Contemporary Chinese Political Economy and Strategic Relations: An International Journal Vol. 7, No. 2, August 2021, pp. 877-924

The Huawei Paradox: Future Tech Risks and Unravelling Interdependence

David **Morris***
Corvinus University of Budapest

Abstract

One firm has become emblematic of risk in the deteriorating geopolitical contest between the United States and China. Huawei is a Chinese, and global, leader in next generation telecommunications but is feared by the US and some of its allies as a potential vector of cyber-attacks including espionage and state-directed sabotage, as well as constructing digital standards and infrastructure that will extend Chinese state influence globally. A paradox is that in the absence of trust and international cooperation, firms such as Huawei cannot disprove normative worst-case risk scenarios. The logic of the Huawei paradox threatens decoupling and bifurcation of the world into two rival technological systems, with repercussions for international security, international relations and the international economy. A political risk analysis concludes that the risks originate from geopolitical factors rather than factors specific to the firm and can therefore only be resolved (if there is political will) at the level of global or regional governance with enforceable rules, norms and standards and at the national level with risk avoidance or improved risk management and mitigation measures.

Keywords: *geopolitics, technology, cybersecurity, political risk, Huawei*

1. Introduction

Transformational new technology has moved to the centre of the emerging geopolitical contest between China and the United States (US), with tech weaponised by state actors to gain advantage, offensively exploiting vulnerabilities, as well as a new focus on protecting against cyber threats to national security. Further, the competition has extended into third countries with competing visions of global governance in developing rules and standards for the new digital economy. China has long protected its domestic tech against perceived security threats, while at the same time deepening and broadening global tech interdependence through engagement in global value chains. The US, on the other hand, has lost confidence in interdependence with China and has embarked on a campaign of economic blockade, extending beyond US borders and including an increasing number of China-related supply chains. Huawei, a leader in Fifth Generation (5G) communications networks, which are widely expected to underpin emerging, transformational fourth industrial revolution technologies, was first singled out by the US and some of its allies with alarming claims of espionage risks and threats to national security. Further, the US and others have become concerned that Huawei and other Chinese firms are constructing international infrastructure and developing global rules and standards that will extend Chinese state power. The paradox is that claims of security risks or state influence – even without compelling public evidence of malicious intent – cannot be disproved within the normative discourse of geopolitical pushback against China's rise. In spiralling distrust between the US and China, expectations are growing that complex tech interdependence will collapse and multiple regions of competing tech rules, norms and

standards will develop, decoupling the two major economies and contributing to a new Cold War.

As the Huawei case is a rapidly changing contemporary case, this discussion of the Huawei paradox is based primarily on a survey of the contemporary literature, think tank reports and media, on which a political risk analysis is based. A series of interviews with key stakeholders and experts has also been incorporated into the analysis, to understand how specialists identify and assess the risks, although the interview-based research has not been completed at the time of writing, and the research project on which this paper is based is continuing. As a preliminary conclusion, some tentative future scenarios are sketched for varying degrees of geopolitical contest or complex interdependence in 5G and other technologies.

The implications of the Huawei debate are far broader than one firm or even one industry. Emerging technologies such as 5G wireless communications are widely expected to play a critical role in transformative new industries and value chains, which may empower the international community to address a wide range of social, economic and environmental problems, while simultaneously generating a new range of risks. The race to build and deploy such new capabilities is underway. The Fourth Industrial Revolution (Schwab, 2016) is expected to be driven by a convergence of emerging technologies including super-fast communications, artificial intelligence, big data, robotics and quantum computing, all digitally connected to a so-called Internet of Things. With high-speed automated processes, an exponential increase in efficiency and productivity is envisaged that will reshape economies. If the new tech on the horizon lives up to expectations, it may have potential to reshape the world as dramatically as the first, second and third industrial revolutions. The champion firms of these new technologies, including Huawei for 5G communications, might therefore be positioned to have

as much transformational impact as the champion firms of the earlier digital economy, and earlier industrial revolutions.

On the cusp of this technological breakthrough, however, the tech world is splintering into rival camps. Both China and the US are pursuing policies to build separate systems of tech governance, rules, norms and standards, and the US and some of its allies have in recent years stepped up actions to decouple from Chinese tech. Whether this trend is motivated primarily by risk reduction or geopolitical competition, or a combination of both, remains unclear, but there are certainly risks in deeper and broader tech interdependence, just as there are risks in decoupling. It is further unclear whether risks might be better managed by investing in new forms of complex interdependence or, on the other hand, whether complete tech decoupling is even feasible. These questions rest upon US and Chinese geopolitical imperatives and actions as much as questions of global tech governance. This discussion of the Huawei case must therefore be placed in the context of, firstly, US predominance in the Third Industrial Revolution and, secondly, China's new tech aspirations to lead the Fourth Industrial Revolution, before exploring questions of political risks and global policy.

2. US-China Tech Competition

Technological innovation in the early twenty first century was dominated by US firms. Powered by its massive national research and development capabilities, fuelled in earlier times by significant government subsidies and defence and intelligence budgets that dwarfed all other nations and were deployed to see off competitors such as Japan, the US generated innovations such as the internet and its firms dominated global computer and semiconductor value chains. The technological breakthroughs of the Third Industrial Revolution led to the

creation of new information platforms that have transformed economies and societies, and built the largest and most powerful monopolistic corporations the world has ever seen, such as Google, Microsoft and Facebook. With the US and other advanced economies influenced by neo-liberal principles of minimal regulation, free markets and open societies, these firms expanded internationally with few constraints and fiercely resisted attempts at regulation. Indeed, the backbone of the digital economy, the internet, evolved with only limited private sector oversight (for example in administering domain names) but had no agreed set of international rules, norms or standards. The public good opportunities of the information age were evident, with billions interacting with platforms such as Google and Facebook, and notably these firms adopted values that mirrored the US faith in open information exchange. The risks of an information free-for-all however became evident by the second decade of the twenty first century, with the rise of disinformation as a social and political phenomenon that rocked even the foundations of US democracy, as well as fuelling ethno-nationalist populism around the world. The business models of the giant US digital platform companies, to surveil and monetize data on users, raised significant risks themselves, which are beyond the scope of this paper to explore but which are matters of intense debate in open and closed societies alike.

Moreover, the first-stage digital economy emerged at a time not only of prevailing neo-liberal social and economic policy but also neo-conservative foreign policy, with the US committed to wielding its post-Cold War unipolar power to enforce its will, including two decades of warfare in the Middle East, and a period of waning US enthusiasm for the inevitable compromises inherent in multilateralism. The absence of multilateral rules or enforcement of cyber security standards also provided an environment in which the US and its allies in its

"Five Eyes" intelligence-gathering network (Australia, Canada, United Kingdom and New Zealand) regularly used the Internet, telecommunications companies such as AT&T and new platforms such as Google and Facebook to conduct espionage against foreign and domestic targets (*The New York Times*, 15th August 2015; Snowden, 2019; Biddle, 2020). Of course, other powers with less open societies also engaged in similar actions and, as we shall see below, the expectation that China is doing the same, potentially utilising firms such as Huawei as a vector for espionage, has become central to the new cyber security debate.

Meanwhile, China has emerged as a competitor to the US, after four decades of modernisation and rapid, state-driven development. China benefited from embracing complex interdependence with the major advanced economies, including the US, through bilateral trade and investment, its integration into the World Trade Organisation and global value chains. China has developed a highly competitive technology sector as a result of a subsidised drive for greater self-reliance as well as transforming its role in global value chains, from low value assembly to designing and manufacturing higher value components. Initially highly reliant on foreign investors for technology transfer, a powerhouse innovation culture has developed in recent years. Shenzhen, a traditional centre of China's opening up to the global economy, now stands out as a private-sector dominated "new Silicon Valley", featuring thousands of start-up and highly successful tech firms including internet platform giant Tencent, drone innovator DJI and telecommunications leader Huawei. China's burgeoning innovation culture is reflected in its rapid growth of patent registrations, which surpassed the US in number for the first time in 2019 (World Intellectual Property Organization, 2020). China has now become a world leader in ecommerce, mobile payments, cloud computing and ICT exports (Zhang and Chen, 2019).

Indeed, China is leading in at least one of the critical emerging technologies of the Fourth Industrial Revolution, 5G high-speed wireless internet equipment and services, and is highly competitive in artificial intelligence, quantum computing and other new technologies. In the characteristic manner of China's party state, the government has developed a series of plans and policy measures to drive innovation in technology, such as the Made in China 2025 initiative, Internet Plus and the 2017 Next Generation Artificial Intelligence Development Plan. The Chinese government has also actively begun to develop rules and standards for the digital economy, including a domestic Cybersecurity Law and a China Standards 2035 Plan under development. At the same time, it has kept a tight leash of digital censorship consistent with its authoritarian style of governance and fear of international influence, with a sophisticated firewall preventing Chinese citizens from accessing foreign information that is deemed politically subversive. In multilateral forums, China and the US have therefore approached questions of global technology governance from different positions.

China's ambitions for tech leadership have been met with alarm amongst policy makers in the US (Zenglein and Holzmann, 2019). Chinese corporate practices are commonly criticised not only for forced technology transfer through joint venture requirements, but cyber-espionage and hacking to steal corporate secrets (RWR Advisory Group, 2019). After 2017, when the Trump Administration declared China a "strategic competitor", the US began a rolling series of economic blockades and a narrative war. While US tech firms tended to oppose the more geopolitically-inspired restrictions Washington began placing on tech interdependence with China, half of US tech firms nevertheless supported the specific US restrictions on Huawei, discussed below (Birnbaum and Lapowsky, 2021). The Biden Administration continued to widen the net of global restrictions on Chinese technology firms

(Reuters, 17th March 2021), including placing sanctions on a growing number of Chinese supercomputing organisations (*South China Morning Post*, 13th April 2021).

China has reacted to the more confrontational approach from the US by doubling down on its industrial strategy to drive further tech innovation, and made technology self-reliance a central feature of its Fourteenth Five-Year Plan, unveiled in early 2021, describing tech development as a matter of national security. In 2020, it strengthened export controls on items deemed to be of national security importance, including extra-jurisdictional application mirroring similar US laws (Congressional Research Service, 2020). The US and China actions and counter-actions all appear likely therefore to reduce tech interdependence as transformational new technologies are deployed in the coming decade.

3. The Huawei Case

Huawei Technologies Co. Ltd was the first and most prominent firm to be singled out in the US-China tech contest, as a claimed cyber-security risk. Over decades, Huawei has invested in a massive research and development effort to achieve its market-leading position in 5G telecommunications. Like other globalised Chinese firms, it became deeply embedded in international value chains, partnering with firms and governments around the world, developing communications network equipment and infrastructure, and consumer communications products and services. The firm certainly challenges US aspirations to maintain technological dominance, although no US firm has become globally competitive in 5G and indeed many US firms had – until the bans on Huawei and other Chinese technologies - built supply chain integration with Huawei products and services. Huawei has long been considered a

national security risk by the security establishment of the US and some of its allies because of its opaque private sector structure, the military background of its founder, Ren Zhengfei, and other personnel links to state security services (Balding, 2019). Nevertheless, no evidence has been presented publicly of widely-repeated claims that Huawei has facilitated espionage. In turn, Huawei has consistently denied such claims.

Huawei was first banned from installing a 5G network on national security grounds in August 2018 by Australia, a staunch US ally. Australia's decision, closely coordinated with the US, was reportedly based on intelligence assessments of potential cyber-risks to critical infrastructure, raising the alarm level of the narrative from traditional espionage to feared weaponization of new technologies. Not only might Chinese firms theoretically be required by the Chinese Government, it was feared, to compromise Australia's 5G network (*The Sydney Morning Herald*, 24th September 2018, 12th June 2019, 31st January 2020; Hartcher, 2021), but Australia was considered incapable of mitigating risks of implanted network coding or equipment backdoors that might be used to threaten operations of critical infrastructure (Reuters, 22nd May 2019; *The Sydney Morning Herald*, 31st January 2020).

Following the Australian decision, the US administration stepped up its campaign against Huawei. In May 2019, the US Commerce Department placed Huawei on a trade blacklist, including restricting access to US components, citing national security concerns (Lim and Ferguson, 2019). The US move and subsequent actions underlined American asymmetric market power based on its continued technological superiority in advanced semiconductors, on which firms such as Huawei depend (Fernandes, 2019).

In a dramatic episode in December 2018, the US requested Canada to arrest and detain Huawei's chief financial officer, Meng Wanzhou, while she transited Vancouver airport. The US sought her extradition for fraud, charging that Meng covered up attempts by Huawei entities to evade US sanctions against Iran. The personalised action against Meng (who happened to be the daughter of Huawei's founder Ren Zhengfei) suggested an element of geopolitical theatre. Targeting a senior executive was a highly unusual action and, indeed, while numerous US and other international firms have been pursued for violating US sanctions against Iran, senior executives have not typically been arrested or taken into custody (Sachs, 2018). The drama continued with China detaining two Canadians, Michael Kovrig and Michael Spavor, on spying charges, in what appeared to be alarming tit-for-tat punishment of Canada. Further, in 2019, Huawei was charged by the US with stealing intellectual property (Department of Justice, US, 2019).

In early 2020, the US government provided US$1 billion for telecommunications carriers to "rip and replace" Huawei and other Chinese-sourced equipment from US networks (Heater, 2020). In May 2020 the US Department of Commerce introduced new requirements for foreign chip makers that use US technology to apply for a licence to sell chips to Huawei, then a few months later closed that loophole altogether, in a further squeezing of Huawei's supplies of advanced semiconductors (Department of Commerce, US, 17th August 2020; *Nikkei Asian Review*, 19th August 2020).

Further, the Trump administration's economic coercion was matched with a new ideological "clean" versus "dirty" narrative. In August 2020, the US government unveiled a so-called "Clean Network", an alliance of "trusted" countries and firms committed to removing "authoritarian malign actors, such as the Chinese Communist Party" from their cyber supply chains (Department of State, US, 11th August

2020). It was accompanied by a range of new measures securitising tech supply chains, increased investment in strategic research and development to compete with China, a fund for re-shoring semiconductor manufacturing to the US and a US$60 billion International Development and Finance Corporation to encourage developing countries not to buy from Chinese suppliers (Capri, 2020).

Despite the US campaign against Huawei, the firm nevertheless continues – at the time of writing - to be an attractive partner to a wide range of governments, firms and consumers across much of the world because of its technological leadership and cost competitiveness. Huawei has partnerships with more than fifty international carriers to provide 5G network equipment and services (*CNN Business*, 5th December 2019). In the advanced market of Europe, there is a highly competitive environment between, Huawei – on the one hand – recognised as the leader in 5G network technology as well as being the lowest cost supplier, and – on the other hand - Ericsson, considered by many in the industry to provide higher quality. Huawei has won contracts to supply half of the 5G network in Germany and Spain, while on the other hand Ericsson has won contracts in Norway and Hungary (Fletcher, 2019).

Both Germany and the United Kingdom (UK) planned to proceed with Huawei for non-core components of their 5G networks despite confidential US security briefings (Ikenson, 2019; *South China Morning Post*, 28th January 2019; *The Telegraph*, 13th January 2020), although after the US extended its sanctions on Huawei, impairing its likely future capabilities, the UK announced it would phase out all Huawei equipment by 2027 (Department for Digital, Culture, Media & Sport, UK, 14th July 2020). UK intelligence agencies have scrutinised Huawei, which allows full examination of its hardware and software products by local security experts at a jointly-managed cybersecurity evaluation centre. While the

centre has reported technical issues of concern in Huawei's engineering processes, it has not found these were the result of Chinese state interference (*South China Morning Post*, 13th April 2020). Huawei has established similar "cyber security and transparency centres" in several countries including Belgium and Germany, although the European narrative surrounding Huawei remains centred on geopolitics rather than engineering.

In the developing world, no countries have been willing – so far – to give up the option of utilising Huawei, despite US pressure, with the exception of India, a rival of China, which has opted for other suppliers. Huawei has been a longstanding provider of wireless networks (from 3G to 4G) and other services and products to countries from the Asia Pacific to Africa (*Ecns.cn*, 4th June 2019). Huawei has also been a key actor in China's so-called "digital silk road" partnerships, in which Chinese banks provide a mix of concessional and commercial finance to support developing countries in building satellite, underwater and terrestrial communications networks and so-called "safe cities" and "safe ports". These latter systems utilise artificial intelligence and surveillance technology for security services including facial and voice recognition, sentiment analysis and relationship mapping, all ostensibly aimed at improving public safety and crime detection. These programs have been accused by US and other observers of exporting the Chinese "surveillance state" model (Dirks and Cook, 2019; Hillman and McCalpin, 2019). Critics point to risks that Huawei and its Chinese partner firms are establishing infrastructure that could provide the Chinese government access to data from foreign countries, extending Chinese governance models and enabling authoritarian surveillance and social control (Polyakova, 2019). Huawei has even been accused of providing intercepted data to African governments to spy on, locate and silence political opponents (McMaster, 2020; Hillman and Sacks, 2021).

Further, the pervasive role of Chinese firms in providing these new technologies and establishing interoperability, market dominance and industry rules and standards is represented by critics as extending the influence of the Chinese state. While firms from other countries also export surveillance and other tech, those from authoritarian China are represented as embodying the risk that China is seeking to shape and control not only the domestic but also the international digital economy (Hoffman, 2021).

Huawei has thus become central to the debate, in particular in the US and its allies but also in an increasing number of countries that are interdependent with both the US and China, about cyber risks. These risks are heightened as the new high-speed connectivity capabilities of 5G will generate an exponentially greater number of potential vulnerabilities across the anticipated Internet of Things, with a theoretical threat of weaponization at any one of those points of vulnerability.

4. Methodology

Understanding risk in any approximately proportionate way is controversial. Humans do not have a good track record of predicting risks. In relation to cyber risks, trust is lacking that governments, technologists or others are able to provide us with a framework to understand risks and geopolitics has become the default framework for the cyber risk discourse. To be sure, the deepening, broadening and transformation of the digital economy is enlarging the risk environment, creating exponentially more points of potential risk, and we might reasonably believe that state actors are actively exploring these vulnerabilities to leverage political (or geopolitical) advantage, as well as other actors such as criminal organisations and other kinds of hackers.

In an attempt to move beyond the binary geopolitical framework of the contemporary discourse, a political risk framework is utilised in the discussion below, including these key steps (as recommended by Sottilotta, 2017): risk identification, risk analysis, risk assessment and, finally, an outline of risk management approaches. Political risk is traditionally understood in international business literature to be concerned with comprehending, forecasting and responding to "macro" and "micro" non-economic discontinuities, such as socio-political, cultural or other factors in the external environment that impact on international actors (Robock, 1971). Macro factors are commonly identified at the country level, sometimes described as the "catalogue school" (Jarvis, 2008), because such an approach tends to generate a list of salient factors in the national governance environment that generate risks, from policy instability to corruption and law and order issues. Micro factors are usually understood to be those that are generated by a particular firm or a particular project (Alon and Herbert, 2009). In all cases, a risk indicates a likelihood of an event or process that can be identified, understood and managed or mitigated (Fägersten, 2015), even if there will always be uncertainty about factors that can inevitably be perceived subjectively (Kobrin, 1979).

There is a further category of political risk that is expected to relevant to this case: geopolitical risk. This is a term traditionally applied to measurable conflicts or other events or processes disrupting international peace and security such as, for example, Russia's hybrid warfare tactics in Ukraine or the quantifiable destruction caused by international terrorism (Wernick, 2006). More particularly for this discussion, geopolitical risk has also been understood as describing the effects of major power competition, usually represented in positivist, zero-sum surveys of "objective" factors such as competition for resources, ports and industrial regions (Sykulski, 2014). Whether the US

campaign against Huawei can be reduced to a zero-sum attempt to squeeze out a geopolitical rival, or whether it raises more complex questions including technological security, remains an unanswered question in the literature, and is explored in the stakeholder and expert interviews. The claimed risks certainly arise because of the geopolitical contest between the US and China, and therefore can be understood as geopolitical risks.

Political (or geopolitical) risk can be assessed quantitatively and qualitatively. International financial institutions, political risk advisory firms and scholars (such as Alon and Martin, 1998) have developed elaborate models with weightings for each risk and produce rankings for risk to provide general guidance for decision makers. This approach can be applied, for example, to predicting the likelihood of political instability or corruption in a particular business environment or for estimating effects of war or terrorism. However, many political (and geopolitical) risks are processes that are more usefully investigated qualitatively (Fitzpatrick, 1983). The evolving case of Huawei in the contemporary, deteriorating geopolitical climate, will be discussed here in qualitative terms, drawing from the contemporary literature, expert think tank and China analyst newsletters, media and other material in the public discourse, as well as an ongoing series of stakeholder and expert interviews, with observations from the first phase of interviews reflected in the discussion below. In the contemporary discourse, there is no consensus around the claimed risks, with competing narratives about international relations and subjective views about security, governance, economic and social implications. A political risk framework is therefore developed to break down the issues, identifying risks, assessing risks and (tentatively) predicting scenarios. This framework will then form the basis of a further round of questions to stakeholders and experts in the second phase of the research, to be published at a later date.

In the first round of research interviews, 17 stakeholders and experts were approached for interview, from six different countries, with four declining to be interviewed and six interviews completed at the time of writing: Huawei's vice-president, Cyber Security and Privacy; former Huawei vice-president, Global Government Affairs; an associate professor of the US Asia-Pacific Center for Security Studies; the director of Australia's Centre for Responsible Technology; a former senior Hungarian telecommunications official; and editor of the *Journal of Telecommunications and the Digital Economy.* The interviews were semi-structured, to stimulate discussion about opportunities, risks, threats and the conditions in which each arise.

After recording the interviewee perspectives, identified risks and risk factors, analytic induction was deployed to identify key themes and patterns, the dynamic interplay between conditions and risk factors, to identify core concepts. Propositions were then framed against plausible scenarios, in the process of developing a proposed framework for proportionate risk management. The validity and reliability of the data and the appropriateness of the proposed framework will be further tested in future rounds of interviews, further literature review and from peer review. The conclusions of this paper are therefore tentative, as the research project is not yet complete.

5. Risk Identification

5.1. Security Risks/Threats

The claims on the public record that Huawei could be a vector for, firstly, cyber-attacks such as sabotage of critical infrastructure, are very serious claims indeed. The claims indicate that, even if likely in only "worst case" scenarios of major power confrontation or conflict, a perceived cyber-attack risk exists, which could indeed constitute a

security threat if actualised against strategic infrastructure or systems. Secondly, the espionage claims represent qualitatively different, although also serious, security questions. Even in "normal" conditions of geopolitical competition, without escalation to confrontation or conflict, states can be expected to engage in espionage, including cyber-espionage. Given the well-established evidence of electronic espionage by the US and its "Five Eyes" partners, including utilising technology in China, it is highly likely that China also utilises all available means to conduct espionage in foreign jurisdictions. Huawei's widespread presence in international telecommunications networks therefore could be considered to generate a reasonably-founded espionage risk although no publicly-available evidence of such exists and the firm denies it would agree to government demands for spying. Thirdly, Huawei's involvement in digital silk road partnerships between China and a wide range of developing country partners is claimed to generate a security risk that China will export its "surveillance state" model. Overall, the Huawei paradox raises considerable security risks in the literature.
Interviewees confirmed (or denied) these as the relevant risks, which will be further discussed below:

- Cyber-attack on critical infrastructure
- Espionage
- Surveillance state

5.2. Interdependence Risks

The campaign against Huawei (on the basis that it is a Chinese, albeit private sector, firm) in itself might also be considered to undermine international cooperation and complex interdependence. In a state of geopolitical contest that seeks to prevent Huawei's (and other Chinese firms') continued integration into global value chains, it becomes less

likely the international community will be able to develop functioning global rules, norms and standards for the digital economy. The US-led "Clean Network", for example, seeks to encourage its allies to decouple from Chinese supply chains and potentially divides the digital economy into at least two spheres of rules, norms and standards, just as China's "Great Firewall" had already driven a wedge in the global internet. Weakened international cooperation will in turn undermine global governance institutions which might otherwise build and sustain rules, norms and standards to reduce risks. Further, the potential demarcation of the digital economy into US-led and China-led spheres risks would tend to strengthen the foreign influence of these major powers over other states within their spheres, including not only favouring firms originating in each major power but increasing the likelihood states may be influenced to support their major power partner on other matters from international rule-making to targeting firms (or even individuals representing firms) from third countries.

Further, Huawei presents a stark example of the risk of economic coercion by a major power, with the US targeting a private sector firm and wielding a range of state measures to constrain the firm in international markets. In the absence of evidence on the public record of any wrongdoing (although, to be sure, potential risks), the action sets an alarming precedent for how economic coercion may be deployed by major powers against other international firms as the geopolitical climate continues to deteriorate. It increases the likelihood of counter-measures and therefore generates risks for a wide range of other international firms. The implications of the actions against Huawei transmit throughout global supply chains, with all international firms that supply Huawei impacted by US executive and legislative restrictions and liable to sanction for not conforming. As noted above, the result may ultimately be decoupled supply chains, which would generate

adjustment costs as well as long term costs of duplicating and in some cases sourcing from higher cost suppliers. Firms on both sides will lose access to valuable markets. The Huawei dilemma as discussed in the literature raises serious questions about future international economic cooperation and may pose, as a consequence, a risk to the entire globalisation process in new tech.

Interviewees identified the following risks, to be further discussed below:

- Rules/norms/standards
- Foreign influence
- Economic coercion
- Disrupted supply chains
- Fractured globalisation

Table 1 Identified Risks

Security risks/threats	**Interdependence risks**
Cyber-attack	Rules/norms/standards
Espionage	Foreign influence
Surveillance state	Economic coercion
	Disrupted supply chains
	Fractured globalisation

6. Risk Analysis

6.1. Security Risks/Threats

The central security concern rests upon a theoretical proposition that Chinese-sourced technology underpinning international communications systems could be weaponised by the Chinese state. The US and its allies, amongst others, distrust the authoritarian Chinese party state and fear its growing technological and military capabilities. Despite being a private firm, it is feared Huawei could be co-opted to serve the national security objectives of the Chinese government and forced to facilitate espionage or cyber-attacks (Gilding, 2020). Article 7 of China's National Intelligence Law of 2017 is often cited, which requires that Chinese firms and their employees cooperate with national intelligence agencies lawfully carrying out their work (Girard, 2019). Indeed, any major power might be expected to utilise communications and other networks for intelligence. The US government has equivalent powers to those it fears China wielding (Eisenstein and Halpert, 2018).

The risk of espionage would appear on the face of it to be realistic. After all, it is well documented, including in the Snowden and WikiLeaks revelations, that the US and its Five Eyes partners (Australia, Canada, United Kingdom and New Zealand) similarly engage in espionage (Snowden, 2019), including co-opting Apple, Facebook, Google and other firms to collect data (Biddle, 2020). There is no reason to believe China is not doing the same, regardless of the geopolitical climate and regardless of standard government denials. The perennial risks of espionage raise highly technical questions about capabilities of detection and protection. Indeed, most unauthorised or malicious, so-called "bad actors" in 4G networks have been found to be authenticated users rather than rogue outside actors (Mc Daid, 2020). These are relevant questions not only in relation to Huawei, but for all

telecommunications systems and the complex global supply chains for equipment and software. Nevertheless, as most communications are expected to be encrypted by the time 5G networks are fully implemented, it is unclear how even an implanted "back door" would allow a supplier to access such data without the relevant encryption keys.

The risk of cyber-sabotage is much more dependent on the state of the geopolitical climate. In a state of contest, confrontation and potential conflict, there is considered to be a risk that technically undetectable malicious code or "kill switches" are implanted into 5G networks, which could be used for cyber-attacks on critical infrastructure. Such aggressive actions might have been less likely during previous years when the US and China and other countries were cooperatively engaged in building interdependent economies. Indeed, Huawei has been intent on building its international reputation as a trusted provider of state-of-the-art technology and it would appear to be self-defeating to allow itself to be used as a platform for hostility against its customers. In the new era of geopolitical competition however, featuring new flashpoints of confrontation, economic decoupling and more aggressive positioning by both the US and China, the risks become more likely that firms such as Huawei (or indeed firms on the US side) might be co-opted or, perhaps more likely, compromised without their knowledge for aggressive security operations. This is not a risk specific to the firm, but a risk of hostile state action.

Looking forward, the security of 5G networks will become even more important for the connected technologies of the future, with critical infrastructure connected to such networks. Indeed, risks will not only be generated by major power geopolitical contest but governments will also need to protect against cyber-attack from other states, criminal organisations or rogue individuals. Whether Huawei can be enlisted as a

partner in protecting against such risks, or whether it is a vector of risk, will depend upon normative perspective.

Further, countries along the so-called digital silk road that are cooperating with Huawei to build "smart city" and "smart port" infrastructure may see more opportunities than risks, while observers from liberal democracies will be concerned about how such infrastructure might in turn be used for surveillance and social control. Geopolitical scholars in the US and its allies depict the digital silk road infrastructure, surveillance and satellite navigation systems as schemes to gain strategic access to data, capture markets and influence, projecting Chinese norms and systems, including through training programs, and generating risks that China could in future use operational control of smart city or port data to create surgical cyber-attacks (Hemmings, 2020). Again, this represents more of a concern about state action, and a normative perspective that Chinese programs are illegitimate and intrinsically authoritarian, rather than exhibiting evidence of a danger posed specifically by Huawei itself. After all, US, European and Japanese firms also export facial recognition technology that could be used to target groups or individuals but are not accused of exporting authoritarianism. How safe city or other programs are deployed by host governments is, at the end of the day, a matter for them rather than China (Weiss, 2019).

6.2. Interdependence Risks: Global Governance

The Huawei case exposes a critical gap in global governance. Inadequate rules, norms, standards and institutions exist to manage risks of globally interconnected technology. In the absence of rules, norms, standards and institutional enforcement, technologies generating risks have developed ahead of technical capabilities to manage those risks. Indeed, some technical experts claim the complexity of telecommunications

technology renders it impossible to guarantee against malicious code or backdoors in equipment (Lysne, 2018; Chang, 2020). Nevertheless, the risk of malicious action has not prevented the international community from developing – and abiding by – rules, norms, standards and institutions in numerous similarly complex areas of strategic importance, such as nuclear technology, food safety or aviation. The lack of discussion about governance options for emerging technologies is therefore remarkable.

Governance of 5G telecommunications has become embroiled in the US-China geopolitical contest, as has governance of the internet. The US has opposed any expansion of the mandate of the International Telecommunications Union (ITU) to govern digital communications. Meanwhile China, has developed a clear ambition to be rule-setter and norm maker in internet governance and cyber sovereignty (Schia and Gjesvik, 2017; Wang, 2020), as well as in other transformational technologies such as blockchain and its applications in finance, manufacturing, transport, food safety and public security (*South China Morning Post*, 2nd December 2019; Stockton, 2020). Across its digital silk road partnerships with developing nations, China has promoted uniform standards for 5G rollout (consistent with those set by the ITU), as well as for artificial intelligence and satellite navigation systems (Chan, 2019). China will likely wield influence amongst its technological partners in the rules, norms and standards that will develop over time. China – together with firms such as Huawei - has been actively promoting its cyber governance model at World Internet Conferences, the ITU, the International Standardisation Organisation and the International Electrotechnical Commission and the two United Nations (UN) working groups, the Group of Governmental Experts and the Open-Ended Working Group.

While the US has begun to participate more actively in these forums in recent times, a fundamental clash of world views makes it unlikely consensus can be achieved. The Chinese government's aims in cyber governance include maintenance of social stability and protection from foreign influence. China's approach to cyber governance is therefore focused on the state's ability to control content, which includes network security, while Western approaches have resisted a state-centric approach to rule-making. China proposes global standards for data security, while the US is moving to establish its so-called "Clean Network" to set standards amongst a set of "trusted" partners. Huawei's stated commitment to working with industry to develop common standards is again an engineering solution for a geopolitical problem.

A "China Strategy Group", comprising academics, policy-makers and tech experts, recommended to the incoming Biden Administration that a global body will be required for tech standard setting and recommended "multilateral trust zones" and other strategies such as technical requirements to manage risks in those areas in which cooperation will be of mutual interest (China Strategy Group, 2020). Whether the recommendations will be adopted is unclear at the time of writing. The World Economic Forum (*Global Technology Governance Report 2021*) has also made a set of recommendations for global tech governance including key fields such as AI, blockchain, Internet of Things, mobility and drones, noting not only the challenge of cybersecurity but a lack of regulation of emerging tech in areas that risk privacy, liability and accountability, as well as misuse and the challenges of cross-border differences. New tech such as autonomous vehicles, for example, will require unrestricted flow of data, while still safeguarding user privacy and ensuring equivalent safety of operation across borders.

The Huawei paradox, combined with the politics of fear and blame during the Covid-19 pandemic of 2020, has amplified the different approaches of the US, with its lack of a governance framework for data security and recent opposition to multilateral solutions, and China, with its Cyber Security Law and claimed support for global cyber governance. It appears for the foreseeable future the law of the cyber jungle will persist at the global level. Meanwhile, at a regional level in at least one part of the world, the European Union (EU), with its comprehensive Cybersecurity Act, General Data Protection Regulation (GDPR) and Directive on Security of Network and Information Systems (NIS), models the most advanced attempt at rules, norms and standards to guide cyber risk management, to be discussed further below.

6.3. Interdependence Risks: Economic Weaponization

The Huawei case has also become a prime exhibit of the weaponization of economic interdependence and its undermining. The denial of supply of advanced semiconductor chips to Huawei (and other Chinese firms) by the US appears likely to drive China to double down on its strategy for not only self-reliance and alternative sources of supply but indeed dominance in next generation technologies. It may take some years, but China can be expected to develop a semiconductor industry to rival the US-controlled supply chains in time. While it is impossible to prove a counterfactual, it has been suggested by Kennedy (2020) that a more "principled interdependence" between US and Chinese supply chains rather than decoupling might have sustained US semiconductor leadership, slowed China's technological advance and offered opportunities for joint work on risk management. Coercion has been chosen over cooperation in what may yet prove to be a turning point in the deteriorating geopolitical contest between the US and China,

extending to impact more and more firms and industries at the time of writing.

The economic costs of excluding Huawei alone are considerable. A Huawei-commissioned Oxford Economics report (2019) predicted that restricting Huawei from competitive tenders will lead to increased 5G investment costs of between eight percent to 29 percent over a decade and would have a cost to GDP in 2035 from US$2.8 billion in Australia to US$21.9 billion in the US. For US semiconductor firms, the export controls on sales to Chinese buyers constitute a major risk to their global business strategies. In a survey of exports in the first four months of 2018, Capri (2018) found Qualcomm relied on China for 60 percent of revenue, Micron over 50 percent and Broadcom about 45 percent. A Boston Consulting Group report forecast a full decoupling with China would reduce the US chip sector revenue by 37 percent and lower its market share to 30 percent, while China's market share would rise from three percent to 31 per cent (Varas and Varadarajan, 2020). Further, as the geopolitical climate worsens, there is a risk that China will retaliate against US or allied firms. Tit-for-tat economic coercion between China and the US will pose significant economic risks for third parties, with both states likely to deploy more expansive export controls, other sanctions and anti-sanctions, and restrictions on joint research and development (Thomas-Noone, 2020).

Farrell and Newman (2019) coined the phrase "weaponised interdependence" for this phenomenon of a state deploying economic coercion to leverage its asymmetrical power over a global network and "chokepoint effect" to deny network access to an adversary. Now that the US has set the precedent in its campaign against Huawei, how else the tactic might be deployed is not yet clear, with fears in China, for example, that the US could target international payments through its SWIFT system (Zhao, 2020). To be sure, once the process is initiated

against a firm or a sector, entire supply chains will be disrupted. The potential evolution of a new global economy that moves away from market-led globalisation towards state-led spheres of geopolitical influence is uncertain at this point, but 2018-2021 may yet turn out to be a tipping point towards a much more geopolitically-infused international business environment. Geopolitical risk analysis is therefore likely to receive much more attention in international business literature.

7. Risk Assessment

The assessment of security, international relations and economic cooperation risks for 5G networks must be made in the context of not only contemporary international relations but over the life of such networks. This means planning for scenarios, including worst-case scenarios. The theoretical capability for cyber-attack on critical infrastructure, for example, might not be as serious a risk in most contemporary scenarios as heightened geopolitical narratives may suggest (although Russia would be a counterpoint to this assessment, which is beyond the scope of this paper), but such attacks might become a realistic threat in future worst-case scenarios in which the major powers are escalating confrontation or engaged in conflict.

Any qualitative assessment of risks must take into account two key concepts, likelihood and consequence. The type of political risk will depend on whether the factors generating the risk arise at the firm level, the country level or as a result of the geopolitical environment. Huawei as a firm has been claimed to pose security risks because of the nature of the Chinese party state and the risks are therefore China risks, or geopolitical risks, rather than specific to the firm itself. Equally, the interdependence risks that are generated by the case appear to be not simply because of Huawei itself but arise from the diverging interests of

the US and China, characterised in particular by the lack of global governance rules, norms, standards and institutions for new tech. Further, in relation to economic interdependence risks, Huawei again appears to be simply the trigger case for an emerging trend in the new geopolitical contest for the US and China to deploy economic coercion, to reconfigure supply chains and indeed to reshape globalisation according to geopolitical agendas and, consequently, abandoning the neoliberal and internationalist market-led phase of globalisation that characterised previous decades.

Accordingly, the Huawei case can be assessed as a prime example of geopolitical risk and can therefore only be understood in the context of the international relations, security and economic policies of the major powers. Suppliers and partners of Huawei and indeed any strategically important firms from China or the US must therefore plan to manage geopolitical risks in the current environment. There has traditionally been very little cross-fertilisation between business literature on political risk and international relations literature on interdependence (Fägersten, 2015), yet this discussion demonstrates that risks for governments, firms and communities in the Huawei case are entirely bound up in questions of interdependence and will require new approaches to risk management.

Generalised cyber risks (leaving aside the Huawei case) can be assessed as highly likely and potentially high consequence. There is therefore a critical need to build stronger cyber security defences, to mitigate against espionage (from whatever source) and to protect against weaponised cyber-attacks in future.

The digital silk road might be assessed in the developing world as bringing more opportunities than risks, while the US and allies are likely to perceive highly likely risks of increased Chinese state and economic influence. A further threat assessment evoking the use of Chinese tech

for deployment of state surveillance would appear, however, to be geopolitically inspired, given non-Chinese firms also export similar equipment.

The risks to complex economic interdependence are likewise normative. While the opportunities of globalization were generally regarded to bring economic benefits as well as benefits for international cooperation from integrated supply chains, a normatively positive attitude to dependency on Chinese tech has been difficult to find a voice in the US and its allies in recent times, notwithstanding the opportunity to develop greater cooperation and indeed joint risk management. More likely is that the US and its allies will pursue at least limited decoupling, generating highly probable risks of undermining the globalization process and fracturing it into rival regions, with highly likely economic costs. Further, sustained US sanctions to undermine Chinese tech may indeed generate further confrontation and will certainly encourage China to double down on its strategy for self-reliance and to seek global leadership in transformational new tech.

The risk assessment that is often overlooked is the question of global tech governance. As major economies begin the rollout of the new tech of the fourth industrial revolution, there is indeed a highly consequential opportunity to reduce and manage risks by building a globally agreed system of rules, norms and standards with compliance and enforcement mechanisms, that is supplier-blind and that strengthens cyber security all round. This appears at the time of writing to be highly unlikely. More likely is that across emerging and developing economies of Asia and other regions, Chinese rules, norms and standards will become dominant and that the US and allies will carve out a separate network of tech governance. The question that will require continuous assessment will be the extent to which a Balkanised tech governance

will result in tech weaponization, confrontation and potential cyber conflict in future.

8. Risk Management

Experts interviewed for this research tended to agree that cyber risk management should take a "zero-trust" approach that is blind to suppliers and that applies layers of monitoring and testing for vulnerabilities, as threats could actually come from anywhere – not just one particular geopolitical competitor at any one time. Equally, risk management, should be developed according to internationally agreed rules, norms and standards, as well as institutions for enforcement. This is widely considered common sense by industry experts but is lost in the geopolitical discourse. In the new technologies, by contrast, the US laissez-faire approach has dominated, although as discussed below the EU has introduced sophisticated regulations to protect against cyber risks that may provide a way forward.

Nevertheless, the risk of a major power acting to weaponise interdependence has now been demonstrated by the US campaign against Huawei and it is equally conceivable that China, too, could weaponise interdependence in the new technologies in which it leads. Neither major power is solely at risk here and both have the capacity to generate risks, or indeed threats. Other states will therefore make a proportionate risk assessment in relation to Huawei with an eye to the geopolitical environment, including in which context cyber and other risks are likely and in which context they would be of high consequence. Governments must also build their technical capabilities to monitor and mitigate identified cyber risks.

The interplay between security and economic factors such as supply chains and trade and investment policies must also be weighed as part of

any risk assessment and development of a risk management strategy. An EU coordinated risk assessment (European Commission, 29th January 2020) noted that the technological change represented by 5G will increase the overall attack surface for potential cyber threats, across networks and in software development and update processes, as well as in relation to reliance on network operators and their role in the supply chain. Without naming Huawei, it drew particular attention to the importance of the individual risk profile of suppliers and the increased risk of dependency on a single supplier.

Each state will have sensitive assets and vulnerabilities and will need to ensure that it has regulatory, monitoring and technical capabilities to protect against risks to those sensitive assets and vulnerabilities. States need to develop and deploy extremely high system security strategies for cyber risk assessment and mitigation in an increasingly complex environment of global supply chains, involving thousands of actors and sources of software code. Further, to protect citizens from the risks posed by both Chinese and US firms, states will need data protection capabilities, with regular audits of data collection processes by international firms, ideally overseen by independent regulators.

The EU has become a leader in grappling with the new cyber-risk management challenges, including its cybersecurity standards, and GDPR to safeguard data integrity. The EU toolbox of risk mitigating measures includes strengthened regulatory powers and technical improvements to improve security of 5G networks and equipment, including restricting "high-risk" suppliers (understood as originating in countries without democratic checks and balances) from providing core network assets and diversification of vendors to avoid dependency on one supplier. Further, it recommends strengthening local EU capacities to supply 5G and post-5G technologies. Cybersecurity risks are assessed

first at the national government level and member states and Union institutions, agencies and other bodies are to develop jointly coordinated Union risk assessment that builds on these national risk assessments (*ibid.*). The provisions restricting core network services recognise that control of the core network is more valuable for espionage than non-core components, the latter only providing access in local areas (Taylor, 2020).

There is however a danger in Europe, unlike the US, that telecommunications providers have neglected their capabilities to manage their own networks, often outsourcing to equipment vendors, including Huawei. Relying on Huawei to monitor cyber risks that some claim originate from or through Huawei would appear to be unwise. Governments taking a risk management approach need to require service providers to maintain full service technical expertise and comprehensive security capabilities, and to ensure they maintain reliable monitoring capabilities, or to develop automated solutions (Hubert, 2020).

Diversification of the supply chain offers an important risk mitigation measure. If at some time in the future, a particular supplier is identified as constituting a likely and consequential risk, it will be less costly to avoid risk if a diversity of suppliers is available and already present in the market. Nevertheless, as in most industry sectors, telecommunications supply chains are highly globalised and it is not only Chinese firms that source components from China, so it should be expected that governments will seek to diversify entire supply chains over time if they remain concerned about cyber risks emanating from China in particular. Equally, economic coercion risks emanating from the US export controls on its advanced semiconductors will force countries and firms not part of the US-led "Clean Network" to source new suppliers and to develop new supply chains, as is already underway (Capri, 2020). Proposed Open Radio Access Networks (O-RAN) may

offer future opportunities to allow multiple vendors to operate 5G services interchangeably, without one firm providing all of the infrastructure or components. Chinese as well as US firms are participating in O-RAN development, but the model is as yet unproven (RWR Advisory Group, 2021). While some industry actors see O-RAN as an opportunity to prevent Chinese proprietary end-to-end service provision and to expose source components to greater security, it also provides the opportunity for Chinese firms including Huawei to build trust over time in a form of cyber governance, including industry standards, that remains open to Chinese firms to participate.

As noted above, the dramatic increase in encryption is likely to mitigate risks of espionage. Control over data integrity can also be strengthened (although not guaranteed) by requiring that data is stored within national borders rather than exported to other jurisdictions. China mitigates cyber risks (from, for example, the US), by requiring that all data storage is held within China's national borders and is subject to its domestic cyber security legislation. To mitigate against cyber-attacks, duplication of critical functionality is one option, although costly, to allow for an alternative network to replace a compromised network (Lysne, 2018). For those governments that can afford it, highly sensitive networks, such as emergency services and national security, can be maintained independently, although this also is an expensive option.

Finally, national governments have a widely-recognised power to regulate trade and investment on national security grounds and this provides potential, although unexplored, opportunities in this case. Instead of a ban, for example, a government could approve a foreign supplier but only on the condition that it forms a new, domestically-based joint venture with a domestic firm that has adequate monitoring capabilities to mitigate cyber risks. Huawei has offered to license its technology to US firms (Huawei, 9th September 2019) and presumably

could be required to do so by other jurisdictions, with national firms building and operating the network, with rewritten source codes, inspections of equipment and software and other processes to meet national security requirements. Huawei has already moved to manufacture 5G network equipment in France for the European market and all of its chipset security is conducted in Finland (Huawei, 27th February 2020). Such risk management options of course would require political goodwill if they are to build trust, which appears unlikely in the current environment.

9. Conclusion

The new technologies of the fourth industrial revolution are generating a whole new set of geopolitical and interdependence risks. While Nye (2011) predicted cyber power would be more diffused than other forms of power, just as earlier observers expected of the information revolution, the shape of the world emerging in the 2020s remains the domain of the nation state. The dominant power, the US, is determined to maintain its position, including resisting global governance in cyber governance and by wielding the power of the state against the claimed risks of Huawei. Meanwhile, China is developing powerful cyber-capabilities to match its growing economic power and is seeking to set the agenda in global governance, yet it is deeply distrusted amongst liberal democracies in particular. In a rapidly deteriorating climate of geopolitical contest, confrontation and even conflict are no longer out of the question. Risks of cyber-espionage and sabotage, as well as weaponization of information and artificial intelligence, therefore become assessed by states as realistic security threats. No rules or institutions exist to sanction rule-breaking or to rebuild confidence and trust. At the time of writing, it would appear the world is headed

Table 2 Indicative Risk Management Framework

Interdependence	**A realist middle path?**	**Decoupling**
Supplier-blind, robust national cyber security defences	Robust national cyber security defences	Exclusion of rival suppliers to avoid risks, augmented by robust national cyber security defences
New multilateral institutions to coordinate and enforce rules, norms and standards for the digital economy	Regional "trusted" groupings with best practice rules, norms and standards	Regional "trusted" groupings with normative rules, norms and standards
Deepened global value chains and interoperability, built upon trusted supplier partnerships	Exclusion of high-risk suppliers but maintenance of global value chains and interoperability, with measures to build trust	Two (or more) separate and self-reliant tech systems, featuring weaponised interoperability and continued geopolitical contest

towards a spiral of decoupling strategically important supply chains and the construction of two rival systems, one led by the US and one by China.

Even in a decoupled world, security risks will remain and there is an urgent need for more technical research on risk management capabilities. At the national level, precautionary measures and enhanced risk management strategies are essential. These are likely to remain highly contested matters for some time to come.

To date, the digital economy has generated natural monopolies that control vast amounts of data, extract value and gather more and more power. These monopoly actors are now the largest firms in the world, and most originate from the US. The lack of governance of the digital economy raises a broader range of risks than China alone. Decision makers have failed to date to comprehensively grapple with the new rules that may be needed to reduce the risks of these natural monopolies seizing more power over governments, the economy and individuals.

The Huawei debate is not simply about the rise of one firm from China to threaten US supremacy. Huawei is a proxy for fear of China itself, its likely future capabilities and possible intentions. Whether China acts according to high risk or threat scenarios is, of course, heavily contingent on the state of the international system and whether it descends into conflict or whether international cooperation can be maintained.

The US and some of its allies appear to so deeply distrust China that they are unwilling to attempt to find new international rules, norms, standards and institutions to govern a new, interdependent digital economy. We should be careful what we wish for. By branding China as an unacceptable risk and decoupling from its world-leading firms, rather than developing risk management strategies and systems for complex interdependence, we may reinforce China's historical geopolitical fear of

encirclement, and over time encourage its government and firms to behave in exactly the way we fear. Of course, if the worst-case scenario analysts are correct, we could be headed in that direction anyway.

The Huawei paradox is therefore more than simply a problem of international business but represents a crisis of interdependence in the international system, driven not only by collapsing trust in a supply chain, but the larger questions of whether it is possible in the 2020s to build processes of engagement, co-existence, norms, verification and enforcement to maintain international peace and security.

Note

* David Morris is Vice-Chair of the United Nations Asia-Pacific Sustainable Business Network, which advises the UN Economic and Social Commission for Asia and the Pacific and hosts the annual Asia-Pacific Business Forum. He is a former Australian and multilateral diplomat, who recently represented the international organisation of Oceania, the Pacific Islands Forum, as Pacific Trade and Investment Commissioner in China. He is completing his PhD at Corvinus University of Budapest, where he is Research Fellow conducting an Erasmus+ Jean Monnet Research Network on European Union-Eurasian Economic Union-Belt and Road Initiative relations. He is Senior Research Fellow at the Research Center for Pacific Studies, Beijing Foreign Studies University. He has an MBA from Henley Business School and a BA (Hons) from the University of Sydney. <*Email: david@davidmorrisprojects.com*> <*Twitter: @dm_aus*>

References

Alon, Ilan and Theodore T. Herbert (2009). A stranger in a strange land: Micro political risk and the multinational firm. *Business Horizons*, Vol. 52, Issue 2, pp. 127-137.

Alon, Ilan and Matthew A. Martin (1998). A normative model of macro political risk assessment. *Multinational Business Review*, Fall 1998. *<https://www.academia.edu/668635/A_normative_model_of_macro_political_risk_assessment>*

Balding, Christopher (5th July 2019). Huawei Technologies' links to Chinese state security services. *SSRN*. *<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726>*

Biddle, Sam (2020). The filthy hypocrisy of America's 'clean' China-free Internet. *The Intercept*, 7th August 2020. *<https://theintercept.com/2020/08/06/the-filthy-hypocrisy-of-americas-clean-china-free-internet/>*

Birnbaum, Emily and Issie Lapowsky (2021). How tech workers feel about China, AI and Big Tech's tremendous power. *Protocol*, 15th March 2021. *<https://www.protocol.com/policy/tech-employee-survey/tech-employee-survey-2021>*

Capri, Alex (30 March 2020). COVID-19 impact on business: Will the pandemic trigger more state intervention in business strategies? (Hong Kong: Hinrich Foundation.) *<https://hinrichfoundation.com/trade-research/global-trade-research/thought-leadership/covid-19-impact-on-business-will-the-pandemic-trigger-more-state-intervention-in-business-strategies/>*

Chan Jia Hao (2019). All may not be smooth along China's digital silk road. *The Interpreter*, 20th Aug 2019. Sydney: Lowy Institute. *<https://www.lowyinstitute.org/the-interpreter/all-may-not-be-smooth-along-china-s-digital-silk-road>*

Chang, Gordon G. (2020). *The great US-China tech war*. New York, NY: Encounter Books.

China Strategy Group (Los Angeles, CA, US) (2020). Asymmetric competition: A strategy for China & technology – Actionable insights for American leadership. *<https://assets.documentcloud.org/documents/20463382/final-memo-china-strategy-group-axios-1.pdf>*

CNN Business (5th December 2019). Huawei sues US government over new FCC restrictions. *<https://edition.cnn.com/2019/12/05/tech/huawei-us-ban-lawsuit/index.html>*

Congressional Research Service (US) (26th October 2020). China issues new export control law and related policies. *Insight*. *<https://fas.org/sgp/crs/row/IN11524.pdf>*

Department of Commerce (US) (17th August 2020). Commerce Department further restricts Huawei access to U.S. technology and adds another 38 affiliates to the entity list. *<https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and>*

Department for Digital, Culture, Media & Sport (UK) (14th July 2020). Huawei to be removed from UK 5G networks by 2027. *<https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027>*

Department of Justice (US) (28th January 2019). Chinese telecommunications device manufacturer and its U.S. affiliate indicted for theft of trade secrets, fraud, and obstruction of justice. *Justice News*. *<https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade>*

Department of State (US) (11th August 2020). The Clean Network safeguards America's assets. *Fact Sheet*. *<https://www.state.gov/the-clean-network-safeguards-americas-assets/>*

Dirks, Emile and Sarah Cook (2019). ANALYSIS: China's surveillance state has tens of millions of new targets. *China Media Bulletin* 139 - October 2019. Washington, D.C.: Freedom House. *<https://freedomhouse.org/report/china-media-bulletin/2019/china-media-bulletinkey-individual-police-*

databases-tiktok>

Ecns.cn (English-language website of China News Service) (4th June 2019). China's Huawei, AU sign MoU to strengthen technical partnership on ICT. *<http://www.ecns.cn/news/sci-tech/2019-06-04/detail-ifziupva1116191.shtml>*

Eisenstein, Ilana H. and Jim Halpert (2018). CLOUD Act bolsters US government powers to obtain data stored abroad: Data protection, privacy and security alert. *DLA Piper*, 12th April 2018. *<https://www.dlapiper.com/en/us/insights/publications/2018/04/us-cloud-act-authorizes-search-warrants-for-data-stored-abroad/>*

European Commission (29th January 2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Secure 5G deployment in the EU – implementing the EU toolbox. *<https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2020/01/POLITICO-5G-toolbox-Communication-of-the-EU-Commission-January-29-2020.pdf>*

Fägersten, Björn (2015). Political risk and the commercial sector – Aligning theory and practice. *Risk Management*, Vol. 17, No. 1, pp. 23-39. *<https://doi.org/10.1057/rm.2015.5>*

Farrell, Henry and Abraham L. Newman (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, Vol. 44, No. 1, pp. 42-79. *<https://doi.org/10.1162/isec_a_00351>*

Fernandes, Clinton (2019). What's at stake in Trump's war on Huawei: Control of the global computer-chip industry. *The Conversation*, 1st October 2019 (updated 3rd October 2019). *<https://theconversation.com/whats-at-stake-in-trumps-war-on-huawei-control-of-the-global-computer-chip-industry-124079>*

Fitzpatrick, Mark (1983). The definition and assessment of political risk in international business: A review of the literature. *The Academy of Management Review*, Vol. 8, No. 2, pp. 249-254. <*https://www.jstor.org/stable/257752?seq=1*>

Fletcher, Bevin (2019). Telenor ditches Huawei, taps Ericsson for 5G RAN in Norway. *Fierce Wireless*, 13th December 2019. <*https://www.fiercewireless.com/5g/telenor-ditches-huawei-taps-ericsson-for-5g-ran-norway*>

Gilding, Simeon (2020). 5G choices: A pivotal moment in world affairs. *The Mandarin*, 29th January 2020. <*https://www.themandarin.com.au/124337-5g-choices-a-pivotal-moment-in-world-affairs/*>

Girard, Bonnie (2019). The real danger of China's national intelligence law. *The Diplomat*, 23rd February 2019 (*China Power* blog). <*https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/*>

Hartcher, Peter (2021). *Red zone: China's challenge and Australia's future*. Melbourne, Australia: Black Inc.

Heater, Brian (2020). Senate passes 'rip and replace' bill to remove old Huawei and ZTE equipment from networks. *TechCrunch*, 28th February 2020. <*https://techcrunch.com/2020/02/27/senate-passes-rip-and-replace-bill-to-remove-old-huawei-and-zte-equipment-from-networks/*>

Hemmings, John (2020). Reconstructing order: The geopolitical risks in China's Digital Silk Road. *Asia Policy*, Vol 15, No. 1, pp. 5-21.

Hillman, Jonathan E. and Maesea McCalpin (2019). Watching Huawei's "safe cities". *CSIS Brief*, 4th November 2019. Washington, D.C.: Center for Strategic & International Studies. <*https://www.csis.org/analysis/watching-huaweis-safe-cities*>

Hillman, Jennifer and David Sacks (2021). China's Belt and Road: Implications for the United States. *Independent Task Force Report* No. 79. New York: Council on Foreign Relations (CFR). <*https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/#about-the-task-force*>

Hjortdal, Magnus (2011). China's use of cyber warfare: Espionage meets strategic deterrence. *Journal of Strategic Security*, Vol. 4, No. 2. <*https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss*>

Hoffman, Samantha (2021). Double-edged sword: China's sharp power exploitation of emerging technologies. *Sharp Power and Democratic Resilience Series*, April 2021. Washington, D.C.: International Forum for Democratic Studies, National Endowment for Democracy (NED). <*https://www.ned.org/wp-content/uploads/2021/04/Double-Edged-Sword-Chinas-Sharp-Power-Exploitation-of-Emerging-Technologies-Hoffman-April-2021.pdf*>

Huawei Technologies Co., Ltd. (9th September 2019). Ren Zhengfei's interview with New York Times op-ed columnist Thomas L. Friedman. <*https://www.huawei.com/en/facts/voices-of-huawei/ren-zhengfeis-interview-with-new-york-times-op-ed-columnist-thomas-l-friedman*>

Huawei Technologies Co., Ltd. (27th February 2020). Huawei announces it will open manufacturing plant for wireless products in France. *Press Release*. <*https://huawei.eu/press-release/huawei-announces-it-will-open-manufacturing-plant-wireless-products-france*>

Hubert, Bert (20th January 2020). 5G: The outsourced elephant in the room. *berthub.eu*. <*https://berthub.eu/articles/posts/5g-elephant-in-the-room/*>

Ikenson, Daniel J. (2019). Blacklisting Huawei could cost trillions, so let's look before we leap. *Commentary*, 5th July 2019. Washington, D.C.: Cato Institute. <*https://www.cato.org/publications/commentary/blacklisting-huawei-could-cost-trillions-so-lets-look-we-leap*>

Jarvis, Darryl Stuart (2008). Conceptualizing, analyzing and measuring political risk: the evolution of theory and method. *Lee Kuan Yew School of Public Policy Research Paper Series* No. LKYSPP08-004. Singapore: Lee Kuan Yew School of Public Policy, National University of Singapore. <*http://dx.doi.org/10.2139/ssrn.1162541*>

Kennedy, Scott (2020). Washington's China policy has lost its Wei. *CSIS Brief*, 27th July 2020. Washington, D.C.: Center for Strategic & International Studies. <*https://www.csis.org/analysis/washingtons-china-policy-has-lost-its-wei*>

Kobrin, Stephen J. (1979). Political risk: A review and reconsideration. *Journal of International Business Studies*, Vol. 10, pp. 67-80. <*https://doi.org/10.1057/palgrave.jibs.8490631*>

Nikkei Asian Review (19th August 2020). How a handful of US companies can cripple Huawei's supply chain. <*https://asia.nikkei.com/Spotlight/Huawei-crackdown/How-a-handful-of-US-companies-can-cripple-Huawei-s-supply-chain?del_type=1&pub_date=20200819190000&seq_num=7&si=83867*>

Lim, Darren and Victor Ferguson (2019): Huawei and the decoupling dilemma. *The Interpreter*, 28th May 2019. Sydney: Lowy Institute. <*https://www.lowyinstitute.org/the-interpreter/huawei-and-decoupling-dilemma*>

Lysne, Olav (2018). *The Huawei and Snowden questions: Can electronic equipment from untrusted vendors be verified? Can an untrusted vendor build trust into electronic equipment?* Cham, Switzerland: Springer International Publishing AG. <*https://doi.org/10.1007/9783-319-74950-1*>

Mc Daid, Cathal (3rd December 2020). How to build a secure 5G network, and protect Alice and Bob from each other. (London: GSMA.) <*https://www.gsma.com/aboutus/workinggroups/how-to-build-a-secure-5g-network-and-protect-alice-and-bob-from-each-other*>

McMaster, H.R. (2020). How China sees the world – And how we should see China. *The Atlantic*, May 2020. <*https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/*>

Nye, Joseph S., Jr. (2011). *The future of power.* New York, NY: PublicAffairs.

Oxford Economics (London) (2019). Restricting competition in 5G network equipment: An economic impact study. (Report commissioned by Huawei.) December 2019. <*https://resources.oxfordeconomics.com/hub*

fs/Huawei_5G_2019_report_V10.pdf>

Polyakova, Alina (2019). Exporting digital authoritarianism (*Rules Based Audio* podcast episode). In: Kelsey Munro (2019), Exporting digital authoritarianism - Podcast out now: Could China and Russia's models of high-tech population control and manipulation spread to other countries? *The Interpreter*, 17th December 2019. Sydney: Lowy Institute. *<https://www.lowyinstitute.org/the-interpreter/exporting-digital-authoritarianism-podcast-out-now>*

Reuters (22nd May 2019). RPT-SPECIAL REPORT-Hobbling Huawei: Inside the U.S. war on China's tech giant. *<https://www.reuters.com/article/huawei-usa-5g/rpt-special-report-hobbling-huawei-inside-the-u-s-war-on-chinas-tech-giant-idUSL4N22Y02S>*

Reuters (17th March 2021). U.S. subpoenas Chinese communications firms in probe of national security risks. *<https://www.reuters.com/article/us-usa-china-commerce/u-s-subpoenas-chinese-communications-firms-in-probe-of-national-security-risks-idUSKBN2B92OH>*

Robock, Stefan H. (1971). Political risk: Identification and assessment. *Columbia Journal of World Business*, Vol. 6, No. 4, pp. 6-20.

RWR Advisory Group (Washington, D.C., US) (2019). Assessing Huawei Risk: how the track record of the CCP should play into the due diligence of Huawei's partners and customers. *RWR Reports (In-depth reports on the risk factors and threat implications of economic and financial statecraft)*, May 2019. *<https://www.rwradvisory.com/assessing-huawei-risk/>*

RWR Advisory Group (1st April 2021). Chinese companies active in the architecture of Open RAN. *<https://www.rwradvisory.com/wp-content/uploads/2021/04/RWR_ORAN_Report_4-2021.pdf>*

Sachs, Jeffrey D. (2018). The war on Huawei (Project Syndicate, 11.12.18). *Pearls and Irritations: John Menadue's Public Policy Journal*, 14th December 2018. *<https://johnmenadue.com/jeffrey-d-sachs-the-war-on-huawei-project-syndicate-11-12-18/>*

Schia, Niels Nagelhus and Lars Gjesvik (2017). China's cyber sovereignty. *NUPI Policy Brief* 2017-02. Oslo, Norway: Norwegian Institute of International Affairs (Norsk utenrikspolitisk institutt (NUPI)). <*http://hdl.handle.net/11250/2434904*>

Schwab, Klaus (2016). *The Fourth Industrial Revolution*. Cologny/Geneva, Switzerland: World Economic Forum.

Schwab, Klaus (14th January 2016). The Fourth Industrial Revolution: What it means, how to respond. (Cologny, Switzerland: World Economic Forum.) (First published as "The Fourth Industrial Revolution: What It Means and How to Respond" in *Foreign Affairs*, 12th December 2015.)

Snowden, Edward J. (2019). *Permanent record*. New York, NY: Henry Holt and Co.

Sottilotta, Cecilia Emma (2017). *Rethinking political risk: Concepts, theories, challenges*. New York, NY: Routledge.

South China Morning Post (Hong Kong) (28th January 2019). UK approves Huawei's restricted use in 5G networks, handing lifeline to Chinese telecoms giant. <*https://www.scmp.com/tech/big-tech/article/3047945/uk-approves-huaweis-restricted-use-5g-networks-handing-lifeline*>

South China Morning Post (2nd December 2019). Will the China of tomorrow run on the technology behind bitcoin? <*https://www.scmp.com/news/china/politics/article/3040132/will-china-tomorrow-run-technology-behind-bitcoin*>

South China Morning Post (13th April 2020). Cybersecurity at top of Huawei's agenda as Europe decides on 5G infrastructure. <*https://www.scmp.com/tech/big-tech/article/3079455/cybersecurity-top-huaweis-agenda-europe-decides-5g-infrastructure*>

South China Morning Post (13th April 2021). US-China tech war: Supercomputer sanctions on China begin to bite as Taiwan's TSMC said to suspend chip orders. <*https://www.scmp.com/tech/tech-war/article/3129362/us-china-tech-war-supercomputer-sanctions-china-begin-bite-taiwans*>

Stockton, Nick (2020). China launches national blockchain network in 100 cities. *IEEE Spectrum*, 20th March 2020. <*https://spectrum.ieee.org/computing/software/china-launches-national-blockchain-network-100-cities*>

Sykulski, Leszek (2014). Geopolitical risk in the analysis of international relations. *European Journal of Geopolitics*, Vol. 2, pp. 132-144. <*https://www.academia.edu/39847124/EUROPEAN_JOURNAL_OF_GEOPOLITICS_2_2014_Leszek_Sykulski_GEOPOLITICAL_RISK_IN_THE_ANALYSIS_OF_INTERNATIONAL_RELATIONS*>

Taylor, Malcolm (2020). Why the UK is right to use Huawei 5G technology. *Verdict*, 28th January 2020 (updated 30th January 2020). <*https://www.verdict.co.uk/huawei-5g-uk-technology/*>

The New York Times (15th August 2015). AT&T helped US spy on Internet on a vast scale. <*https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?referringSource=articleShare*>

The Sydney Morning Herald (24th September 2018). How China is driving Australia and Trump into each other's arms. <*https://www.smh.com.au/politics/federal/how-china-is-driving-australia-and-trump-into-each-other-s-arms-20180924-p505mr.html*>

The Sydney Morning Herald (12th June 2019). New communications minister denies Huawei ban will hurt Australia's 5G rollout. <*https://www.smh.com.au/politics/federal/new-communications-minister-denies-huawei-ban-will-hurt-australia-s-5g-rollout-20190612-p51wup.html*>

The Sydney Morning Herald (31st January 2020). The man who stopped Huawei: A former spook speaks out. <*https://www.smh.com.au/national/the-man-who-stopped-huawei-a-former-spook-speaks-out-20200131-p53wi6.html*>

The Telegraph (UK) (13th January 2020). United States presents Britain with fresh intelligence on Huawei risks in last-ditch attempt to block deal. <*https://www.telegraph.co.uk/politics/2020/01/13/united-states-presents-britain-fresh-intelligence-huawei-risks/*>

Thomas-Noone, Brendan (16th June 2020). Tech wars: US-China technology competition and what it means for Australia. (Sydney: United States Studies Centre, University of Sydney.) <*https://www.ussc.edu.au/analysis/us-china-technology-competition-and-what-it-means-for-australia?utm_medium=email&utm_campaign=PUBLICATION%20ALERT%20%20Australia%20left%20vulnerable%20in%20US-China%20tech%20war&utm_content=PUBLICATION%20ALERT%20%20Australia%20left%20vulnerable%20in%20US-China%20tech%20war+CID_30ef124862712d92ca0d39a536a11a61&utm_source=USSC%20Campaign%20Monitor&utm_term=Tech%20wars%20US-China%20technology%20competition%20and%20what%20it%20means%20for%20Australia#australia-and-the-evolving-us-china-struggle-for-technological-advantage*>

Varas, Antonio and Raj Varadarajan (9th March 2020). How restricting trade with China could end US semiconductor leadership. (Boston, Massachusetts: Boston Consulting Group (BCG).) <*https://www.bcg.com/en-hu/publications/2020/restricting-trade-with-china-could-end-united-states-semiconductor-leadership.aspx*>

Weiss, Jessica Chen (2019): A world safe for autocracy? China's rise and the future of global politics. *Foreign Affairs*, July/August 2019. <*https://www.foreignaffairs.com/articles/china/2019-06-11/world-safe-autocracy*>

World Intellectual Property Organization (Geneva, Switzerland) (7th April 2020). China becomes top filer of international patents in 2019 amid robust growth for WIPO's IP services, treaties and finances. <*https://www.wipo.int/pressroom/en/articles/2020/article_0005.html*>

World Economic Forum (Cologny, Geneva Canton, Switzerland) (published 2nd December 2020). *Global Technology Governance Report 2021: Harnessing Fourth Industrial Revolution technologies in a COVID-19 world*. <*https://www.weforum.org/reports/global-technology-governance-report-2021*>

Zenglein, Max J. and Anna Holzmann (2019). Evolving Made in China 2025: China's industrial policy in the quest for global tech leadership. *MERICS Papers on China*, No. 8 | July 2019. Berlin: Mercator Institute for China Studies (MERICS). <*https://www.merics.org/en/papers-on-china/evolving-made-in-china-2025*>

Zhao Changhui (2020). Using SWIFT settlements to threaten China will backfire. *Global Times* (China), 30th June 2020. <*https://www.globaltimes.cn/content/1193106.shtml*>

Zhang, Longmei and Sally Chen (2019). China's digital economy: Opportunities and risks. *IMF Working Paper* WP/19/16. Washington, D.C.: International Monetary Fund. <*https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459*>

Interviews

1. Banhidi, Ferenc. Telecommunications consultant; former senior official, Hungarian telecommunications authority; current Hungarian representative Body of European Regulators for Electronic Communications. Budapest, December 17, 2019.
2. Gregory, Mark. Editor, *Journal of Telecommunications and the Digital Economy*. Via Zoom, April 12, 2021.
3. Hemmings, John. Associate Professor, Daniel K. Inouye Asia-Pacific Center for Security Studies. Via Zoom, April 16, 2021.
4. Lacey, Simon. Senior Lecturer, International Trade, University of Adelaide; former Vice-President, Global Government Affairs, Huawei. Via Zoom, April 9, 2021.
5. Lewis, Peter. Director, Center for Responsible Technology. Via Zoom, April 9, 2021.
6. Mika, Lauhde. Vice-President, Cyber Security and Privacy, Global Public Affairs, Huawei. Via Zoom, June 8, 2021.