Digital Divide: Geotechnology, Politics and the International System

Johnson Wong [Student No. 6316783]

Graduate School of Public and International Affairs

Major Research Paper

Summer 2020 Submission

Supervisor: Dr. Peter Jones

Table of Contents

Abstract

The international order is undergoing a transformation with much of it being driven by technological innovation. While states jostle for position in this modern global hierarchy, new and old alliances are forming along two strategic streams: On one side are mostly Western democratic countries led by the United States, and the other side consists of autocratic and illiberal states led by China and Russia. Whereas the incentives of globalization and capitalism will compel states to cooperate economically, this new order will be politically and digitally divided. Not only will this irrevocably alter the liberal international system that has dominated the last 50 years, it will tip the balance of power in favour of regional hegemons.

While this major research paper will show that the continued era of an American-led liberal international order may be uncertain, there are still powerful institutional pressures that could intervene and influence the trajectory of history.

Digital Divide: Geotechnology, Politics and the International System

Technological innovation is one of the most important goals that a state can devote resources towards. In popular literature, technology is described as the 'great equalizer' between states (Choucri, 2012, 128); technological innovation enables relatively small powers to affect change in the international system that exceed their predicated power capabilities based on more typical metrics like population, gross domestic product and military size. For many countries, the power of the state is measured by its ability to influence regional neighbors, and whether that type of influence can be projected further abroad. The strength of that influence can be assessed through both soft power indicators like pop culture, religious affiliation and common social norms, as well as hard power indicators more commonly measured by military strength, nuclear capabilities, and being a member of a security alliance. For the last quarter century, only the United States (US) has been able to overwhelmingly exert its influence globally and in doing so, has dominated the international system. In fact, when it comes to its hard power capabilities, the US is the only country that can deploy a military force anywhere in the world – supported by a standing army of 480,000 soldiers, and with an approximately equal number in its reserve service (Cancian, 2020, 1). As well, US technological superiority provided by well-known Silicon Valley companies, its free-market brand of liberalism established through global institutions, and its popular culture expressed through Hollywood, are recognized worldwide. Its economic power, measured in gross domestic product, is estimated at over $20 trillion dollars, and its industries dominate multiple sectors such as financials, medicine and consumer goods (World Bank, 2018). This manifestation of hegemony is unparalleled in world history and has contributed to a relatively stable international system.

That is, until now. Aligned with the United States' own 'pivot to Asia' foreign policy during the Presidency of Barack Obama, the US recognized that Asia would be the next emergent region to play a critical role in the future of the international system (Iwamoto, 2017, 1). The region was undergoing a complex transition – some call it a transformation – that was realigning relationships among states and concepts of sovereignty, asserting different normative values across the world stage, and changing the balance of power; the scale of this transition had not been witnessed since the height of the Cold War. Undoubtedly, global power is reorienting towards Asia, but also the former Eurasian power of Russia who, like China, appear to be seeking a broader multipolar international system in order to secure its own national security and gain influence over others (Ciolan, 2014, 633). This global transition of the international system is being enabled and, in many respects, exacerbated by technology, technological change and, through the contemporary engine of economic innovation, the Internet. While global financial, media and consumer systems are now more integrated than ever before, normative values about the structure of those systems and how they should interact are being re-examined – especially by the Chinese and Russians. The United States' norms and values benefited from the technological revolution because it created some of the most important technologies used today and therefore, was able to set the underlying rules for their application. However, a peace created by a hegemon cannot be sustained forever, for multiple challengers will emerge from the peace and attempt to disrupt the status quo. Indeed, as Friedman argues, economic wealth and capital is distributed through globalization, and as a result, a hegemon's power begins to fragment and the accumulation of wealth and power that was once centralized becomes decentralized within the larger system (Friedman, 2002, 36). In essence, it is not just simply about the ability of a

hegemon to maintain power over the long-term, but through its efforts, it will also inadvertently create the conditions for challengers to emerge.

Geotechnology and politics

Firstly, the definition of geotechnology for the purpose of this major research paper refers to the interaction between technology and the rules, regulations, norms and structures that govern technological innovation and development, and its influence on state power and global politics (Triolo, 2020, 2). Geotechnology not only looks at the technical aspect of how technology is developed, but also considers whether underlying socio-economic structures, prevailing values, and design principles of the technology itself can shape state behaviour and the international institutions governing its use. In contemporary state politics, technology is changing the global balance of power in dramatic ways. From new technical standards being considered for emerging telecommunications infrastructure, the increasing militarization of cyberspace, to the programming language used to develop applications, all these factors demonstrate that technology has a considerable impact on the international system. Admittedly, technology alone is not the only determinant of power, but its interaction with other political, social, economic and environmental forces makes it a supreme enabler to those other agents. Molnar describes the example of surveillance technologies becoming ubiquitous across societies enabled by a technological environment that is providing unprecedented means for governments and the private sector to monitor individuals in every facet of their life. The result is that there are few, if any, everyday practices that do not create some sort of ‘digital exhaust’ or ‘data shadow’ whereby personal behaviours, interests, associations and geo-locational patterns are mirrored in multiple forms (Molnar, 2017, 382). Taken together, the Internet’s global reach and utility as a tool for

political, economic and social change is increasingly becoming the main driver for global wealth, political engagement, and national security (Thiel, 2017, 220). Geotechnology matters now more than ever because of the global reach of the Internet and the ability to enable (or disable) individual and state participation in the global community based on the preferences of those states that control the levers of power.

An evolving international system

That being said, technology itself does not intentionally favour a great power's economic system or values over another. A networked system is agnostic insofar that its interests are not self-serving and can be used either to support political engagement or to curtail political protests – often simultaneously depending on the environment. It is state leaders and those in authority that assign a purpose to technology, and those states are increasingly divided along historical and political lines. There is the US and its liberal democratic allies on one hand, and on the other, an increasingly powerful group of authoritarian states, most notably led by China and Russia. Over the last decade, political discourse in many Western democratic countries have taken a gradual shift towards exploiting political divisions through a combination of identity politics, neo-nationalism and wealth inequality. In a growing trend, political systems across the Western world are assimilating extremist and radical groups into the mainstream political discourse, such as in France and Germany (the *National Front* and *Alternative for Deutschland*, respectively), the now defunct *Tea Party* in the United States, Bolsenaro's triumphant *Alliance for Brazil*, and Durete's popular *People of the Town's Party* in the Philippines. These are not isolated cases – the election of authoritarians within democracies reflect the growth of authoritarian ideals and values around the world (Luce, 2017, 99). The Western liberal model that has been championed by the US,

Canada and other countries is slowly losing its appeal with alternative models of political systems being considered, in some cases, preferred. Muller ponders, "[The] question has arisen whether China and other illiberal states rather present an alternative route for the international order to take, one which questions the assumption that the western liberal model is the only way to go" (Muller, 2015, 216).

Indeed, championing this alternative model is China, whose one-party system has ruled the mainland since the Maoists defeated the Chinese Nationalists (Kuomintang) in 1949. While the Chinese have emphasized in their policy and public communications both domestically and abroad a desire for a 'peaceful rise' within the existing international framework, many of their actions over the last decade have caused concern from their neighbors – in particular from US allies like Japan and South Korea, as well as regional adversaries like India and Vietnam. While a nuclear war in the region is highly unlikely, a limited war to achieve certain political goals, such as reunification with Taiwan, is probable. Sidorenko speculates that, "… the purpose would be to challenge the existing security arrangement and create a new regional order whereby a more destructive future war can be avoided" (Sidorenko, 2015, 1260). At the same time, Russia's experiment with democracy after the fall of Communism in 1991 has failed. Over the last decade in Russia, there has been a significant concentration of power in Vladimir Putin, who has most recently put forth a constitutional amendment to make him President until 2036 – effectively ensuring his appointment for life in the Russian Federation (The Guardian, 2020). While modern day Russia does not possess the same potential global power capabilities as China, these examples are evidence of a trend by authoritarian states to consolidate power as continued American hegemony is challenged. In fact, the quasi-alliance between the former communist countries of Russia and China has revived notions of a new geopolitical rivalry – or a "Cold War

2.0" – to challenge the existing international order. This is not a struggle based on the ideology of Marxism but driven by Chinese and Russian technocrats. Karaganov says, "In the late days of the previous Cold War, China and the Soviet Union were antagonists. Now they stand together. The Russian–Chinese alliance is becoming an objective reality even though it has not been formalized" (Karaganov, 2018, 89). A possible renewed alliance between these former allies also appears to be more strategic in its goals in that it does not contemplate dismantling the existing liberal order; rather, it is more interested in working to create a separate space for themselves and their allies. In 2014, Foreign Minister Wang Yi, during his opening remarks at the Symposium on International Development and China's Diplomacy, appeared to take a page from the liberal playbook and argued, "… countries, regardless of their sizes or levels of development, should respect each other's sovereignty, independence and territorial integrity as well as each other's choice of development path and values" (Xinhua News Agency, 2014). This new space would be aligned with their own political structures and governments, social values and technological systems. To facilitate those changes, China and Russia are, in a host of international forums, working groups, and standard-setting bodies, collaborating to actively institute new global standards for technological development that align and operationalize their authoritarian vision (Adonis, 2019, 274). While technology may not have a political opinion, state actors certainly have a vision, and geopolitical rivalry has arrived in the digital era.

Thus, this paper will examine how geotechnology will underpin and accelerate a digital divide between the great powers which will fundamentally alter the international system. The first section of this paper will describe the key drivers of this disruption from a technological, economic and cultural perspective. The first part will broadly explain what is 5G and the importance of this technology within the paradigm of great power politics; then, there will be an

analysis of key economic sources of conflict, particularly the central role of China in the global manufacturing supply chain; the last part will take a comparative view of values as they relate to the development of technology, and how culture contributes to the divide between liberal democracies and authoritarian states. The second section of this paper will examine how these drivers impact the notion of sovereignty, and how global alliances will accelerate the bifurcation of global systems, including technological standards and the Internet itself. The final section of the paper will describe this emerging international system and how the digital divide could manifest, raise important criticisms of this analysis, and answer the question as to whether this future is inevitable.

Drivers for change

5G and the networked future

Geotechnology is a relatively new field that looks at the relationship between geopolitics and technology, and the effects of how technology, intentional or otherwise, are shaping the political strengths of states (Bremmer, 2019, 1). From empowering liberal democracies through social media political campaigns, to strengthening dictatorships with unprecedented surveillance capabilities and data analytics, geotechnology is creating opportunities and systems for the state to shape the citizen (Yang, 2014, 111). Further, geotechnology encompasses not only what are the technical features included in the latest iPhone, but also encompasses what regulations and standards are used to develop and build those devices – as well as who owns the software, patents and licenses to use them. 5G is the 5th generation mobile network that is currently being developed that will set the new global wireless standard. Paul Triolo from Eurasia Group (2018)

explains as smartphone cameras and screens became more advanced, demand for data applications such as video streaming exceeded the performance capacity of existing 4G networks. The 4G network architecture faced limitations in terms of the number of devices able to connect simultaneously, and the ability to achieve very high data rates for modern applications, such as streaming high-definition videos. 5G was designed from the ground up to handle a massive number of devices, high-data rates and applications that require very fast and reliable communications with minimal latency, or lag, such as connected and autonomous vehicles. To deliver these features, 5G networks are divided into three primary network "slices," each serving a different primary function:

- **Enhanced mobile broadband (eMBB):** This portion of the network, likely to be rolled out first and to use aspects of existing 4G LTE architecture, enables much higher download speeds for smartphones and other devices, up to ten times faster;
- **Ultra-reliable low-latency communications (uRLLC):** This segment is designed for many applications including autonomous vehicles, which require there to be little or no gaps in communication for mission-critical applications such as road obstacle sensing and command and control. This portion of the network will require considerable investments in new equipment to get communications capacity nearer to roads and buildings. It also requires new antenna designs and smaller equipment that will provide dense coverage.
- **Massive machine-to-machine communications (mMTC):** This segment is designed to handle billions of new sensors and other "edge" devices that will communicate among themselves and with other parts of the network, also known as the Internet of Things (Triolo, 2018, 7).

It is obvious that 5G will dramatically change how individuals, businesses and the state will interact with one another in this super-networked, always-connected digital universe. This new technology will enable greater opportunities for enhancing individual life, but also pose serious security concerns given the number of connected devices and the potential data generated through each transaction.

Politics of 5G

As previously mentioned, 5G by itself is not a security threat per se – indeed, it is just the next, more advanced version of technology that already exists. However, much of the public debate related to 5G has been about data and the systems being developed, most of it in the space of artificial intelligence which will be necessary to manage and process the amount of information generated from connected devices (Triolo, 2020, 3). As part of a larger shift in the technological ecosystem, proponents and critics of the technology point to the vast amount of information collected by 5G towers, the complexity of simultaneous actions needed to manage artificial intelligence applications, and uncertainty related to the consequences of storing this amount of data on next generation cloud services within so-called 'smart cities'. 5G is meant to tie these technologies and capabilities together into a coherent and seamless network across physical territory and cyberspace.

The Defense Innovation Board, in their report of the *5G Ecosystem: Risks and Opportunities for the DoD* (US Department of Defense), highlight that the US 5G bandwidth standard that has been adopted by the military is currently at odds with the rest of the world, particularly China's own standard. This decision has slowed US progress on implementing and deploying the technology. Without US leadership, China has been able to make substantial

advances and have taken the global lead in the design, promotion and deployment of their version of the 5G specification (Medin and Louie, 2019, 3). As with previous technological transitions, 5G will entail similar potential risks and rewards, but on a much more global scale. The challenge for the US government is that it is behind not only in finalizing its technical specifications for the 5G spectrum, but that through a series of government-led decisions, a large portion of the spectrum has been allocated to the military; this will pose a challenge to the commercial and consumer sector which has historically been the driving force behind the adoption of new technologies (Medin and Louie, 2019, 10). At the same time, the Chinese have embarked on a strategy of viewing 5G as one component of a grander 'Digital Silk Road' initiative to ensure that leading Chinese platform players such as Alibaba, Tencent, and Baidu, as well as Huawei and other state-backed telecommunications carriers can take advantage of the Digital Silk Road umbrella and national market access provided by Belt and Road Initiative (BRI) projects to compete in emerging markets against US companies, specifically in areas related to powering smart cities, cloud services, mobile payments and social media applications (Triolo, 2020, 1). In doing so, they will be able to augment and promote Chinese technology standards through a unified approach that can influence local governance, law, trade and security (Hemmings, 2020, 6).

In fact, tying 5G technology to BRI investment is a tactic by which China will be able to lock developing and developed countries to its 5G technological systems. The BRI is a global development strategy that aims to connect countries, through infrastructure development and investment, and move countries closer toward Beijing's economic vision (The State Council, 2020). This approach involves making direct investment funds and resources to local and state governments in a bid to win infrastructure contracts to facilitate trade. For developing countries,

BRI projects are viewed as ‘modernization’ initiatives that so far have linked over 70 other countries geographically along BRI corridors towards China. In 2017, these economies received 35% of global foreign direct investments and accounted for 40% of global merchandise exports (The World Bank, 2018). For more developed Western countries, BRI investment is more diverse with funding focusing on the development of civil aviation, smart ports, energy development and telecommunications. Thus far, few Western democratic countries have accepted BRI funding, fearing reliance on Chinese equipment and investment dollars for critical state infrastructure poses too high a risk to national security. The World Bank posits that special provisions would need to be taken into consideration and even with robust oversight, BRI projects already pose a higher-than-normal risk, not including all the other types of risks that major infrastructure projects face, such as debt risks, governance risks (corruption and procurement), standard infrastructure, environmental and social risks (The World Bank, 2018). In developing countries, these issues are more acute as governments can be unstable, and institutions weaker; BRI could trap developing countries in debt-webs – and other forms of commitments – which they would be unable to escape. While most Western democratic countries have been wary of BRI funding, Italy became one of the first Western country – and G7 member – to accept BRI funding in 2019, with deals amounting to $2.8 billion, including investments in port infrastructure in Trieste, Genoa, and Palermo, with the objective of giving Chinese goods faster access to Europe (Chatzky, 2019).

Impacts of 5G

Clearly, the global rollout of 5G is important because it will determine the next international standard for implementation of the technology, how telecommunication networks

will be built, and who will make the money between participants in the 5G ecosystem. Companies whose technology becomes the industry standard for 5G will receive royalty payments from other ecosystem participants. Unlike 3G and 4G, where China was largely relegated to the sidelines in the standards-setting process, China has been heavily involved in the standards process for 5G – a recognition that it sees this moment as an opportunity to assert its power and influence (Triolo, 2018, 8; Schiller, 2011, 99 – 100). The current debate about 5G standards is extremely important because of its integrator role in a wide range of future applications. For the first time, 5G integration will necessitate the reliance on artificial intelligence as a key technical component, which raises the specter of having foreign AI technology in the technical "heart" of another country's national security systems. In addition, 5G matters now because of the 'first-mover' principle which predicts that the first commercial deployment of 5G will gain a massive advantage as governments, businesses and consumers adopt that standard for their devices and applications. The first-mover thus has the ability to set the parameters for the technology, including the exclusive rights to certain intellectual property patents, standards and gain default market penetration (Medin and Louie, 2019, 6). This also means that the first-mover of 5G technologies will also benefit from a massive advantage as more businesses and consumers adopt their version of the protocol, it will make it very difficult (and costly) to change those standards once physical infrastructure – like telecommunication towers and software applications – have been constructed, developed or purchased.

Historically, it was Western countries and allies – particularly Japan – that had dominated the telecommunications space. European companies, like Ericsson and Nokia, were first to come out with 2G technologies in the mid-1990s which quickly propelled those countries networks, regulatory frameworks and licenses to the top, generating significant economic benefit to their

economies. By the end of 1999, Japan took the leadership role in 3G technologies – called i-mode service – and were able to generate on a per-packet basis up to 91% of economic value from the proceeds. Estimates suggest that Japanese telecommunications carriers and developers generated $9 billion a year by 2007 and $12.8 billion by 2008 in domestic value alone. Subsequently, the US took the lead on 4G – resulting in key players like Apple, Google, and AT&T spinoff Lucent Technologies – as well as other US technology companies, to dominate this area. In 2011, wireless industry GDP totaled $195.5 billion. By 2014, when 4G reached 40% penetration in the US, wireless industry GDP was $332.9 billion – a increase of nearly 70% (Recon Analytics, 2018). For these reasons, there is tremendous pressure by companies, especially Chinese state-owned companies, to roll-out 5G technology as quickly as possible and push early adopters to use their version of the technology. In building momentum, they are able to snowball the effect of their first-mover advantage and become the only solution in a country before other competitors, like US or Scandinavian companies, are able to enter the marketplace.

On this matter, the threat posed by Chinese leadership on 5G, particularly from Chinese state-backed companies like Huawei, raises significant concern among Western democratic countries. As 5G is deployed around the globe, there is fear that the technology used by Beijing to surveil its own citizens will threaten the national security of Western countries. Data gathered from 5G will be able to provide unprecedented insights into citizen behaviour, and be used to shape public opinion and discourse, as well as enhance law enforcement capabilities. The three major multilateral agreements governing these aspects of cross-border data flows are the European Union's General Data Protection Regulation (GDPR), the Cross Border Privacy Rules (CBPR), and the digital trade portion of the Comprehensive and Progression Agreement for Trans-Pacific Partnership (CPTPP). Countries in Europe and Asia are gradually aligning their

domestic regulatory frameworks for data with these agreements. However, O'Hara and Hall note, "Where China and the United States are each large centralized markets, enabling the gathering of giant quantities of data to fuel their algorithms, Europe is more fragmented, both in terms of markets and in terms of the dominant tech companies, and this decentralization is exacerbated by the GDPR's stern regulation of data sharing" (O'Hara and Hall, 2018, 7). Other large players like India and Brazil are also considering how to interoperate with these data regimes or risk becoming digitally isolated (Triolo, 2019, 2). For the moment, US privacy laws are pushing against requirements from the European Union, which has traditionally enacted stricter rules with respect to the collection and manipulation of individual citizen data. However, this push is not universal across the country and is still highly debated between regulatory, legal and corporate leaders.

At the same time, corporations driving these data provisions (and liberalizations) are competing against state interests that are seeking special exemptions based on national security grounds. The concern related to Huawei is that they would build, on behalf of the Chinese government, backdoors and traps in their technology and equipment platforms that would provide access to sensitive and top secret information and data for the Chinese government. Ward Elcock, former Director of the Canadian Security and Intelligence Service explains in an interview with CBC Radio, "Traps and points of accessibility that are effectively hidden from users, but make it easier for some who are aware of the traps and back doors to access the technology, or to gain access through the technology to whatever is traveling through the technology — whether that's strictly communications and/or any other information that's traveling through it" (CBC Radio, 2018). These types of national security threats and potential technological backdoors have also been identified by the UK and United States national security

agencies (NCSC, 2020; Kaska, Beckvard and Minárik, 2019, 7). The security dilemma posed by Huawei, and other vendors from authoritarian governments, is extremely complex as Western countries seek to balance between stimulating the economy, protecting national security concerns, modernizing infrastructure at reasonable costs, and complying with the international trade regime. Western democratic countries are wary of Chinese domination of this space due to incidents and sustained accusations by many countries of Chinese companies engaging in corporate and technological espionage, including stealing commercial patents and personal information (Triolo, 2020, 8; Choucri, 2012, 144). Approving Huawei technologies into the core systems of state infrastructure would essentially be giving a direct entry to the most sensitive parts of the government and society.

Even as this debate remains unresolved among Western allied countries, China is moving forward and pushing its narrative about the role of data and how it should be used. To create this alternative market, China has created, through its own state-backed companies, mirrored versions of all major global technology platforms. For instance, Facebook, Google and Twitter all have their Chinese versions in WeChat, Baidu, and Weibo, respectively, which are not only larger in terms of total number of users, but also more economically profitable than their American versions. In fact, the domestic Chinese market alone in 2019 was estimated at over 850 million internet users, compared with the United States at about 290 million users (Statista, 2019), and is larger than the existing global penetration rate of all global users for those three social media platforms combined. The only potentially larger base of users in the future to challenge the Chinese market will be Indian. Coucri notes, “In terms of numbers alone, China’s population exhibits a very high cyberspace presence. Such numbers suggest that China will become the

largest Internet user, far outstripping the United States, with India possibly becoming the second largest user" (Choucri, 2012, 57).

Lastly, the reason why 5G changes the game is because one of the key corporate players in setting the global standard, Huawei is legally bound to comply with the Chinese Communist Party (CCP). Under Article 7 of the Chinese National Intelligence Law of 2016 requires all companies "to support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organizations that support, cooperate with, and collaborate in national intelligence work" (Kaska, Beckvard and Minárik, 2019, 11; Duchâtel and Godement, 2019, 13). In the same manner, the 2014 Counterintelligence Law with its implementing acts lays down obligations for "relevant organizations and individuals" to provide information, facilities, or other assistance, and states that relevant organizations and individuals "must not refuse" cooperation. It goes without saying that these Chinese legal obligations are also enforced, from a Western perspective, by an opaque judiciary that is not functionally independent from the CCP and is not subject to public oversight regarding judicial decisions. Moreover, not only does Huawei have a legal obligation to support the CCP in areas of national security, the Huawei corporate leadership is politically and personally connected to the party leadership (Kaska, Beckvard and Minárik, 2019, 19). The state-backed Chinese Development Bank was instrumental in providing the initial funding for Huawei technology research during the early days of the company, and was thus able to influence its corporate vision to focus on improving the lives of Chinese citizens through technology, so long as these improvements did not interfere with the political rights of the state party.

Economy and technology

It is impossible to emphasize the significance of 5G, technological modernization, and the redrawing of the international system without discussing the economy. Indeed, great power rivalry typically includes some sort of economic competition, such as access to natural resources or consumer markets. Contemporary state rivalry – involving updated tactics that leverage the exploitation of strategic resources or manufacturing capabilities – suggest the creation of two potentially countervailing military and political-economic alliances that are in conflict for control over key continental focal points and littoral resources (Hall, 2019, 5). While there are debates about which economic model is better for financial prosperity and wealth generation (and some would argue equality), broadly speaking, many countries have benefited from globalization and the capitalistic economic framework led by the US since Bretton Woods (Crouch, 2019, 15). The modern state and the economic prosperity that has been achieved globally can be measured by increasing global wealth and decreasing rates of extreme poverty. It is these two factors which have resulted in some of the most remarkable economic changes around the world. While China alone accounts for much of this remarkable success, the last few decades of worldwide economic growth has also included many countries in Africa, South America and South East Asia, and has resulted in 1 billion fewer people living on less than $1.25 U.S. dollars a day, a threshold that the World Bank defines as extreme poverty (Radelet, 2015, 5). While there remains much work to do, the data points towards an undeniable trend: As countries adopt free-market capitalism, they must also implement common economic practices and regulations in order to benefit from the rules-based international marketplace. Ironically, Western economies no longer have the monopoly on advancing these free-market enterprises, and the highest rates of wealth generation are increasingly shifting to state-backed companies within authoritarian states. So, while

authoritarians may be playing by a different set of domestic state rules, they are successfully achieving a capitalist modernity through their own political system (Deudney and Ikenberry, 2009, 3). The strength of the capitalist market economy has penetrated formerly socialist-communist states, like China and Russia, with impressive success.

Indeed, economic growth and prosperity has been a necessary condition for authoritarian governments to retain their popularity and legitimacy. Without economic progress, their countries would not be internationally competitive, and their own legitimacy and political power could be thrown into question (Kurlantzick, 2016, 19). One of the differences between free-market systems like those found in most Western democracies, versus authoritarian state-backed capital market systems like China and Russia, is the company's relationship with the dominant political party, and whether their success is contingent on the political power of the state. In the technology space, state-backed enterprises are crucial in countering the US-led coalition in governing the Internet. In the case of China and Russia, there is internal opposition to what they perceive as inequitable domination of the political economy of the Internet by US companies in which they have responded by promoting domestic digital media champions. "Leading national enterprises are not solely brought up rhetorically, but are brought to participate in interstate events under the banner of the Internet sovereignty brand. Baidu and Yandex have played a particularly prominent part in this emerging trend" (Budnitsky and Jia, 2018, 601). As 5G and the telecommunications sector becomes a pivotal facet to project power abroad, more attention is being geared towards ways to monetize the data gathered by those systems. Constructing 5G infrastructure will cost billions of dollars, but the return on investment in terms of royalties, patents and new economic wealth generated by data will be significant. O'Hara and Hall say, "Indeed, the strength of 5G in collecting and harvesting data is one of the advantages of this

technology" and will be "… another growing source of advantage for China [as its] internet economy generates far more data than any other, partly because of its size and partly because much Chinese commerce has moved on from cash to electronic payments. The social media app WeChat has become dominant in China, not only for communication with friends, family and work colleagues but also for mobile payments." (O'Hara and Hall, 2020, 8).

The role of supply chains

China is the world's global superpower when it comes to manufacturing. Based on a United Nations report published in 2018, China accounted for 28.4% of global manufacturing output calculated on a value-added basis in US dollars, ahead of the United States at 16.6% and Japan at 7.2% (Statista, 2019). In terms of strategic technological inputs into the system, aside from the United States, Japan, South Korea and a handful of other countries, no other state plays such a key role in the global supply chain of computers, smartphones and electronics. The Chinese have strategically focused domestic industrial policy in building and improving their manufacturing sector as a means to ensure parity with other great powers to, "… centralize trade and mitigate vulnerabilities that make China vulnerable to supply-chain disruption" (Brown and Iverson, 2018, 384). The speed of manufacturing, and the ability to create sophisticated products quickly and at a low-cost cannot currently be accomplished as reliably anywhere else in the world. The result is an international supply chain dependent on Chinese manufacturers as a matter of expertise and to contain costs. This strategy, beginning as early as in 2009, demanded that foreign companies whose products were sold to the government be developed in China, and enforced the mandatory creation of joint-partnerships with local companies and third-party logistical providers. As these local companies learned from their Western counterparts, the

Chinese government also issued product standards and specifications that forced foreign suppliers to develop special versions of their applications for China, allowing Chinese equipment makers to circumvent Western patents and royalties (McCrea, 2016, 51; Hout and Ghemawat, 2010).

This dependency on Chinese supply chains poses several problems. First, global dependence on Chinese manufacturers of core components of technological systems are continually vulnerable to corporate theft and espionage. This is a well-known problem and has been identified by several governments and technology companies since businesses started to locate in China (Kaska, Beckvard and Minárik, 2019, 10). According to a 2017 report by the United States Trade Representative, Chinese theft of American intellectual property costed the US between $225 billion and $600 billion annually (USTR, 2017). Even though Chinese technology companies are often backed by state resources, they are still unable to compete with American and other international companies, especially in software development. One reason is that the US has a lighter regulatory approach to innovation and can drive investment through rapid innovation and experimentation. The Global Entrepreneurship and Development Index (GEDI) collects data on the entrepreneurial attitudes, abilities and aspirations of the local population and then weights these against the prevailing social and economic 'infrastructure', including aspects such as broadband connectivity and the transport links to external markets. According to the GEDI, the US ranks number one on the index (GEDI, 2018). In contrast, the Chinese model tends towards heavy regulatory measures with a more top-down approach to ensure compliance with state objectives, which have the effect of slowing down the pace of innovation. According to the GEDI, China ranks 43 out of 137 countries (GEDI, 2018). That being said, the Chinese do possess an ability to rapidly scale-up once a solution or technology

has been approved by the state. With respect to 5G deployment, the population density is much higher in China and therefore the benefits of 5G are expected to be realized there sooner than elsewhere. In the meantime, China will still copy Western software solutions as there is still a generally positive stereotype of foreign brands among the Chinese population due to this image having been shaped over many years (Hout and Ghemawat, 2010; Özer, Zheng and Ren, 2014, 2442).

The second issue with supply chains being dependent on China is that global technology companies are restrained in their ability to retaliate against the Chinese government because they rely on the Chinese consumer market to bolster revenues internationally. For instance, McKinsey and Company estimate that the online retail transaction value for digital goods in China is $1.5 trillion dollars – this is larger than the online retail market of the next 10 markets combined (McKinsey Digital, 2019, 1). As a result, not only do global technology companies need the Chinese consumer marketplace to be profitable, but to do so will require careful management in their response – or perceived retaliation – to corporate and industrial espionage. The political fallout of Western technology companies being shut out of the Chinese consumer marketplace could be disastrous for a company's ability to be profitable and meet shareholder expectations. In the current economic climate, decoupling from China has thus far not been a successful gamble.

As previously mentioned, economic success is a function of Chinese political necessity, and the Chinese Communist Party leverages foreign economic entanglement with its own bid for leadership in technology and Internet governance as a way to realize broader geopolitical goals. The strategy to link socio-economic progress through technical standards and norms has long been a tool of the United States. Timmers argues that, "Legislation for strategic autonomy based on "like- mindedness" may be formulated in an inclusive but also in an exclusive way. Examples

of the latter are the USA's trade and foreign direct investment restriction and, in particular, its Entity List" (Timmers, 2019, 15). By setting the agenda on internet governance and integrating global economies through complex international supply chains and domestic regulatory rules, China uses its central position to steer outcomes in the international system to better align it towards its own definition of governance. The authoritarian agenda therefore is to work within the liberal institutions that have created the conditions for economic success, and seize them to meet Russian and Chinese political goals. Karaganov says, "Now neither Russia nor China is trying to impose their models of development or ideology. However, they are offering an alternative. China is building an effective non-liberal economic model as an alternative to the liberal economic agenda" (Karaganov, 2018, 86). In Beijing, economic prosperity is considered an international value that aligns with the Chinese culture and sense of position in the world, but political concepts of liberalism and democracy are foreign. Brown and Iverson explain this philosophical partition clearly:

> Foreign philosophical underpinnings and independent adjudication is perceived as Western-dominated, which creates distrust. This originates from perceptions within the Communist Party of China that international law writ large is a foreign construct, derived from liberalism and European traditions, which are closely associated with imperialism. Beijing has long complained that the global order was constructed when China was weak, and the rules of the game were rigged against it. This is in large part because this current system organizes Asia as a multilateral versus hierarchal conglomeration of states (Brown and Iverson, 2018, 377).

Undeniably, China cannot achieve this re-ordering of the international system alone; instead, the Chinese have amassed a broad network of allies with whom it can rely upon to support the way it does business without interfering with their own political system. This focus on separating politics and economy is being replicated in a Chinese state-driven cyberspace.

The United States created the modern-day Internet as a communications and information-sharing tool between the military and academia, and with it, has been able to achieve remarkable success in commercializing it through a decentralized model of internet governance. The role that the military and academia played at the outset in the development of the Internet did not result in a state-dominated system; instead, a highly differentiated, hybrid structure developed, in which the legitimacy of the system was based on experts. Commercial actors such as Internet service providers and hardware developers (and later also content providers and Internet-based suppliers of services) played a major part in the cooperative structures of Internet governance (Thiel, 2017, 218). Authoritarian powers, like China and Russia, believe that a state-driven model of the Internet is possible if the right conditions exist, such as an expectation of the state to advance individual wealth, or to reflect a peoples' narrative of themselves. If the state can build a system that integrates these key principles – whatever they may be – then a differentiated political system is possible, and in some cases even preferable over liberalism and democracy. For these arguments, the next section will explain the culture of division driving the digital divide.

The culture of division

The United States and China recognize the importance of the Internet and cyberspace as a tool for improving economic prosperity, strategic communications and national security; yet, the perspective that each country brings in terms of how they view cyberspace differs due to nationalistic characteristics. Certainly, these approaches are not uniform and can be challenged within the national discourse – particularly in the United States, less so in China – however, the values, norms and culture of a nation manifest in the intangible soft power versions of

institutions that they lead and compete with one another in the international system. This divergence forms the basis of geopolitical and geo-economic tensions between the US-led West against China and Russia (Simons and Kukartseva, 2019, 84).

Western liberalism and the Internet

The philosophy of technology is the study of the nature of technology and its social effects. Western philosophy is based on a set of inquiry dating back to Ancient Greece, and when applied to technology, stems from Logos as the universal principle of order and knowledge, which underlines the rational application of technology, basing ethics on the first Logos and first philosophy (Cao, 2011, 1611). Modern liberalism is grounded in the philosophy of free thought, debate and notions of cooperation among states to achieve common goals through institutions. The concepts of free inquiry, democracy and humanitarian principles play a key role in the design of technological systems today, and manifest in ideas like net neutrality, distributed networks, and freedom of content. The Internet Corporation for Assigned Names and Numbers (ICANN), the international body that regulates the domain name registry of the Internet, operates its policy-making on a "multi-stakeholder-model that is community-based, taking a consensus-driven approach with the idea that Internet governance should mimic the structure of the Internet itself – borderless and open to all" (ICANN, 2020). These principles guide the US-founded organization in how it views Internet content, its underlying organizational structure, and its operations. In fact, Secretary Michael Chertoff and General James Cartwright have said of ICANN that the organization shares the American values of "freedom and democracy", and that these values should be spread around the world and shared by others as a basis for security at home through a free and open Internet (ICANN, 2020). Because of its inclusive approach,

ICANN is one of several key bodies in the regulation of cyberspace that are facing a political struggle for control of its guiding principles and governance structure, others include the International Telecommunication Union and Internet Governance Forum (Adonis, 2019, 271; Schiller, 2011, 97). Authoritarian states and non-US-allied countries have argued that as long as ICANN remains part of the US government, there will be suspicions about its actual neutrality and whether it is just a tool to project US power further into the domestic space of other countries (Schiller, 2011, 98).

Not surprisingly, in most Western democratic countries, cyberspace is another forum for political expression that encourages creativity, free association, and provides the means for individuals to influence politics:

> For advanced industrialized countries with competitive political systems, interaction and communication in cyberspace have become natural extensions of normal politics. In the United States, for example, a cursory look at the uses of cyberspace for specific political purposes shows some distinct patterns. In terms of day-to-day politics, communication by means of cyber venues is well established, large, growing, and with few observable constraints. People use email to discuss political events and send links to information of relevance. Many try to influence their friends and engage in political discussions on blogs where users can share ideas and debate topics. Political groups solicit donations on their websites, and supporters can transmit donations through credit cards online. Political groups can also organize meetings and rallies with expectations of greater efficiency over the Internet (Choucri, 2011, 142 – 143).

With the advent of social media, the ability and opportunity to create more informal connections and contribute to national and international conversations is more accessible and low-cost than ever before. Major social media and internet companies have long resisted the US federal government's calls to regulate online content on national security grounds. In fact, companies that represent the most popular Silicon Valley technology companies have appeared before federal congressional inquiries related to misinformation, hate speech and privacy in 2018 and 2019, to reiterate that while they have made improvements to their system to remove harmful

content, they must balance their interventions with the First Amendment and the freedom of expression (Washington Post, 2018; Politico, 2019).

Meanwhile, a United States Senate Report that was published on Russian interference in the 2016 presidential election on September 13, 2019, found that, "... the IRA [the St. Petersburg-based Internet Research Agency] sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Kremlin (United States Senate, 2020, 4). These challenges to the liberal version of an open and free internet reflect the culture and values from which the Internet was created. Hence, one way to target and negatively influence these norms, state actors like China and Russia use misinformation and disinformation campaigns to generate uncertainty and sow seeds of doubt. O'Hara and Hall state, "Disinformation is a particularly potent weapon against the West, where speech is freer (and it is easier to spread ideas), and where controlling the public sphere is seen as rather alien" (O'Hara and Hall, 2020, 11). Therefore, the Internet was built on the culture and values of Western liberalism – particularly the US' version – and its underlying governance model reflect those features.

Authoritarian governments and cyberspace

In contrast to the Western approach of rationalism and free inquiry, the Chinese approach to relationships is an important concept to understand as it provides insight into how China views technology and its relationship with state governance. As a more collectivist society preoccupied with social harmony and order, Leung, Brew, Zhang and Zhang note in their studies of *Harmony and Conflict: A Cross-Cultural Investigation in China and Australia* (2011) that ways of handling disputes are subject to cultural differences, and highlights finding in multiple studies on

disputes which show that East Asians are more likely to exhibit conflict avoidance than Westerners. For instance, Chinese people reported higher levels of conflict avoidance than Americans. In a similar study on Japan, conflict avoidance was also higher than Americans. The tendency for East Asians to avoid conflict is typically attributed to the influence of the Confucian value of harmony, which encourages people to tolerate interpersonal disagreement and transgression, and studies have found that the Chinese have higher concern than Americans for the other disputant and a perception that a direct approach would hurt a relationship (Leung et al, 2011, 796). This idealization of harmony and social order is fundamentally important as a cultural value borne from history and philosophy about foreigners – particularly non-Chinese. Schreer explains, "It is worth pointing out that for most of its modern history, China indeed had to focus on securing its land borders against the threat of invasion and instability" (Schreer, 2019, 512). The notion of the 'other' is a particularly powerful social and relational construct within East Asian society that it is considered in the study of ethics and morality, and which social pressure compels compliance with these norms in a very powerful way. Understanding the other is important in various interactions as it projects certain expected behaviours from individuals in an intuitive manner. Consequently, it also encourages more trust in the government by making certain "rights" or "freedoms" that Westerners may find fundamental to their humanity, easier to forgo if others are also expected to act in a similar fashion. Stapleton says, "Although ethical behaviour is an individual responsibility, social and institutional dynamics make it is easier to behave ethically in a community which values, supports and actively encourages ethical behavior" (Stapleton, 2016, 302).

Further to the primacy of relationships, how individuals see their own interest is worth highlighting. In terms of how negotiations are achieved, Americans are primarily guided by an

"interest" frame in which negotiators are motivated to maximize outcomes. This assumption underlies most current Western conflict models. In contrast, the negotiation behaviors of East Asians are best described as primarily guided by a "relational" frame in which harmony plays an important role (Leung et al, 2011, 804). Once again, the emphasis on harmony is a fundamental precept in Chinese culture – and other Asian cultures following the teachings of Confucius – as individual sacrifice is stressed in order to achieve broader social and community goals. While this principle may seem only applicable as a social construct, understanding this idea helps to explain how China operationalizes this construct in cyberspace. Adonis explains that China, "… promote[s] digital sovereignty through four important pillars: non-interference for internal affairs; data sovereignty; security concerns; and commerce. China exerts its digital sovereignty campaign at the domestic level by establishing its well-known Great Firewall, separating their internet ecosystem from the rest of the world, whilst actively promotes its internet and digital firms abroad" (Adonis, 2019, 270). The role of the state in this function is self-anointed and takes on the responsibilities of a 'benevolent official' in a relational hierarchal frame where the state is responsible for and expected to preserve social harmony, ensure economic prosperity and peace. The Chinese accept controls on content in cyberspace, including ubiquitous video and audio surveillance, as well as social controls that most Westerners would view as an infringement on individual liberalities, interests and rights. That said, the Chinese are not alone in accepting a greater role of the state in the daily affairs of their personal life. Russia has also been known to reject liberal ideals; historically, it has expressed its national character as traditionally patriarchal, masculine and a nation where a conservative military state with a strong army is considered as one of the most important parts of its political body (Simons, 2011, 82). Therefore, the portrayal by Western media that the Russian state government is trespassing on citizen freedoms is

fundamentally a construct of a Western paradigm projected onto others and which is unable to accept non-universality of liberal values and norms. Ciolan further explains, “Russia’s image was constructed also in opposition to “the other”. In this case, the other is represented by Western society. The self-image of Russia as a great power also means that the country expects to be treated as an equal by the other international actors. Nevertheless, Russia’s perception is that it is treated as a “second class state” by the Western states” (Ciolan, 2014, 637). Hence, the culture and values shared by China and Russia are important in understanding how they view technology and internet governance. It is not simply a difference in opinion about how technology should operate, but it is about a fundamental disagreement about the purpose and characteristics of the technology itself, what its purpose is vis-à-vis the state, and the principles it should operate on. For example, Jayne Docherty argues in the context of negotiations and mediation, one should not assume a concept of ‘rationality’ means the same thing to everybody and that the term can be misapplied when used to express a different point of view as culture may lead others to see the balance of pros and cons around an issue differently (Jones, 2015, 73). While repeated cultural interactions can help identify patterns, understanding the authentic meaning behind those interactions can be more challenging. In order to find a common interest among different groups of people, in this case Chinese and Russian technocrats within international standard setting institutions, competing ideas and interests expressed through “high context” interactions and “low context” dialogue can result in outcomes that are interpreted as challenging the process itself. The opportunity that authoritarian states see during this time of liberal uncertainty, coupled with the strength of their centralized state apparatus and renewed sense of national identity, is that they have an obligation to reshape the philosophical imperatives governing technological systems to better suit their own ambitions.

Governing cyberspace

This fundamental difference in understanding how 5G technological innovation as a tool of the state reflected in cultural norms is at the crux of the digital divide in the international system. The principles that guide ICANN which seek a "multi-stakeholder, community-based and consensus-driven approach" to the governance of the Internet, is anathema to the harmonious and strong central state championed by autocrats and their allies. The liberal governance model of technological innovation based on pluralism, freedom and consensus, are linked to Western democracy which in turn challenges the legitimacy of the authoritarian rule of the state. To maintain their political power, and unable to escape the trappings of technological modernity, China, Russia and other authoritarians will be determined to build a separate "other"-net to compete with the Western version, and in some cases, surpass it. Muller argues,

> The proclaimed differences are in interpretation and implementation, with China emphasizing the issue of priorities and progressive realization and rejecting the liberal model not as such, but the notion that it is the only model. In one respect, this reflects the indeterminacy and generality of the rhetoric of the 'international community'. However, it also raises the question of the nature of the international community. In some liberal views, all roads lead to liberal democracy along more or less western models. However, a truly pluralist international society which accommodates cultural diversity and accepts the principle of self-determination, would accept that countries can also take a different development path, as emphasized by China (Muller, 2015, 236).

While modern liberal democracies seek to accommodate diverse perspectives and build a plural political order, geopolitical interests based on nationalistic factors continue to dominate the discourse (Sidorenko, 2015, 1260). Even within liberal governments themselves, various data protection laws are becoming a point of contention between countries, with the European Union taking a more teleological vision about its universal development model and placing its model above geopolitical power politics and nationalism, to encompass a historical imperative that they believe should be replicated around the world (Browning, 2016, 110). The irony is that a liberal

system that values and respects plurality should accept equal but alternative value systems as legitimate (Muller, 2015, 219).

Digital sovereignty and the primacy of alliances

The three drivers mentioned above, 5G standardization, strategic economic dependency, and competing normative values, are transforming the international system and will result in a digital divide. Globalization continues to increase socio-economic transactions between states, and the growth of cyberspace has created economic value from consumer data. Various state operators compete with each other for consumer dollars while, at the same time, the need to cooperate to connect their networks with each other – using internationally recognized protocols – is creating tension between the public good of a seamless system, and the private interests of operators and the state (O'Hara and Hall, 2020, 10). Controversies related to 5G standard-setting by companies that are supposed to be impartial are contributing to a difficult process for all major players involved. Huawei, the leading Chinese operator that is participating on the 5G standard-setting consortium, has been repeatedly accused of being under the influence of the central Chinese state party. This poses a challenge in the existing liberal model of standard-setting for, if Huawei succeeds in its efforts to control the technical standards of 5G, will secure for the Chinese state a much bigger stake (and control) of the 5G patent licensing system. Once standards have been set and essential patents defined, companies must build to the agreed standards and pay royalties to patent licensees as required (Triolo, 2018, 10). These are supposed to be separate – and most importantly, independent – processes, but there is little doubt among the international 5G and telecommunications community that the Chinese state is directing

Huawei in order to obtain a substantial stake in the upcoming technological transition in order to secure its political and economic ambitions. It is important to note that once standards are set, governments and companies will be compelled to follow them or risk being non-interoperable with the rest of the world. In some cases, this is the strategic vision for China: By controlling the vast majority of 5G licensing patents and creating networked systems that only work with Chinese-branded equipment, it will be able to project its digital power abroad and force compliance. Without access to Chinese equipment, and a licensee payment system that is indebted to a Chinese state-backed company, antagonistic states will quickly become isolated and find themselves cut off. Sidorenko argues that, "The world is becoming more unified, but not safer; traditional regional conflicts are escalating into geopolitical conflicts ushered by the phenomena of globalization and all the changes and nuances it brings to the economic, political, socio-cultural and spiritual spheres" (Sidorenko, 2015, 1261).

The relativity by which actors are able to influence the political discourse and debate state sovereignty has never before been so uncertain, with the digital world becoming the new arena for states to challenge existing norms, values and economic systems of the past. The digital realm offers a different variation of sovereignty challengers that include the dynamics of non-state actors, such as private companies, civil society, non-governmental organizations, and even individuals, to question the legitimacy of the state and its relationship to external actors and those within the state (Timmers, 2019, 12; Adonis, 2019, 268). The fundamental challenge and struggle for states to maintain their independence in this space relies upon the extent to which state control of the technological tools, systems and structures are within their influence, and the extent to which they are able to maintain the independence of their national security networks without being isolated from the rest of the world.

Therefore, to achieve this global network based on common standards and shared values, an alliance of liked-minded partners is needed to buttress this digital divide. Timmers says, "Like-mindedness is based on shared values, whether these pertain to the individual (such as respect for privacy and autonomy) or to economy (liberal market economy) or to society and democracy (independent judiciary, freedom of expression, free elections) or to international relations (respect for the system of sovereign states and multilateralism). A wide range of governance tools can be mobilized for supervision, decision-making, and certification" (Timmers, 2019, 15). In the context of the digital divide, countries allied with authoritarian regimes will align their 5G technical standards, find commonalities in terms of political structure, and seek to share in the economic union driven by the divide. Alliances – especially historical alliances – will play a key role in accelerating this digital divide through collaboration between liked-minded states on both sides of the gap. The alliance between cooperating states will not just be an alliance of authoritarians – rather, it will be based on a common set of values and norms shared by the people and state government. These norms and values, as previously mentioned, will originate primarily from common values about the role of the state, its obligations to its peoples, and the extent that it is seen as legitimate by its citizens. Even in democracies, it is feasible for a country to ally itself with China if it finds that it shares more in common with the CCP than the US.

Like-minded values

Truly, China's foreign policy is renewing previous efforts tried in the past that sought to establish in international law the Five Principles of Peaceful Coexistence: mutual respect for each other's territorial integrity and sovereignty; mutual non-aggression; mutual non-interference

in each other's internal affairs; equality and mutual benefit; and peaceful co-existence. The Principles were first formulated in a treaty with India in 1954. They were subsequently adopted by twenty African and Asian states during the Asian-African Conference at Bandung in 1955, which contributed to the establishment of the Non-Aligned Movement in 1961 (Muller, 2015, 225 – 226). Common 5G standards across those participating countries would enhance economic ties. The idea behind enhancing BRI investments between alliance members would be to bolster the shared interests of participating countries to ensure a common approach is maintained on a variety of issues, including the management of cyberspace. Western liberal democratic countries are already in a military alliance (North Atlantic Treaty Organization), a surveillance alliance of English-speaking countries (Five-Eyes), and a quasi-economic alliance built around bilateral and multilateral trade agreements through the Washington Consensus. At the same time, Beijing and Moscow have increasingly cooperated in the security and strategic realm within their region, regardless of sometimes conflicting interests. Recently, the pressure on China to secure its extensive land border with Russia militarily has decreased significantly, and Sino-Russian rapprochement has been a major enabler for China's expansion elsewhere (Schreer, 2019, 511). Whether this rapprochement lasts or becomes formalized in some way will be indicative of Russian and Chinese ambitions on the international stage. An alliance that ties political, military, socio-economic and technological factors would seriously challenge the supremacy of the existing global liberal order.

Towards a fractured Internet

Accordingly, the most likely outcome from this new technological race will be a desire to implement a particular standard – as quickly as possible – in order to gain an economic

advantage and accelerate the decision by states to choose a side that represents their interests. The cyber-alliance between China and Russia has never been more strategic and coordinated – and this time there are complementary actions by both governments to engage in strategic discussions to create this divide. Back in 1998, the Russians proposed to the United Nations a draft resolution entitled "Developments in the Field of Information and Telecommunications in the Context of International Security" to the United Nations General Assembly. The document introduced the overarching discursive claim of the Internet sovereignty brand, it being the central role of the state and interstate organizations in governing the Internet (Budnitsky and Jia, 2018, 599). The goal of bringing forward this concept was to influence the agenda of these organizations, while simultaneously displace the American-led coalition and the incumbent liberal normative framework. O'Hara and Hall explain further, "More important than this diplomatic pressure to change the system, therefore, has been the application of power by various national and supranational institutions to the delicately balanced system itself, to try to "push" the internet into a different type of model. This realpolitik is having an effect, and it is clear that the internet, as originally conceived by the primarily American white male technologists who founded it, is morphing into something else" (O'Hara and Hall, 2020, 2). Even within the United States, there is a tension between the idealism about Internet principles based on free speech, free association and other aspects of individual liberty that resonate with a libertarian audience in Silicon Valley, versus the corporatism and political commercialization of the Internet in Washington. This uncertainty for the future of the Internet in the United States, home to the Internet's founding governing bodies, is creating a space for other values to gain legitimacy. There will be no need for a military war as the future version of conflict, those over ideas, corporate profits, data and opinions, will be fought online. For China, this is perfectly acceptable

and in-line with its long-term strategic vision, “In line with this longer history, China’s leaders have consistently acted out of a conviction that China must develop ‘its own cyberspace’” (Schiller, 2011, 99). It is not just the idea that a separate internet could influence or exist outside what we know to be the Internet today, but that the fundamental characteristics that liberal democracies take for granted as an inherent character of what the Internet is, and its purpose will be radically reinterpreted. The mechanisms by which these principles play out both in the personal and broader social sphere will be unrecognizable – or rather, undesirable – to those on the other side of the digital divide. Western governments will continue to use the Internet to strengthen political accountability, exchange information and data, and engage in commerce; whereas, authoritarian governments will focus their efforts on enhancing collective harmony, shape positive social narratives that favour the state party, accumulate economic wealth, and strengthen their political power. This division will create two separate cyberspaces that reflect the underlying technological infrastructure, regional economic blocs, and values of the leading states and their allies.

The future of the international system

The fracturing of the technological space, including the Internet itself, will be exacerbated by different 5G standards, state-backed economic systems, and misunderstanding of culture resulting in the revival of geopolitical conflict within the international system. On the one hand will be the liberal democratic alliance, led by the United States, with members from NATO, Five-Eyes, and its Pacific allies like Japan and South Korea, who have already signed onto an Information Sharing Agreement in 2014 (Fröhlich and Loewen, 2018, 35). On the other hand, the

authoritarian alliance will be led by China and Russia, nearly all the Central Asian states allied with Moscow, and many countries receiving substantial infrastructure development and investment as part of the BRI, like Sri Lanka, the United Arab Emirates and Zambia. In fact, in those countries, China is helping to develop cyber laws similar to the 2016 China Security Law as a condition of receiving BRI funding (Hemmings, 2020, 16). These competing versions of the technological space will create an international system that will look hegemonic at the regional level, divided by perceived historical spheres of influence, but globally it will function as a bipolar system (Scholvin, 2011, 34 – 35). As these paths diverge even more, and with it expectations about how technology is supposed to function, "crossing the floor" will become more difficult as state systems are entrenched – and indebted – onto their side of the divide; sunk costs will compel states to remain within the existing alliance structure even if political actors decide otherwise. Hemmings argues that, "The marriage of information and communications technology to infrastructure has perhaps been the winning formula for China. This has allowed Beijing to promote its own standards, companies, and digital currency, granting it the benefits of new captive markets for Chinese tech firms, rich sources of data for analysis, and tools for leverage over foreign political and business elites" (Hemmings, 2020, 20). Authoritarian governments will gravitate towards political and cyber-rules created by the Russians and Chinese that enhance their own political control, while still participating in a prosperous global economic system without the political reprisals from the US hegemonic order. The historical language of class conflict and Marxism will be useful tools to legitimize political power in some countries (even if it is not really believed), while the underlying technological structure and shared values will be what really binds the alliance between states. Yang summarizes this approach concisely, "The idea of a Chinese dream is smart. Because dreams are in one's mind, it provides ample

room for individuals to give play to their own imagination. Thus, even as the idea of a Chinese dream shares the strong national characteristic of the Mao era, it differs from the totalizing ideology of class struggle and revolution in that earlier time" (Yang, 2014, 110).

The international system will see the creation of regional economic blocs and a Chinese-led bipolar alliance system that will enhance trade and telecommunications with one other, similar to what occurred during the Cold War with Marshall Plan participants and Molotov Plan members, but with far more resources and strategic vision, underpinned by technological interdependency. This re-ordering of the international system will place a premium on regional hegemony as a key feature of the new international system. China will focus its efforts to achieve regional hegemony in Asia, both as a way to project its own power and limit the US' in the region (Mearsheimer, 2014, 18; Sidorenko, 2015, 1264). The short-term result will be that the United States will be pushed out of the Asian hemisphere, with a limited role supporting its allies in Japan and South Korea who will be under constant Chinese pressure. South East Asian countries like Thailand, Malaysia and Singapore will most likely gravitate towards the US-led model as well, but navy skirmishes in the South China Sea will destabilize the region as China consolidates its military strength with its newest blue-water navy ships (Cole, 2013, 2). The future of Taiwan remains uncertain and could be the flashpoint for a military war in the region. As well, new arenas of cooperation and conflict will emerge in the Arctic as climate change opens up the Arctic ocean for shipping and natural resource development. To put it simply, "Russia is an attractive partner to China in the Arctic. Beijing does not regard Moscow as a strategic threat" (Unknown author, 2018). The United States will continue to assert its self-declared exceptional role around the world, but it will be unable to do this convincingly over regions claimed by the Russians and Chinese. Senior Chinese military officials had already

proposed to divide up the Pacific Ocean into ‘spheres of influence’ back in 2007 and 2009; they were premature back then, but their objective remains the same in this regard (Schreer, 2019, 513).

Equally important, global institutions will need to readjust their governance and dispute resolution mechanisms to account for an international system along this new alliance structure. New concepts of international law will be proposed that reflect the normative principles of authoritarians and the role of the state in ensuring social harmony and respecting state preferences in governance. Cleavages between interpretation of international law – technical ones for now – will be exploited by China as a way to slowly erode existing Western conceptions of jurisprudence, including independence, impartiality and precedent. Whereas China expresses normative support of these concepts, it maintains control over the interpretation, application and implementation of these norms by its resistance to accept the interpretive authority of those same international institutions. In areas of international law where norms are very developed and there is a lot of jurisprudence, the Chinese stance will erode these norms over the long-term. This trend will be extended to various facets of international law to a new arena of interaction, one constructed that alters the concept of “sovereignty”, “law”, or the idea of “social order” (Muller, 2015, 232; Choucri, 2011, 69). As well, China will play a leading role on ICANN and assert its right to direct the international body; for the first time, top-level domain names will employ Chinese characters which had been proposed to ICANN as far back as 2009, but which they will have no choice but to comply (Schiller, 2011, 102). This new international system will return to a historical model that will look unfamiliar to people over the last 200 years but reflect the international system over 2000 years earlier in the Han and Tang dynasties which saw China as one of the distinguished global powers at the time.

Criticisms

Nevertheless, there are questions that arise about the idea of geotechnology underwriting a new international order and whether China's ascendance and the emergence of a powerful socio-economic and technological bloc of authoritarian countries can emerge and be at least – if not more – powerful than one built on the liberal order. Will the global uncertainty of the century result in a series of conflicts between the two cyber-alliances outlined in this paper? The strength of liberal democratic prosperity was built on not a desire for specifically American hegemony (although that certainly was a byproduct of the system), but rather an appeal to principles that were deemed more 'noble' and inherent to human rights, appealing to pluralistic concepts of multilateralism and consensus-building to arrive at decisions. Indeed, Western liberals will point to the strengths of global and international institutions to engage recalcitrant countries in a non-threatening way by integrating them into a global international order shaped through an inclusive approach. The incentive to engage came from the lessons of the Cold War whereby American security interests were secured through an approach built on a robust yet sophisticated set of ideas about a desirable post-war political order. Although containment overshadowed it, the postwar liberal democratic order was deeply rooted in the American experience and an understanding of history, economics, and the sources of political stability (Ikenberry, 2011, 82). To engage internationally was to recognize the malleability of the system and therefore, it was unnecessary to create a rival system of governance – online or otherwise – when rules could be proposed that reflected ones' own values, norms and interests. Deudeny and Ikenebrry (2009) argued that, "Compared to older orders, the contemporary liberal-centered international order provides a set of constraints and opportunities-of pushes and pulls-that reduce the likelihood of

severe conflict while creating strong imperatives for cooperative problem solving" (Deudney and Ikenberry, 20019, 7; Ikenberry, 2011, 88). Both authors also raise the point that China and Russia are already substantial players and stakeholders in many international institutions, including the United Nations where both have permanent seats and veto power (2009, 8). There are also other global institutions, like the International Monetary Fund and the World Bank where developing states can get a bigger voice by taking on a leadership role and buying into the concept of the institutions. Ultimately, they argue that, "The pathway to modernity for rising states is not outside and against the status quo but rather inside and through the flexible and accommodating institutions of the liberal international order" (Deudney and Ikenberry, 2009, 8).

Taken further, if the digital divide described in this paper is a result of not being recognized in the current global order, then existing global institutions – as a function of how they operate – will necessarily find room for accommodating other values, norms and standards. Consequently, a more equal international system will emerge that will reflect the political interests of its varied member states. There will not be a need to divest from existing international institutions if it is possible to change the character of the institutions themselves from within and through the existing liberal framework. It is only natural to want to influence the ideas that govern international institutions and this is not the first time that international institutions changed how they operated. For example, the international system evolved to think about security not just in terms of states and geopolitics, ideas of individual human security (and insecurity) became necessary features of the twentieth century discourse (Martins, 2019, 105).

Economically, it also makes sense for countries like China and Russia to be engaged in the international economic system to enhance their own prosperity and thereby continue to legitimize their own authoritarian rule. The premise is that the longer capitalism takes root and

functions in a society, the result will be liberalism. Indeed, Deudeny and Ikenberry argue that the success of regimes such as those in China and Russia is not a refutation of the liberal vision; rather, the success of those autocratic states is because of their access to the international liberal order, and they remain dependent on its success (Deudney and Ikenberry, 2009, 2). Therefore, authoritarian governments will not risk their political success on creating a separate system of governance, whether it is in the physical or cyberspace. Authoritarians are already on tenuous political ground, long-term legitimacy in the long run requires more openness, not less, and require expanding orders of trade liberalization, private consumption and foreign investment. These basic characteristics of Western liberal institutions and market forces only work effectively if all states play the same game and agree to the rules – even if they are intertwined with Western and American values. To solve collective problems, especially in a regional capacity which includes disputes over islands, territory and natural resources, liberal institutions have the best track record – and arguably hope – for a non-violent solution. It is therefore up to the United States, China and other key regional powers to work with both allies and rivals and "mitigate regional and global tensions that can potentially lead to wasteful arms races and wider regional conflicts" (Hall, 2019, 6). Institutions work by allowing member countries to discuss issues in non-partisan ways and come-up with resolutions that, while a compromise, avoid conflict and long-term uncertainty that could negatively affect the market. For instance, following the end of the Cold War, the United Nations was used as a place to "dump intractable conflicts" in order to act as an impartial forum to discuss matters – even if they did not reflect the core interests of the great powers (Barnett and Finnemore, 2004, 127). As long as there is uncertainty, economic considerations will play a significant role for political leaders to look after their own self-interest. As Mearsheimer put it simply, "In a world of economically interdependent states, leaders have a

marked aversion to conflict, for fear it will put an end to prosperity as well as their political careers" (Mearsheimer, 2011, 50).

From a purely pragmatic point of view, there is also the argument that the Americans are using security as an excuse to shut the Chinese out of the 5G race and that national security concerns, while not entirely untrue, are blown out of proportion. The US and its allies are using security as justification for shutting other potential rivals out in order to protect their own corporations and intelligence-gathering exercises (South China Morning Post, 2019). The United States and its Western allies already own much of the telecommunications space as a result of their domination of the 2G, 3G and 4G technologies. By targeting Huawei and linking it the government security apparatus of the Chinese Community Party, the Americans are merely sowing suspicion to generate controversy among indecisive states still unsure about China's intentions. In fact, the astonishing leak by Edward Snowden regarding the National Security Agency's massive surveillance and spying program showed that the Americans were not to be trusted either when it came to personal information and data (Macaskill and Dance, 2013). The explosive revelation showed just how sophisticated the American spying program was and the involvement of well-known US technology companies like Yahoo, Microsoft and Google, demonstrated that there was no real material difference between their obedience to US law, and Huawei's necessary compliance with CCP's legal framework. Likewise, other US technology companies, like Amazon and Apple, have been caught eavesdropping on users through so-called "smart spies", which are home electronic automated assistants (e.g., Alexa, Siri, etc.). The companies have had to publicly apologize for their devices listening in on conversations, searching internet histories and reading private email, to sell personalized ads, and to gain insights in citizen behaviour and trends (The Washington Post, 2019; The Guardian, 2019).

Plainly, the argument can be made that it is a bit hypocritical to call Huawei a security threat when there is evidence to show that the US and its technology companies engage in the same nefarious behaviours that it is accusing the Chinese technology company of; in fact, they are probably better placed to succeed given their significant advantage and entrenched status.

In the end, the liberal order built by over a century of American hegemony is a powerful structure that will not disappear because of an emerging challenger – or challengers – to its existence. "The bottom line is that the United States worked hard for over a century to gain hegemony in the Western Hemisphere, and it did so for sound strategic reasons. After achieving regional dominance, it has worked equally hard to keep other great powers from controlling either Asia or Europe" (Mearsheimer, 2011, 11). Its strength is not because of the values and principles that are fundamental to the working of those institutions, rather the intrinsic function of institutions – the ability to work towards consensus, to have dialogue instead of diversions, and to see multilateral cooperation in a rules-based setting – allows countries, irrespective of political party and governance, economic strength or culture, to work together towards a common goal. Pluralism is a powerful panacea to the problems of globalization; international institutions respond by adapting to changing and challenging scenarios around the world. Yet, despite the shortcomings of institutions to resolve conflict quickly, the solutions developed in multilateral organizations and institutions appear to be more durable because within them lies the solution borne from dialogue and debate. They are enduring because they have gone through many possible permutations and where diverse perspectives are considered. The strength of liberal institutions, therefore, is not that they are unable to solve a problem expeditiously, but that they naturally take time to work out what is truly the issue in order to find a solution. Delays are not an excuse but represent something worth waiting for. Barnett and Finnemore stress that

"Institutions are the singular answer to promoting interdependence and solving the myriad of collective action problems in environmental, economic, and security affairs because they offer rational, impersonal and nonviolent means of derailing with conflict and enable states to overcome narrow self-interest and achieve long-term cooperation" (Barnett and Finnemore, 2004, 172).

Is conflict inevitable?

Despite the power of institutions and the strength of international organizations to resolve conflicts, the digital divide brought on by technology, economic self-interest, and centuries of culture, will necessarily disrupt the existing international system. Even within Western liberal democratic countries, there continues to be significant systemic confrontations as long-running grievances remain unresolved, such as historical racial divisions, the surge in right-wing populism, and a growing inequality gap. Internationally, there is a shift in the character and ability of international institutions themselves to resolve disputes through existing mechanisms, such as the ABM treaty, the CFE treaty, and the INF treaty. These are a few examples of the breakdown of existing international constructs (Hall, 2019, 4). At the same time, China will continue to offer, in partnership with its Russian and other Eurasian allies, an alternative political model that will emphasize the values and qualities which are important to those societies: social stability, economic prosperity, and national strength. Zhao summarizes this argument "In the final analysis, there is a choice between a Confucius capitalist China that is trying to integrate with a socially and ecologically unsustainable planetary capitalist order and a renewed socialist China that is leading a post-capitalist and post-consumerist, sustainable developmental path as part and parcel of an alternative globalization" (Zhao, 2013, 27). The separation between

capitalism and political liberalism is an intentional strategy meant to demonstrate that state governance can be effective without political change. The Chinese model will also emphasize regional strength while avoiding ideas about global tyranny so long as the US continues to be portrayed as an international bully and troublemaker that acts with impunity. On the character about the Internet itself, the seeds of doubt had already been made in various forums: "At the Forum of Independent Local and Regional Media in 2014, Putin labeled the Internet 'a special CIA project', adding that the United States wanted to retain their monopoly over it" (Budnitsky and Jia, 2018, 607).

The digital divide will become another point of division to separate the global community this century, and as a means for authoritarians to consolidate power. While military conflict may be avoidable, cyberconflict and the use of hybrid warfare – involving careful coordination between state and non-state actors – may take place more often as state forces engage online in efforts to upset the new status quo. The benefits of technology, such as 5G and beyond, may also challenge trends and perspectives about values and culture on both sides as societies and the role of technology to support individual, corporate or state interests evolve.

Despite the conviction I have about the inevitably of an impending digital divide, it also raises the question as to whether this re-ordering of the international system is a permanent feature or is merely a phase in the development cycle of states. The Western liberal economic order has lasted more than a half-century and brought some of the greatest economic prosperity and positive humanism to the world, all without a catastrophic global war. Is it then possible that in spite of a competing cyber-alliance, states can find common ground and avert a disastrous global conflict? While history does not provide many examples of peaceful transitions of power within the international system, we are living in unprecedented times.

Bibliography

Adonis, Abid A. (2019). Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy. *Global: Jurnal Politik Internasional*, Pages 262–282.

Barnett, Michael and Finnemore, Martha. (2004). *Rules for the World: International Organizations in Global Politics*. Ithaca: Cornell University Press.

Brown, Kerry and Iverson, Meghan. (2018). Assessing China's challenge. In *Handbook on the United States in Asia* (pp. 366-389). Cheltenham: Edward Elgar Publishing Limited.

Browning, Christopher S. (2017). Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the 'New Cold War'. *Political Geography*, Pages 106–115.

Bu, Lambert, Wang, Jacob, Wang, Kevin Wei and Zipser, Daniel. (2019). *China Digital Consumer Trends 2019*. McKinsey Digital.

Budnitsky, Stanislav and Jia, Lianrui. (2018). Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance. *European Journal of Cultural Studies*, Pages 594–613.

Cancian, Mark F. (2019). U.S. Military Forces in FY 2020: Army. Part of *U.S. Military Forces in FY2020: The Struggle to Align Forces with Strategy*. Center for Strategic and International Studies.

Cao, Gui Hong. (2015). Comparison of China-US Engineering Ethics Educations in Sino-Western Philosophies of Technology. *Science and Engineering Ethics*, Pages 1609–1635.

CBC Radio-Canada. (2018). *Security Experts Sound Alarm About Canada's Ties to Chinese Tech Company Huawei*. Canadian Broadcasting Corporation.

Chatzky, Andrew. (2019). *China's Belt and Road Gets a Win in Italy*. Council on Foreign Relations.

Choucri, Nazli. (2012). *Cyberpolitics in International Relations*. Cambridge: The MIT Press.

Ciolan, Ionela M. (2014). The Role of the "New Cold War" Concept in Constructing Russia's Great Power Narrative. *CES Working Paper*, Pages 625–647.

Clement, J. (2020). *Countries with the Highest Number of Internet Users 2019*. Statista.

Cole, Bernard D. (2013). China's Navy Embraces Technology: Western Science, Chinese Culture? *The Study of Innovation and Technology in China Research Brief*, Pages 1–3.

Crouch, Colin. (2019). *The Globalization Backlash*. Cambridge: Polity Press.

Deudney, Daniel and Ikenberry, John G. (2009). The Myth of the Autocratic Revival: Why Liberal Democracy Will Prevail. *Foreign Affairs*, Pages 77–93.

Doward, Jamie. (2020). *Putin Takes Next Step to Staying in Power Till 2036*. The Guardian.

Duchâtel, Mathieu and Godement, François. (2019). *L'Europe et la 5G : le cas Huawei*. Paris: Institut Montaigne.

Fowler, Geoffrey A. (2019). *Alexa Has Been Eavesdropping on You This Whole Time*. The Washington Post.

Friedman, Jonathan. (2002). Champagne Liberals and the New 'Dangerous Classes': Reconfigurations of Class, Identity, and Cultural Production in the Contemporary Global System. *Social Analysis: The International Journal of Anthropology*, Pages 33–55.

Fröhlich, Stefan and Loewen, Howard, Eds. (2018). *The Changing East Asian Security Landscape: Challenges, Actors and Governance*. Wiesbaden: Springer VS.

Gardner, Hall. (2019). *IR Theory, Historical Analogy, and Major Power War*. London: Palgrave Macmillan.

Gertheiss, Svenja and Herr, Stefanie. (2017). Approaching International Dissidence: Concepts, Cases, and Causes. In *Resistance and Change in World Politics, Global Issues* (pp. 1–44). London: Palgrave Macmillan.

Global Entrepreneurship Index. (2018). *2018 Global Entrepreneurship Index rankings*. The Global Entrepreneurship and Development Institute.

Hemmings, John. (2020). Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road. *Asia Policy*, Pages 5–21.

Hout, Thomas and Ghemawat, Pankaj. (2010). *China vs the World: Whose Technology Is It?* Harvard Business Review.

Internet Corporation for Assigned Names and Numbers. (2020). *Get Started*. ICANN.

Ikenberry, John G. (1996). The Myth of Post-Cold War Chaos. *Foreign Affairs*, Pages 79–91.

Inkster, Nigel. (2016). *China's Cyber Power*. London: Routledge.

Iwamoto, Kentaro. (2017). *A Look Back at the Obama Administration's Pivot to Asia*. Nikkei Asian Review.

Jones, Peter. (2015). *Track Two Diplomacy in Theory and Practice*. Stanford: Stanford University Press.

Kaska, Kadri, Beckvard, Henrik and Minárik, Tomáš. (2019). *Huawei, 5G and China as a Security Threat*. Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence.

Karaganov, Sergey. (2018). The New Cold War and the Emerging Greater Eurasia. *Journal of Eurasian Studies*, Pages 85–93.

Kirkbride, Paul S. and Tang, Sara F. Y. and Westwood, Robert I. (1991). Chinese Conflict

Preferences and Negotiating Behaviour: Cultural and Psychological Influences. *Organization Studies*, Pages 365–386.

Krammerer, Peter. (2019). *Why Pick on Huawei When All Advanced Technologies, Including Those from the US, Carry Security Risks*? South China Morning Post.

Larsen, Henrik B. L. (2020). NATO's Democratic Retrenchment: Hegemony After the Return of History. New York: Routledge.

Leung, Kwok, Brew, Frances P, Zhang, Zhi-Xue, and Zhang, Yan. Harmony and Conflict: A Cross-Cultural Investigation in China and Australia. *Journal of Cross-Cultural Psychology*, Pages 795–816.

Levine, Alexandra S. (2019). *The Capitol's Most Pressing Tech Hearings*. Politico.

Luce, Edward. (2017). *The Retreat of Western Liberalism*. New York: Grove Press.

Lynskey, Dorian. (2019). *'Alexa, are you invading my privacy?' – The Dark Side of Our Voice Assistants*. The Guardian.

Macaskill, Ewen and Dance, Gabriel. (2013). *NSA Files: Decoded*. The Guardian.

Martins, Bruno O. (2019). Global Affairs and the Politics of Security Technologies. *Global Affairs*, Pages 105–106.

McCrea, Bridget. (2016). 5 Ways to Address Supply Chain Risk. *Supply Chain Management Review*, Pages S48–S51.

Mearsheimer, John J. (2014). Can China Rise Peacefully? In *The Tragedy of the Great Power Politics*. New York: W. W. Norton & Company.

Medin, Milo and Louie, Gilman. (2019). *The 5G Ecosystem: Risks & Opportunities for DoD*. Defense Innovation Board.

Molnar, Adam. (2017). Technology, Law, and the Formation of (Il)Liberal Democracy?

Surveillance and Society, Pages 381–388.

Muller, Wim. (2015). China an Illiberal, Non-Western State in a Western-centric, Liberal Order? *Baltic Yearbook of International Law*, Pages 216–237.

National Cyber Security Centre. (2020). *NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks*. GCHQ.

Office of the United States Trade Representative. (2017). *2017 Special 301 Report*. Trade Policy Staff Committee.

O'Hara, Kieron and Hall, Wendy. (2018). *Four Internets: The Geopolitics of Digital Governance*. Waterloo: Centre for International Governance Innovation.

Oxford Analytica Daily Brief Service. (2018). *International: Cyber conflict will be more destructive*. Oxford: Oxford Analytica Ltd.

Oxford Analytica Daily Brief Service. (2018). *International: Polar Silk Road will alter geopolitics*. Oxford: Oxford Analytica Ltd.

Özer, Özalp, Zheng, Yanchong and Ren, Yufei. Trust, Trustworthiness, and Information Sharing in Supply Chains Bridging China and the United States. *Management Science*, Pages 2435–2460.

Radelet, Steven. (2015). *The Great Surge: The Ascent of the Developing World*. New York: Simon & Schuster Paperbacks.

Recon Analytics. (2018). *How America's 4G Leadership Propelled the U.S. Economy*. Recon Analytics LLC.

Richter, Felix. (2020). *China Is the World's Manufacturing Superpower*. Statista.

Romm, Tony and Harwell, Drew. (2019). *Facebook, Google and Twitter face fresh heat from Congress on harmful online content*. The Washington Post.

Schiller, Dan. (2011). Geopolitical-Economic Conflict and Network Infrastructures. *Chinese Journal of Communication*, Pages 90–107.

Scholvin, Sören. (2011). Emerging Non-OECD Countries: Global Shifts in Power and Geopolitical Regionalization. *Economics, Management, and Financial Markets*, Pages 19–43.

Schreer, Benjamin. (2019). Towards Contested 'Spheres of Influence' in the Western Pacific: Rising China, Classical Geopolitics, and Asia-Pacific Stability. *Geopolitics*, Pages 503–522.

Sidorenko, Ekaterina V. (2015). Geopolitical Conflicts as a Result of Transformation of the Modern World Order: Reality and Prospects. *Humanities and Social Sciences*, Pages 1255–1267.

Simons Greg, Kukartseva, Marina .A. (2019). New Cold War and the Crisis of the Liberal Global Order. *Outlines of Global Transformations: Politics, Economics, Law*, Pages 77–93.

Stapleton, Larry. (2016). International Systems Stability, Culture and Advanced Technology. *Artificial Intelligence and Society*, Pages 301–303.

The State Council. (2015). *Full text: Action Plan on the Belt and Road Initiative*. The People's Republic of China.

The World Bank. (2018). *Belt and Road Initiative*. International Bank for Reconstruction and Development.

The World Bank. (2020). *GDP (current US$).* World Bank National Accounts Data, and OECD National Accounts Data Files.

Thiel, Thorsten. (2017). Turnkey Tyranny? Struggles for a New Digital Order. In *Resistance and Change in World Politics, Global Issues* (pp. 215–242). London: Palgrave Macmillan.

Timmers, Paul. (2019). Challenged by "Digital Sovereignty". *Journal of Internet Law*, Pages 11–20.

Triolo, Paul. (2018). Eurasia Group White Paper: The Geopolitics of 5G. *Eurasia Group*, Pages 1–19.

Triolo, Paul, Allison, Kevin, Brown, Clarise and Broderick, Kelsey. (2020). The Digital Silk Road: Expanding China's Digital Footprint. *Eurasia Group*, Pages 1–13.

Triolo, Paul, Allison, Kevin and Kelly, Thao N. (2019). Special Report: US Will Resist EU Global Data Privacy Push. *Eurasia Group*, Pages 1–4.

United States Senate. (2019). *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election.* Report of the Select Committee on Intelligence.

Various Authors. (2012). The New Cold War? *The International Economy*, Pages 13–19.

Wang, James, Olivier, Daniel, Notteboom, Theo, and Slack, Brian, Eds. (2007). *Ports, Cities, and Global Supply Chains*. London: Routledge.

Xinhua News Agency. (2014). *Full Text of Foreign Minister Wang Yi's Speech on China's Diplomacy in 2014*. China Daily.

Yang, Guobin. (2014). The Return of Ideology and the Future of Chinese Internet Policy. *Critical Studies in Media Communication*, Pages 109–113.

Yuan, Jingdong. (2018). Managing U.S.–China rivalry in East Asia. In *Handbook on the United States in Asia* (pp. 345–365). Cheltenham: Edward Elgar Publishing Limited.

Zhao, Yuezhi. (2013). China's Quest for "Soft Power": Imperatives, Impediments and Irreconcilable Tensions? *Javnost-The Public*, Pages 17–30.