Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Standardising the splinternet: how China’s technical standards could fragment the internet

Stacie Hoffmann , Dominique Lazanski & Emily Taylor

To cite this article: 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

To link to this article: https://doi.org/10.1080/23738871.2020.1805482

Published online: 29 Aug 2020.

Submit your article to this journal

Article views: 1162

View related articles

View Crossmark data

JOURNAL OF CYBER POLICY
2020, VOL. 5, NO. 2, 239–264
https://doi.org/10.1080/23738871.2020.1805482

Standardising the splinternet: how China's technical standards could fragment the internet

Stacie Hoffmann[a], Dominique Lazanski[b] and Emily Taylor[c]

[a]Digital Policy and Cyber Security, Oxford Information Labs, Oxford, UK; [b]Last Press Label, London, UK; [c]Oxford Information Labs, Chatham House, Oxford, UK

ABSTRACT

China's drive for technological dominance has resulted in a long-term, government-driven national strategy. This includes the creation of native technologies which reflect local policies and politics, micromanagement of the internet from the top down, and the use of international standards development organisations (SDOs), such as the UN agency the International Telecommunication Union (ITU), to legitimize and protect these technologies in the global marketplace. Alternate internet technologies based on a new 'decentralized internet infrastructure' are being developed in SDOs and marketed by Chinese companies. In a worst-case scenario, these alternate technologies and a suite of supporting standards could splinter the global internet's shared and ubiquitous architecture. They also pave the way to a new form of internet governance, one that is multilateral instead of multistakeholder. A fragmented network would introduce new challenges to cyber defence and could provide adversaries with a technical means to undermine the norms, predictability and security of today's cyberspace – which would also impact human rights and widen the digital divide. Western nations and like-minded allies need to intensify their cooperation with one another, international partners such as the EU, and other stakeholders like industry, academia and civil society to understand and limit the potential ramifications of these new technical developments. This paper aims to shed light on how China's activities in SDOs contribute to the execution of its long-term technical, economic and political strategic ambitions.

Abbreviations: 3GPP: 3rd Generation Partnership Project; BRI: Belt and Road Initiative; DDoS: Distributed denial of service; DII: Decentralized Internet Infrastructure; DLT: Distributed ledger technology; DNS: Domain name system; DOA: Digital Object Architecture; EU: European Union; GDPR: General Data Protection Regulation; GSMA: GSM Association; IANA: Internet Assigned Numbers Authority; IEC: International Electrotechnical Commission; IETF: Internet Engineering Task Force; IGF: Internet Governance Forum; IMEI: International Mobile Equipment Identity; IoT: Internet of things; IP: Internet Protocol; IPv6: Internet Protocol Version 6; ISO: International Organisation for Standards; ITU: International Telecommunications Union; ITU-T: International Telecommunications Union Standardization Sector; MAC: Message

ARTICLE HISTORY
Received 11 May 2020
Revised 12 June 2020
Accepted 13 July 2020

KEYWORDS
Standards; China; decentralised internet infrastructure; security; governance

CONTACT Stacie Hoffmann stacie.hoffmann@oxil.co.uk

authentication code; MIIT: Ministry of Industry and Information Technology; NATO: North Atlantic Treaty Organization; OID: Object identifier; OSI model: Open Systems Interconnection model; SAC: Standardization Administration of the People's Republic of China; SAMR: State Administration for Market Regulation; SDO: Standards development organisation; SG: Study Group; TCP/IP: Transmission Control Protocol; TSAG: Telecommunications Standards Advisory Group; UN: United Nations; WIPO: World Intellectual Property Organisation; WTO: World Trade Organization; WTSA: World Telecommunication Standardization Assembly

1. Introduction

In 2018, Huawei started to socialise its version of 'decentralized internet infrastructure' (DII) at the International Telecommunications Union (ITU), stating that the current internet has 'fundamental problems' and vulnerabilities related to hacking, centralisation and biases (Light Reading 2018). By late 2019, Chinese delegations were stepping up their public messaging of the 'decentralized internet' model and core technical components – referred to as 'New IP' (Jiang 2019) – with presentations at a variety of the ITU's Telecommunication Standardization Sector (ITU-T) meetings[1] and a side session at the Internet Engineering Task Force (IETF) 106 ("IETF 106 Side Meetings" 2019; "ITU-T TSAG C (2019-09-23)" 2019).

The technology presented by Huawei amounts to a reinvention of the internet's core architecture and the Transmission Control Protocol and Internet Protocol (TCP/IP). If successful, it could splinter the global internet and would result in a shift away from multistakeholder internet governance. The technology and its implications raised alarm bells for some government delegations. However, for frequent participants in the ITU, the proposal only confirmed a long-held suspicion that the standards being championed by China are creating the technical underpinnings for an alternative internet. Such a move would be consistent with China's stated aim to become a technological superpower, underpinned by its Made in China 2025 strategy (Delfs 2018), Standards 2035 report (SESEC 2018) and the Belt and Road initiative (Manuel 2017; Cave et al. 2019).

The authors predict that the new technologies proposed by China will create a more network-centric internet that enables fine-grained controls in the foundations of the network, changing the way people and things connect and how data is collected and used. Ultimately, China's focus on 'decentralized' technologies will lead to more centralised, top-down control of the internet and potentially even its users, with implications for security and human rights.

Technical standards – lightweight, open and interoperable – have played a central role in holding the internet together as a single, global network which enables technological innovation and economic growth. Traditionally, standards have been an enabler of the internet's existing 'end to end' principle with 'dumb pipes' (e.g. networks and routing) that treat data in a neutral way and allow innovation to occur at the edges of the network (Wu n.d.). Internet standards have traditionally been developed through consensus. Despite the apparent fragility of the processes, to date, technical standards have proven remarkably resilient at holding together a single, global internet, largely through convention. But as geopolitics infects the internet's deep technical layers, there is no guarantee that the future will look like the past.

The process of standardisation of a certain technology can take years and is far removed from the usual image of the internet as a fast-evolving environment. The return on investment for cash-strapped governments and first-to-market technology companies makes it hard to justify continuing participation in SDOs like the ITU and IETF. Yet, for states that stay the course, technical standards can be:

- A source of strategic and commercial advantage;
- Justification and legitimisation for national regulation on technology; and
- A means to embed alternative approaches to human rights into the technology.

At a technical level, the internet can be broken or manipulated by a patient adversary fragmenting the global network into national and regional splinternets.

The Snowden revelations in 2013, followed by allegations of electoral interference conducted through social media, have dampened early utopian visions of the internet. Public discourse has questioned the ethics of US platforms' business models and the US lost moral authority as the champion of a global, free and open internet (Deibert 2015; Zuboff 2019). Europe positioned itself as the gold standard of privacy through instruments like the General Data Protection Regulation (GDPR) and radical court judgments in the Court of Justice of the European Union (EU)[2]. However, there has been a failure of like-minded countries to create a consistent and inclusive message about the importance of internet freedom and openness for innovation and development (Taylor and Hoffmann 2019).

Additionally, there has been a failing by many in internet governance organisations (including SDOs) to acknowledge the challenging and complex issues that arise for developed *and* developing countries, such as privacy, cybersecurity, consolidation and privatisation (ISOC 2019). Without a logical place to land or an appropriate multistakeholder forum to develop open and rights-respecting solutions, complex issues have been left unresolved (Taylor and Hoffmann 2019). Meanwhile, governments like China and Russia have seised the opportunity to shape next generation internet technologies that are more authoritarian and less human rights-respecting, sometimes modelled after Western policies like the UK's Investigatory Powers Act (Hern 2015). China in particular sees the market potential for these technologies.

It is opportune timing to propose such a significant shift in technology. Concurrently, new technologies like 5G will change the way networks are built and run (5G PPP Architecture Working Group 2019), and there is both concern and support for moving towards 'encrypted everything' protocols, particularly in IETF standards (Rashid 2019). For example, implementations of DNS over HTTPS (DoH) encrypts sensitive data in transit, but could restructure domain name resolution technically, as well as how it is governed (Hoffmann 2019; Bennett 2019). Such technologies pose both a threat and an opportunity for authoritarian governments.

Cyber capacity building and enhancing resilience are key to cybersecurity and cyber defence, whether through strengthening resilience, information-sharing, adopting cyber norms or training. Stakeholders including industry, academia and civil society play key roles in achieving these aims as reflected in current multistakeholder internet governance processes. This paper will show why standards and multistakeholder engagement are an important component of any cyber strategy.

The benefits of a norms-based, predictable, secure and open cyberspace is recognised by institutions like NATO and the Global Forum on Cyber Expertise (GFCE) as well as across like-minded countries (NATO 2019; Global Forum on Cyber Expertise n.d.). Consistent with the Tallinn Manual and the UN Group of Governmental Experts (UN GGE), the UK, as well as all NATO members, recognises that international law applies to cyberspace (UNODA n.d.; NATO 2016, para. 72). Yet, the application of the law of armed conflict is contested by several countries, including China (Hsu and Murray 2014). Tensions and disagreements surrounding this issue contributed to the collapse of the 2017 UN GGE process (Hitchens and Gallagher 2019). However, the UN GGE process is underway again, as is a parallel Open Ended Working Group (OWEG) (De Tomas Colatin n.d.). Alternative internet architectures and technologies could weaken existing norms, principles and processes such as these.

Developments in internet standards, especially at such a critical time of evolution, have not been closely followed by most countries, including Western countries developing and exporting technology. A worst-case scenario could result in a complete break resulting in two or more ‘internets’. At minimum, there will be a new array of networking technologies that must be understood by all in order to support global cyber stability and security. As a result, supporters of the global, free and open internet should come together now before losing more ground to an authoritarian vision for the internet’s future.

This paper provides background on decentralised internet infrastructure, standardisation, China’s strategy (see sections 2 and 3), explores the alternative DII technologies being standardised in the ITU and briefly looks at other international standards development organisations (SDOs) (see section 4). It then analyses the potential impact on current multistakeholder internet governance (see section 5). The technical review focuses on three technologies (object identifiers (OIDs), distributed ledger technology (DLT), and future networks) as well as plans to create new protocols. Together, these technologies start to build a picture of China’s long-term goals.

2. The globalisation of a Chinese internet

2.1. Politics of technology

China has long understood the intersection of policy, technology and standards in a way that most Western democracies are only starting to grasp. Technology is not detached from policy, regulation or society – it is explicitly or implicitly impacted by these factors (DeNardis 2011). Ultimately, China is leveraging policy and technology in a top-down approach to protect local markets, increase global market reach and ensure Communist Party ideals are upheld (Swinhoe 2019). China’s first National Cyber Security Strategy marks cybersecurity as a ‘new territory for sovereignty’ (United States Information Technology Office n.d.; Rosenzweig 2016). It links the political and social elements of technology, identifying economic security, political security, cultural security and social stability as ‘grave risks and challenges’ (Cheung 2018; Creemers 2016). These elements are often reflected in standards work despite falling outside the remit of technical standards.

Under President Xi Jinping, links between national security, cybersecurity and technology have been reinforced (e.g. through the National Intelligence Law) (Roberts, Moraes, and Ferguson 2018; Liu 2020). Increasingly common names in SDOs like Huawei, Tencent, and China Telecom are in China's top 50 cybersecurity firms[3] (Cheung 2018). This relationship supports some of the national security concerns expressed by the US and Australia in relation to China and 5G (Hewett 2020). Technologies being developed by these industry players translate into SDOs. For example, in ITU-T Study Group (SG) 17, five of the twelve work items on cloud computing and big data infrastructure security have editors from a China Telecom 'research and development center', China Telecom Guangzhou R&D Center (RealWire 2007; "ITU-T Work Program Q8/17" 2017).

Given the sensitive topics included in some standards, there are links between China's work in the ITU and instances of human rights abuse. Chinese companies ZTE, Dahua and China Telecom have been standardising facial recognition technology at the SDO

(Gross, Murgia, and Yang 2019). It is suspected that these or similar technologies are being used in Uighur 're-education camps'. Hikvision, a Chinese surveillance company on the US sanctions list, is an editor of surveillance standards at the ITU (Rollet 2019). It marketed surveillance equipment in 2019 which claimed to be able to identify Uyghur ethnicity (Feng 2018).

A Chinese approach to technology naturally favours multilateral internet governance rather than today's decentralised, open and multistakeholder model. The country has long lacked confidence in the multistakeholder model, because the Chinese government views multilateral negotiations as the only legitimate type of negotiation on global issues. And with growing power, the Chinese government is unlikely to accept existing institutions seen as 'Western' (Chen 2009; Schneider-Petsinger et al. 2019).

In order to attract allies and lobby in other fora, the Chinese government claims the current governance structure lacks equal (government) representation and has failed to address issues important to non-Western and developing nations. The Chinese government and its allies use a variety of tactics and language to undermine trust in the internet, its technical infrastructure as well as its governing mechanisms. Chinese delegates give voice to their positions at ITU-T advisory meetings and seed doubt in the most foundational elements of trust in the internet, such as root authorities, through initiatives like DII.[4] Another tactic has been for China and its allies to refuse to adopt key international instruments (such as the Budapest Convention[5]) on the grounds that it was created by the Council of Europe in 'the West'. Currently, there is a duplicative, and potentially harmful, process in the UN being led by Russia to impose multilateral, binding solutions only to cybercrime[6] (Hakmeh and Peters 2020). This process, if concluded successfully by Russia, China and their allies, would take private sector technology companies out of any solution to combat cybercrime, though these companies are often the first to detect and mitigate crime on the internet.

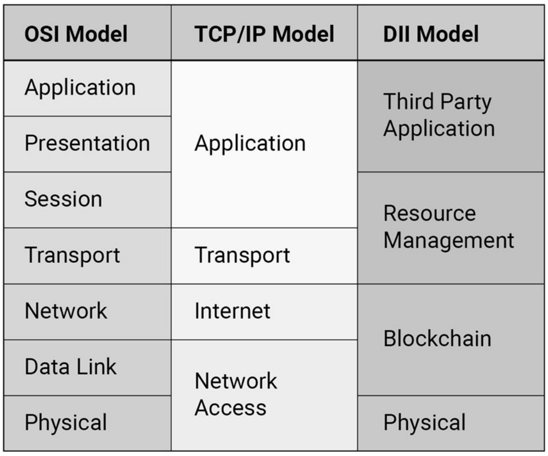
At the same time, the future of the global internet is also threatened by standards supported by Western stakeholders that either work in DII's favour (e.g. 5G) or threaten the internet's root zone (e.g. DoH) (Rutkowski 2020; Huston 2019). However, stakeholders, including government, industry and civil society, have worked together to situate and further develop disruptive technologies within today's internet governance structure. DoH and its multistakeholder group, the Encrypted DNS Deployment Initiative, is one example (EDDI 2019). In 2017, the IETF initiated a 'Decentralized Internet Infrastructure' research group focusing on infrastructure services (IETF 2020). This group is completely different to the Huawei proposals, in that it brings research of deployed decentralisation to the IETF, rather than proposing a new internet architecture. Confusingly, however, it has the same name as the Huawei proposals. This example elucidates two points: one is the repurposing of language, often reflecting Western policy narratives, by Chinese delegates to fit Chinese aims; the other is the ability to address the issues highlighted by China in DII within existing multistakeholder governance fora. By contrast, the multilateral ITU, where China is primarily standardising DII, is being positioned to take over the governance role.

2.2. Decentralised internet infrastructure

Any technology has the capacity to impact significantly the lives of individuals, their human rights, and participation in society (Hillman 2018; Shahbaz and Funk 2019). China's use of technology for political means is no longer focused on blanket control through the Great Firewall; it now deploys a mix of people and technology to deliver a more nuanced, targeted, and impactful system (Miao 2020). Standardisation of DII will support and enable a variety of applications, such as China's social credit system, which uses identifiers to link people to a permanent record and effect, for example, their ability to buy tickets or access the internet (Kobie 2019; Dai 2019). DII and related technologies focus on putting 'trust' in the network, building webs of data logs and moving away from Western approaches to encrypted communications to enable tools like deep packet inspection[7] and censorship.

China is making a network-centric internet that merges internet layers, specifically the data link (OSI layer 2) and network layers (OSI layer 3)[8] (see Figure 1). It restructures internet architecture and reconceptualises identifiers. It also marks a move away from the internet's historic 'best effort' principle[9], promising instead a guaranteed quality of service and low latency ("New IP Technologies" 2019). Despite being marketed as 'decentralizing', the technologies (e.g. distributed ledger technology (DLT)) actually enable centralised control and command of the internet, through fine-grained micromanagement and surveillance, likely supported by 5G's edge computing (Table 1).[10]

The merger of data link and network layers facilitates centralised control. It moves intelligence away from the end nodes of the internet stack (i.e. application layer) into the



OSI Model	TCP/IP Model	DII Model
Application	Application	Third Party Application
Presentation		
Session		Resource Management
Transport	Transport	
Network	Internet	Blockchain
Data Link	Network Access	
Physical		Physical

Figure 1. Comparison of internet layer models.

Table 1. Comparison of internet layer models.

OSI Model	TCP/IP Model	DII Model
Application	Appilication	Third Party
Presentation		Application
Seesion		Resource
Transport	Transport	Management
Network	Internet	Blockchain
Data Link	Network	
Physical	Access	Physical

'dumb pipes' of the internet and the hands of network operators and infrastructure providers. Considering the largest mobile and telecommunications operators in China (such as China Unicom, China Telecom and China Mobile) are all state-owned, this collapses control into the hands of state entities. A logical result is the central micromanagement of services, access controls, and application of policy and regulation at the point of connection. It is also no surprise that many Chinese delegations engaging in SDOs are network operators (including those above) and infrastructure providers (e.g. Huawei).

3. How standards work

3.1. Why standards matter

A standard is an agreed-upon, technical specification for a service, task or operation. Standards specify protocols that allow software and users to interact and interoperate and play a vital role in the growth and development of the global telecommunications and internet industry.

Through standardisation, a technology can become recognised and protected by international institutions such as the United Nations (UN) and World Trade Organization (WTO). Adoption of certain technical standards, particularly if required by national law, can have potentially harmful consequences such as impeding competition by locking consumers into a specific, outdated or substandard technology.

There are currently more than two hundred consortia organisations and bodies working on one or more layers of technical communications and networks standards-making, including internet standards, web standards and telecommunications standards (Schneiderman 2015). Despite the ITU only having a mandate to develop *telecommunication* standards, the ITU management and certain member states, including China, continue to seek ways to duplicate mobile network communication and internet standards developed in other SDOs (International Telecommunication Union n.d.). The ITU's scope creep is openly supported by Secretary General Zhao who, for example, has marketed the ITU as the 'technology' (not telecommunication) agency (Zhao 2017).

Within this complex ecosystem, there are generally two kinds of standards-making organisations: multilateral and multistakeholder (Lazanski 2019). Each SDO functions differently with agreed upon norms and rules; three are of particular interest to China.[11] ISO and IEC are a combination of both multilateral and multistakeholder, as national bodies coordinate and approve delegations made up of governments and industry. The ITU is a multilateral organisation in which governments, and not industry, hold decision-making power in negotiation and agreements. Sector (i.e. industry) members may participate in standards development and debate. The state-firm diplomacy between states as key power holders and weaker industry[12] at the ITU reflects China's view of 'multistakeholder' internet governance (Chen 2006).

One main reason China is active in multilateral SDOs, aside from easy access, is that technologies compliant with standards developed in those fora are legally prevented from being barred in international trade (World Trade Organization n.d.). In essence, this gives an incentive to China to make sure all of their national standards and technology are standardised primarily through these three organisations. This is an important vehicle for China and its companies to standardise technologies in order to enable and ensure their place in global trade.

3.2. China and standards

At this time, Chinese delegations are among the largest participating in SDOs – consistently the largest at the ITU, the 5th largest at the ISO and make up 10% of all attendees at the IETF (IETF 2020). Increasingly, companies like Huawei, China Mobile, China Unicom, Alibaba and ZTE are playing a larger role in both multilateral and multistakeholder SDOs acting as negotiators in forums like 3GPP and experts in multilateral organisations like the ITU. Additionally, Chinese nationals also hold key governance positions in these organisations, such as director, chair, vice-chair and rapporteur.[13] Chinese nationals are the heads of the ITU and International Electrotechnical Commission (IEC)[14] and are currently vying to run the World Intellectual Property Organisation (WIPO) (Lynch 2019), among other multilateral, UN affiliated organisations (Okano-Heijmans, van der Putten, and van Schaik 2018).

Conversely, participation of delegations of governments from Western countries has decreased. Such governments prefer industry-led, market-driven standards which reflect the demand for standards from the companies and organisations who use them. As a result, Western governments let industry lead on SDO participation and prioritisation. Generally, this does not translate into participation in the ITU, which is a multilateral organisation with a limited role for industry and specialising in international telecommunications. These changes have slowly evolved over the last 20 years in the ITU-T. For example, membership of sector members has dropped from 650 to 188 in that time period (Lazanski 2019).

China undertakes an organised and systematic approach to standardising technology, agriculture and manufacturing, to ensure consistency and legitimacy (Seaman 2020). In 2018, China enacted legislation to streamline local, regional and national standards into a single, national process (Association of Equipment Manufacturers 2018). It consistently invests significant resources and embedded standards development within numerous arms of the state. The Standardization Administration of the People's Republic of China (SAC) (Standardization Administration of the P.R.C., n.d.) holds overall responsibility for standards work across China. The SAC represents China and the National Committee at international SDOs including the ISO (International Organization for Standardization n.d.) and IEC. It coordinates the implementation of national and international standards within China and Chinese projects overseas, like the Belt and Road Initiative (BRI) (2018). Required uptake of Chinese-origin standards is a common element of contracts with foreign countries (Schneider-Petsinger et al. 2019; Hillman 2018).

China has taken a new approach to standards through reform introduced in the Standards Law 2018 (SESEC Team 2017). The law introduced a number of changes to the organisation of standards in China, but also encouraged international participation in global SDOs, which includes the following goals:

1. Actively participate in international standardisation activities (not only ISO/IEC, but more international/influential SDOs).
2. Encourage Chinese enterprises and experts to participate in development and revision of international standards.
3. Adopt international standards based on China's actual conditions or needs.
4. Promote the two-way adoption of Chinese standards and foreign standards for application in respective countries, including mutual recognition of standards.

Additionally, a new initiative called Standards 2035 will involve a strategic review of standards and extend its national and international strategy across all areas.[15] The project is due to report on progress in the spring of 2020.

To date, no North American or European country or region has a similar strategy.

4. Standardising an alternate internet

4.1. The ITU and multilateral standards

Alongside the increase in Chinese participation at the ITU came an increase of Chinese-driven work items and contributions. Such behaviours are consistent with China's strategies to promote Chinese *national* standards and develop indigenous intellectual property, of which technology is an important aspect (Kennedy 2017). This section looks at the following three DII-related technologies and how they are being standardised in the ITU-T to support China's development of alternative internet technologies:

- Object identifiers (OIDs);
- Distributed ledger technologies (DLT), including blockchain; and
- Network 2030.

For more information about focus areas and related work items in the ITU, see Appendix 1.

4.2. Identifiers and ITU-T

Identifiers are a key component of the TCP/IP protocols which underpin the internet. To gain traction, any technology which seeks to replace TCP/IP must offer a system of unique identifiers. Identifiers can be the repository of personal information or assigned to track individuals and devices. Identifiers have a long history at the ITU but have recently expanded beyond intended remit. Currently the standardisation of identifiers takes place in three study groups within the ITU-T.[16]

In the last twelve years, work has been undertaken at the ITU on identifiers outside the interoperable and technically viable group of identifiers deployed globally in mobile networks and on the internet. Though work items in any study group should be member-led, the ITU management has deviated from standard procedure and supported work on identifiers for Digital Object Architecture and IoT which met significant opposition by some members.

Often there are fundamental concerns over security and resilience of these proposes systems and the potential for misuse which mirror the concerns of proposed identifiers in New IP – in particular, the reliance on a one-to-one relationship between an identifier and a 'thing', such as a phone or server. In addition, there is concern that the ITU would govern the internet's identifiers, not dissimilar to how it governs international number resources today, but in place of multistakeholder organisations like the Internet Corporation of Assigned Names and Numbers (ICANN).

Digital Object Architecture (DOA) was developed by Bob Kahn (one of the internet's 'founding fathers' who together with Vint Cerf, invented the TCP/IP protocols) in the mid-1990s as a method of identifying and locating repositories of information and the detailed elements they hold online (Cerf and Kahn 1974). DOA is made up of three key components: the identifier or resolution system, the repository system and the registry system. One significant difference between the DOA system and TCP/IP is that DOA is proprietary, not open. It is overseen by a non-profit foundation created to manage the technology, called the DONA Foundation ("About DONA" n.d.). Additionally, DOA requires a licence from the Corporation for National Research Initiatives (CNRI, founded by Bob Khan) – downloading the code is agreement to the licence. It also requires a licence of Java to run, and has a potential single point of failure between the identifier and the repository which would cause security and privacy issues (Rogers 2016; Sharp 2016). Because of these technical issues, while the system has been widely adopted for archival and document management by using a barcode, it has never been widely used for a digital object like a website.

The issue with DOA also exemplifies the governance issues embodied by New IP proposals at the ITU. As attempts to standardise DOA in the ITU-T continued, and was pushed by ITU leadership, Bob Kahn (on behalf of DONA) agreed a Memorandum of Understanding with the ITU. The UN organisation will take over the management of the technology in the event the DONA Foundation terminates, which may happen if and when Kahn leaves the organisation. If DOA were widely adopted, the ITU would stand to gain revenues from hosting the repository for DOA identifiers for the internet and charge for the allocation of those numbers to users. The ITU would also act as the technology's governing body and public policy focal point, a position which its critics have long believed to be the ITU's aim.

The United States was never happy that the UN was entering such an agreement with a technology rivalling the open, interoperable suite of internet protocols (Dourado 2016). Some governments and organisations have voiced concern about the technology and governance structure (Durand 2019; Global Partners Digital n.d.). There is ongoing contention surrounding why the ITU is standardising a singular, proprietary technology, with the enthusiastic support of Russia and Saudi Arabia in particular. This led to speculation that the actors in ITU are attempting to standardise an alternate internet (Dourado 2016; "Focus Group on Technologies for Network 2030" n.d.).

The deployment issues relating to DOA resulted in a gradual waning of interest, aided in part by persistent questioning and resistance by Western countries, organisations and companies. However, Chinese delegation members unexpectedly began to introduce work items into ITU-T study groups.[17] In 2019 a new work item was proposed in SG17 called *A Decentralized Framework for Object Identifier Resolution.*[18] The Chinese authors proposed an object identifier resolution system to replace the current Domain Name System (DNS) system on which the internet runs in order to address issues of performance, stability, privacy and security. The use of alternate technologies for identification on the internet and the DNS would lead to less predictability in cyberspace and new questions around norms and governance.

4.3. Distributed ledger technology and ITU-T

For some, today's internet is increasingly consolidated, seen as a network of privatised networks provided by American companies like Google, Facebook and Microsoft (Song 2018; ISOC 2019; Taylor and Hakmeh 2020). China is capitalising on this perspective. China currently views trust on the internet as 'centralized', and argues this leads to a single point of failure and the need for a new, 'decentralized' infrastructure[19] ("Decentralized Internet Infrastructure (DII)" 2018). From China's perspective, centralised trust could be understood as the certificate authorities (such as IdenTrust and GoDaddy) currently offering digital certificates for websites (W3Techs 2020), consolidation in DNS resolution, (Radu and Hausding 2020), or even the management of the DNS root zone by the Internet Assigned Numbers Authority (IANA). Additionally, the IETF's current 'encrypt everything' approach is counter to Chinese interests – not only does it work against tools like censorship, but it could also consolidate data with a shrinking number of Western tech giants.

To counter 'centralization', China is incorporating distributed ledger technologies (DLT) into its decentralised internet infrastructure as a facilitator of controls, data collection and management. Aspects of internet technologies linked to DLT include identity and access management, networking, system management, and data processing and management. For example, Huawei claims identity management via blockchain[20] provides a 'highly reliable, traceable, and collaborative' tool to allow 'legitimate users or devices' to access services once verified by 'organisations' (Huawei 2018). These technical aspects are then linked to concepts like 'trust', 'security', 'anonymity' and 'integrity'[21]. Huawei's marketing materials for DII include a 'blockchain layer' to facilitate what is being billed as 'decentralized trust' and is the foundation for the 'internet resource management layer' (i.e. IP addressing and DNS) and 'trusted application layer' ("Decentralized Internet Infrastructure (DII)" 2018). This aligns with China's national blockchain development strategy (Huawei 2018).

However, critics of New IP and other DII-related proposals do not support the claim that the DNS is centralised, or that DLTs are the solution to problems related to consolidation. Although many of the biggest players in DNS resolution are Western companies (such as Google, Cloudflare and Amazon), this does not paint the whole picture. Google is the most popular DNS provider, resolving about 13% of internet traffic – while the number two spot belongs to OpenDNS which resolves 1.82% of internet traffic, far behind the leader of the pack (Z 2018). Another study shows the eight largest players account for 53.7% of DNS resolution, meaning the remaining 47.3% is resolved by other providers, such as local internet service providers (Foremski and Gasser 2019). Furthermore, with the growth in content delivery networks (CDNs) it is likely that traffic is resolved locally. The DNS is, and will be, a globally distributed network.

Perceived centralisation is used to support claims that the DNS' current structure makes it vulnerable to distributed denial of service (DDoS) attacks, is not fit for purpose, or adaptable to internet growth, ultimately hindering development (Sharp 2016). In March 2019, Chinese companies submitted two separate contributions[22] to ITU-T Study Group 13 using this justification, introducing a new decentralised DNS root based on blockchain. If successful, such technology could fracture the internet's root zone. However, these claims ignore the rapid recovery from large scale DDoS attacks on the DNS, such as the Dyn attack in 2016, demonstrating the internet's distributed and resilient infrastructure (Bursztein 2017).

To China's other claim, DLTs are not inherently decentralised or human rights respecting. Design and deployment are key factors of a technology's characteristics. In this alternative infrastructure DLT characteristics would support centralised management of access control and application of policy and regulation at the DII 'blockchain layer' – in other words, at the point of network connection. This is because DLT is a technology that records information or functions based on parameters set by an authorised authority. Authorised entities could be allowed to make requests of the network (e.g. not allowing a phone to connect or blocking content) and this command could be quickly shared across the network.

For example, China's Social Credit system is based on the cooperation of government agencies and corporations to collect, aggregate and analyse data. An internet based on DLT, which automatically collects and shares data with designated entities, would streamline this task. Use of DLT in these ways could result in harmful impacts on human rights such as privacy and freedoms of association, expression, thought and assembly (Liang et al. 2018; Al-Saqaf and Seidler 2017; Bernal 2016).

There is a common misconception that DLTs will help limit surveillance through encryption and decentralised control. However, placing DLT at the centre of internet technologies engenders regulatory and human rights issues, including data processing, retention and immutability (Article 19 2019). For example, in a Chinese model, governments (or state-owned entities) are likely to have 'ownership' and control over DLT, and thus the processing of data. DLTs can facilitate mass surveillance by acquisition and tracking of individuals' data (e.g. IP addresses (European Parliament and Council of European Union 2016, sec. 30) through assigned IDs with a digital ledger, potentially preventing anonymity online. This ledger could be shared with relevant authorities or broken by allowing third party access (e.g. government).

Using DLT as a central element of internet infrastructure requires acknowledgement of complex security and trust concerns (Scheier 2019) – in contrast to the inherent trust and security claimed by Chinese delegates (Lu, Tong, and Zhu 2019). It is not uncommon for language of 'trust' to replace 'security' in Chinese DII-related discussions. This is concerning because it indicates that the principle of 'security by design' – at least in the Western context – is not being adopted in DII's development. In the long term, this could negatively impact cybersecurity globally.

4.4. Network 2030 and ITU-T

China is also using the banner 'Network 2030' to advocate for DII, through a Focus Group[23] established in July 2018. The purpose of an ITU-T Focus Group is to see if there is enough member interest to create work in a new area. The remit of this Focus Group is directly related to DII and includes the identification of technical capabilities required for networks (e.g. 5G and 6G) including 'new communication mechanisms', network architecture, and functionality ("Focus Group on Technologies for Network 2030" n.d.).

Focus Group Network 2030, chaired by Huawei, is due to complete its work by October 2020. Output that is expected is a report that includes the technical details of the infrastructure, terms and definitions and the delivery time plan for standardisation.[24] Additionally, the timing is perfect, as the new structure of the ITU-T will be decided at the World Telecommunication Standardisation Assembly (WTSA) meeting in November 2020 where China will likely be lobbying for a dedicated space to legitimately explore, and standardise, DII technologies like New IP. However, the work of the Focus Group and the technologies it is proposing are too nascent for standardisation (e.g. 'holographic-type communications') although the deliverables may be used to streamline standards development (FG NET-2030 2019).

To date, Network 2030 work has been high level, but in October 2019 Huawei presented 'New IP' as a new type of network architecture which is data-centric and converges fixed mobile and satellite technologies ("Focus Group on Technologies for Network 2030", n.d.). The technical details had been presented at a meeting of ITU-T Study Group Chairs and advisory group (TSAG) a month previously[25], with specific proposals for a 'future' internet architecture. The proposal argued for a long-term work plan to develop a top-down network design that would place the ITU-T in a guiding role for future global internet developments (Huawei 2019).

Although the Focus Group has yet to conclude, Chinese delegations are already proposing new work items in the ITU to advance Network 2030. Examples include work in Study Group 11 on transport layer, network control and management, and signalling and protocols in New IP networking ("SG11: Signalling Requirements, Protocols, Test Specifications and Combating Counterfeit Products" n.d.). Proposals to Study Group 13 focus on a 'decentralized trustworthy network infrastructure' ("SG13: Future Networks, with Focus on IMT-2020, Cloud Computing and Trusted Network Infrastructures" n.d., 13). If adopted, these work items would significantly quicken standardisation of technologies specifically advertised to offer alternative solutions to today's global internet and support a multilateral form of internet governance.

4.5. Forum shopping and duplication

The issues associated with the ITU-T are not isolated. There is increased Chinese participation across other SDOs. China's drive to internationalise national standards, be a global technological super power and become a competitor to the US in developing and developed markets (Schneider-Petsinger et al. 2019) means that China regularly forum shops or duplicates effort to develop its standards. Importantly, these discussions need to take place in appropriate SDOs and internet governance fora within the context of existing internet technologies, including interoperability and backwards compatibility.

Being member-driven and industry-led, in the ISO, the default is that work will begin on a proposed topic unless there is serious objection. Experts in international SDOs have seen first-hand the forum shopping effort exercised by China, particularly related to smart city standards[26]. For example, after developing a Chinese smart parking lots standard in the ITU-T, a strikingly similar Chinese work item was initiated in ISO[27]. It is unclear why Chinese delegates felt the need to duplicate the national standard in different forums.

W3C is an SDO focused on the development of web and application layer technologies. Chinese delegates are known for contributing technologies developed by the W3C to the ITU-T, but with slight modifications and a Chinese approach. The ongoing geopolitical tug of war between China and the US, and in particular the addition of Chinese entities on the US Entities List, will likely increase duplication of effort at the web application and operating system layers as China aims to be a serious competitor in the near future. This could lead to splintering at the internet application layer.

Unfortunately, forum shopping and duplication of effort also results in work progressing in inappropriate SDOs. For example, developing protocols like New IP makes Network 2030 better suited to the IETF where internet protocols are standardised. It is possible earlier versions were circulated at the IETF but not successfully initiated. A side session at IETF 106 (November 2019) indicated an appetite from Huawei to move the New IP work into the IETF – or coordinate with the ITU-T at minimum – once the Focus Group concludes. However, it is unclear how or if this could be done as no existing mechanism is in place. The logistical issues are now compounded by the ITU-T's interest in keeping work 'in-house' to carve out their place in future standards development and internet governance.

This brings to the fore increasingly important issues – how to identify where work belongs, how to keep it in the correct forum and how to reinforce existing forums' ongoing relevance as the internet evolves. For instance, the IETF may consider how to fold in China's Network 2030 research without rushing to standardise something that is not yet a proven technology, or risk losing this chance to less appropriate and more political forums like the ITU-T.

5. Splinternet

5.1. Impact on a norms-based, predictable, secure and open cyberspace

The alternate technologies being standardised have the potential to break the global, free and interoperable internet into two or 200 distinct intranets. This differs from other value-driven incarnations of a splintering internet (O'Hara and Hall 2018) in that this entails a technological decoupling and would have implications throughout the internet layer stack. However, there is no clear consensus on how this would happen in practice.

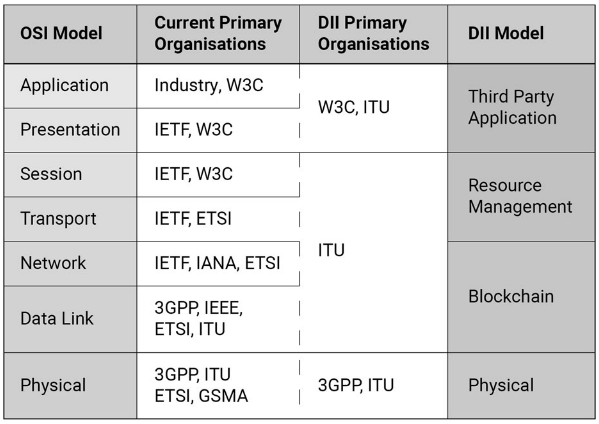
Most experts do not believe the aim is two non-interoperable internets (Woo and Fitch 2020). Firstly, globalised markets are too intertwined to completely sever ties, and China hopes to expand into developed markets. Secondly, a severing of those ties could lead to mass unrest in countries that take such an approach – something to be avoided. Yet even a fracture in the underlying technologies of the internet will make it more difficult for like-minded countries and other stakeholders to support strong and resilient collective defences relying on today's tools. The emergence of DII could significantly upset the internet landscape, threatening the norms-based, predictable, secure and open cyberspace.

If China's alternative technologies are successful, a new DII will not require existing internet governance organisations (e.g. IGF, ISOC), technical coordinators (e.g. IANA), or industry-led standards (e.g. IETF, W3C). Instead, alternative technologies will rely on Chinese national standards, bootstrapped to international standards through forums like the ITU, ISO and IEC, and governed through the ITU's multilateral structure. In this fragmented environment, the role of stakeholders supporting the free and open internet becomes more difficult as it will not have the stability of one cyber governance ecosystem, instead there could be 'Western' and 'Eastern' systems (see Figure 2). The 'Eastern' system would consolidate technical standardisation (along with version control and thus internet evolution) with internet governance of resources such as identifiers within an intergovernmental system (Table 2).

Instead of multistakeholder forums, China prefers to use 'discursive power' to influence global governance (Schneider-Petsinger et al. 2019). Ideally, China employs discursive power in a multilateral organisation with which China has a long relationship and reinforces the role of governments in regulating the internet, has more authoritative decision-making than multistakeholder forums like ICANN and moves governance out of the reach of industry, civil society and academia (Negro 2019; Article 19 2017). In essence, the multilateral ITU – the favoured location for governments looking to exert more authoritarian control over the Internet and apply 'UN bloc politics' (Lazanski 2019; Nye and Joseph 2014).

Nevertheless, there is risk, particularly for the West, if this approach is taken. For instance, the possibility of China locking customers into a digital walled garden for a technological generation – just enough time for what remains of Western competition to die off in certain markets (e.g. technical equipment/infrastructure) (Hoffmann, Bradshaw, and Taylor 2019). This would also widen the digital and human rights divide between Western nations and those adopting DII technologies. The attraction of DII technologies for some regimes is that they could enable countries to decouple or disconnect from the current global internet, temporarily or permanently, thus disenfranchising their citizens from global communication, access to information and trade. China is already achieving these aims to an extent with the Great Firewall, but DII's centralising technologies will make these tools more globally accessible because they will be international standards.

The ability to isolate some or all of a national network, while remaining connected to the global internet engenders new tools for offensive and defensive capabilities in cyberspace. There is a need to understand the complexities and potential risks of innovative abilities to decouple, isolate and attack networks using different technologies so that



OSI Model	Current Primary Organisations	DII Primary Organisations	DII Model
Application	Industry, W3C	W3C, ITU	Third Party Application
Presentation	IETF, W3C		
Session	IETF, W3C	ITU	Resource Management
Transport	IETF, ETSI		
Network	IETF, IANA, ETSI		Blockchain
Data Link	3GPP, IEEE, ETSI, ITU		
Physical	3GPP, ITU ETSI, GSMA	3GPP, ITU	Physical

Figure 2. Primary governance organisations by internet layer.

Table 2. Primary governance organisations by internet layer.

OSI Model	Currenet Primary Organisations	DII Primary Organisations	DII Model
Application	Industry, W3C	W3C, ITU	Third Party Application
Presentation	IETF, W3C		
Seesion	IETF, W3C	ITU	Resource Management
Transport	IETF, ETSI		
Network	IETF, IANA, ETSI		Blockchain
Data Link	3GPP, IEEE, ETSI, ITU		
Physical	3GPP, ITU, ETSI, GSMA	3GPP, ITU	Physical

governments and industry can build capacity among like-minded allies supporting a free, open and secure cyberspace and improve resilience to new threats. At an operational level, there is a need to understand how new technology could break foundational elements of the global internet, such as the root zone and the internet's hitherto universal systems of unique identifiers.

In essence, standardising DII will increase the threat landscape by introducing new security uncertainties across the stack. DII reconceptualizes security, focusing on 'trust' in the network in place of layered security by design. Analysis is required to understand what security should look like in DII, and where and how to ensure best practices are adopted.

Multiple versions of internet technologies undermine the predictability of cyberspace, negatively impacting international cooperation reinforcing a norms-based, secure and open cyberspace. Existing processes to develop norms for responsible state behaviour in cyberspace such as the UN GGE could be disrupted. Furthermore, it will be more difficult to share best practices and proven solutions to cybersecurity-related issues if fundamentally divergent or non-interoperable technologies are being used in different environments. There should be a review as to whether existing (and developing) norms and best practices will be fit for purpose in a world with multiple options of internet infrastructures and governance models.

5.2. Selling the Chinese model

Chinese technologies are intended for the global marketplace, particularly countries that share similar authoritarian views on micromanagement, multilateral internet governance and centralised technology. China's strategic position with respect to technological innovation is not only indicative of the drive to be a major global technology supplier (Zenglein and Holzmann 2019), but also the ambition to unlock untapped markets using technologies protected under international trade law, especially through the Belt and Road Initiative (BRI) and the ever-expanding Digital Silk Road (Kuo and Kommenda n.d.; World Economic Forum 2018). Although countries relying heavily on Western aid may not adopt Chinese vendors due to the risks that would pose (Liang et al. 2018), in the Pacific region China has recently wrested a number of small nations from Australian influence using BRI development and financial tactics (*The Economist 2020*).

Support for the Chinese model comes from strategic partnerships based on mutual interests. Many are recipients of Belt and Road Initiative investment and many are classified as developing countries. Others include Russia and Saudi Arabia, both engaged in the ITU (McCarthy 2019; Nye and Joseph 2014) China and Saudi Arabia recently signed 35 investment agreements, including smart city development, at an investment forum (Invest Saudi 2019).

China has a long-term strategy and is marketing what it sees as the future – a new internet. It is seeking support now to carry out the standards development that is required in the near future and laying groundwork for the market access to follow.

6. Conclusion

China is promoting a vision of today's internet that is centrally governed by Western institutions, not inclusive, and which penalises those that are not historically part of the global internet governance community. The Chinese version of a 'decentralized internet infrastructure' and its 'New IP', is billed to address these issues by reconfiguring basic elements of the internet such as trust mechanisms (e.g. public key infrastructure, use of encryption), the name space (i.e. the Domain Name System (DNS)), and internet protocols via a multilateral forum. It could also restructure the concept of internet layers, and move away from the internet's 'best effort' principle (Li 2018). Technical standards being developednow are being used to legitimize this approach and the supporting multilateral governance model.

In doing so, China has appropriated current tropes in international policy discussions – concerns over privacy and encryption, or the rapid concentration of the internet's technical and application layers into the hands of a few players – to create a perception of necessity for DII and New IP's 'decentralized' technologies because Western internet governance institutions have failed to address these issues.

A closer look at the technical proposals reveals that they would in fact lead to more centralised (i.e. government) control over networks and users' data and would imply a multilateral governance system for the Internet through the ITU. This approach disregards the multistakeholder groups currently working to address concerns related to issues like internet consolidation and 'encrypted everything'. It is also apparent that China is sure of an international market for its technologies through outreach and development initiatives such as the Digital Silk Road, under the protection of international standards and WTO trade rules. Ultimately governments will be supplied with the tools they need to create an internet with more control over their citizens. We have started to see examples already in China with the Social Credit system and use of surveillance technologies in response to the coronavirus outbreak (Mozur, Zhong, and Krolik 2020).

At a minimum, we can expect new technologies, whether Western or Chinese, to contribute to the potential splintering of the internet's most foundational and unifying elements, such as technical standards. Technological splintering could include networks and architectures, protocols, applications or even devices. Through analysis of China's participation in SDOs, we can see where splintering might occur as the DII and New IP initiatives being socialised move towards a network-centric and centrally micromanaged architecture based on alternate technologies.

For like-minded stakeholders supporting a norms-based, secure and open cyberspace, this translates into a restructuring of security and trust on the internet and an adverse impact on the alliance's ability to protect and defend its networks. A proliferation of alternate internet technologies will increase the internet's threat landscape, decrease predictability and potentially destabilise existing and future norms for responsible state behaviour in the online environment.

There is an urgent need for governments to intensify their collaboration and coordinate with like-minded stakeholders (e.g. industry, academia and civil society) through multistakeholder mechanisms to engage strategically in standards development and communicate a clear message globally.

In light of the current direction of travel of China, we have four key recommendations:

- Like-minded countries should create a Strategic Standards Group (SSG) for the sharing of information, discussion on approaches to the making of global standards and analysis of forthcoming standards. The SSG should leverage stakeholder expertise including industry, academia and civil society to build capacity and there should be ongoing coordination with these stakeholders, as well as other experts in strategy development and execution, and human rights.
- Like-minded stakeholders should work together to create and amplify a unified approach and cohesive message related to the benefits of one, free and open internet for users, innovators and governments.
- Like-minded stakeholders should work together to promote the adoption of best practices and *internationally recognised* standards. Like-minded governments in particular may play a role in identifying and promoting internationally recognised standards and/or those standards which have not been formally recognised, or contain concerning content identified by, allies.
- Stakeholders should engage in ongoing review of global and regional multistakeholder internet governance and standards forums to assess successes and failures with the aim to strengthen these forums and promote open dialogue to address complex issues at the intersection of technology and policy. This includes the politics of standards, their impact on policy and human rights, and engagement with relevant stakeholders who might not otherwise be involved (Table 3).

Table 3. Work Items in ITU-T and their Relationship.

Work item information				Related to		
Title	Work item	Study group	Question	DLT	Identity	Network 2030
O/11 Integrated space-terrestrial network signalling and protocols in new IP networking; P/11 Protocols for the control and management of high precision and deterministic IP	New work item questions for 2021-24	11	New			X
Framework and requirements of Decentralised Trustworthy Network Infrastructure	Y.DNI-fr	13	2	X		X
Requirements for distributed ledger systems	F.DLS	16	22	X		
Architecture for a name resolution service in information centric networks	H.ICN-NRArch	16	21		X	
Identification mechanism for unmanned aerial vehicles using object identifiers	X.677 (ex X.uav-oid)	17	11		X	
Decentralised IoT communication architecture based on information centric networking and blockchain	Y.dec-IoT-arch	20	3	X		
Reference framework of converged service for identification and authentication for IoT devices in decentralised environment	Y.IoT-CSIADE-fw	20	6		X	
Also see Focus Group Network 2030						X

Notes

1. For example, the Telecommunications Standards Advisory Group meeting in September 2019. See Contribution 83, *'New IP, Shaping Future Network': Propose to initiate the discussion of strategy transformation for ITU-T.*
2. See, for example, *Google v AEPD and Mario Costeja Gonzalez (ECJ C-131/12, 2014), Digital Rights Ireland CJEU C-293/12 and C-594/12, and Maximillian Schrems v Data Protection Commissioner* (CJEU, C-362/14, Oct 2015).
3. These companies mainly focus on developing Chinese technologies for data, information and cloud security.
4. For example, see TSAG Contribution 83, entitled 'New-IP-shaping future Network' (Huawei, September 2019).
5. The Budapest Convention has been ratified by 20 non-members of the Council of Europe on 6 continents including the US, Japan, Israel, Ghana, Australia and Chile. While Russia is the only member to not have signed or ratified the treaty (Council of Europe n.d.).
6. Komaitis, Konstantinos, @kkomaitis, Tweet, *This is how countries voted at Russia's recent #cybercrime resolution ….* 30 December 2019, 5:11pm. https://twitter.com/kkomaitis/status/1211696440340144128
7. For example, see SG13 work item 'Mechanism of deep packet inspection applied in network big data context' (Y.bDPI-Mec), base text TD507-WP2.
8. This paper uses the 7 layer Open Systems Interconnection (OSI) model developed by the International Organisation for Standards (ISO) (Cloudflare n.d.). Network access is managed by the data link layer which controls how devices connect and the identification of protocols and data formats. The network layer, also known as the internet layer, uses protocols known as TCP/IP to route packages. In DII this would be New IP.
9. To date the foundational technologies of the internet run on the 'best effort' principle, meaning that there is no guaranteed quality of service or data delivery. This helps to keep the internet standards lightweight and interoperable. However, China would like to place greater focus on quality of service and latency requirements in core technologies.
10. It is important to note the differentiation between the use of particular terms in diplomatic circles versus technology environments. As language is transferred between these spheres, and with different (and often loaded) meanings, this can lead to general misunderstandings and opportunistic manipulation. In this case, 'decentralized' is a primary example.
11. 3GPP, IETF and others are multistakeholder and primarily industry-led because industry has incentives to create standards from technical protocols that they are currently using in their networks or products.
12. Although academia and civil society organisations such as human rights defenders may join the ITU, this is largely in observer status and hindered by the prohibitive cost of the ITU's 'pay to play structure'. However, stakeholders may join national delegations open to a multistakeholder approach.
13. For example, Noah Luo of Huawei Technologies is currently Chair of ITU-T SG16 (Multimedia). Huawei employees were also the chairs of recently closed ITU-T focus groups on DLT (FG-DLT) and data processing and management (FG-DPM).
14. For instance, the ITU Secretary General is Houlin Zhao, and the president of IEC is Yinbiao Shu.
15. As mentioned above, according to discussions in the ISO with the Chinese delegation in November 2019, the report is due out in spring 2020. See (SESEC 2018, 2020; "China Standard 2035" 2018; Seaman 2020).
16. Study Group 20 on IoT, Study Group 17 on Security and Study Group 2 on Operational Aspects, including numbering.
17. The Russian government has deployed DOA to create a repository of mobile phones. However, the deployment still requires the use of current identifiers like the IMEI and MAC address in order to actually identify mobile phones (Pirmagomedov 2018). This is likely to be the way that Russia is registering all mobile phones after passing a law in 2019 mandating mobile phone registration in the country.

18. Alibaba (China) Co., Ltd., MIIT, SG17 Contribution 720, Proposal on a new work item: *A Decentralized Framework for Object Identifier Resolution,* September 2019.
19. See also TSAG Contribution 83, entitled 'New-IP-shaping future Network' (Huawei, September 2019).
20. Blockchain is one particular implementation of DLT technology. There are many versions of blockchain. DLT and blockchain are not synonymous.
21. For example, see SG17 work item X.dlt-sec, *Security considerations for using distributed ledger technology data in identity management*.
22. Study Group 13 on Future Networks meeting, Contribution 693.
23. Focus Groups are open for participation by non-members of the ITU, and do not have binding outputs (i.e. they do not create or agree standards).
24. See https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx for current draft report document. Accessed 3 June 2020.
25. September 2019 TSAG meeting, Contribution 83.
26. Another example of forum shopping is a rejected new work item proposal in ITU-T SG17 on CCTV and surveillance. A similar work proposal was later accepted in the ISO JTC1/SC27 and revisions to ISO/IEC 27032 are now underway.
27. See smart parking lot standard ITU-T Y.4456 and similar work in ISO TC268/SC1.
28. China is the only country to have mandated the use of IPv6 thus far.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Stacie Hoffmann Stacie advises industry, policy makers, regulators, and civil society on the intersection of technology and policy. Her areas of expertise include cyber and information security, emerging technologies, and technical standardisation. She is an experienced researcher, writer, and speaker. Previously, Stacie has worked on 5G/mobile technology, the Internet of Things (IoT), Artificial Intelligence (AI), Over-the-Top (OTT) services, data protection, and the Internet addressing (DNS) ecosystem. She is a regular commentator on broadcast news, including BBC World News, is a CESG certified Cyber Security/Information Assurance Auditor Practitioner and holds a certificate in ISO/IEC 27001 Information Security Management Principles.

Dominique Lazanski is a London-based international Internet and cybersecurity policy and standards consultant. She is the Director of her own company, Last Press Label. She has worked for companies like Yahoo!, eBay and Apple as well as for the UN. She is widely published and has spoken on cyber policy issues across the globe. She has a BA from Cornell University, master's degrees from the London School of Economics and the University of Bath and she is current finishing her PhD.

Emily Taylor CEO, Oxford Information Labs Limited. Associate Fellow of Chatham House International Security. Editor, Journal of Cyber Policy (Routledge, Taylor & Francis). Qualified lawyer (non-practising), specialising in cybersecurity, internet law and governance including data protection, intellectual property and surveillance laws. Author of numerous reports on cybersecurity-related issues. Devised and teach compact seminars and master classes on internet law for regulators and post-graduate students. Sought-after chair, moderator, trainer and commentator on cyber issues, including for broadcast news, the Guardian, Slate, Wired, SC Magazine and New Statesman, and the BBC Now Show.

References

5G PPP Architecture Working Group. 2019. "View on 5G Architecture." *5G PPP*. https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf.

Al-Saqaf, Walid, and Nicolas Seidler. 2017. "Blockchain Technology for Social Impact: Opportunities and Challenges Ahead." *Journal of Cyber Policy* 2 (3): 338–54. doi:10.1080/23738871.2017.1400084.

Article 19. 2017. "Privacy: Yes! But Not at the ITU." Article 19. October 16. https://www.article19.org/resources/privacy-yes-but-not-at-the-itu/.

Article 19. 2019. "Blockchain: Technology Alone Cannot Protect Freedom of Expression." Article 19. July 1. https://www.article19.org/resources/blockchain-technology-alone-cannot-protect-freedom-of-expression/.

Association of Equipment Manufacturers. 2018. "China Launches New Enterprise Standard Law." *Association of Equipment Manufacturers*, January 26. https://www.aem.org/news/china-launches-new-enterprise-standard-law/.

"Belt and Road Initiative". 2018. *The World Bank*, March 29. https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative.

Bennett, Richard. 2019. "DoH Creates More Problems Than It Solves." *CircleID*, September 16. http://www.circleid.com/posts/20190916_doh_creates_more_problems_than_it_solves/.

Bernal, Paul. 2016. "Data Gathering, Surveillance and Human Rights: Recasting the Debate." *Journal of Cyber Policy* 1 (2): 243–64. doi:10.1080/23738871.2016.1228990.

Bursztein, Elie. 2017. "Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis." *Cloudflare*, December 14. https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/.

Cave, Danielle, Alex Joske, Fergus Ryan, and Elise Thomas. 2019. *Mapping China's Tech Giants*. Barton: Australian Strategic Policy Institute. https://chinatechmap.aspi.org.au/.

Cerf, V., and R. Kahn. 1974. "A Protocol for Packet Network Intercommunication." *IEEE Transactions on Communications* 22 (5): 637–48. doi:10.1109/TCOM.1974.1092259.

Chen, Yin. 2006. "Panel 1 Setting the Scene." Presented at the Internet Governance Forum, Athens, Greece, October 30. https://www.intgovforum.org/cms/IGF-Panel1-301006.txt.

Chen, Yin. 2009. *#IGF09 - Chen Yin - Taking Stock and Looking Forward*. https://www.youtube.com/watch?v=Ou1cAUXOluc.

Cheung, Tai Ming. 2018. "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities." *Journal of Cyber Policy* 3 (3). doi:10.1080/23738871.2018.1557234.

"China Explores Approaches to Improve Standardization Governance". 2019. *Seconded European Standardization Expert in China* (blog). November 22. https://www.sesec.eu/china-explores-approaches-to-improve-standardization-governance/.

"China Standard 2035". 2018. CNStandards.net. http://www.cnstandards.net/wp-content/uploads/2019/03/China-Standard-2035.pdf.

Council of Europe. n.d. "Details of Treaty No. 185 Convention on Cybercrime." *Council of Europe.* Accessed 2 March 2020. https://www.coe.int/en/web/conventions/full-list.

Creemers, Rogier. 2016. "National Cyberspace Security Strategy." *China Copyright and Media* (blog). December 27. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

Dai, Sarah. 2019. "China's Face-Scan Tech Now Stretches to Trash Cans and Public Housing." *South China Morning Post*, August 2. https://www.scmp.com/tech/policy/article/3020977/chinas-facial-recognition-mania-now-extends-public-housing-and-trash.

Deibert, Ron. 2015. "The Geopolitics of Cyberspace After Snowden." *Current History*. www.currenthistory.com/Deibert_CurrentHistory.pdf.

Delfs, Arne. 2018. "Germany Toughens Stance and Blocks China Deal." *Bloomberg.Com*, August 1. https://www.bloomberg.com/news/articles/2018-08-01/germany-said-to-block-company-purchase-by-chinese-for-first-time.

De Tomas Colatin, Samuele. n.d. "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace." *CCDCOE*. Accessed 2 March 2020. https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/.

DeNardis, Laura, ed. 2011. *Opening Standards: The Global Politics of Interoperability*. Boston: MIT Press.

DONA Foundation. "About DONA". n.d. *DONA Foundation.* Accessed 2 March 2020. ' https://www.dona.net/aboutus.

Dourado, Eli. 2016. "How Russia and the UN Are Actually Planning to Take Over The Internet." September 12. https://thehill.com/blogs/congress-blog/technology/295320-how-russia-and-the-un-are-actually-planning-to-take-over-the.

Durand, Alain. 2019. "Digital Object Architecture and the Handle System." *ICANN*, October 14. https://www.icann.org/en/system/files/files/octo-002-en.pdf.

EDDI. "Encrypted DNS Deployment Initiative". 2019. Encrypted DNS Deployment Initiative. https://www.encrypted-dns.org.

European Parliament and Council of European Union. 2016. "General Data Protection Regulation." EUR-Lex, 27 April 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:02016R0679-20160504.

Feng, Emily. 2018. "China Steps up Surveillance on Xinjiang Muslims." *Financial Times*, July 18. https://www.ft.com/content/c610c88a-8a57-11e8-bf9e-8771d5404543.

FG NET-2030. 2019. "New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis." International Telecommunication Union. https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Deliverable_NET2030.pdf.

"Focus Group on Technologies for Network 2030". n.d.-a. *International Telecommunication Union*. Accessed 27 January 2020a. https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx.

"Focus Group on Technologies for Network 2030". n.d.-b. UK 5G Innovation Network. Accessed 3 March 2020b. https://uk5 g.org/attend/focus-group-technologies-network-2030/.

Foremski, Paweł, and Oliver Gasser. 2019. *DNS Observatory: Monitoring Global DNS for Performance and Security*. Prague, Czech Republic: Powerpoint Presentation, IETF Meeting. March. https://datatracker.ietf.org/meeting/104/materials/slides-104-maprg-dns-observatory-monitoring-global-dns-for-performance-and-security-pawel-foremski-and-oliver-gasser-01.

"General Data Protection Regulation. 2016. *EUR-Lex*. April 27. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:02016R0679-20160504.

Global Forum on Cyber Expertise. n.d. "About the GFCE." *Global Forum on Cyber Expertise*. Accessed 7 May 2020. https://thegfce.org/about-the-gfce/.

Global Partners Digital. n.d. "ITU Explainers: Digital Object Architecture." Global Partners Digital. Accessed 2 March 2020. https://www.gp-digital.org/wp-content/uploads/2017/10/itu-doa2.pdf.

Gross, Anna, Madhumita Murgia, and Yuan Yang. 2019. "Chinese Tech Groups Shaping UN Facial Recognition Standards." *Financial Times*, December 1. https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

"GSTA and IP Unity Glenayre Deploy Voice Portal Solution for China Telecom". 2007. *RealWire*, June 19. https://www.realwire.com/releases/gsta-and-ip-unity-glenayre-deploy-voice-portal-solution-for-china-telecom.

Hakmeh, Joyce, and Allison Peters. 2020. "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet." *Council on Foreign Relations*, January 13. https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

Hern, Alex. 2015. "China Introduces Its Own 'Snooper's Charter.'" *The Guardian*, December 29. sec. Technology. https://www.theguardian.com/technology/2015/dec/29/china-introduces-its-own-snoopers-charter.

Hewett, Jennifer. 2020. "UK Splits from Australia and US over Huawei." *Australian Financial Review*, January 27. sec. telecommunications. https://www.afr.com/companies/telecommunications/uk-splits-from-australia-and-us-over-huawei-20200127-p53v5c.

Hillman, Jonathan. 2018. "China's Belt and Road Initiative: Five Years Later." *Center for Strategic & International Studies*. https://www.uscc.gov/sites/default/files/Hillman_USCC%20Testimony_25Jan2018_FINAL.pdf.

Hitchens, Theresa, and Nancy W. Gallagher. 2019. "Building Confidence in the Cybersphere: A Path to Multilateral Progress." *Journal of Cyber Policy* 4 (1): 4–21. https://www.tandfonline.com/doi/abs/10.1080/23738871.2019.1599032.

Hoffmann, Stacie. 2019. "Understanding DNS Over HTTPS - DoH." August 19. https://oxil.uk/blog/understanding-dns-over-https-doh/.

Hoffmann, Stacie, Samantha Bradshaw, and Emily Taylor. 2019. “Networks and Geopolitics: How Great Power Rivalries Infected 5G.” *Oxford Information Labs*. https://oxil.uk/publications/geopolitics-of-5 g/.

Hsu, Kimberly, and Craig Murray. 2014. “China and International Law in Cyberspace.” US-China Economic and Security Review Commission Staff Report.

Huawei. 2018. “Huawei Blockchain Whitepaper: Toward a Trusted Digital World.” https://www.huaweicloud.com/content/dam/cloudbu-site/archive/hk/en-us/about/analyst-reports/images/4-201804-Huawei%20Blockchain%20Whitepaper-en.pdf.

Huawei. 2019. “New IP: Shaping the Future Network.” Presented at the ITU-T TSAG, Geneva, Switzerland, September. https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2019-09-30-itu-t-tsag-ietf-iab-ls-on-new-ip-shaping-future-network-attachment-3.pptx.

Huston, Geoff. 2019. “DNS Wars.” *CircleID*, November 5. http://www.circleid.com/posts/20191105_dns_wars/.

IETF. 2019. “IETF 106 Side Meetings.” *Internet Engineering Task Force*. https://trac.ietf.org/trac/ietf/meeting/wiki/106sidemeetings.

IETF. 2020. “IETF 106 Registration System.” *IETF*, March 3. https://www.ietf.org/registration/ietf106/attendance.py.

International Telecommunication Union. n.d. “ITU Mandate.” Accessed 27 January 2020. https://www.itu.int/en/about/Pages/whatwedo.aspx.

International Telecommunication Union. n.d. “Focus Group on Technologies for Network 2030.” Accessed 27 January 2020. https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx.

International Organization for Standardization. n.d. “SAC.” ISO. Accessed 2 March 2020. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/member/00/16/1635.html.

Invest Saudi. 2019. “35 Agreements Signed at Saudi-Chinese Investment Forum - News.” *Invest Saudi*, February. http://investsaudi.sa/en/node-2509/.

ISOC. 2019. “Consolidation in the Internet Economy.” Internet Society 2019 Global Internet Report. https://future.internetsociety.org/2019/.

“ITU Mandate”. n.d. *International Telecommunication Union*. Accessed 27 January 2020. https://www.itu.int/en/about/Pages/whatwedo.aspx.

“ITU-T TSAG C (2019-09-23)”. 2019. *International Telecommunication Union*. https://www.itu.int/md/T17-TSAG-190923-C/en.

“ITU-T Work Program Q8/17 2017–2020”. 2017. *International Telecommunication Union*. https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17&q=8.

Jiang, Sheng. 2019. “New IP Networking for Network 2030.” Presented at the Fifth ITU Workshop on Network 2030, International Telecommunication Union, October 15. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf.

Kennedy, Scott. 2017. “The Fat Tech Dragon: Benchmarking China’s Innovation Drive,” 29 August. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170829_Kennedy_FatTechDragon_Web.pdf?.6agddecKW.hKNzCkVYvvUSDsQCeK9mN.

Kobie, Nicole. 2019. “The Complicated Truth about China’s Social Credit System.” *Wired UK*, June 7. https://www.wired.co.uk/article/china-social-credit-system-explained.

Kuo, Lily, and Niko Kommenda. n.d. “What Is China’s Belt and Road Initiative?” *The Guardian*. Accessed 28 January 2020. http://www.theguardian.com/cities/ng-interactive/2018/jul/30/what-china-belt-road-initiative-silk-road-explainer.

Lazanski, Dominique. 2019. “Governance in International Technical Standards Making: A Tripartite Model.” *Journal of Cyber Policy* 4 (3): 362–79.

Li, Richard. 2018. “Towards a New Internet for the Year 2030 and Beyond.” Presented at the Third Annual ITU IMT-2020/5G Workshop and Demo Day, Geneva, Switzerland, July 18. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201807/Documents/3_Richard%20Li.pdf.

Liang, Fan, Vishnupriay Das, Nadiya Kostyuk, and Muzammil M. Hussain. 2018. “Constructing a Data-Driven Society: China’s Social Credit System as a State Surveillance Infrastructure.” *Policy & Internet* 10 (4): 415–53.

Light Reading. 2018. “Decentralized Internet Infrastructure (DII).” *Light Reading*, November 20. https://www.lightreading.com/blockchain/decentralized-internet-infrastructure-(dii)/v/d-id/747708.

Liu, Xuanzun. 2020. "Chinese Military Adopts New Rules against Cybersecurity Risks - Global Times." *Global Times*, February 19. https://www.globaltimes.cn/content/1180128.shtml.

Lu, Haiyang, Peishan Tong, and Rong Zhu. 2019. "Does Internet Use Affect Netizens' Trust in Government? Empirical Evidence from China." *Social Indicators Research*. December. doi:10.1007/s11205-019-02247-0.

Lynch, Colum. 2019. "China Seeks to Lead the U.N.'s Intellectual Property Organization, WIPO." *Foreign Policy*, November 26. https://foreignpolicy.com/2019/11/26/china-bids-lead-world-intellectual-property-organization-wipo/.

Manuel, Anja. 2017. "China Is Quietly Reshaping the World." *The Atlantic*, October 17. https://www.theatlantic.com/international/archive/2017/10/china-belt-and-road/542667/.

McCarthy, Kieron. 2019. "China and Russia Join to Battle 'illegal Internet Content,' Which Means What You Fear It Does." *The Register*, October 9. https://www.theregister.co.uk/2019/10/09/china_russia_internet_treaty/.

Miao, Ying. 2020. "Managing Digital Contention in China." *Journal of Cyber Policy* 7: 1–21. https://doi.org/10.1080/23738871.2020.1748079.

Mozur, Paul, Raymond Zhong, and Aaron Krolik. 2020. "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags." *The New York Times*, March 1. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

NATO. 2016. "Warsaw Summit Communiqué." NATO. http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NATO. 2019. "Cyber Defence." NATO. September 6. http://www.nato.int/cps/en/natohq/topics_78170.htm.

Negro, Gianluigi. 2019. "A History of Chinese Global Internet Governance and Its Relations with ITU and ICANN." *Chinese Journal of Communication* 13 (1): 1–18. doi:10.1080/17544750.2019.1650789.

"New IP Technologies". 2019. Draft 4. Shenzhen: Huawei. https://support.huawei.com/enterprise/en/doc/EDOC1000173015?section=j001.

Nye, Jr, and S. Joseph. 2014. "The Regime Complex for Managing Global Cyber Activities." CIGI, Chatham House. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Nykolas, Z. 2018. "DNS Market Share Analysis — Identifying the Most Popular DNS Providers." *Medium*, April 9. https://medium.com/@nykolas.z/dns-market-share-analysis-identifying-the-most-popular-dns-providers-80fefb2cfd05.

O'Hara, Kieron, and Wendy Hall. 2018. "Four Internets: The Geopolitics of Digital Governance," no. 206: 28.

Okano-Heijmans, Maaike, Frans-Paul van der Putten, and Louise van Schaik. 2018. "A United Nations with Chinese Characteristics? | Clingendael." December 18. https://www.clingendael.org/publication/united-nations-chinese-characteristics.

Pirmagomedov, Rustam. 2018. "Combating Counterfeiting in Russia. Key Challenges." *ITU*, July 23. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180723/Documents/6_Rustam%20Pirmagomedov.pdf.

Radu, Roxana, and Michael Hausding. 2020. "Consolidation in the DNS Resolver Market – How Much, How Fast, How Dangerous?" *Journal of Cyber Policy* 5 (1): 1–19. doi:10.1080/23738871.2020.1722191.

Rashid, Fahmida Y. 2019. "The Fight Over Encrypted DNS: Explained." *IEEE Spectrum: Technology, Engineering, and Science News*, November 27. https://spectrum.ieee.org/tech-talk/telecom/security/the-fight-over-encrypted-dns-boils-over.

Roberts, Anthea, Henrique Choer Moraes, and Victor Ferguson. 2018. "Geoeconomics: The Chinese Strategy of Technological Advancement and Cybersecurity." *Lawfare*, December 3. https://www.lawfareblog.com/geoeconomics-chinese-strategy-technological-advancement-and-cybersecurity.

Rogers, David. 2016. "Digital Object Architecture." *Mobile Phone Security*, October 22. https://mobilephonesecurity.org/tag/digital-object-architecture/.

Rollet, Charles. 2019. "Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up." *IPVM*, November 11. https://ipvm.com/reports/hikvision-uyghur.

Rosenzweig, Paul. 2016. "China's National Cybersecurity Strategy." *Lawfare* (blog). December 27. https://www.lawfareblog.com/chinas-national-cybersecurity-strategy.

Rutkowski. 2020. "WTSA-2020: Reflecting on a Contemporary ITU-T Role." *CircleID*, February 15. http://www.circleid.com/posts/20200215_wtsa_2020_reflecting_on_a_contemporary_itu_t_role/.

Scheier, Bruce. 2019. "Blockchain and Trust." *Schneier on Security*, February 12. https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html.

Schneiderman, Ron. 2015. "International Standards Development Organizations Defined." In *Modern Standardization: Case Studies at the Crossroads of Technology, Economics, and Politics*, 1st ed., 253–66. John Wiley & Sons, Ltd. doi:10.1002/9781119043492.oth.

Schneider-Petsinger, Marianne, Dr Jue Wang, Dr Jie Yu, and James Crabtree. 2019. "US–China Strategic Competition: The Quest for Global Technological Leadership." *Chatham House*, November 7. https://www.chathamhouse.org/publication/us-china-strategic-competition-quest-global-technological-leadership.

Seaman, John. 2020. *China and the New Geopolitics of Technical Standardization*. Paris: French Institute of International Relations. January. https://www.ifri.org/en/publications/notes-de-lifri/china-and-new-geopolitics-technical-standardization.

SESEC. 2018. "Chinese Standards 2035, the Standardization Strategy Research Is Kicked off – Sesec.Eu." *Seconded European Standardization Expert in China*, May 24. https://www.sesec.eu/24-05-2018-chinese-standards-2035-the-standardization-strategy-research-is-kicked-off/.

SESEC. 2020. "SESEC IV Webinar 11: China Standards 2035 – Sesec.Eu." *Seconded European Standardization Expert in China*, June 2. https://www.sesec.eu/events/china-standards-2035/.

SESEC Team. 2017. "Standardization Law of People's Republic of China: Issued on 4 November 2017." *Seconded European Standardization Expert in China Project*. https://www.sesec.eu/app/uploads/2018/01/Annex-I-China-Stadnardization-Law-20171104.pdf.

"SG11: Signalling Requirements, Protocols, Test Specifications and Combating Counterfeit Products". n.d. *International Telecommunication Union*. Accessed 29 January 2020. https://www.itu.int/en/ITU-T/studygroups/2017-2020/11/Pages/default.aspx.

"SG13: Future Networks, with Focus on IMT-2020, Cloud Computing and Trusted Network Infrastructures". n.d. *International Telecommunication Union*. Accessed 29 January 2020. https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.aspx.

Shahbaz, Adrian, and Allie Funk. 2019. "Freedom on the Net 2019: The Crisis of Social Media." *Freedom House*. https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media.

Sharp, Chip. 2016. "Overview of the Digital Object Architecture (DOA)." *Internet Society* (blog), October 25. https://www.internetsociety.org/resources/doc/2016/overview-of-the-digital-object-architecture-doa/.

Song, Steve. 2018. "Internet Drift: How the Internet Is Likely to Splinter and Fracture." *Digital Freedom Fund* (blog). https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/.

Swinhoe, Dan. 2019. "China's MLPS 2.0: Data Grab or Legitimate Attempt to Improve Domestic Cybersecurity?" *CSO Online*, October 28. https://www.csoonline.com/article/3448578/chinas-mlps-20-data-grab-or-legitimate-attempt-to-improve-domestic-cybersecurity.html.

Taylor, Emily, and Joyce Hakmeh, eds. 2020. "Special Issue: Consolidation of the Internet." *Journal of Cyber Policy*. *Taylor & Francis* 5 (1). https://www.tandfonline.com/toc/rcyb20/current.

Taylor, Emily, and Stacie Hoffmann. 2019. "EU-US Relations on Internet Governance." *Chatham House.* https://oxil.uk/publications/eu-us-relations-internet-governance/2019-11-14-EU-US-Relations-Internet-Governance2.pdf.

The Economist. 2020. "The Digital Side of the Belt and Road Initiative Is Growing," February 6. https://www.economist.com/special-report/2020/02/06/the-digital-side-of-the-belt-and-road-initiative-is-growing.

United States Information Technology Office. n.d. "China Publishes First National Cybersecurity Strategy." United States Information Technology Office. Accessed 2 March 2020. http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy.

UNODA. n.d. "Developments in the Field of Information and Telecommunications in the Context of International Security." *UN Office for Disarmament Affairs.* Accessed 3 March 2020. https://www.un.org/disarmament/ict-security/.

W3Techs. 2020. “Usage Statistics and Market Share of SSL Certificate Authorities for Websites.” *W3Techs*. March 2020. https://w3techs.com/technologies/overview/ssl_certificate.

“Welcome to SAC”. n.d. *Standardization Administration of the P.R.C.* Accessed 16 January 2020. http://www.sac.gov.cn/sacen/.

“What Is The OSI Model?”. n.d. *Cloudflare*. Accessed 2 March 2020. https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/.

Woo, Stu, and Asa Fitch. 2020. “The Great U.S.-China Tech Divide.” *The Wall Street Journal*, January 20. https://www.wsj.com/articles/the-great-u-s-china-tech-divide-11579542441.

World Economic Forum. 2018. “China Is Building a New Silk Road, and This One Is Digital.” *World Economic Forum*, August 18. https://www.weforum.org/agenda/2018/08/china-is-building-a-new-silk-road-and-this-one-s-digital/.

World Trade Organization. n.d. *Agreement on Technical Barriers to Trade*. Geneva: World Trade Organization. https://www.wto.org/english/docs_e/legal_e/17-tbt.pdf.

Wu, Tim. n.d. “Network Neutrality FAQ.” *TimWu.Org*. Accessed 2 March 2020. http://www.timwu.org/network_neutrality.html.

Zenglein, Max J., and Anna Holzmann. 2019. *Evolving Made In China 2025: China’s Industrial Policy in the Quest for Global Tech Leadership*. Berlin: Mercator Institute for China Studies. https://merics.org/en/report/evolving-made-china-2025.

Zhao, Houlin. 2017. “ITU Council 2017: State of the Union Address.” Presented at the ITU Council 2017, Geneva, Switzerland, May 15. https://www.itu.int/en/osg/speeches/Pages/2017-05-15.aspx.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

Appendix 1

ITU-T focus areas and sample work items potentially related to decentralised internet infrastructure and New IP.

Standards development and research on DII-related technologies at the ITU has focused on areas including:

- Network technologies and architecture;
- Fine grained control for authentication, authorisation, and access controls;
- Naming, numbering and addressing, and IPv6[28] in particular; and
- A move away from the internet’s ‘best effort’ principle and increasing focus on quality of service and reducing latency.

These focus areas have manifested in the ITU-T under different guises and study groups (SGs). For instance:

- Protocols and test specifications (SG11);
- Future networks and cloud (SG13);
- Multimedia (SG16);
- Security (SG17); and
- The Internet of things (IoT) and smart cities (SG20).

In the SGs there is focus on specific technologies linked to DII, such as:

- Object identifiers (OIDs);
- Distributed ledger technologies (DLT), including blockchain; and
- Network 2030.