Managing the new political risks in the technology sector

2021

Willis Towers Watson

Managing the new political risks in the technology sector

Table of contents

Foreword

By Sara Benolken

Global Industry Leader for Technology, Media and Telecommunications
Willis Towers Watson

Recently there has been a sea change in the relationship between the technology sector and politics. Like many other sectors, the technology industry has grappled with the consequences of rising economic nationalism and trade wars. Unlike other sectors, the technology sector has increasingly become a political target, as a result of political perceptions – some would say misperceptions – of the market dominance of certain companies and the social impacts of new technologies.

At such a time, reports such as this one, on the new political risks facing the sector, have an important role to play. The report opens with a set of panel interviews with technology executives, ranking the top risks facing the sector. It is always fascinating to hear the political views and concerns of our peers. The report also includes essays by geopolitical analysts on some of the top risk issues identified. We hope these views from experts will shed light on how these important political risk issues are perceived outside the sector.

In this report you will also find callouts presenting views from the Technology, Media and Telecommunications and Financial Solutions teams at Willis Towers Watson.

As we seek to grow our own knowledge of the industry's unique people and risk challenges, we look forward to publishing more such research in the future. I hope you find the report useful and welcome your feedback.

Section 1: Introduction

By Stuart Ashworth

Global Director of Political Risk for Corporates, Financial Solutions
Willis Towers Watson

If we ever thought we could survive without the technology sector, we now know otherwise. As countries worldwide went into lockdown beginning in the winter and spring of 2020, technologies that did not exist even a decade before became our lifelines. Videoconferencing, cloud computing, and high-speed internet at employees' homes enabled at least some parts of the economy to carry on. New technologies became the main channel through which many of us reached out to loved ones and obtained news and entertainment. The social and economic impact of the COVID-19 pandemic, absent these new technologies, does not bear thinking about.

For technology companies, 2020 was also a year of heightened risk. At one time, many companies in the sector were able to treat political risk as an afterthought. The classic academic studies of political risk in the 1970s and 80s found that use of advanced technology, and vertical integration, made companies less likely to suffer expropriation or government intervention, in part because a subsidiary reliant on high technology could not be operated without the participation of the foreign partner.[1]

How times change. Today, the technology sector is in the crosshairs of government regulators worldwide, and has become the central battleground in an acrimonious trade war between the US and China. Many readers might hitherto have associated the term "expropriation" with the oil sector in Latin America. In 2020, "expropriation" became the term of choice for newspapers describing US policy towards certain Chinese technology firms.[2]

Perhaps as result, at Willis Towers Watson, we have seen the technology sector become an increasingly large share of our book of business for political risk insurance. In an effort to understand this phenomenon, we commissioned Oxford Analytica to conduct research into the new political risks facing technology companies. Oxford Analytica convened an expert panel of technology sector executives, to produce the risk radar that appears in the next section, and commissioned scholars in its global expert network to produce peer-reviewed essays on three of the top risks the panel identified: "what next for US-China conflict;" "political uses and abuses of technology;" and "tech supply chains in a world of economic nationalism."

There was a time when technology companies arguably took pride in operating beyond the reach of government restrictions. Tech moved quickly; public policy moved slowly. As you will see in the pages that follow, that situation is changing, with governments taking an increasingly assertive stance on technology regulation even as civil society raises difficult questions about the political role played by new technologies.

What risks will technology companies face as their sector becomes central to geostrategic competition? How are technology companies managing these new threats? We hope you will find Oxford Analytica's findings on these subjects to be useful.

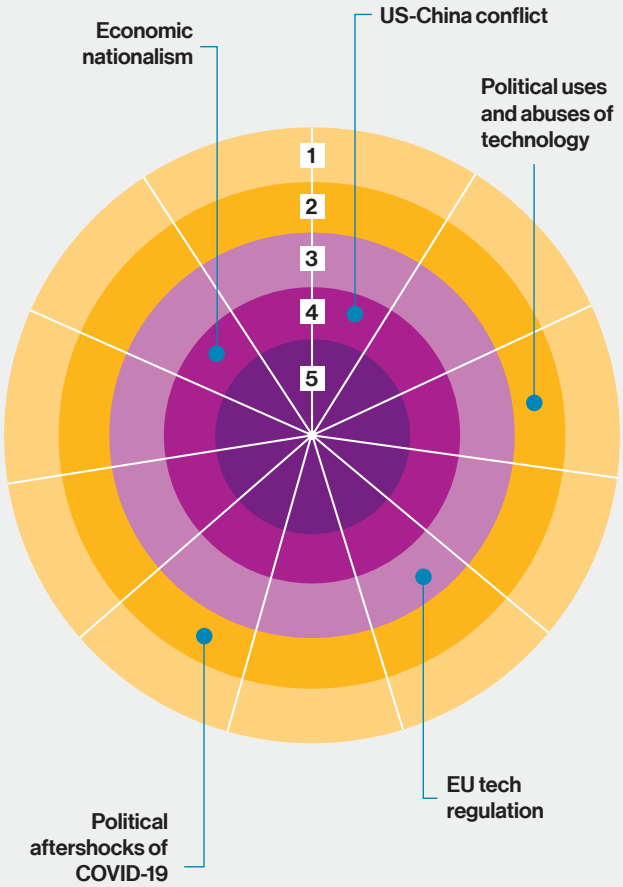
We sincerely thank the Oxford Analytica contributors who authored the following essays, but most of all we thank the expert panel of technology executives who guided the research for their time and insights.

[1] Thomas A Poynter. 1982. Government intervention in less developed countries: The experience of multinational companies. Journal of International Business Studies, 13(1): 9-25. Stephen J. Kobrin. 1987. Testing the bargaining hypothesis in the manufacturing sector in developing countries. International Organization, 41(4): 609-638. Stephen J. Kobrin. 1980. Foreign enterprise and forced divestment in LDCs. International Organization, 34(1): 65-88.
[2] https://www.ft.com/content/235b431c-bf4d-4baf-b84a-ff8ab5f45761; https://news.cgtn.com/news/2020-08-07/The-U-S-may-lose-in-Trump-s-TikTok-war-SKObhCD0Pu/index.html; https://fortune.com/2020/09/24/tiktok-trump-china-deal/

Section 2: The political risk radar

Political risk radar for the technology sector (ranked by number of mentions)

Fig 2 – Risk Radar 2021



Source: Oxford Analytica interviews with the executive panel. "Mentions" count the number of panelists who mentioned each risk topic.

To identify the top political risks facing the technology sector in 2021, Oxford Analytica convened a panel of external affairs and risk management professionals at five of the world's largest technology companies. Firms headquartered in the US and Europe were selected. Oxford Analytica then conducted in-depth interviews with this panel of executives, to produce the risk radar that appears at left. Below, for each risk on the radar, Oxford Analytica summarizes some of the interview highlights. The views expressed do not necessarily reflect those of Willis Towers Watson.

US-China conflict

The global pandemic has had many striking political risk consequences. Governments imposed export restrictions on goods seen to be both scarce and "strategic," including pharmaceuticals, food products, and medical devices. Political leaders, particularly in Eastern Europe, Africa, and Latin America, were accused of using the pandemic as an excuse to muzzle political opposition or postpone elections. But perhaps no geopolitical development was of greater concern than the rapid deterioration in relations between the world's two largest economies, the US and China. "COVID-19 has slowed the progress to phase two of the trade deal between US and China," as one of our technology sector panelists argued.

According to the panel, the trade war between the US and China was having significant strategic and operational consequences for companies. "What will be the impact for Taiwan and Hong Kong?" one panelist asked. Another commented: "the Hong Kong security law is an issue in terms of where the sector bases itself in the region."

European panelists were also deeply concerned about the trade war. "Chips are major problem, because at some level all aspects of chip production and development ends up in US IP [intellectual property]," said one executive we interviewed. "For instance, even chip lithography, which is dominated by Japanese companies, is based on US technology." As a result, US political decisions have global repercussions, which is a concern given that – in the words of another panelist – "there is a huge amount of political risk in the US."

One of the most striking developments of 2020 was the continued development of so-called "entity lists," an approach adopted by both the US and China, that threatened specific companies with loss of access to markets or production locations. Most panelists expressed skepticism about how quickly technology

supply chains could shift in response to political pressures (as one panelist put it: "supply chains will not necessarily change that much, although the PR and messaging around them will"). Yet these entity lists were seen as having the potential to be both effective and extraordinarily costly. "Significant changes to the supply chain will arise if entity lists are 'codified' over time," said one executive. "Such very real restrictive measures, coupled with incredible uncertainty about what happens next, would impact (and are impacting) the sector."

Most panelists believed that these issues would persist past the November US election. There was, to be sure, some optimism about the US-China relationship after President Trump leaves office, at least in terms of a "renewed opportunity for dialogue." But most panelists saw the current trade conflict as one outgrowth of a broader geostrategic struggle for dominance. (Some possible paths for this struggle are outlined in the essay section, below.)

Economic nationalism

Another striking geopolitical trend that the pandemic appeared to accelerate was the trend towards economic nationalism. "Reshoring" was a buzzword long before anyone had heard of COVID-19, but the pandemic seemed to focus the minds of political leaders on such goals. Economic recovery packages in China and Europe, for instance, contained provisions that attempted to groom national champions in "strategic" sectors, including pharmaceuticals, agriculture, and high technology.

Panelists expressed concern about the damage that such efforts could cause. "Our sector is extremely interdependent, and given the emphasis on scale, it depends on a certain set of conditions being in place – including goods, distribution, and talent," as one executive noted. Such requirements make it difficult for technology companies to respond to political imperatives without making great sacrifices in competitiveness. (An issue taken up in more detail in the essay section, below.)

Other panelists pointed out that even companies that might wish to reshore their supply chains would face obstacles. "How can we plan and invest if we do not understand who we can employ and which corporations are at risk?" one panelist asked. "Meaningful supply chain investment will not happen until there is more clarity." A company based in Europe expressed similar concerns about its home region. "Is manufacturing possible in Europe?" said our panelist. "There is so much complementary infrastructure in place where we currently operate. As such, if it [reshoring] happens, it will take time."

Of course, economic nationalism encompasses more than just concerns about the location of production. For technology companies that operate globally, national restrictions pose a wide range of challenges. "Nationalism is a significant concern," one panelist noted. "For us, it is impacting not only our supply chain, but also distribution and data security considerations." Panelists in the US, interviewed before the election, expressed deep concern about immigration policy. "How is innovation achieved?" one asked rhetorically. "It all depends on the ability to attract human talent! Can we do this in an increasingly hostile world?"

EU tech regulation

Although global political coordination in response to the pandemic was disjointed at best, there was at least one region of the world where international cooperation took a large step forward in 2020. In July of that year, after five hard days of negotiation, the European Council hammered out a deal on a greatly expanded common budget and the first ever issuance of a common debt instrument for the European Union. The deal still needs to be ratified and agreed by other European institutions; but Europe appears to be taking significant steps towards greater integration. (See the separate report available from Willis Towers Watson and Oxford Analytica: "European Politics after COVID-19.")

Even that positive geopolitical development has posed potential headaches for technology companies. "US-China trade disputes and EU regulation are key risks for us," as one panelist noted. The European Union appears to be attempting to lead the world in many areas of technology regulation – including privacy, data protection, and antitrust. (As of this writing, in late November 2020, European Union announcements on new rules that would force technology companies to engage in data sharing with rivals have provoked a sharp response from US political and business leaders.) Panelists expected that this trend towards more intrusive regulation of the sector would only continue. "We expect Europe to promote the GDPR equivalent of global supply chain regulations, including environmental impact, human rights, and more," said one executive.

Panelists also expressed concerns about more traditional forms of political risk in Europe. “Brexit has been a huge area ... for companies in terms of planning,” one US executive commented. Another panelist expressed surprise that future political risks had not received higher billing. “Many right-wing groups in European countries are poised to gather momentum as economic pressures increase,” he argued, noting that dissatisfaction with government management of COVID-19, and pressures from migration issues, could exacerbate these political risk issues in 2021.

Political uses and abuses of technology

In the United States, especially in the wake of the 2016 election, technology companies found themselves in the spotlight regarding the political uses of their products and services. Some commentators alleged that new technologies had been used, both by US and foreign organizations, to sway the presidential election outcome.

In 2020, such concerns about the political uses of new technologies only increased. Optimism that technology would enable democracy – based, for instance, on early stories about the role that social media may have played in the Arab Spring – was in some cases replaced by pessimism about technology-enabled authoritarianism. Dictatorial regimes were reported to have used new technologies to censor both traditional and social media and monitor the activities of citizens using biometric tools. “How does this [political use of new technologies] threaten the sector?” one panelist asked rhetorically. “Trust in the sector declines. This has impacts – directly and indirectly – on sales, recruitment, countries of operation, and cost of management.”

Technology has also played a significant role in social unrest. Famous examples include the role of broadcast text messaging in the “people power” revolutions in Southeast Asia, Central Asia and the Middle East – not to mention the use of the Blackberry in the so-called “London riots” of 2011. As social unrest once again becomes a serious concern in the US and Europe, one panelist wondered: “Given this, how should companies position themselves? How will governments respond to this?” Another noted: “It has not got to the point of people campaigning against most technology companies. Yet.”

This issue is explored further in the essay section, below.

Political aftershocks of COVID-19

For the final issue on the technology risk radar, our panel members nominated the political repercussions of the global pandemic. There was concern that institutionally weak governments might face collapse as a result of unprecedented stresses. “COVID-19 induced economic recessions are likely to be felt in 2021 and 2022, perhaps even 2023, and will increase political risk in many countries and regions,” said one panel member.

One major concern was the political repercussions of the pandemic’s uneven impacts. While some individuals and some industries have thrived during the COVID-19 era, at least in a narrow economic sense, others have suffered greatly. “The tail of COVID will be very long on economics and politics,” one technology executive contended. “It [the pandemic] will escalate border and immigration issues, economic disparity concerns, and racial concerns.” In the autumn of 2020, many people continue to be most concerned with day-to-day survival. Once those concerns pass, there could be a political reckoning. “Attention will turn to those who have been less impacted [by the pandemic], which might mean more tax and regulation for those groups,” this executive said.

Managing the new risks

While the main focus of our panel was on identifying the top risks to the sector, we also asked some questions about political risk management. The responses, in many cases, described new capabilities. “My role did not exist five years ago,” said one executive in external affairs. “At that time, only one or two US tech companies had meaningful political risk capabilities and expertise, mainly because of what happened [in US antirust] in the 90s, but this is changing rapidly.”

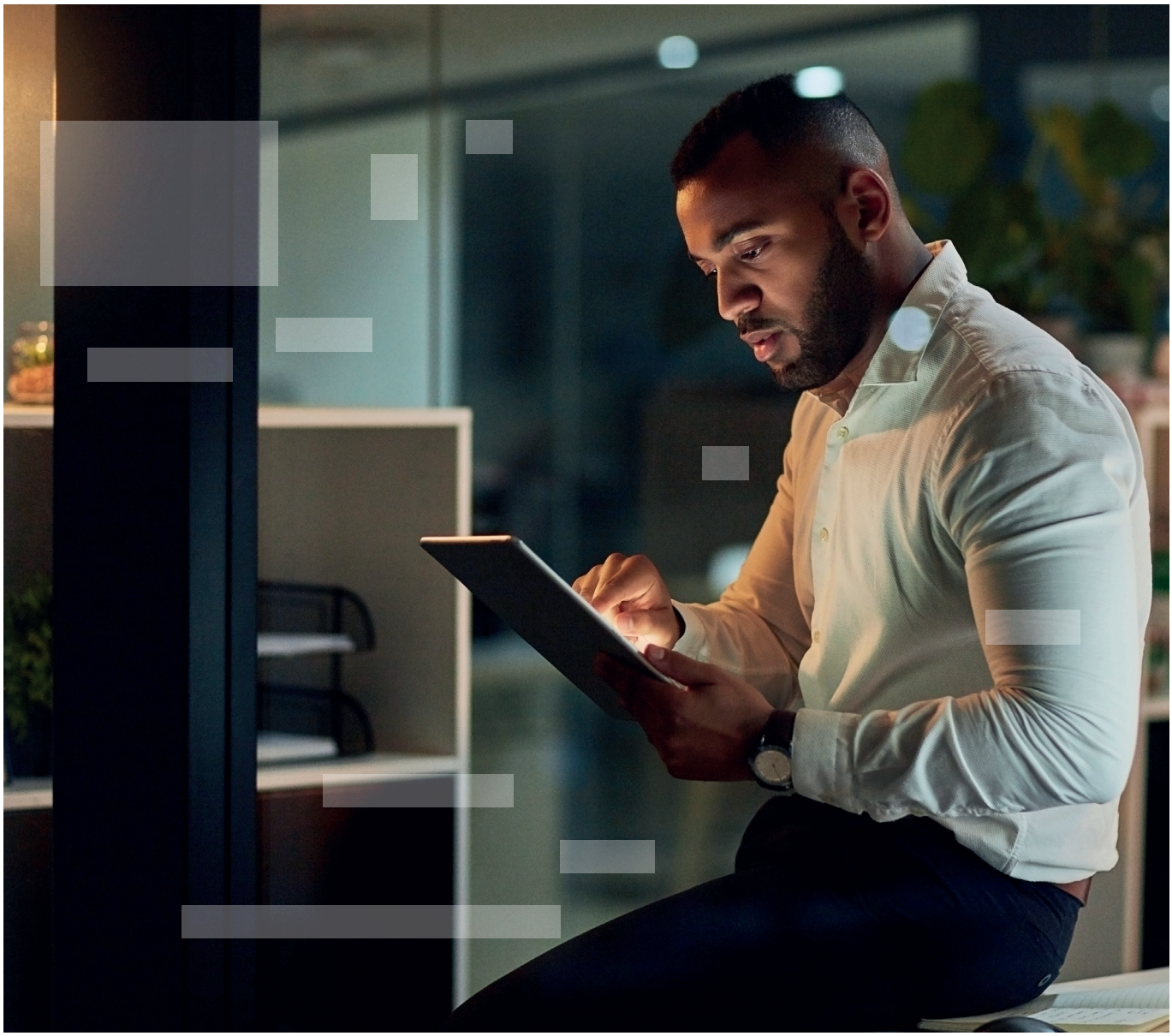
We asked where responsibility for political risk management was located, and received a diverse array of responses. “Now everyone owns political risk!” one panelist claimed, given that geopolitical issues impact business continuity for the supply-chain function, cyber security, and operational security. Another panelist said the locus of responsibility for political risk mitigation was with the public policy team for each of the company’s business units.

Other panelists described new capabilities as well as changes in where responsibilities were located. “Two or three years ago the Procurement Department bore the brunt of [political] risk assessment, but now all departments have to put in place mitigation plans,”

said one executive. Another said: “scenario and war games planning used to be done every three or five years, but now it is an annual exercise, because volatility has increased enormously.”

A panelist in a defense technology company, perhaps more accustomed to dealing with geopolitical issues, noted that political risk has been systematically assessed “as part of our planning process every three years.” In addition, the group strategy and planning function was responsible for identifying emerging political risks as part of a horizon scanning review, conducted every two months. This research served as a “major annual input to the integrated strategic business plan.”

For more on managing the new political risks in the technology sector, see the next section, Will Big Tech be the new Big Oil?



Will Big Tech be the new Big Oil?

By Laura Burns
US Political Risk Product Leader, Financial Solutions
Willis Towers Watson

If "data is the new oil," as the saying goes, might Big Tech be the new Big Oil?[1] In Daniel Yergin's 1992 best seller The Prize: The Epic Quest for Oil, Money, and Power, he follows the history of the oil industry from its beginnings in the 1850s up to the 1990s – and by extension, follows the geopolitical history of the world during that time, given that control of energy resources was often central to geostrategic competition among nations.

Today, it appears that competition for dominance in high technology may become central to geostrategic competition, with the US, Japan, Europe and China backing "national champions" in the industry as they seek to enhance the position of their respective countries, value systems, and technological standards.

Of course, this contest for tech dominance is taking place in a world of multinational corporations, some with revenues on a scale comparable to nations. The commercial strategies and supply chains of these Big Tech companies run orthogonal to the geopolitical objectives of Host Countries and Home Countries, so, in a word, this contest could get "messy."

Consider the following hypothetical future scenarios, which are not intended to refer to any specific company or historical event:

A Western multinational has a long term sales contract with a Chinese firm involved in 5G. By U.S. Government Executive Order, the US firm is banned from doing business with its Chinese customer. The financial damages incurred include the unpaid invoices on items already shipped plus pre-shipment expenses of component parts and some lost profit; the sum of which is over $50M.

A Western multinational corporation has a substantial and profitable subsidiary operating in China. One of its employees tweets via their Twitter account in support of Hong Kong protests and several other employees "Like" the post. The Company's Home Government then publicly criticizes the Chinese government. Despite efforts to de-escalate the situation, the company begins experiencing selective discrimination including audits resulting in prohibitively large fines. Ultimately a key license is revoked without which the firm essentially cannot operate in China. The financial damages include the loss of equity in that subsidiary from being forced to close it down including a year of lost revenue totalling $750M.

Insuring tech risks in the political risk insurance market

In both of these circumstances, political risk insurance could help mitigate the financial loss. Political risk insurance was born out of the post-WWII era as a tool for governments to promote a return to cross-border trade and investment by insuring the political and credit perils investors confronted. Today the market is robust and dynamic; able to support $3 Billion of capacity per Insured program through close to sixty private markets, multilaterals, and many Export Credit Agencies (ECAs).

Premiums are based on the rate-online multiplied by the limit per layer. Those rates generally range from 0.30% - 3.00%. Policies are multi-year with a key benefit of coverage being the policy is non-cancellable and rate guaranteed by the insurance company, even in cases where the risk situation deteriorates mid-term.

Many technology companies already utilize this market for substantial political risk insurance programs and therefore have the capacity and terms "grandfathered in" for the life of their multi-year policy.

For new technology insureds coming to market, there may be some challenges. Companies in the semiconductor or artificial intelligence space may face appetite and capacity constraints. But for many technology risks, the market generally remains open and affordable as of today, although this could indeed change as geostrategic competition in the sector escalates.

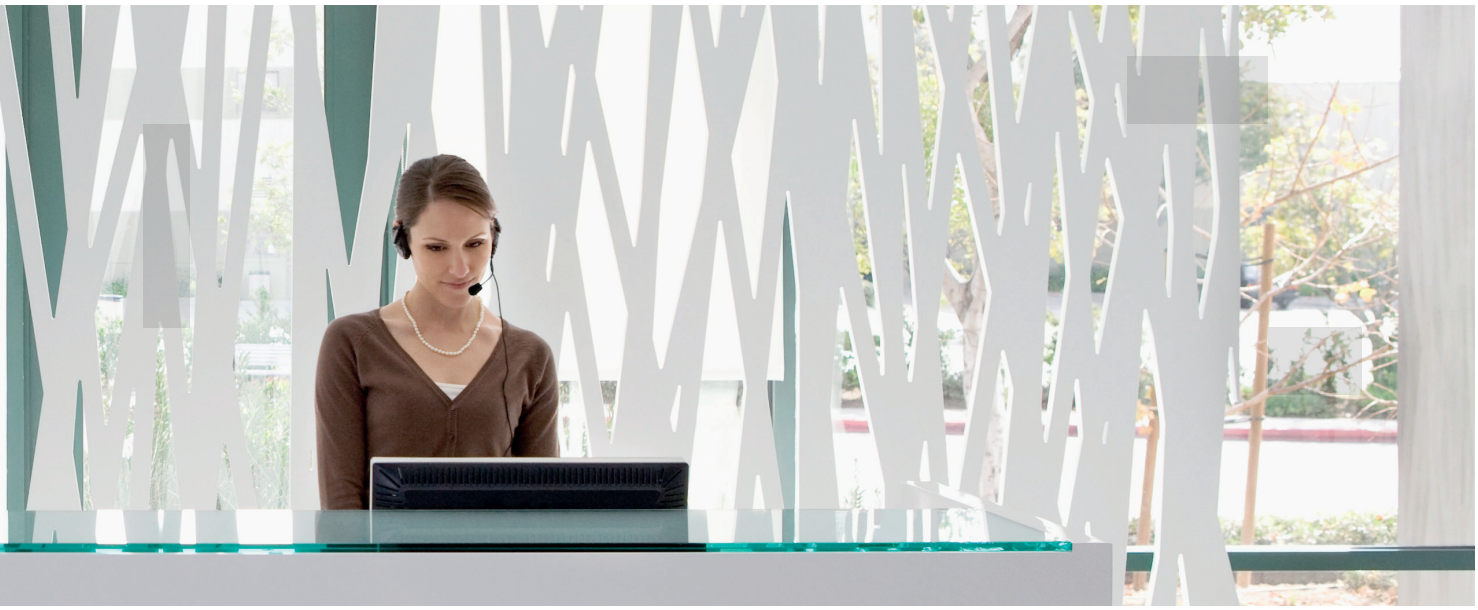
With the onset of COVID-19, and the geopolitical tensions that have heightened over the past year, the market has hardened slightly with carriers being more selective and applying more scrutiny and due diligence with new inquiries. Capacity for China and Asia at large is generally available although there has been some reduction in appetite for China risks due to rising tensions between the US and China, or more broadly tensions between China and the West.

Regarding any effect the outcome of the U.S. Presidential election may have on both risk levels and underwriter appetite for technology risks, we and many analysts share the view that while the political "style" of the new administration may differ from its predecessor, U.S. positions on most key issues with China are likely to remain unchanged (for instance, on Taiwan, on the South China Sea, and on the need to compete strategically in the technology sector). On issues involving human rights such as Hong Kong, the new administration, if it is keen to resume global leadership on human rights, may induce more flashpoints and risks for companies.

We advise global companies to take a proactive approach in their political risk management, and consider political risk insurance with urgency, as these risks will likely continue to increase, and therefore market capacity will likely continue to shrink and rates trend upwards.

Paramount in this risk and market environment is the importance of framing the risk to underwriters and strategic structuring of a program. Working with a strong specialist in political risk insurance will ensure the nuances of the investment and bespoke coverage needs will be captured in an optimized insurance (or other risk management vehicle) terms and conditions.

[1] https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/



Section 3: What next for US-China conflict?

Our panel of technology executives expressed concern that geostrategic competition between the US and China could reshape the global commercial landscape for their sector. We asked scholars from Oxford Analytica's expert network, along with the company's in-house analysis team, to develop forecasts and scenarios regarding how US-China relations could evolve over the medium to long term, and the political risks that could result. This analysis is the invention of Oxford Analytica's experts and not intended to refer to any specific company or companies. The views expressed do not necessarily reflect those of Willis Towers Watson.

The strategic landscape

From a more advanced position, the US is seeking to forestall the rise of a competitor. China, on the other hand, is attempting to buy the time it needs to achieve a greater degree of parity with its prime strategic counterpart. The measures that both sides have taken over the past few years, and are likely to take in the future, will have an outsized impact on the highly integrated and interdependent digital and global economy.

To illustrate our baseline expectation and various possible scenarios that could arise, we have created a simple impact metric (as indicated in the accompanying graphic). Measures appearing at levels 1 and 2 reflect our baseline expectation of developments in relations between the US and China over the medium term. The business implications of these measures could be serious and costly, potentially creating a global divide of standards and regulations, but tensions would remain commercial and economic. A military or diplomatic clash, accident or misjudgement would be required to escalate tensions to level 3.

A true China-US Cold War would be far more expensive and dangerous than their antagonism today

Collateral impact

- **Low:** Little to no impact on third parties
- **Medium:** Numerous third parties have to take it into account OR direct impact on small number of third parties
- **High:** Direct material impact is global or affects a significant number of third parties

	Escalation level	1 Likely to trigger response but not necessarily retaliation	2 Likely to provoke material response or retaliation	3 Significantly increases risk or impact of military conflict
MILITARY	China	FONOPs off the coast of Hawaii Surveillance flights off Californian coast	Military exercises in the Caribbean Mine areas of the South China Sea where the United States conducts Freedom of Navigation Operations	Export long-range missiles to US adversaries Establish bases overseas Upgrade nuclear arsenal; abandon 'no first use'; hair-trigger alert Demonstrate military capabilities and resolve against weaker adversary Covertly support anti-US terrorist groups
	United States	Actively support opposition to China-friendly governments in third countries	Sale of advanced weaponry to Taiwan	Covertly train and equip Uighur, Tibetan and Hong Kong militants
DIPLOMATIC	China	Take South China Sea out of play with multilateral treaty formalising status quo Tit for tat closure of diplomatic missions or expulsion of journalists	Provide aid to US adversaries	Establish defence alliances
	United States	Ratify UNCLOS Encourage Japanese remilitarisation ? Tit for tat closure of diplomatic missions or expulsion of journalists	Recognise Tibetan government in exile	Recognise territorial claims at odds with China's Diplomatic relations with Taiwan Formal military alliance with Taiwan Drop one-China policy
ECONOMIC	China		Dump dollar reserves Force 'unreliable entity list' companies to exit China	Embargo of strategic exports to United States and allies (eg, rare earths) Withdraw protection of US intellectual property within China
	(Both)	Targeted measures against Chinese/American businesses and limitations on data exchange Cut off supplies of high-tech goods 'War footing' public investment in technological and industrial independence	Ban transfers of commercial data between US and China	
	United States	Force China into military space race	Ban inward Chinese investment Ban exports to China of all products containing semiconductors Expansion of 'entity list' to include Chinese firms with major US exports/investments	Actively attack China's economy to undermine CCP legitimacy
INFORMATION	China	Russia-style active disinformation campaign aimed at political destabilisation	Doxing of US public figures	Exfiltration and leaking of information that significantly compromises US political stability or national security
	United States	Publicise Chinese repression of Uighurs in majority-Muslim societies	Ban Chinese students/ immigrants Actively undermine Chinese internet censorship	Aggressive online campaign to stir up discontent in China and destabilise CCP rule

Source: Oxford Analytica analysts and expert contributors.

Measures impacting the technology sector

Digital technology has been a central element in emerging tensions between China and the US. For its part, from a policy perspective, the US has sought to limit China's efforts to acquire foreign technologies, whether overtly via research collaboration projects, investment in foreign businesses or mandated technology transfer, or via covert actions such as espionage and intellectual property theft.

From a messaging perspective, the US administration has sought to highlight the authoritarian application of digital technologies within China – such as facial recognition and location tracking in Xinjiang – and played on public concerns about data sovereignty and privacy to underscore the role of China's government in private-sector technology firms and China's expanding global digital footprint.

China, for its part, appears to see its dependence on US technology as a vulnerability, particularly given the preponderant position the US enjoys not only in the global digital economy, but also in its technical and political governance arrangements.

Both countries have recently sought to reduce technical dependence on the other. The US government has signalled its intention to repatriate technological manufacturing, for instance through the proposed Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act. China, for its part, has a raft of plans concerning "new infrastructure" such as big data, artificial intelligence, semiconductors and other technology areas to ensure self-reliance.

In extremis, it is possible to imagine the development of two entirely separate technological ecosystems, one Western and one Eastern, with many products and software having limited interoperability with the other – a Cold War within the technology sector, in a manner of speaking. In such a scenario, technology companies with operations on both sides could face increasing levels of political risk as the divide becomes more pronounced.

Below, we outline the steps taken thus far in the direction of such a bifurcation of the global technology sphere.

Export restrictions

The US has expanded the use of its "entity list" export restriction system, originally created in 1997 in an effort to limit proliferation of weapons of mass destruction, to limit the provision of particular technologies to numerous Chinese businesses. Businesses have been included for alleged violations of sanctions against Iran, for involvement in surveillance systems in Xinjiang, and for contributing to Beijing's military-civil fusion agenda.

China has passed a new draft Export Control Law, and its draft Data Security Law includes potential retaliatory measures against countries restricting exports to China. In the meantime, it has updated regulations to prevent the transfer of technology in Chinese companies to the US, where Chinese companies are acquired by US buyers. In the future, the Ministry of Commerce is reported to be considering restricting exports of hardware manufactured in China by European firms if European countries ban certain Chinese telecommunications technology providers.

The "unreliable entity list," although a response to the US entity list system, may prove to have a broader remit. The announcement of the list by China's Ministry of Commerce envisioned possible sanctions including trade restrictions, investment restrictions, restrictions on travel or work permits for individual employees, fines, and unspecified additional measures.

Import restrictions

The US has strengthened limitations on the purchase of Chinese telecommunications equipment, and issued wide-ranging national security-based limitations on technology purchases. A range of measures, including the Secure 5G and Beyond Act, the Clean Network Initiative, and the Secure and Trusted Communications Networks Act further limit imports of Chinese technology.

China has announced that it is developing an "unreliable entity list" of foreign businesses, which may particularly focus on any companies that are seen to have taken politically-motivated actions involving China. Furthermore, the Cybersecurity Law and subordinate regulations impose supply chain reliability and technical security requirements for technology purchases by critical infrastructure operators.

Data handling and cross-border data flows

While the US has, thus far, not limited data flows to China, measures against certain Chinese mobile technology companies, including the banning of transactions between US individuals and entities and some of these companies, mark a shift. Various US government departments have indicated data access by Chinese companies might constitute threats that would be considered in policy decisions.

China, meanwhile, is building an emerging data framework that would require, inter alia, security checks before the outbound transfer of personal data, and mandate data gathering within China to be conducted by domestic businesses. A broad draft Data Security Law imposes security review for all "data activities" that might affect national security.

Investment limitations

China has long limited or banned foreign investment in crucial sectors, including value-added telecommunications services, telecommunications infrastructure, and online content. China's unreliable entity list system, noted above, could also lead to the sudden imposition of investment restrictions, targeting specific foreign companies on a discriminatory basis. The US is now using the CFIUS mechanism to scrutinize Chinese investments more thoroughly, and tightening stock market listing regulations.

Managing political risks in the technology sector

By Fredrik Motzfeldt
GB Industry Leader for Technology, Media and Telecommunications
Willis Towers Watson

While the prospects for the global technology industry look promising as we enter 2021, increasing political tensions and worsening trade disputes are likely to have profound and disruptive effects not only on society as a whole but on the environments in which these companies and their customers operate.

Breakthroughs in such areas as artificial intelligence, automation, and other disruptive technologies are increasing productive potential and opening up new investment opportunities but also making the risk landscape more complex. Entire new industries are emerging, which could have a significant impact on the size and shape of the world's tech sectors and the companies that operate within them. The combination of the internet, artificial intelligence, network capable devices, data analytics, cloud computing, and machine and deep learning capabilities will continue to transform our world, the way we work, and the talent companies need. New technologies will enable virtual business and operating models that we have never seen before. But these developments are also changing the risk landscape.

Companies across all sectors are grappling with how these developments will affect their core business models, consumer expectations and the way each company interacts with its clients. Most industries and sectors of the economy worldwide have been impacted by the COVID-19 outbreak and overall political turmoil in 2020, with political and regulatory uncertainty continuing to add to the challenges facing most companies globally. Nonetheless, the world's technology market is expected to grow overall in the period of 2020 to 2025. Digital solutions and technologies are helping to cope with challenges posed by COVID-19. The current pace and wide adoption of remote working and other digital technologies have been unprecedented with massive investments across most industry sector. The technology sector has seen the benefits but is also facing new risks and challenges as a result.

For technology companies, 2020 has been a year of heightened risk. COVID-19 and trade disputes have disrupted the global supply chain of the major technology companies and in certain cases shut down entire production lines and supply chains for extended periods of time. Rising political risk is at the top of executives' list of concerns with companies feeling increased pressures in areas such as access to talent (including work visa restrictions), regulation of intellectual property and in political challenges to alleged dominant market positions and ownership structures.

Despite the tricky situation, technology companies are working to strengthen their risk management, business continuity, crisis resilience and overall response to risks. They are updating plans for recovery and recognising the importance of building and stress-testing a variety of risk and impact scenarios to be better prepared for what is to come. Increased work is being undertaken in identifying areas of risk and opportunity and to better be navigating through the crisis. Many 'established' industry trends have been disrupted or cut short following the COVID-19 outbreak and many of the predictions put forth in early 2020 are now, in our opinion, either invalid or on hold. Disruptions related to COVID-19 are also affecting raw materials supply and causing an inflationary risk on products. The risk landscape facing technology companies has also changed materially and will most likely continue to evolve for some time to come.

We therefore believe that technology industry executives need to apply a 4 to 5 year view of the political risk landscape, looking through a different window/lens at a world that is continuing to change dramatically and with the recognition that the economic uncertainty, yet to be fully felt, could well require a rapid shift in strategy. The five forces shaping the "new" or perhaps "next" normal (metamorphosis of demand, altered workforce, changes in resiliency, new expectations, regulatory uncertainty and the evolution of the virus) should be reflected in technology companies' approach to Insurance and Risk Management strategy and solutions. WTW would advise business leaders worried about the future to take action to manage risk more proactively today. The high level of uncertainty in and changes to their global operating environment means that increased agility and a heightened awareness of risks will be key to success.

Section 4: Political uses and abuses of technology

In this essay, scholars from Oxford Analytica's expert network assess the risks for technology companies arising from the political uses of their products and services. The analysis reflects the scholars' views and not necessarily those of Willis Towers Watson.

Current use of technology by authoritarian regimes

Governments, particularly in the emerging world, have been heavily criticized for use of technologies for **firewalls and censorship**. The Russian government is reportedly taking steps to incorporate elements of China's so-called "Great Firewall" approach by isolating certain elements of the country's Internet from the rest of the world. In Egypt, President Abdel Fatah el-Sisi's government has allegedly carried out more idiosyncratic measures in an effort to manage online dissent, resulting in the blocking of at least 500 news websites and the jailing of numerous Egyptians for posts on Twitter and Facebook. In recent years, women have been jailed for speaking out against sexual harassment online, and the LGBTQ community has faced arrests and raids on public gatherings. A Cairo administrative court is reportedly currently deciding whether to block access to YouTube, the second most popular social media platform in Egypt, on a more comprehensive basis.

Authoritarian states around the world are using Deep Packet Inspection to monitor citizens and censor content that is deemed unlawful. Pakistan's national telecommunications regulator has reportedly deployed Western technologies as part of its nationwide web monitoring system, including equipment for monitoring and analyzing all of Pakistan's incoming and outgoing internet traffic. While authorities have denied the existence of such a web monitoring system, the reported moves could reflect both the country's ongoing fight against terrorism and, arguably, the state's reliance on censorship.

Governments in the emerging world are increasingly deploying **biometric systems**. Some of the world's largest democracies are developing the use of facial recognition systems against those engaged in political protests, opening the way for more authoritarian regimes to do the same. Earlier this year, police in Delhi used facial recognition software to identify people who were demonstrating against the government's controversial Citizenship Amendment Act.

Actions by advanced economies are likely to be mimicked and may be abused

The EU's Central Identity Repository (CIR), which is now expected to become operational in 2023, has been designed to hold the records of over 300 million people and will allow police forces across the EU to search and cross-check the records of immigrants and visitors from outside Europe. The database has already been criticised by human rights activists and observers who are concerned the CIR will be used to track down migrants for deportation.

In Kenya, the government's 60-million-dollar mass biometric registration campaign has been criticized by minority groups and civil rights campaigners who are concerned about its potential for abuse and lack of data protection. While more than 20 million Kenyans have enrolled so far, reports have emerged of state agencies who have threatened to cut off services to those who refuse to register.

India has announced plans to build a nationwide repository which will be able to match images of ordinary Indians extracted from sources including video footage to a database of criminals. While India currently has no laws overseeing personal data protection, a comprehensive privacy bill introduced in December 2019 has alarmed digital and human rights experts by carving out broad exemptions for authorities to access the personal data of its citizens.

New laws foreshadow future developments in political uses of technology

Russia's "sovereign internet law", introduced in 2019, gives the Kremlin the ability to restrict access to the Internet in "emergency" situations. The technologies installed to implement this law could also increase the ability to censor. A recent report by Roskomsvoboda, a Moscow-based digital rights group, counted nearly 440,000 incidents in 2019 where individuals faced barriers when trying to access online sources of information.

Several countries have passed new legislation to outlaw disinformation during the pandemic. Human rights groups are concerned that these new laws could be used by authoritarian regimes to stifle dissent or criticism. A new law in Saudi Arabia makes spreading rumours on social media punishable by prison terms of up to five years (as part of an effort to counter false information regarding the pandemic). In the United Arab Emirates, spreading fake information about the coronavirus in the country could lead to jail sentences ranging from three years to life according to the UAE's Ministry of Interior.

The pandemic has increased government use of information technology across the world, and certain Asian governments have shown that technologies can play a central role in containing the spread of the virus. The pandemic could thus be used to justify the need for greater monitoring of people in terms of where they travel, who they meet, and the extent to which they are adhering to government instructions. The use of contact tracing as means of isolating those exposed to the COVID-19 virus is just one example.

For authoritarian governments, which have cited, for instance, the improvement of traffic patterns or combating crime as the reasons for cameras in public spaces, the pandemic has created cover to increase surveillance using new technologies, which will almost certainly be exploited in the year ahead.

Section 5: Tech supply chains in a world of economic nationalism

Our executive panel expressed scepticism that political imperatives would be effective in reshaping global supply chains – especially in the technology sector. ("Supply chains are not as fungible as people think," was one such comment.) We asked scholars from Oxford Analytica's expert network to provide their view. The analysis reflects the scholars' views and not necessarily those of Willis Towers Watson.

Traditional policy measures have a limited impact on technology value chains

COVID-19 has heightened speculation about the contraction of global supply chains and the near-shoring or re-shoring of manufacturing back to Europe and North America. However, because of the unusual nature of technology value chains, there would be far higher costs for countries looking to re-shore production or otherwise narrow the geographic scope of business activity, in the technology sector as compared to other sectors.

Technology value chains differ from more standard product supply chains in fundamental ways. The shape of the latter are in large part dictated by retailers or finished product manufacturers who make key decisions about product selection or development. These more typical supply chains tend to be vertically integrated with key parts, sub-systems, production equipment, and in many cases final goods outsourced to Tier 1 suppliers, each of which in turn makes its own decisions regarding the structure of supporting lines of components and materials suppliers. Supply chain competitiveness depends mainly on cost considerations and the ability to deliver a competitively priced product to consumers while meeting quality standards and delivery schedules.

Technology value chains can resemble this standard model in regard to established product lines of legacy, "generic" technologies. For high-value technology goods, however, the sources and pace of innovation is generally the major determinant of overall value chain competitiveness.

In the case of technology companies, decisions regarding the locations of final product design and development depend to a large extent on the cost, capacity, and upstream and downstream innovative capabilities of highly specialized materials and components producers. The specialized producers, in turn, make their own value chain decisions in response to similar criteria. Technology value chains also have a high software and services content that is integral to the value proposition they offer customers. Technology value chains are highly complex as a result, and difficult to shift without loss of economic value. These factors have determined the global diffusion of technology value chains, as well as their dynamic and fluid nature as new networks of suppliers and technology partners, many of them start-ups, evolve rapidly. Companies often globalize these value chains in order to source new technologies and IP from around the world, as well as to locate or outsource product development, design, and manufacturing facilities to regions with comparative advantages best suited to those business functions, whether these advantages are proximity to large markets, low labor costs, ready access to materials or innovation ecosystems, or access to well-developed logistics infrastructure.

Because technology value chains are complex, companies in the technology sector are less likely to respond to ordinary policy measures such as incentive payments, tariffs, quotas, or other trade restrictions. Companies will often find that absorbing the resulting economic losses is less costly than adjusting their global patterns of innovation and production.

The pandemic has resulted in managerial innovation in technology value chains, and may lead to sustained shifts in the medical technology sub-sector

The pandemic is one factor that has led to significant innovation in technology value chains in only a few short months. However, with some exceptions, this innovation does not appear to have led to reshoring.

The pandemic, or rather government and business reactions to rapidly rising rates of infection, resulted in temporary, and in some cases permanent, production closures on the part of suppliers, threatening both the security and resiliency of manufacturing supply chains and technology value chains, especially when critical materials, components, or products are concerned.

To date, there is no evidence that the pandemic is leading to a widespread localization of product supply chains. Import dependence has increased as merchandise imports have remained more buoyant than GDP in all major economies, except for China.

Nevertheless, companies have had to mitigate supply chain risks. Within technology value chains, they are responding by:

- Implementing more sophisticated data analysis tools to forecast demand and identify supply risks.
- Undertaking flexible supply contracts.
- Expanding procurement to multiple sources and where possible developing local sources of supply, including a greater degree of vertical integration within their business.
- Increasing inventories of critical products and components.
- Deploying more flexible automated production processes that will allow them to respond more rapidly to changing market conditions and emerging business opportunities.
- Enhancing the flexibility of delivery channels through multiple modes of transportation.
- Enhancing logistics, maintenance, warranty, and other customer services.

In medical technology, changes in value chains have been more significant. Many manufacturers in non-medical sectors have turned their product development and production capabilities to fill supply gaps for critical health care products as well as the components and materials required for their production – creating, in effect, new value chains in the sector. At the same time, governments are investing heavily in domestic manufacturing capacity and supporting infrastructure related to products that can be used to fight the pandemic. While new product development and manufacturing capabilities will result from these initiatives, their long-term sustainability will depend on the ability to innovate new product lines and compete internationally in terms of cost, quality, and availability.

Regulatory restrictions may lead to shifts in value chains, at a cost

While ordinary trade measures are unlikely to shift technology value chains, regulatory shifts could do so – albeit at a significant cost. These measures are being contemplated for a variety of reasons, ranging from environmental concerns to geostrategic competition.

Examples of such measures include:

- US measures to restrict the procurement of Chinese technologies and the export of critical US technologies.
- Measures taken by the US, its other Five Eyes partners, the European Union, and Japan to block the adoption of Chinese 5G wireless, drone, and other information and communication technologies.
- Data localization requirements implemented by public authorities that restrict the collection, storage, and accessibility of personal, government, and other types of data.
- Measures barring the import of carbon-intensive or environmentally damaging materials and components.
- Requirements for supply chain traceability and enhanced quality control, especially with respect to food and medical products.
- Higher standards of corporate social responsibility imposed on sourcing and procurement practices.
- Measures to restrict applications of machine learning and other forms of artificial intelligence.

Because these measures are costly, because the technology sector is growing as a share of value-added in many advanced economies, and because the political clout of the technology sector is expanding rapidly, policies such as these are likely to be constrained by their economic consequences. Where the technology sector is smaller, such measures are more likely to be adopted – and constrain the sector's future growth.

Measures to encourage innovation may also shift value chains, but risk undermining competitiveness

The above analysis may appear to paint a picture of value chains that are static. Far from it: technology value chains evolve rapidly, often in response to pressures of innovation.

To the extent that it does make business sense to concentrate aspects of technology value chains in developed economies like North America and Europe, it is more likely to be for purposes of leveraging their research and start-up innovation ecosystems, developing new, more specialized, higher-value, higher-margin technologies and technology applications, and taking advantage of government investment programs for new product development and production.

There have been numerous examples of government efforts to leverage the sector's responsiveness to innovation with measures to encourage the growth of domestic technology clusters, for instance:

- India's recent announcement of its indigenous innovation strategy.
- Increases in government subsidies in support of US semiconductor and other materials and components manufacturers.
- The widespread increase in state support for domestic research and development and technology companies and incentives to build strategic alliances among companies to counter dominant market actors.

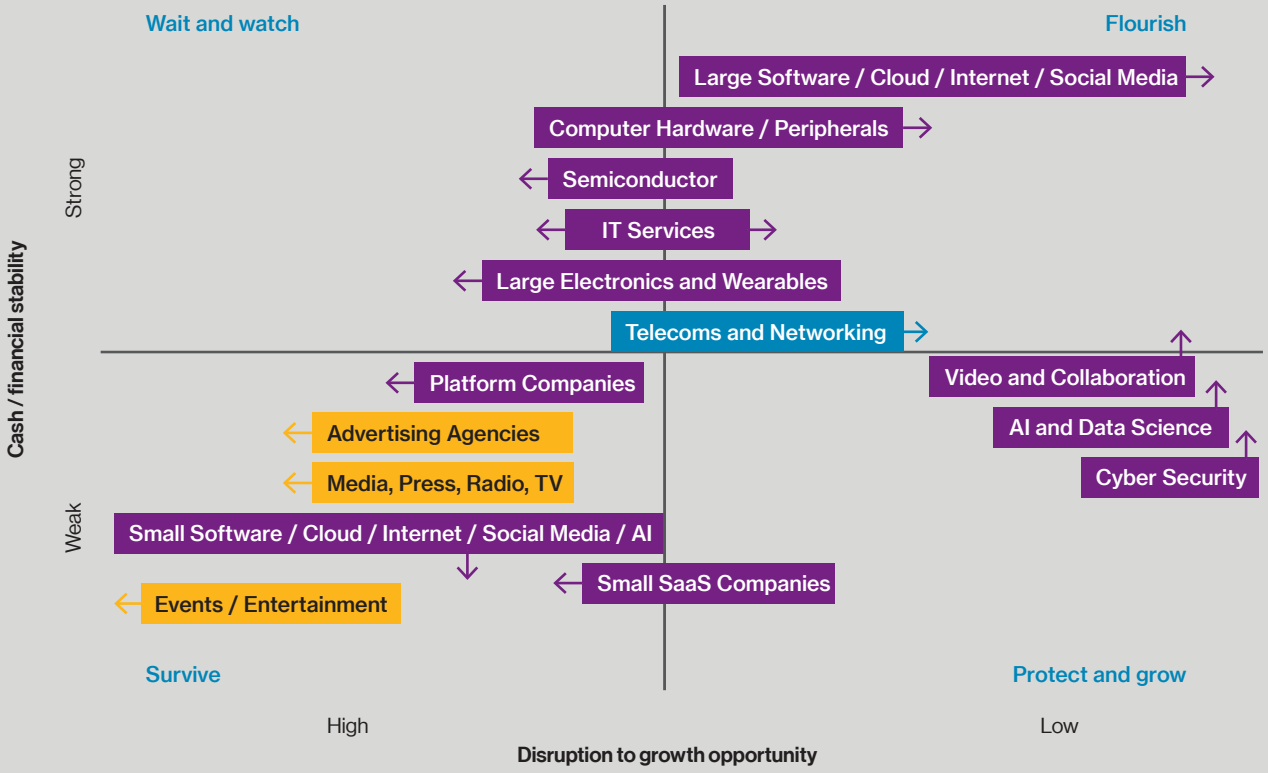
Such measures, along with the harder regulatory shifts discussed above, could lead to significant value chain localization. However, these measures risk inadvertently undermining the global competitiveness of the companies involved.

Protective restrictions that reduce the efficiencies and flexibility of technology value chains will inevitably lead to a misallocation of resources, overcapacity in lower value product lines, and an inability to keep up with the pace of innovation. They are not likely to be sustainable without massive state investments. For governments resorting to greater degrees of technology nationalism, it will be difficult to avoid succumbing to the so-called "Galapagos Syndrome," where value chains become highly adapted to serve niche markets, and unable to complete globally. In sub-sectors where scale economies are important, such national technology champions may be unable to survive without the need for more and more subsidies, or extensive protective trade barriers.

The WTW Technology, Media and Telecommunications Futures Report: a sneak preview of risks on the horizon!

By the WTW Technology, Media and Telecommunications Practice

Fig 1 – Expected performance of technology sub-sectors following the disruption from COVID-19



Arrows show likely direction of subsectors as the pandemic lasts longer

**Source: WTW Technology Industry Team*

In the first half of 2021, Willis Towers Watson will publish its 'WTW Technology, Media and Telecommunications Futures Report: Risks on the horizon!'. This report, created with input from the Willis Research Network, will aim to help companies strategically plan as well as mitigate the risk implications brought about through the advancement of technology. The research will allow WTW to continue to help corporate decision makers prepare for a more strategic role and allow companies to better prepare for the changing risks. Among the key issues that the 2021 report will highlight are the following:

- The impact of inclusion and diversity 'societal pressures' on the Technology industry. There is a perception of lack of inclusion and diversity, including but not limited to gender and race, in the tech sector.
- US Visa H1B restrictions and the implications for US tech firms that are not able to hire sorely needed tech talent as a result.
- The perception that leading tech companies are 'de-facto monopolies' and the anti-trust investigations and calls for breakup of certain large US tech firms by some members of the US Congress.

Please look out for the report in April. Above is a graph of expected sub-sector performance in the wake of COVID-19, based on research conducted by the WTW Technology Industry Team.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW E100001/12/20

FPS1433

willistowerswatson.com

Willis Towers Watson