An Analysis of China's Proposal to Control and Centrally Manage the Internet

Alan Dupont
Adjunct Professor, University of New South Wales

Abstract: Governments and telecommunications companies have invested heavily in measures designed to protect overall system security. But these measures may not be enough if China is successful in setting the rules and designing the architecture of a new internet, because the one-party state's internet vision reflects authoritarian values that are diametrically opposed to ours. China has suggested a radical change to the way the internet functions to the International Telecommunications Union. This would bake authoritarianism into the architecture underpinning the web, giving state-run internet service providers granular control over citizens' use. The authoritarian state's ability to monitor and control undersea fibre optic cables is emerging as a major national security issue for Australia and other democracies. The world could split into two separate information worlds, one led by the US and the other by China. A Balkanised internet is not in Australia's interest. We must engage with friends and allies to come up with a fit-for-purpose world wide web that is more efficient, secure, user friendly and compatible with democracy.

Keywords: Internet, security, China, 'Balkanisation', democratic alternative.

Our Wired World

Imagine trying to manage the impact of the coronavirus without the internet and a robust telecommunications sector. If we could not communicate and transact in real time, economic activity would grind to a halt and social contact would be even more difficult. And there would be no COVID-safe App, an important tool in the government's recovery strategy.

Already more wired than most nations, Australia's digital world is expanding rapidly as the coronavirus has forced business, schools, universities and government services online. Video conferencing platforms like Zoom are booming and the much-maligned National Broadband Network is finally starting to realise its potential. But if these networks were to become untrustworthy or disrupted for any length of time it would be hard for the country to function effectively.

http://doi.org/10.18080/jtde.v8n2.298

Fortunately, we are now much better informed and protected from many cyber threats. Passwords, anti-virus software and cyber security are firmly entrenched in our personal lives and business culture. Governments and telecommunications companies have invested heavily in measures designed to protect overall system security. But these measures may not be enough if China is successful in setting the rules and designing the architecture of a new internet, because the one-party state's internet vision reflects authoritarian values that are diametrically opposed to ours.

China's New Internet Protocol

China has suggested a radical change to the way the internet functions to the International Telecommunications Union, a United Nation's body established to standardise global telecommunications technologies, services and operations. The Chinese proposal envisages a different standard for core network technology called New IP (Internet Protocol) that it claims would make the internet more efficient and better structured for the digital age (Joseph, 2020).

Experts agree that the internet should be upgraded to deal with a world in which machines, as well as humans, are connected. And most countries accept that today's model of internet governance is broken and needs reform. But they do not agree on how a new internet should function. This has given China an opening to argue for an alternative internet that would replace the open, unified world wide web with a more fragmented, patchwork of national internets which China calls "cyber sovereignty".

Critics contend that New IP would bake authoritarianism into the architecture underpinning the web and give state-run internet service providers granular control over citizens' use. An investigation by the *Financial Times* found that the new protocol would require the network to have tracking features and a "shut-up command", which could enable governments to arbitrarily deny users access, a major departure from the current internet system which acts as an agnostic postman that simply moves data around (Gross & Murgia, 2020).

Acceptance of the proposal by the governing ITU at its November meeting in India would allow countries to choose the existing Western-designed internet or move to China's version. Many developing states in Asia, Africa and Latin America could choose the latter, which would help realise a long-term Chinese digital foreign policy goal — to entrench Chinese standards and technology as the foundation stones of the future internet, since the new global network would be designed and built by Chinese engineers, led by Huawei, the controversial telecommunications giant.

http://doi.org/10.18080/jtde.v8n2.298

"What differentiates us from China now is that in the west the public can still mobilise and have a say", says Harvard social scientist, Shoshana Zuboff, as quoted in Gross & Murgia (2020). "What China wants is a technological infrastructure that gives them the absolute control which they have achieved politically, a design that matches the totalitarian impulse. So that is frightening to me and should be frightening to every single person."

The US is highly unlikely to accept this outcome because internet power is mostly held by four large American corporations: Apple, Google, Amazon and Facebook. New IP would end this virtual oligopoly, accelerate China's march to technology leadership and facilitate the export of its authoritarian model globally. If no consensus emerges, which seems probable, the world could split into two separate information worlds, one led by the US and the other by China.

A Balkanised internet is not in Australia's interest. A fractured digital world would vastly complicate e-commerce and trade, restrict the free flow of information, reduce international collaboration and human interaction and leave us vulnerable to the exploitation of our relatively open system by authoritarian states secure behind their digital firewalls.

To prevent these outcomes, the government will need to engage with friends and allies to come up with a fit-for-purpose world wide web that is more efficient, secure, user friendly and compatible with democracy. In the meantime, it needs to have a strategy in place to ensure that China's proposal does not win the day at the critical ITU meeting in November.

Capturing Tech Ecosystems

New IP is only one of several China-associated tech security challenges that the government will have to confront. Techno-economist, Julian Snelder, as quoted in Dupont (2020), says that the technology divide is becoming more evident in other areas of the global economy too, with Beijing relentlessly focused on developing and promoting a "Chinese tech stack" comprising integrated layers of linked software and hardware that could allow it to capture entire market ecosystems in user countries.

International organisations are also targets for China's rules-setting agenda. In March, the UN announced that it would partner with Chinese tech giant Tencent, which owns the highly popular app WeChat, to celebrate its 75th anniversary via videoconference and to discuss, among other topics, solving global pandemics. However, all conversations would be visible to Tencent in unencrypted form and accessible to Beijing which shows scant respect for privacy. Hong Kong academic, Lokman Sui, as quoted in Wong (2020), sees this as "the UN normalising and validating Chinese state surveillance" and says that Tencent censored information about the coronavirus and contributed to its spread.

http://doi.org/10.18080/jtde.v8n2.298

Beijing's expanding web includes Zoom, which relies on software developed by Chinese companies legally obliged to provide their government with user data. The videoconferencing platform has been banned by our Department of Defence as well as NASA, entrepreneur Elon Musk's SpaceX, and the New York public school system (Vigliarolo, 2020), highlighting security and human rights concerns about the exposure of sensitive data to Chinese Communist Party surveillance.

The Cable Wars

Trust in the internet could be further eroded by the cable wars, a developing new battleground at sea.

Four hundred internet enabling undersea cables carry around 98 percent of the world's digital traffic, including emails, texts and more than US $10 trillion of financial transactions (Riechmann, 2018). Cheaper and more efficient than satellites, these fibre optic pipes are the communications backbone of the world economy and Western militaries. This makes them priority targets for intelligence collection by submarines and oceanographic vessels equipped with sophisticated hacking technology designed for deep-sea tracking and tapping top-secret communication cables.

Undersea cables have long been intelligence targets. During the Cold War, the US navy sent divers into the Sea of Okhotsk to install listening devices, hoping to garner vital clues about the Soviet Union's nuclear submarines (Blitz, 2017). But the biggest concern today is that these cables could be deliberately severed or jammed with special equipment to interrupt vital communications and military links in times of conflict (Bennett, 2019).

China and Russia pay close attention to where these cables run to identify chokepoints and vulnerabilities. The Chinese navy has a modern oceanographic and submarine fleet able to access the dense network of undersea cables that crisscross the Pacific, linking Australia with Asia and the world (Lew, 2019). Russia has been aggressively probing global networks with spy ships and converted nuclear submarines that deploy deep-sea submersibles like the highly secretive Losharik, capable of cutting cables at depths that would be difficult to repair (O'Neill, 2019).

An emerging strategic problem for Australia, the US and other democracies is how to protect these cables from intelligence exploitation and attack.

The US has already taken defensive measures to tighten control over its critical telecommunications infrastructure. The US Justice Department recently blocked a partially constructed US-Hong Kong undersea cable, the first time the US has denied an undersea cable

http://doi.org/10.18080/jtde.v8n2.298

licence on security grounds because of the Chinese partner's close links to Beijing and concerns about Hong Kong's declining autonomy (Harris, 2020).

Ensuring that undersea cables are laid by trusted companies along routes less easily disrupted is an essential element of an effective counter strategy. For Australia, this means lessening dependence on cables that run through the disputed South China Sea and avoiding those built and controlled by Huawei, now a viable option as the world's longest fibre-optic undersea cable linking the US with Southeast Asia nears completion.

Telecommunications Infrastructure and National Security

Built by Nevada-based Trans Pacific Networks, this intercontinental cable project is supported by the US International Development Finance Corporation, established last year by the Trump administration to compete with China's digital Silk Road initiative (McBeth, 2020). The 15,200-kilometre cable will run from the northern Californian port town of Eureka to Guam and then follow a route to the south of the Philippines before entering the Makassar Strait en route to Singapore. There will be a branch to Tanjung Pakis, 50 kilometres north of Jakarta. When completed in 2022, the cable will form a critical element of the region's digital infrastructure, increasing internet speed while reducing costs.

A Darwin branch would open up substantial commercial and strategic opportunities for Australia. National access to a trusted, high capacity subsea fibre-optic cable would deepen our engagement with Southeast Asia's 480 million internet users and Indonesia and Singapore in particular. Indonesia is on track to become one of the largest e-commerce markets in the world and Singapore is the third most important financial centre, having recently surpassed Hong Kong.

Australian Defence Force (ADF) activities in northern Australia are constrained by the Top End's thin telecommunications infrastructure and inadequate high-speed data links. If the North is to become a critical national security hub and forward operating base for the ADF, it will need a lot more bandwidth to support the sophisticated operations, training and exercises necessary to achieve these ambitions. Fast, secure, high bandwidth data is a prerequisite for virtually all modern defence and intelligence platforms, ships, aircraft and drones, including our F-35 joint strike fighters, P-8 Poseidon maritime patrol aircraft and the state-of-the-art Triton surveillance drones we are acquiring from the US.

Connecting to the TPN subsea cable would provide a major data boost that could make northern Australia an attractive training destination for regional friends and allies by enabling the integration of Queensland and the Northern Territory's world class, but siloed, training ranges. It would also turbocharge our data-dependent, fledgling space industry and enhance

http://doi.org/10.18080/jtde.v8n2.298

our capacity to launch Australian owned and built satellites for commercial and national security purposes from the developing space port on the Gove Peninsula (We have lift off, 2019).

Strengthening our telecommunications architecture

A core lesson from the coronavirus pandemic is that improved national resilience and sovereign capabilities are essential to future-proof Australia from external shocks. Strengthening our telecommunication infrastructure should be a strategic priority because the risks are mounting.

A decade ago Karl Rauscher, an advisor to the US government on cyber security, drew attention to the vulnerability of undersea cables and the possibility of catastrophic failure to the global economy should they be disrupted by human action or natural disasters like earthquakes (Liebowitz, 2011). The problem is now much more serious because the demand for bandwidth has increased sharply to meet the insatiable appetite for internet-based services. This has resulted in many new submarine cable systems being laid on established routes, adding to congestion and forming undersea choke points (Sunak, 2017).

To make matters worse, there is little redundancy in the undersea cable system, particularly for intercontinental communications. Satellites cannot come close to making up the difference should key cables fail (Heilprin, 2020). Several choke points have already been adversely affected by natural disasters and illegal anchoring, resulting in multiple faults to cables and serious disruption to global communications. In 2006, an earthquake off southern Taiwan caused significant cable damage, slowing internet and telephone traffic across parts of Asia (Choe & Arnold, 2006).

Worries about terrorists and hostile states attacking major choke points were heightened in April 2013, when operators had to deal with disruptions to multiple undersea communications cables linking Europe to the Middle East and Asia. Alarm bells sounded when the Egyptian coastguard caught three divers trying to cut one of the main cables on the seabed a few hundred yards offshore from the port city of Alexandria (Kazaz, 2020).

Of greatest concern to Australia is the Luzon Strait to the north of the Philippines which is the world's largest undersea cable choke point, followed closely by the Malacca Strait (Sunak, 2017). The Luzon Strait and adjacent South China Sea are now effectively controlled by the Chinese navy, so Defence and the intelligence community should be thinking hard about the implications for the security of sensitive communication links critical to military capability and intelligence collection. Diversifying our cable traffic away from the South China Sea is the key to maintaining the integrity of our telecommunication system.

http://doi.org/10.18080/jtde.v8n2.298

But it would be a mistake to regard protecting undersea cables and the openness of the internet as exclusively national security projects. The COVID-19 pandemic has brought home to all Australians the importance of the internet for everyday life. It is the indispensable communications highway that underlays virtually everything we do. A closed, untrustworthy system would negatively impact on business, trade, research and industry as well as our privacy and democratic freedoms.

Recommendations

The government would be well advised to take a more holistic approach to telecommunications policy that transcends narrow commercial considerations and places a premium on risk reduction rather than cost reduction, a lesson driven home by the pandemic. Narrow, market-based calculations should be replaced by a more strategic approach that takes better account of the need for sovereign capabilities to improve national resilience, and factors in the cost of relying on systems that don't pass the democratic values test.

Although it might be more efficient, a controlled, politicised internet with built-in shut-up commands would be detrimental to privacy, personal access and security. It is not a system we should support, even if it means inflaming relations with China already under strain from past disputes and the worsening trade conflict. Australia's national interests cannot be left in the hands of other countries to determine if we value our independence.

References

Bennett, A. (2019). Submarine Cables and Infrastructure Vulnerabilities: Threats from Private and State Actors. https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1954&context=student_scholarship

Blitz, M. (2017). Secrets haunt the still-classified Operation Ivy Bells, a daring Cold War wiretapping operation conducted 400 feet underwater. *Popular Mechanics*, March 30. https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping/

Choe, S.-H. & Arnold, W. (2006). Asian Quake Disrupts Data Traffic. *New York Times*, December 28. https://www.nytimes.com/2006/12/28/business/worldbusiness/28quake.html

Dupont, A. (2020). Mitigating the new Cold War: Managing US-China trade, tech and geopolitical conflict. Analysis Paper 8, *Centre for Independent Studies*, May. https://www.cis.org.au/app/uploads/2020/05/ap8.pdf

Gross, A., & Murgia, M. (2020). China and Huawei propose reinvention of the internet. *The Financial Times*, March 28. https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2

http://doi.org/10.18080/jtde.v8n2.298

Harris, M. (2020). Google and Facebook turn their backs on undersea cable to China. *Tech Crunch*, February 7. https://techcrunch.com/2020/02/06/google-and-facebook-turn-their-backs-on-undersea-cable-to-china/

Heilprin, J. (2020). U.N. group sees risk to underwater cables. *Arête News*, February 11, 2020. https://aretenews.com/u-n-group-sees-risk-to-underwater-cables/

Joseph, M. (2020). Inside China's controversial mission to reinvent the internet. *Thakoni*, March 28. https://thakoni.com/inside-chinas-controversial-mission-to-reinvent-the-internet/

Kazaz, N. (2020). Subsea cable damage claims: The Legal Approach. *Submarine Telecoms Forum*, *111*, March, 48-51. https://www.bda.bm/wp-content/themes/b4st-master/docs/BDA_Submarine_Telecoms_2020.pdf

Lew, L. (2019). The Chinese survey ships that cause ripples in Vietnam and across the South China Sea. *The South China Morning Post*, August 10. https://www.scmp.com/news/china/diplomacy/article/3022065/chinese-survey-ships-cause-ripples-vietnam-and-across-south

Liebowitz, M. (2011). Internet's Undersea Cables Need Revamp to Prevent Catastrophe. *NBC News*, March 14. http://www.nbcnews.com/id/40538984/ns/technology_and_science-security/t/internets-undersea-cables-need-revamp-prevent-catastrophe/#.XwVhpkBuK74

McBeth, J. (2020). US, Indonesia in digital challenge to China's BRI. *Asia Times*, February 14. https://asiatimes.com/2020/02/us-indonesia-in-digital-counter-to-chinas-bri/

O'Neill, M. (2019). 'Top secret' submarine's mysterious mission. *News.com.au*., July 4. https://www.news.com.au/technology/innovation/military/top-secret-submarines-mysterious-mission/news-story/ec51b5acf0ad4a5b8a0ca8434972ecb6

Riechmann, D. (2018). Could enemies target undersea cables that link the world? *AP News*, March 31. https://apnews.com/c2e7621bda224e2db2f8c654c9203a09

Sunak, R. (2017). Undersea Cables Indispensable, insecure. *Policy Exchange Report*. https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf

Vigliarolo, B. (2020). Who has banned Zoom? Google, NASA, and more. *Tech Republic*, April 9. https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/

We have lift off, Arnhem Space Centre given tick of approval (2019, October 21). Retrieved from https://darwininnovationhub.com.au/arnhem-space-centre/

Wong, S.-L. (2020). UN's partnership with Tencent at odds with its push for global unity. *The Financial Times*, April 11. https://www.ft.com/content/192f8d60-ac18-415d-b700-78ce5735a5b6

http://doi.org/10.18080/jtde.v8n2.298