China: strategic use of standards to further domestic and international ambitions

This response to the request for information on the **Study on People's Republic of China (PRC) Policies and Influence in the Development of International Standards for Emerging Technologies** document number 86 FR 60801 and NIST-2021-006 is filed on behalf of Dominique Lazanski, Emily Taylor, Carolina Caeiro and Kate Jones.

The authors of this response have more than 20 years' experience working in Internet governance, international and human rights law, cybersecurity and technical standards. Dominique Lazanski has participated in ITU-T Study Groups since 2013 and ITU major conferences since 2012. She also participate in ETSI and the IETF. Along with Stacie Hoffmann, Dominique Lazanski and Emily Taylor are co-authors of a paper, published in Chatham House's peer-reviewed Journal of Cyber Policy in 2020. The paper, **Standardising the splinternet: how China's technical standards could fragment the internet** (see https://www.tandfonline.com/doi/abs/10.1080/23738871.2020.1805482?journalCode=rcyb20) analyses the ways in which the Chinese government, Chinese academia and Chinese industry use their power and influence to attempt the standardisation of proposals that, if approved, would create an alternative, internet-like network that would depart from the Internet's current architecture and protocols. It would create one or more 'splinternets'. Chinese advocacy to support the introduction of so-called 'New IP' leverages two Western policy concerns – Internet security and the growing influence of US tech giants – and claims to solve them by introducing decentralized technologies and enhancing trust on the network through new identification methods. While there continues to be much uncertainty over exactly how the technical implementation of New IP would manifest, it appears that this alternative Internet infrastructure would introduce new controls at the level of network connection and enable bulk data collection, tracking of users and contents through the use of blockchain and permanent identifiers.

The Hoffmann, Lazanski and Taylor article highlights links between China's published strategies such as Made in China 2025, and (more recently) China Standards 2035. The choice of forum, the ITU, would create protections in the international trade of technologies built to New IP standards (if adopted), through the application of World Trade Organisation rules. Through the WTO's Agreement on Technical Barriers to Trade (TBT), technologies standardised through the ITU benefit from immediate clearance to be traded internationally. Thus attempts to standardize New IP can be seen in the context of China's Belt & Road initiatives as laying a pathway to international adoption of a different kind of internet, one that is designed to enable fine-grained controls of individuals and populations.

In 2021, Carolina Caeiro, Kate Jones and Emily Taylor co-authored a book chapter (forthcoming, Human Rights in a Changing World, to be published by Chatham House and Brookings Institution Press), entitled Technical Standards and Human Rights: The Case of New IP (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3907165). The paper concludes that New IP would have a significant impact on fundamental human rights. At its core, New IP would render the Internet an instrument for government control. Changes to the architecture of the network and link layers of the traditional stack would grant those entities involved in managing networks and nodes greater control over internet traffic and users. Far from guaranteeing greater security and privacy, incorporation of blockchain technologies into the Internet's core would become a technological way and a proxy for control by enabling governments and state owned network providers to share, gather, aggregate and analyze data . The distributed ledger characteristic of the blockchain core would provide an immutable record of all activities, and combined with adjustments to naming and addressing protocols, would facilitate surveillance, for example through the identification of an individual's browsing history.

As well as undermining the multi-stakeholder governance models for today's Internet unique identifiers, the New IP proposals would introduce identifiers described as 'bit strings' which are centrally administered and immutable – offering unparalleled tracing over the Internet through the creation of permanent records, such as browsing history. Additionally, the new system of identifiers would enable the disconnection of people, devices, or even regions that are deemed illegitimate, through what New IP depictions describe as the "shut off" protocol[1].

If deployed domestically within contexts of national programmes to use technology to control and monitor the behaviour or ethnic / religious characteristics of people, New IP would make human rights implementation contingent on those individuals meeting certain conditions or responsibilities. Social benefits and freedoms such as freedom of movement may be denied as a form of punishment in order to control behaviour. This is seen through China's social credit system.

The chapter tracks what has happened to the New IP proposals since they were rejected in the UN International Telecommunication Union (ITU-T). Large scale piloting appears to have started domestically in April 2021, with the announcement of a backbone network that will connect 40 leading universities to test what has been advertised as the "Internet of the Future".

Following push-back from multiple country delegations in ITU-T during 2020, including the UK, Norway, 21 EU member states, the European Commission, and several technical organisations, the original New IP proposals were rejected. However, there are signs of a new strategy: standardizing New IP in pieces. There is also evidence of forum shopping by China across different standards organisations and even a US patent application for decentralized blockchain DNS[2].

Over the last ten years, through her first-handed engagement in multiple standards development organisations, Dominique Lazanski has observed Chinese government, Chinese academia and Chinese industry participate in greater numbers and take advantage of their high level of attendance to take on influential leadership roles, especially in the ITU. This trend is highlighted in a recent paper, **Understanding China's Engagement in Technical Standards Bodies** by Fiona Pollock and Emily Taylor (https://oxil.uk/publications/2021-11-07-georgetown-university-china-engagement-technical-standards/) in Georgetown University's publication, Democracy & Society, Volume 18 2021.

In Lazanski's observation, there appears to be coordination between Chinese participants to support Chinese work items which are not necessarily of high quality, but reflect specific research projects or industry specifications. The result is that such specific work seeks to standardize very specific aspects of technologies which does not allow for interoperability or innovation. One of many examples is the

[1] 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.

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

work item **Framework of blockchain-based self-organization networking in IoT environments** or Y.BC-SON which is specific to blockchain, autonomous networking and IoT. The point of this is that standardising such things first allows for Chinese ideology to be embedded in technologies and also paves the way for patents and, potentially, patent payments to be made to Chinese entities. This ensures dependency in this and related technologies for years to come.

The authors of this response would welcome further discussion on these issues and look forward to working with you in the future.

Dominique Lazanski
Director
Last Press Label
dml@lastpresslabel.com

Emily Taylor
CEO, Oxford Information Labs
Editor, Journal of Cyber Policy (Chatham House)
emily.taylor@oxil.co.uk

Kate Jones
Associate Fellow, Chatham House

Carolina Caeiro
Academy Associate, Chatham House