist.com/special-report/2020/02/06/the-digital-side-of-the-belt-and-road-initiative-is-growing.

[7]ICANN Office of the Chief Technology Officer (2020), 'New IP,' p.3, https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf

[8] Carolina Caeiro, Kate Jones, Emily Taylor (forthcoming) Technical standards and human rights: the case of New IP, *Human Rights in a Changing World,* to be published by Chatham House and Brookings Institution Press. https://oxil.uk/publications/2021-08-27-technical-standards-human-rights/

[9] Garfinkel, S. (2003), 'The End of End-to-End?,' MIT Technology review, July 1, 2003, https://www.technologyreview.com/2003/07/01/234174/the-end-of-end-to-end/.

[10] See materials from IETF109 Side Meeting on Future IP Evolution (FIPE) available on GitHub: https://github.com/FIPE-Study/IETF109-Side-Meeting-FIPE.

[11] See IETF Internet Draft 'OCN Use Cases for Industry control Networks' https://datatracker.ietf.org/doc/draft-wmdf-ocn-use-cases/.

[12]See 'HotRFC Lightning Talks at IETF-114,' https://datatracker.ietf.org/meeting/114/materials/agenda-114-hotrfc-sessa-17.

[13] See for example, Contribution 063, "Proposal for initiating a new work item on the requirements and framework of multi-dimensional resource matching based on DLT" by China Telecom, ITU-T´s SG13, July 2022 meeting.

[14] See, for example, Contribution 098, "Proposal to initiate a new work item on" Identification and measurement methods of computing resources and services for computing and network convergence" by China Mobile, ITU-T´s SG13, July 2022 meeting.

[15] Allemann, A. "China wants to patent a decentralised blockchain DNS," Domain Name Wire, May 10, 2021, https://domainnamewire.com/2021/05/10/china-wants-to-patent-a-decentralised-blockchain-dns/.

[16] Hoffmann, S., Lazanski, D. and Taylor, E. (2020), 'Standardising the Splinternet: how China's technical standards could fragment the Internet,' *Journal of Cyber Policy*, 5:2, p. 245. https://doi.org/10.1080/23738871.2020.1805482.

[17] This proposed modification of packet headers is not a novel idea. Similar proposals have been considered in the past, for example, RFC 1887 from 1995 considered a hierarchical model for IPv6 address allocations. The flexibility and affordability offered by the layered Internet model, however, made the current Internet protocols prevail. Hogewoning, M. (2020), 'Do we need a New IP?,' RIPE Labs Blog, April 22, 2020, https://labs.ripe.net/author/marco_hogewoning/do-we-need-a-new-ip/.

[18] Caeiro, Jones and Taylor (2021), *Technical Standards and Human Rights*, p.9.

[19] Garfinkel, S. (2003).

[20] Comparitech (2021), 'Latency vs Throughput – Understanding the Difference,' https://www.comparitech.com/net-admin/latency-vs-throughput/.

[21] For example, proponents of New IP criticised the work conducted at IETF's DetNet arguing that: "DetNet is also far from attempting to identify if or how the services it plans to introduce could be made to operate over the Internet in general; instead, it focuses mostly on the shorter-term goal to enable them in controlled networks within a limited domain." See section 4.5 of IETF Internet Draft entitled "Forwarding Layer Problem Statement" by Bryant, S., Chunduri, U., Eckert, T. and Clemm, A. (latest version from January 24, 2022), https://datatracker.ietf.org/doc/html/draft-bryant-arch-fwd-layer-ps.

[22] As highlighted by the UK National Cyber Security Centre's Protocol Design Principles, it is considered best practice to keep protocol design simple. See NCSC (2020), 'Protocol Design principles,' https://www.ncsc.gov.uk/whitepaper/protocol-design-principles.

[23] Varga, b., Farkas, K., Fedyk, D., Berger, L. and Brungard, D. (2021), 'The Quick and the Dead: The Rise of Deterministic Networks,' IEEE Communications Society, https://www.comsoc.org/publications/ctn/quick-and-dead-rise-deterministic-networks.

[24] In semantic addressing, additional information or meaning is placed into the IP address, and this is used to route packets within the network. A good overview of some approaches to semantic addressing can be found in Section 4.3 of https://datatracker.ietf.org/doc/draft-king-irtf-semantic-routing-survey/ Also see Section 1.4.1.5 below.

[25] ICANN Office of the Chief Technology Officer (2020), 'New IP,' p.24.

[26] See Sharp et al. (2020), *Internet Society Discussion Paper: An analysis of the "New IP" proposal to the ITU-T.*

[27] Hogewoning, M. (2020), 'Do we need a New IP?.'

[28] ICANN Office of the Chief Technology Officer (2020), 'New IP,' p.23.

[29] For instance, there has been much work in the IETF to separate the identifier of an endpoint from its location in the Internet Protocol. As an example, see RFC6830, https://datatracker.ietf.org/doc/html/rfc6830.

[30] ICANN Office of the Chief Technology Officer (2020), 'New IP,' p.23.

[31] Chao, B. and Schulman, R. (2020), *Promoting Platform Interoperability,* report, Open technology Institute, https://www.newamerica.org/oti/reports/promoting-platform-interoperability/interoperability-is-fundamental-to-the-Internet/.

[32] Criticisms point to the centralisation of certificate authorities (such as IdenTrust and GoDaddy), the consolidation of DNS resolution primarily in the hands of Western firms, and even the management of the DNS root zone by the IANA. See Hoffmann, S., et al. (2020), 'Standardising the Splinternet,' p.249. Please, note that concentration is also a concern for other parts of the Internet, including physical infrastructure and applications. While New IP proponents have generally alluded to challenges of centralization, those leveraged more strongly to justify proposed transformations centre on the DNS.

[33] Caeiro, Jones and Taylor (2021), *Technical Standards and Human Rights*, p.9.

[34] https://www.huawei.com/en/technology-insights/industry-insights/innovation/new-ip Huawei (n.d.), 'A Brief Introduction about New IP Research Initiative'.

[35] Loren Kohnfelder and Praerit Garg, The threat to our network, Microsoft, 1999.

[36] ManyNets was first introduced by the Focus Group Network 2030, and then adopted as a feature of New IP.

[37] "Heterogeneous networks" are those that use a variety of transports, physical media and organisational approaches to meet their use cases. IoT Networks, for example, are often organised as a mesh of low-power, low-performance nodes at the most local level while using more traditional technologies to backhaul traffic from the mesh to the servers which accumulate, analyse and visualise the resulting data.

[38] ICANN Office of the Chief Technology Officer (2020), 'New IP,' p.25.

[39] ICANN Office of the Chief Technology Officer (2020), 'New IP,' p. 25

[40] ICANN Office of the Chief Technology Officer (2020), 'New IP,' p. 26

[41] Note that while transport protocols like TCP and QUIC can provide assurance for delivery and that upper layer protocols can attempt to do this on top of UDP, the timing of the delivery of the packets and the perfect ordering of the packets is not, in principle, possible to guarantee at the transport layer. An important development for deterministic networking is the architecture and protocols being designed by the IETF's DETNET Working Group (see https://datatracker.ietf.org/wg/detnet/about/).

[42] Sharp, H. and Kolkman, O. (2020), *Discussion Paper: An analysis of the "New IP" proposal to the ITU-T,* Report, Internet Society, https://www.Internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/.

[43] As explained in the Internet Society report: "The IETF Transport Area develops transport protocols (e.g., Stream Control Transmission Protocol (SCTP), Real-time Protocol (RTP) and Real-time Communications for the Web (WebRTC), and QUIC) and active queue management protocols (e.g., the Low Latency, Low Loss, Scalable Throughput service architecture (L4S) and Some Congestion Experienced (SCE) ECN Codepoint). These increase throughput, lower latency, and further support the needs of real-time and multimedia traffic, while considering interactions with, and effects on, TCP traffic on the Internet." See Sharp et al. (2020), *Internet Society Discussion Paper: An analysis of the "New IP" proposal to the ITU-T.*

[44] As for deterministic networking, as summarised by Internet Society, the following work is currently ongoing across SDOs: (i) IEEE 802.1 Time Sensitive Networking (TSN) Task Group [TSN] is developing extensions to support time sensitive networking using IEEE 802.1 networks; (ii) IETF Deterministic Networking (detnet) and Reliable and Available Wireless (raw) working groups are developing RFCs to support deterministic networking on routed networks and to interwork with IEEE 802.1 TSN; and (iii) 3GPP is defining standards to support its 5G ultra-reliable low latency communications (URLLC) capability over the Radio Access Network (RAN) as well as interworking with 802.1 TSN networking. In addition, ITU-T SG15 is working with IEEE 802.1 TSN and 3GPP (5G) related to its transport- related Recommendations. See Sharp et al. (2020), Internet Society Discussion Paper: An analysis of the "New IP" proposal to the ITU-T.

[45] Hogewoning, M. (2020), 'Do we need a New IP?.'

[46] As summarised by ICANN, IETF is conducting work on Segment Routing (SR), such as that covered in RFC8402. In addition, recent Internet drafts from the Source Packet Routing in Networking (SPRING) Working Group include work on a new IPv6 Segment Routing Header (SRH) to program SR networks. See ICANN Office of the Chief Technology Officer (2020), 'New IP,' p.23.

[47] https://www.ncsc.gov.uk/whitepaper/protocol-design-principles

[48] See https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/

[49] https://www.analysysmason.com/contentassets/e94b9d54c3b3413db85f3200332c5e04/analysys_mason_internets_technical_success_dec2021.pdf

[50] Although note that some specialized Internet standards work goes on in places like the World Wide Web Consortium.