Huawei, Cyber-Sovereignty and Liberal Norms: China’s Challenge to the West/Democracies

Gregory J. Moore

Accepted: 23 May 2022 / Published online: 3 June 2022
© Journal of Chinese Political Science/Association of Chinese Political Studies 2022

Abstract
As China’s global footprint expands and Sino-American competition intensifies, it is apparent that one of the most important arenas for competition between Western Liberal norms and Chinese Communist Party’s (CCP) authoritarian norms is going to come in competing technologies (Western/Korean/Taiwanese 5G/chips vs Huawei 5G/chips) and competing cyber-norms (Western cyber-libertarianism vs Chinese cyber-sovereignty). Inside China, China’s technologies and its cyber-sovereign norms converge. Outside of China, while China champions the norm of cyber-sovereignty, Huawei itself may pose the greatest challenge to sovereign states’ cyber-sovereignty where Huawei controls or otherwise participates significantly as a provider for telecommunications networks, given its relationship to the Chinese state. Is China sincere in advocating cyber-sovereignty as an international norm, or is this just something it is concerned about inside China? Are the laws of China and the technologies and practices of its own Huawei antithetical to China’s own stated norms of cyber-sovereignty? Is cyber-sovereignty simply a stop-gap measure adopted by an insecure regime to justify draconian censorship and thought control at home while it seeks to use its growing presence in 5G telecommunications to expand its surveillance of foreign powers/actors worldwide? Finally, in keeping with the theme of this special issue, does digital orientalism explain the growing tension between China and some of the Western/Liberal powers as it regards competition in 5G? Is the US/West needlessly securitizing Huawei and its 5G, or is there something there worth securitizing? Clarity about these issues and the implications of the answers arrived at are important for nations around the world as China expands its technological reach via Huawei and other national champions.

Keywords China · United States · 5G · Huawei · Cyber-Sovereignty

Gregory J. Moore
gregoryjohnmoore@gmail.com

1 Global Studies and Politics, Colorado Christian University, 8787 W. Alameda Ave., Lakewood, CO 80226, USA
The rise of China and the state of relations between China and the United States are together probably the most important international relations (IR) stories of the twenty-first century. Independent of China-US relations, the imminent arrival of what some call the fourth industrial revolution will be brought about by a combination of quantum computing, artificial intelligence (AI) and 5G (fifth generation wireless communication). While in fact quantum computing, AI and 5G are highly interdependent, this study will focus on 5G, Huawei, and the relationship between 5G technology and norms of cyber-sovereignty on the one hand, and China’s relations with the West/democracies on the other.

While in an ideal world, from a Liberal and/or techno-centric world view, politics/geo-politics would not enter into the advent and rollout of one of information technology’s (IT’s) biggest new technologies—5G—unfortunately it cannot be denied that 5G has been “securitized” [3]. What should be a very exciting time in the advancement of telecommunications technology with the rollout of 5G has instead become highly contested, highly divisive, even to the point of being cause for a possible “digital iron curtain” as nations divide over allowing China’s Huawei a role in construction and/or operation of respective national 5G networks. Why? I will argue here that Huawei and its business have been securitized for very good reasons, for while digital orientalism¹ may in fact be lurking out there, in fact it is not the reason for this securitization or for the problems faced by Huawei. Rather, it will be argued here that it is Huawei’s business model, the nature of the Chinese Communist Party, and the legal relationship between Huawei (and potentially any Chinese company) and the Chinese state that create a potential security problem for nations that do 5G business with Huawei.

**5G, Security and the Technological Lay of the Land**

Let us start by looking at a snapshot (April 2022) of the 5G milieu as we begin to consider the reasons for the securitization of Huawei and its 5G business activities, and the digital divide differences over how to manage it has spawned. For starters, the stakes are high and the choices are limited as it regards the development of 5G technology. Currently the only companies with the ability to construct a complete 5G network are Ericsson (Sweden), Nokia (Finland) and Huawei (China), though this is changing because of a new technology called Open RAN, that is based on a new open standards software, which allows new competitors to build infrastructure until recently the exclusive domain of Ericsson, Nokia and Huawei.² The only companies who can make chips for 5G phones right now are MediaTek (Taiwan, with help from Intel of the US), Qualcomm (US), Samsung (South Korea), and Huawei (China), a very narrow playing field indeed.

---

¹ For a full discussion of “digital orientalism,” please consult Mayer and Mahoney [17] and/or the opening article in this special issue.

² See Woo [37]. In addition, India’s Jio has been working on an indigenous capability to field a full 5G network [31], now made more likely because of a new partnership with Intel [21].
While Huawei is ostensibly “private” in ownership structure, it is a Chinese company and is thus accountable to the Chinese Communist Party, and it is well known that the CCP does not share the liberal values that all the other 5G players share, whether Swedish, Finnish, Taiwanese, American, or South Korean. That makes a difference to some, not so much to others. For example, Australia, Japan, New Zealand, the United Kingdom, Sweden and the United States have directly or indirectly (but effectively) blocked Huawei participation in 5G network construction in their countries. The US has even barred American companies from supplying almost any technology to or engaging in any cooperation with Huawei at all. While France has not directly blocked Huawei’s participation in the 5G marketplace, France’s cybersecurity ANSSI has recommended French telecoms not switch to Huawei and French authorities have moved to phase out Huawei equipment from French networks by 2028 [23]. Other countries have said that while no Huawei participation in critical infrastructure is allowed, using Huawei parts in other dimensions of 5G network building and operations is permissible. Others have allowed Huawei to compete for participation in building 5G networks, but a decision has not yet been made as to whether or not Huawei would be allowed to “win” such a bid to actually build any networks (India, Germany3). Others have put no restrictions on Huawei in their countries, and/or have in fact contracted Huawei to build part or all of their national 5G infrastructure (China of course, Bahrain, Hungary, Kenya, North Korea, South Korea, Thailand and others [23]).

The result of this divergence of views of and the varying degrees of comfort countries exhibit in allowing the participation of Huawei in 5G network building and operations is that some countries may feel forced to choose between Huawei/China and the US, given the recent US campaign against Huawei. As an example, American President Donald Trump has explicitly threatened other Five Eyes member states (Australia, Canada, New Zealand and the UK) and/or NATO member states, saying that adoption of Huawei 5G networks may mean the US stops sharing sensitive intelligence that could be compromised on Huawei networks in those countries. In fact, Canada is the only member of the Five Eyes now not to have banned Huawei, but the mood there appears to be building toward blocking it too [15, 34]. Here we see the specter of the “digital iron curtain” referenced earlier. Consequently, it is possible that the world will separate into two 5G macro systems – those using Huawei technology/hardware, and those that do not.

What is it about 5G that is so divisive, that apparently raises the stakes so high for both China and the West/democracies? The answer to that question is in part a technical one, found in the nature of the technology itself. 3G and 4G wireless technology are dependent upon a central node of communications, a hub and spoke system, if you will. To compromise the security of these systems one would have to

---

3 In Germany’s case, the government has concluded that it will allow Huawei to compete in any 5G projects in the country, but that when the law is ratified (it has not been ratified by Germany’s Bundestag yet), any potential vendors would have to submit a declaration that its network/components could not be utilized for “sabotage or espionage,” and German ministries would have 30 days to draw conclusions. Unless all German parties to such a decision are unanimous in blocking a vendor (for example, Huawei), it would be allowed to move forward with its business. For more, see Thomas [30].
compromise the hub, the center of the system. 5G is different. It is made up of many points, many dots in a communication matrix, that together connect the handset or computer into the network. Compromising any of the nodes locally could be sufficient to compromise the system as it regards the handset or computer in question. In other words, while it is exponentially faster and more capable, it is also more easily breached, more vulnerable in more places. Consequently, the builder and keeper of the network is more important in the case of 5G than in previous generations of wireless technology. Moreover, given the potential of 5G, because of its unprecedented speed and low latency (or quick response time) to extend and amplify the applications of IOT (internet of things) and AI (artificial intelligence) among other things, the vulnerabilities increase exponentially again. With IOT, compromised devices networked via IOT (or devices on compromised networks) could be commandeered or given orders by third parties, and AI applications could potentially be influenced by third parties as well if the network is not secure. For all of these reasons, network security is more critical with 5G communications networks than ever before.

2019–2022 have seen 5G installed in countries around the world, in most cases starting in designated cities with backup 4G/LTE coverage to fill gaps. As the 5G network in a given area expands and the number of handsets with 5G capabilities slowly multiplies as well, more and more traffic will switch over to 5G more and more of the time. The US and South Korea, using Nokia and Ericsson network underpinning, have been early adopters, as has China with Huawei leading the way there.

China’s Solution to 5G and Modern Internet Management: Cyber-Sovereignty

To help deal with the many challenges to internet (and political) governance posed by these new technologies, the Chinese government has proposed a concept called cyber-sovereignty. Cyber-sovereignty (网络主权, wangluo zhuquan) is a concept that was first coined officially in 2010, but came into more regular official usage in 2014 at China’s World Internet Conference at Wuzhen [10, p. 240–41]. Newly installed core leader Xi Jinping had taken lead of the Central Leading Group for Cybersecurity and Informatization, and he was persuaded by arguments among security experts in China that Western notions of internet openness were a threat to the ruling party and that “cyber-sovereignty” was the path China should take. About cyber-sovereignty, James Griffiths says this.

Today, it is the driving policy behind Chinese internet strategy, and represents a major threat to the existing global web order...Cyber-sovereignty seeks to

---

4 Some 5G networks are being built instead as stand-alone 5G networks, avoiding the latency slowing effect of “upswitching” from 4G/LTE to 5G [29].

5 One exception being that South Korea’s LG UPlus provider combines Ericsson, Nokia, Huawei and Samsung equipment [29]. On the US, see Woo [37].
establish an international, as opposed to global, internet. Instead of the world wide web as we know it, countries would each maintain their own national internet, by force if necessary, with the border controls and immigration standards they see fit. The doctrine risks turning the entire world into China, where people use a mirror image of the internet, resembling that outside the Great Firewall, but skewed and misshapen. Within the Firewall, buttressed by legions of censors and protectionists laws, Chinese internet users search on Baidu rather than Google, they share news and photos on WeChat, not Facebook, and shop with Alibaba, not Amazon…Such a vision of the internet – bordered and tightly controlled by government – would be antithetical to the techno-libertarians active in the early days of the web [10, p. 242-43].

The CCP vision of the internet in China is set up so as to serve the ruling party, to protect it from challenges, to keep it in power. Inside China, the CCP seeks to control all information, all narratives, whether via education, publishing, broadcasting, cinema, social media, traditional media, or any other form. The fear among some outside of China is that China will be successful in taking this view of the internet out, beyond its borders and use Huawei and other Chinese companies like ZTE to do it. The prevailing global techno-libertarian or cyber-libertarian norms, even in today’s less liberal form, were and are clearly a threat to the CCP. This is because it cannot control narratives outside of China or those produced by foreigners, which means a wide-open internet would allow these unapproved narratives to enter China and potentially influence politics there. They cannot accept this so they have promoted cyber-sovereignty as the key method by which they can seek to control all narratives within their borders. China has become the key champion of the concept of cyber-sovereignty and has brought some nations along with it in this respect.

Before continuing the discussion of cyber-sovereignty, for a moment let us consider the alternative, the global status quo of recent decades (at least outside of China, North Korea, Iran and others): what we might call a tamed version of techno- or cyber-libertarianism. From its earliest inception, when the sky seemed the limit [2], the advocates of the internet, or World Wide Web, saw the new space they had created as fundamentally and necessarily free. The great internet startups like Google, Yahoo, Amazon, America Online, and Facebook, all depended on this free-wheeling, “wild, wild west” narrative of cyberspace to create their value, to earn their millions, thereby forging new paths to prosperity and knowledge which took down walls of access and privilege and seemingly levelled the playing field for anyone with a computer and a modem. Yet even in the West the cyber-libertarian ethos has not held, as states have taken advantage of new technologies to spy on their own citizens and on foreigners at home and abroad,⁶ as states have put laws and technologies in place to regulate and manage cyberspace, etc. For example, as Weber has pointed out, “70% of world internet traffic.

---

⁶ For a fascinating example of this, see “Citizen Four,” a film by Laura Poitras [24] about the case of Edward Snowden, with real footage of Snowden telling his story in a Hong Kong hotel before going on the run to Russia.
passes through Loudon County, Virginia alone” [35, p. 247]. Certainly, the US government is not unaware of this fact and has, at times, sought to exploit it, along with the techno-dominance of US IT companies like Facebook and Google, as Edward Snowden⁷ and others have sought to point out. Some observers have even called for a “Westphalian moment” as it regards the need for, and in their minds inevitability of, the ushering in of state sovereignty to govern the internet just as states stepped in to better manage their borders/polities in the time of the Peace of Westphalia in 1648 [7]. While the state role has not in the West grown as pronounced as observers like Demchak and Dombrowski envisioned, there has been a growing consensus that the internet needs to be governed more than it has been. This might be seen recently in the US wherein firms like Google, Facebook and Apple seem to have turned a new page, one that now sometimes entails censorship and blockages of free speech of citizens and even the President of the United States to such a degree that in January 2021, the American Civil Liberties Union (no friend of Donald Trump) spoke out against the actions of Big Tech against then-President Trump and other conservatives following the January 6, 2021, attacks on the US Capitol. While there is still a difference between the greater role for state management that China advocates, and the greater role for private management which is more commonly seen in the West [6], it cannot be denied that cyber-libertarianism reached its limits some years ago, and that more and more nations and corporations are concluding that greater management of the internet in their countries is necessary. True as this is, the rise of China’s cyber-sovereignty has challenged this more cyber-libertarian ethos still cherished in the West in very fundamental ways. For certainly it does not take much research or expertise to see, to feel, the difference in the internet experience one might have in China and that which one might experience in countries like the UK or the US. While it is true that the difference between the internet in China and the Western democracies is less one of quality than of quantity of state guidance, the difference remains quite substantial, quite real, all the same.

While each government is free, legally, to determine the parameters of its internet within its own borders, in China’s case it appears that the CCP has now decided that cyber-sovereignty, which might be known as “the internet with Chinese characteristics,” is fit for export, that it should be the default norm for internet governance worldwide. China’s work to help Russia and other countries build their own version of the Great Firewall might be one example. Many observers believe its work to export Huawei 5G systems which will operate under Chinese principles of internet and telecommunications governance, or something like it, and which will be subject to CCP surveillance potentialities is another. China has also worked hard to garner influence in and over ICANN (the International Corporation for Assigned Names and Numbers), particularly after the US gave up full control of the body in 2016. While there are a diversity of views in China about how China should handle its presence at ICANN and ITU (the International Telecommunication Union), China clearly “is a promoter of an alternative to the status quo” [20, p. 117] as it regards internet governance, and prefers a model wherein states are their own arbiters of

⁷ Please note here that this is not intended as a defense of Edward Snowden.
internet norms, rather than having a more liberal, global model. This in essence is cyber-sovereignty, which sounds innocuous and intuitively positive, until one considers the sorts of norms that govern politics and communications in the People’s Republic of China, and the ways in which that sort of system could impact global communications technology and practices under China’s influence. In recent years, an alarming trend has developed: the exporting of Chinese internet censorship itself. The technologies behind the Great Firewall have spread to Russia and other Chinese allies, and countries in Africa, South America and Asia have adopted internet control policies expounded by Beijing, often with the active assistance of Chinese officials and corporations. The space for criticism of China’s actions and policies, always limited within the country itself, has begun shrinking overseas, as Beijing attacks anyone who would offer a dissenting view to its territorial ambitions or Communist Party political hegemony [10, p. 310].

China’s growing strength and influence are not proving to be encouraging of global norms/values of openness and transparency as it regards communications, but rather the opposite, and this has grown even more pronounced in the past year with Covid-19 and Beijing’s desire to control that narrative both at home and abroad. Many have argued that China has been shaped profoundly by the international system and by international norms, and that we should wait as China continues to reform, that the CCP will in time be socialized to accept more Liberal norms [13], whether in internet and communications or in other areas. That was persuasive in 1980, but it is a harder case to make today under Xi Jinping’s tightening grip on China and China’s “wolf warrior diplomacy” abroad [27]. In his study of China’s growing role in international institutions, Johnston [13] argues that there are three microprocesses of socialization that take place: 1. mimicking, 2. social influence and 3. persuasion. Mimicking is the notion that, “I will do X because everyone seems to be doing X and surviving. So, until I know better, X is what I will do.” (xxv) Social influence could be conceived as, “I should do X because others believe X is the appropriate thing to do and I will be rewarded socially for doing so.” (xxv) Finally, persuasion can be seen as the actor saying to him or herself, “I should do X because it is good and normal for me (us) to do so” (xxvi). Johnston’s study is an excellent one, and the case studies presented are sound. However, in recent years China’s political trajectory has taken a more conservative (more authoritarian, leftist in this case) tack. The Chinese leadership may have done some mimicking (1.) in the beginning of its interactions with ITU and ICANN, and may have even been influenced socially (2.) on some aspects of internet governance (after all, it allowed the internet into China early on, rather than taking a more restrictive Pyongyang-esque approach). However, the CCP has clearly not been persuaded (3.) that more mainstream liberal global internet governance norms are in its interest, and as its power, reach and influence grow, in recent years it seems more and more intent on reshaping those global internet governance norms into its own image. In other words, rather than being persuaded by cyber-libertarian norms, it now increasingly seeks to shape the global order in an illiberal, cyber-sovereign direction.
Huawei, Controversy & Contradiction: Cyber-Sovereignty vs Huawei’s/China’s Actions Abroad

What is it about Huawei that draws so much international attention, and so much controversy? Huawei is the company that has the most patents in 5G technology, the company that is perhaps furthest along in 5G deployment, and the company that is by most counts the least expensive option in 5G system construction (thanks in large part to Chinese government subsidies). It is one of China’s national champions, a private company, legally speaking, run by Chinese Communist Party (CCP) member and former People’s Liberation Army (PLA) officer Ren Zhengfei [12], based in China, which boasts a national security law that says, “All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of” [19]. Huawei may be outwardly private, but it is not unaccountable to the CCP, nor is it a typical international IT company. It is an IT company with Chinese (Communist Party) characteristics. It is a company that has reported receiving “hundreds of millions of dollars in [Chinese] government grants each year, including US$220 million in 2018” and “a US$100 billion line of credit from Chinese state-owned banks that enables it to offer financing to customers at below-market interest rates” [11, p. 15]. Huawei is a company accused by Cisco Systems of stealing corporate secrets and pirating software [32], by the US government of enabling remote access of routers Huawei manufactures [9, 60; [32], “was accused by multiple countries of facilitating the use of embedded backdoors by the Chinese government in 2003, 2005, 2007, 2008, 2012 and 2013 [9, p. 66], is accused of committing high level corporate fraud by the US, a charge upheld by Canada’s British Columbia Supreme Court [25], and on the list goes. Huawei is said to have helped build a more repressive and surveillance-centric internet infrastructure in Russia [10, 251–252], and has helped equip and train leaders how to do better surveillance on dissidents in countries including Uganda, Zambia, Ethiopia and Zimbabwe [10, 303–304]. Cyber-sovereignty has been the Chinese government’s policy narrative attempting to give reason and legal standing to these moves.

While China has become a great champion of the notion of national and cyber sovereignty, arguing for stern national control over its internet and draconian, even cyber-totalitarian [18], control over information flows domestically, its 5G national champion Huawei poses some contradictions with cyber-sovereignty conceptually as Huawei operates overseas. Neither Huawei nor the Chinese Communist Party’s Ministry of State Security are known as great respecters of other nations’ information security or individual privacy as they operate abroad, just as they are not known as great respecters of personal information security or privacy as they operate within China.
There is a long record of the misadventures of China’s state-led hacker communities\(^8\) as they’ve worked to absorb billions (trillions?) of dollars of intellectual property from Western firms over the past decades [8–10, 16, 18, 22, 28, etc.], steal personal information from US government employees via the enormous 2017 Equifax breach [1], influence free speech on US university campuses [8], bring PLA officers to the US posing as students to exfiltrate data/information, and on and on. In 2015, when confronted with some of these charges at Sunnylands, California, Chinese President Xi promised US President Obama this would stop, yet while reports show it did recede for a season it did not stop and some of the most egregious acts of corporate espionage, theft and deception were yet to come. For this and other reasons the Chinese Communist Party has often proven to be a rather untrustworthy actor from the perspective of the United States and other governments around the world [14]. So when a company like Huawei, which is legally bound to help the CCP on national security issues [19], wants to set up 5G networks abroad, and argues that it supports information security, information freedom, and personal privacy, it is difficult to believe, whether based on CCP practices in China or the Party-State’s history of often failing to honor such commitments in its conduct abroad.

One of the CCP’s foreign policy mantras is that states should practice non-interference in the affairs of other states, yet there is evidence that Chinese state actors such as the Ministry of State Security or PLA, or companies like Huawei, do not consistently abide by this principle in their own work abroad. The principle of cyber-sovereignty means states determine their own levels of internet openness such that these match the needs and comfort levels of the host country. Yet the charges against Huawei and the Party-State that stands behind it are that it is exactly this which it does not do when working abroad.

The root of the problem is that Huawei is legally bound to serve the Chinese Party-State, such that when Chinese national security could benefit from Huawei’s sharing information with the Chinese state and the state requests such help, Huawei will not be able to protect the information security of nations in which it works, but will have to share such information with that Party-State. There is no other way to read the 2017 National Intelligence Law. In like manner and for the same reasons, Huawei will not be able to protect the privacy of individuals using Huawei systems when it is in the Chinese state’s interest to have that information and it asks Huawei personnel to comply. In fact, it would be against Chinese law for Huawei to withhold such information if that means resisting the will of the Chinese state [19]. Huawei has a corporate interest in acting like any world-class IT company and working to protect the rights and security of host countries, business partners and individuals using Huawei products. Yet even if we are inclined to accept Huawei executives’ statements that indeed this is how Huawei conducts its business [12], we must also face the reality of 1. Chinese law as found in the National Intelligence Law of the
PRC [19], and 2. a history of patterns of abuses of such norms in the conduct of Chinese state actors at home and abroad.

A defender of Huawei might argue that Huawei is not a state actor, should not be blamed for (mis)conduct of state entities, and has not (yet?) been proven definitively in a court of law to have conducted itself inappropriately. How does a skeptic respond to such a line of argument? The case of Sweden seems exemplary here. Sweden is not a geopolitical foe of China’s historically. It does not appear to be a threat to China nor, would one think, is China a threat to Sweden. Yet Sweden, famous for its neutrality, has taken a very hard line against China’s Huawei. In October 2020 the Swedish government decided to ban not only Huawei, but another Chinese IT company, ZTE, as well, from contracts involving the construction of high-speed networks in Sweden. Sweden’s government concluded, moreover, that the four companies competing to build Sweden’s new 5G network must not even use Huawei components in the construction of that network, and those that have used Huawei components in the past must rip those components out and replace them with non-Huawei components [4]. The head of Sweden’s domestic security service (or SAPO), Klas Friberg, explained his country’s policy as follows.

China is one of the biggest threats to Sweden…The Chinese state is conducting cyber espionage to promote its own economic development and develop its military capabilities. This is done through extensive intelligence gathering and theft of technology, research and development. This is what we must consider when building the 5G network of the future [4].

This is strong language from a country like Sweden. Calling China one of Sweden’s “biggest threats” also says a lot considering the more immediate threat to Sweden posed by its neighbor Russia, who has in recent years been pressing Sweden hard in terms of Russian air and sea incursions into Swedish territory. Sweden does have a horse in the 5G race in its Ericson, but it has not banned any other competitors. Mr. Friberg explains why, and key is what the Chinese state has been doing, and its links to Huawei. Even if Huawei has not been definitively proven in a court of law to be guilty of all the things it has been charged with, it is apparent that Sweden and other countries perceive that Huawei is a threat now or in the future. The intelligence agencies of many countries have reached similar conclusions. Huawei clearly has, at the least, a public relations problem. Moreover, it appears that the Chinese government’s narrative of cyber-sovereignty is at odds with the track record of the Chinese Party-State in its operations abroad, and this is one of the key reasons leaders of countries like Sweden, the US, the UK, Australia and many others have found it difficult to trust Huawei or the Chinese government these days.

Securitization and Digital Orientalism

There is one other possible explanation for the disconnect between Huawei’s stated business ethos and its treatment by many, and we must return to it here. Does digital orientalism, the major premise of this collection of articles, explain the harsh
policies of countries like Sweden and the US toward Huawei? Maximilian Mayer and Gregory Mahoney [17] give us a working definition of the term.

We define digital orientalism as re/inscribing a pseudo-otherness, typically resorting to tropes first employed during classical [Said], Cold War, and Sino-logical forms of orientalism [Vukovich], but now used when social, cultural, economic and even political differences have increasingly narrowed through the increasing tilt towards a global technological society in ways that are undermining older national and cultural narratives and associated hegemonies [17, p. 1].

Said’s orientalism construct [26] is an important contribution to the study of colonialism, post-colonial thought, international relations and sociology. There is no reason to challenge it here. It’s application to the digital realm is an interesting and important one. The premise of the editors of this special issue is that the West expected China to evolve into a liberal democracy, but that this has not happened, and moreover this (from the West’s perspective “fundamentally illegitimate”) power has been able to increasingly compete head to head with the US and the West in military, political, economic and technological terms, and this has created deep fear among Western/democratic leaders. Fear is a key part of this orientalist narrative. The argument is that it is fear of this digital, political and cultural other that drives a tough US, Australian, British (for example) policy toward China, and drives a harsh stand toward Huawei. To set this up in a cause and effect framework, then digital orientalism is the independent variable that causes fear in the US and others towards China, that brings about the dependent variable, harsh policies toward China and Huawei specifically. What this would mean is that other factors would not explain the dependent variable, the harsh US/Western policy toward Huawei. The question we will pose here is, is this correct?

There are several potential problems with this argument. First, establishing that fear is an independent variable is not easy. Despite the quality of their work generally speaking, the editors have not done the thick description necessary to establish this. Simply showing tough rhetoric, hawkish views on the US/Western/democratic side (which are indeed there), does not really do the job effectively. Second, we haven’t considered counterfactuals or ruled out other methods that might test our hypothesis or do a better job explaining the outcome we observe (the harsh US/Western policy toward Huawei) than the proposed independent variable, digital orientalism. Following on from this point, I would propose a consideration of the hypothesized independent variable, “China and Huawei pose credible threats to national security of the US and other democracies” as a way to understand the approach the US, Australia, the UK and others have taken toward Huawei.

Securitization provides a way of looking at this issue that is helpful in this case. As Buzan, Waever and de Wilde [3: 25] put it,

Securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects... The way to study securitization is to study discourse and political constellations: When does an argument with this particular rhetorical and semiotic structure
achieve sufficient effect to make an audience tolerate violations of rules that would otherwise have to be obeyed?

There can be no doubt that in the United States, Australia, India and other countries, Huawei’s 5G offerings have been securitized, and this is evident by the “discourse and political constellations” in those and other countries, as I’ve illustrated above. Yet why hasn’t this been the case in all countries? As Buzan et al. note, referencing the work of Arnold Wolfers [3: 30], security threats may be objective/real, or subjective/perceived, and where the twain meet or diverge is not always easy to ascertain. It is possible that A. China’s Huawei is acting as a threat in some countries and not in others. It’s also possible that B. China’s Huawei and its 5G are a threat wherever they operate but some countries don’t yet understand that or don’t believe it. It’s also possible that C. Huawei and its 5G are not a threat and have simply been socially constructed as a threat, needlessly securitized. The notion that digital orientalism is the reason for the securitization of Huawei and its 5G would line up with the last tack, or C.

The argument presented here, however, is that digital orientalism does not explain the US/Western/democratic response to China’s growing illiberal impact on global internet governance or its worrisome presence, via Huawei, in more and more national 5G internet infrastructure schemes. On the contrary, the hypothesis posed here is something like B. above, that real security concerns do, that the securitization of Huawei is not an irrational response to Huawei 5G because of 1. some of Huawei’s actions/track record, 2. the nature of its relations with the Chinese state, and 3. the track record or broader actions (now and in the past) of that Chinese state at home and abroad as it regards media freedoms, intellectual property theft, human rights problems, and more. Having said this, digital (or conventional) orientalism may be lurking in the background and exacerbating technological and political dynamics. I suspect it is. The editors are likely not incorrect in that sense, for certainly there is a sense that China represents a “digital other,” a “political other” and a “cultural other” for Westerners and Liberals in general, and the notion of digital orientalism may explain certain aspects of that. At the same time, the argument presented here is that a careful study of China’s practices in the cyber-realm, whether at home or abroad, make it clear that there are very clear security-centric reasons for concern about China’s and Huawei’s presence in 5G internet infrastructure construction, mobile phone handset production, and even Chinese apps like TikTok and WeChat, which India has banned, and both of which the Trump Administration tried but failed to ban in the US.

US, Australian, British, Swedish and other countries’ increasingly robust pushback against Huawei and other Chinese players in the construction of global 5G infrastructure can be easily understood by studying A. China’s cyber practices at home and abroad, and B. the impact they have on the security (and perceptions of security) of nations they work with. Very simply, those pushing back see what China

---

9 Please see Singer and Friedman [28], Fritz [9], Maurer [16], Griffiths [10], Diamond and Schell [8], Moore [18], etc.
is doing, they don’t like it, and they don’t want Chinese companies to have any major role in constructing telecommunications infrastructure inside their countries. This is because they believe they know what that will lead to, and they don’t believe that is good from their perspectives. If China/Huawei was a player like Nokia, Ericsson or Samsung, the US and these others would not be raising alarms. In fact, the US, Australia and UK have *not* been raising alarms about Nokia, Ericsson or Samsung, the other major players in 5G. Why? Is it digital orientalism? In fact, given that Samsung is Korean, one might expect the US to push back against Samsung, for it too is “oriental,” non-Western, following the logic of Said. We don’t really see that, however. South Korea is a democratic polity and a US ally, so there is no angst on Washington’s part, no concerns about security. Moreover, the South Korean government does not have a history of stealing US IPR, of spying on the US as China has been, or doing anything that could be considered a national security threat toward the US, so there has been no pushback from Washington in the face of Samsung’s growing presence in the US or in US 5G operations.

Some argue that the US simply refuses to yield the number one spot to anyone, whether in technology or in economic dominance. Yet if the US was pushing back against Huawei because the US wanted to be number one, because the US wanted to dominate, why wouldn’t the US fund AT&T, Apple, Google or someone else in the US to be number one? Why wouldn’t the US hinder the advances of Nokia, Ericsson and/or Samsung in the US and elsewhere? We don’t really see any of that, however.

Digital orientalism doesn’t really explain this, in this case. I will argue here that it’s because first, American thinkers do not think in such hierarchical terms as their Chinese counterparts do (they aren’t unified in an obsession with being number 1 as is the case with the Chinese state and its companies; see [18]. Second, the US is not pushing back against Huawei primarily because of market imperatives/motivations, but rather because of concerns about security and lack of trust in the Chinese state and Chinese companies that are subject thereto. The US trusts the leadership of Nokia, Ericsson and Samsung, and they don’t see their home governments (Finland, Sweden and South Korea, respectively) as bent on spying, stealing IPR and undermining free expression at home and increasingly around the world. It’s about the Chinese state’s very bad track record of stealing intellectual property, of suppressing free expression, of cyber-surveillance and hacking, of suppressing truth and suppressing dissidents – increasingly not only inside China but abroad as well.10 Pushing back against Huawei and China’s cyber-sovereignty model has become an existential fight for those who see things in the way I have depicted here. In a telling statement by former Obama National Security Advisor Susan Rice to Canada’s CBC about the security threat Huawei posed to Canada and others, Rice said,

> It’s hard for me to emphasize adequately without getting into classified terrain how serious it is...It gives the Chinese the ability, if they choose to use it, to access all kinds of information. Civilian intelligence, military, that could be

---

10 Again, see Singer and Friedman [28], Fritz [9], Maurer [16], Griffiths [10], Diamond and Schell [8], Moore [18], etc.
very, very compromising. So as much as I disagree with the Trump administration on a number of things, on this I believe they are right [15].

Given how much Rice was opposed to Donald Trump and almost all he stood for, her agreement with him on this issue is striking. It seems clear that this was no election-year posturing on the Trump Administration’s part, though that is how the Chinese government tends to frame it.11 Huawei’s building and operation of 5G networks in other countries poses serious challenges to the security of potentially any host-country, and what is being argued here is that this is the reason for the increasing push-back, the securitization moves, China and Huawei are facing as Huawei tries to expand its 5G operations abroad.

Toward the ends of explaining how and why Huawei 5G gets securitized in some places and not others, I think it is possible to take Buzan, Wæver and de Wilde’s securitization a bit further. I don’t see regional security complexes (a key factor in their work) at play in a prominent way here, because the array of countries that have aligned in opposition to Huawei are more diverse than any regional framework could accommodate, with Sweden, Australia, India, the UK and the US all saying no to Huawei, whereas Germany, South Korea, and Canada are keeping the doors open. The US, for example, has close allies on both sides of this digital divide, and there are members of China’s region/neighborhood who are on both sides of this divide as well, all of which is to say that neither alliance patterns or regional patterns clearly explain the digital divide over Huawei.

I think another concept found in Buzan, Wæver and de Wilde’s work [3] better explains it, with the help of an expansion of another of their concepts. The first concept referenced here is that of security constellations (p. 201). Buzan et al. define them as “a much wider concept than security complexes, reflecting as it does the totality of possible security interrelationships at all levels” (p. 201). They add, “security constellations will almost certainly generate a much fuller set of non-regional subglobal patterns (such as those created by the sets of countries that export copper or those countries vulnerable to seal-level rises” (p. 201–2). Considering the range of Buzan et al.’s “sectors” (i.e., military, environmental, economic, societal and political sectors), it is not clear where one would locate cyber, however. Given that the work being referenced was published in 1998, it seems logical that two new sectors should be added to Buzan et al.’s sectoral framework, and this is the conceptual expansion referenced above: that of cyber and space sectors. While space as sector is yet relatively underdeveloped, cyber is a sector that has grown apace in recent years and should now be considered a sector in its own right, as might be evidenced by the addition of “Cyber Commands” and like agencies to the arsenals of many nations today, whereas none existed only a few short years ago. With the addition of a cyber

11 The problem with this argument is that 1., it assumes Americans pay attention to international affairs like US policy toward Huawei (most do not) and 2., it assumes that Trump would have gained some mileage politically by making such tough anti-China moves, but there is no evidence that is the case. Donald Trump ended up losing the election against Joe Biden, so his tough stance on China doesn’t seem to have won him many kudos, and all indications are that Biden will be tough on China as well, though his policy will likely differ in important ways.
sector and the interrelation of this sector with extant sectors like military, economic and political sectors, for example, it is clearer to see how a security constellation encompassing all of these might interplay so as to bring about the digital divide we’ve seen over Huawei’s participation in 5G network construction. For example, whereas Sweden does not have to worry about a direct military threat from China as it does from neighbor Russia, it does operate in a security constellation wherein China’s economic interests (and actions) and the nature of its political sector/system are such that Sweden perceives a threat. In the same way, whereas South Korea has a more immediate potential threat from China militarily (after all, S. Korea’s mortal enemy North Korea is China’s ally, and S. Korea’s ally the US is China’s chief adversary), it does not apparently view China (or at least Huawei) with as much trepidation as the US does. It may be that it doesn’t see its own interests as being as divergent from China’s as the US does. It may also be that its cool relationship with Japan for reasons of unresolved history puts it in closer ideational orientation to China (with which it shares some anti-Japanese historical angst) than, again, would be the case with the US. Cyber is just one part of a constellation of security interests between these many players and so a simple digital orientalist, geopolitical, economic or alliance-driven explanation alone does not really do justice to the broader complexity of interests and issues that drive issues or sectors like cyber.

**Conclusions**

The Chinese have built a world-class international information technology company in Huawei. Were it not for politics and securitization, it is quite possible that Huawei would become one of the darlings of the global IT industry, as has been the case with companies like Samsung, Apple, Google and Nokia. Unfortunately, it appears that the nature of the state who stands behind that company and uses its power to help Huawei gain access and (that state hopes) dominance in global 5G and other markets, is itself the primary reason it will continue to be an uphill fight for Huawei in the battle for viability in the global 5G marketplace. The track record/conduct of those who run that state does not inspire confidence in those outside of China who value free competition, free expression and technology security.

In conclusion, the editors of this collection are correct that the divide we are seeing between China/Huawei and the democracies over 5G technology is unfortunate and quite dysfunctional from many perspectives, whether economic, technological, political or other. Unfortunately, as long as the Chinese state operates under the rubric of cyber-sovereignty with Chinese (Communist Party) characteristics, it will be difficult to avoid the consequent digital divide, as many nations will not want to risk compromising their security or potentially their freedom for 5G technology.

---

12 I say freedom here because the Chinese state often uses economic clubs to punish those it disagrees with, or those whom do or say things it does not like. A case in point is Australia, whom in the spring of 2020, following a demand for a full investigation from China about the origins of Covid-19, was told by the Chinese Foreign Ministry that if Australia insisted on demanding such an investigation, would be subject to bans and/or limitations on Chinese imports of Australian wine and beef. Australia did not back down and CCP leaders kept their promises. Chinese imports of Australian beef and barley were reduced significantly as a result [27, 33], as has been the case with Aussie wine [5, 36].
no matter how good that technology is or how cheap it might come by partnering with Huawei.

Declarations

Conflicts of Interest  No conflicts of interest are in play here. I have none. Thank you.

References

1. Barret, Brian. 2020. How 4 Chinese hackers allegedly took down Equifax. Wired. https://www.wired.com/story/equifax-hack-china/. Accessed 28 May 2022.
2. Benedikt, Michael. 1991. Cyberspace: Some proposals. In Cyberspace: First steps, ed. M. Benedikt, 119–224. Cambridge: MIT Press.
3. Buzan, Barry, Ole Waever, and Jaap de Wilde. 1998. Security: A new framework for analysis. Boulder: Lynne Rienner.
4. Chan, Kelvin. 2020. Sweden bans Huawei, ZTE from 5G, calls China biggest threat. The Washington Times. https://www.washingtontimes.com/news/2020/oct/20/sweden-bans-huawei-zte-from-5g-calls-china-biggest/. Accessed 28 May 2022.
5. Chandler, Ainslie. 2019. China starts second Australian wine probe as tensions mount. Bloomberg. https://www.bloomberg.com/news/articles/2020-08-31/china-hits-australian-wine-with-second-probe-as-tensions-mount. Accessed 28 May 2022.
6. Choucri, Nazli, and Daniel Goldsmith. 2012. Lost in cyberspace: Harnessing the internet, international relations, and global security. Bulletin of the Atomic Scientists 68 (2): 70–77.
7. Demchak, Chris C., and Peter J. Dombrowski. 2014. Rise of a Cybered Westphalian age: The coming decades. In The global politics of science and technology, ed. Maximillian Mayer, Mariana Carpes, and Ruth Knoblich, 91–113. Berlin: Springer.
8. Diamond, Larry, and Orville Schell, eds. 2013. China’s influence and American interests: Promoting constructive vigilance. Stanford: Hoover Institution Press.
9. Fritz, Jason R. 2017. China’s cyber warfare: The evolution of strategic doctrine, p. 60. Lanham: Lexington Books.
10. Griffiths, James. 2019. The great firewall of China: How to build and control an alternative version of the internet. London: Zed Books.
11. Grotto, Andrew. 2019. The Huawei problem: A risk assessment. Global Asia 14 (3): 13–15.
12. Huawei corporate website. 2021. Questions and Answers. https://www.huawei.com/us/facts. Accessed 8 Mar 2021.
13. Johnston, Alastair Iain. 2008. Social States: China in International Institutions, 1980–2000. Princeton: Princeton University Press.
14. Joske, Alex. 2018. Picking Flowers, Making Honey: China’s Military Collaboration with Foreign Universities. Australian Strategic Policy Institute; https://www.aspi.org.au/report/picking-flowers-making-honey. Accessed 28 May 2022.
15. Kolga, Marcus. 2020. Justin Trudeau must ban Huawei from building Canada’s 5G Network,” Maclean’s. https://www.macleans.ca/opinion/justin-trudeau-must-ban-huawei-from-building-canadas-5g-network/. Accessed 28 May 2022.
16. Maurer, Tim, and Cyber Mercenaries. 2018. The state, hackers, and power. New York and Cambridge: Cambridge University Press.
17. Mayer, Maximilian, and Gregory Mahoney. 2020. Beyond digital orientalism: Exploring China as cyberpower. Journal of Chinese Political Science.
18. Moore, Gregory J. 2020. The true origins of the Sino-American Thucydides Trap. In The US and China: Rising Rivalry, FIIA Report, ed. Bart Gaens and Ville Sinkkonen. Helsinki: Finnish Institute of International Affairs.
19. National Intelligence Law of the PRC. 2017. Chapter 1, Article 7. As translated into English via https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/#_Toc48640897. Accessed 28 May 2022.
20. Negro, Gianluigi. 2020. A history of global internet governance and its relations with ITU and ICANN. Chinese Journal of Communication 13 (1): 104–121. https://doi.org/10.1080/17544750.2019.1650789.
21. Nellis, Stephen. 2021. Intel to work with India’s Reliance Jio on 5G Network Technology. *Reuters*. https://www.reuters.com/technology/intel-work-with-indias-reliance-jio-5g-network-technology-2021-06-21/. Accessed 28 May 2022.

22. Pillsbury, Michael. 2015 *The Hundred-Year Marathon: China’s Secret Strategy to Replace America as the Global Superpower*. New York: Henry Holt.

23. Penettieri, Joe. 2020. Huawei: Banned and Permitted in Which Countries: List and FAQ,” *Channele2e*. https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/. Accessed 28 May 2022.

24. Poitras, Laura. 2014. “Citizenfour,” HBO Films.

25. *Politico*. 2020. Canada Braces for Consequences from China after Huawei Exec Loses Bid to Dismiss Extradition to U.S.”. https://www.politico.com/news/2020/05/27/canada-consequences-china-huawei-extradition-us-284779. Accessed 28 May 2022.

26. Said, Edward W. 1979. *Orientalism*. New York: Vintage.

27. Shih, Gary. 2020. Bristling at calls for Coronavirus inquiry, China cuts Australian beef imports. *Washington Post*. https://www.washingtonpost.com/world/asia_pacific/bristling-at-calls-for-coronavirus-inquiry-china-fires-trade-salvo-at-australia/2020/05/12/29e53058-93fe-11ea-87a3-22d324235636_story.html. Accessed 28 May 2022.

28. Singer, P.W., and Allan Friedman. 2014. *Cybersecurity and cyberwar: What everyone needs to know*. New York and Oxford: Oxford University Press.

29. Speglia, Catherine. 2019. How South Korea Built 5G, and What It’s Learning. *RCR Wireless News*. https://www.rcrwireless.com/20190912/5g/how-south-korea-built-5g-and-what-its-learning. Accessed 28 May 2022.

30. Thomas, Beryl. 2021. What Germany’s New Cyber Security Law Means for Huawei, Europe, and NATO. *European Council on Foreign Relations*. https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/. Accessed 28 May 2022.

31. Tomas, Juan Pedro. 2020. India’s Jio Platform Announces own 5G System. *RCR Wireless News*. https://www.rcrwireless.com/20200716/5g/india-jio-platforms-announces-own-5g-kit. Accessed 28 May 2022.

32. *USCC Annual Report 2012* (Washington, DC: United States China Economic and Security Review Commission, 2012; https://www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf. Accessed 28 May 2022.

33. Visontay, Elias. 2020. After Barley, what next? Australian industries exposed if China trade tensions persist. *The Guardian*. https://www.theguardian.com/business/2020/may/20/australian-wool-producers-particularly-exposed-if-trade-tensions-with-china-rise. Accessed 28 May 2022.

34. *Waterloo Regional Record*. 2022. Editorial: Past Time to Just Say No to Huawei. https://www.therecord.com/opinion/editorials/2022/01/03/past-time-to-just-say-no-to-huawei.html. Accessed 28 May 2022.

35. Weber, Valentin. 2018. Linking cyber strategy with grand strategy: The case of the United States. *Journal of Cyber Policy* 3 (2): 236–257.

36. Westcott, Ben. 2021. How China is devastating Australia’s Billion-Dollar Wine Industry. *CNN Business*. https://www.cnn.com/2021/02/16/business/australia-china-wine-tariffs-dsi-intl-hnk/index.html. Accessed 28 May 2022.

37. Woo, Stu. 2021. The U.S. is Back in the 5G Game. *Wall Street Journal*. https://www.wsj.com/articles/us-5g-companies-11621870061. Accessed 28 May 2022.

---

Gregory J. Moore (PhD University of Denver) is Professor of Global Studies and Politics at Colorado Christian University. He is a member of the (U.S.) National Committee on United States-China Relations, was president of the Association of Chinese Political Studies (2020–2022), and was a fellow at the Foreign Policy Institute of Johns Hopkins University’s School of Advanced International Studies in Washington, 2019–2020. In addition to many articles on international relations, he is the author/editor of *North Korean Nuclear Operationality: Regional Security and Non-Proliferation* (Johns Hopkins University Press, 2014), author of *Niebuhrian International Relations: The Ethics of Foreign Policymaking* (Oxford University Press, 2020), and *An International Relations Research Methods Toolkit* (forthcoming, Routledge, 2023), and has another book in the works on Sino-American relations.