

Council Perspective

Competing in an Age of Digital Disorder

Geopolitical competition and government regulations are poised to remake the digital economy. To manage this complexity and uncertainty today and remain competitive in the future, companies must engage in strategic end-to-end digital transformations.

June 2019

Executive Summary

- The global technological landscape is currently being reconstructed, subjecting the once-free and unfettered transfer of data across borders to new and greater digital walls. Terms such as the “splinternet” and a “digital cold war” are becoming ubiquitous, forcing companies everywhere to shift strategies on everything from procurement to customer engagement. **We are descending into a period of digital disorder.**
- It wasn’t always this way. Almost three decades have passed since the World Wide Web ushered in a period of unprecedented growth in the global exchange of data. The **initial digital order** was characterized by rapid growth in the use of the Internet and a corresponding massive increase in devices that enabled users to connect to the network. The digital revolution has since accelerated incessantly, with **advances in the design and application of digital technologies** that continue to reshape how people go about their daily lives, how companies conduct business, and how entire industries are structured.
- But even as digital technologies continue to evolve, **the global environment for digital is shifting dramatically** for both technology companies and the individuals and companies that rely on their services. These shifts are the result of governments around the world becoming more active in the digital environment, through both intensifying regulatory activity and escalating global competition.
- Much attention is now focused on the “techlash” nature of new policies and regulations on digital, but many governments are in fact seeking to **strike a balance in policies that both maximize digital’s upsides and mitigate its downsides**. Whether those governments are able to successfully and deftly strike such a balance will influence the ability of companies to use digital technologies effectively in the coming years.
- The competition to maintain relevance and international competitiveness in the 21st-century digital economy is intensifying across a variety of technologies, but two in particular stand out: **5G wireless networks and artificial intelligence**. And although many countries are engaged in this competition, the United States and China have emerged as the two leading players in terms of the current level of domestic digital technologies and investments for the future.
- International agreement on how to regulate digital remains elusive, so **companies are increasingly having to manage a complicated set of conflicting rules in key markets**. Furthermore, there is a growing risk that the competition for dominance in important technologies will fragment the global digital economy into smaller “islandized” segments, complicating global supply chains and the operations of international companies.
- We are just at the beginning of this period of digital disorder. **And there is a high level of uncertainty about the digital order that will emerge from the current phase**. Our scenario analysis of the range of future global operating environments for digital technologies suggests that companies should be prepared for radical changes in how the digital economy will operate over the next decade.
- Companies cannot be passive observers of the ongoing digital revolution. They should be actively adapting to the current digital disorder while also preparing for the future digital order by **embarking on strategic end-to-end digital transformation**. Although the appropriate actions will vary based on the exact contours of the emerging digital order, the consistent conclusion across the four scenarios is that this transformation must take place in strategy, customer experience, operations, risk management and compliance, and employees and culture—our SCORE framework.

Introduction

Digital technologies are now prevalent in all aspects of business operations. In fact, one would be hard-pressed to find a company, from large multinational manufacturers to traditional mom-and-pop retailers, that does not leverage digital technologies in some meaningful way. Yet the rapidly shifting technological landscape—from quick innovation and product cycles to growing [digital walls](#) between countries—has fundamentally reshaped the process for investing in and upgrading a business' technological capabilities. It is now not only a crucial procurement decision, but a process that must also account for previously unrelated external factors, including the trajectory of geopolitical tensions.

This is in large part because technology is now a significant front in the growing tensions between the United States and China, with the two countries moving into what may become a digital “[cold war](#).” This may be accelerating the transition to what some observers have described as the “splinternet,” where the digital ecosystems of China on the one hand and the West, led by the United States, on the other become more independent and isolated from one another. Additionally, many countries are trying to align their regulatory environments with both these new geopolitical realities and domestic priorities. This means that the rules are changing in different ways across different countries and affecting everything from personal privacy to data localization laws and sector-specific standards. As a result, a patchwork of new and sometimes conflicting rules affecting all aspects of the economy is growing in complexity—and in real time.

This period of digital disorder adds new layers of complexity to normal business operations. The nationality of your customers matters for how you can communicate with them. The national origin of hardware, software, and data matters for cross-border interoperability and, in some cases, for national security. Companies today therefore cannot be passive observers of the ongoing digital revolution, but rather must actively manage the complexity and uncertainty by engaging in strategic end-to-end digital transformations.

The Digital Transformation Journey

There is an axiomatic reason for businesses' widespread adoption of digital technologies: they introduce new value propositions and generate new sources of value for companies. Data—including both the creation of novel sources of data and the analysis of that data to generate fresh insights—is at the heart of this fundamental change in where economic value resides. In the 21st-century digital economy, data has become one of the defining sources of differentiation for companies. And because data has a natural networking effect, it has enabled some companies to become dominant players in their industries very rapidly—disrupting entire industries in the process.

dig·i·tal

The computer or Internet-based products and platforms that generate, store, process, leverage, and connect immense amounts of data. Digital, then, includes traditional computer processing and smart-device applications as well as emerging technologies, such as artificial intelligence (AI) and quantum computing. —**A.T. Kearney**

Despite the ubiquity of digital technologies, we still see companies at all stages of the digital journey. Digital-native companies tend to infuse digital in all aspects of their operations, but there is a wide range of digital adoption among companies that were not “born digital.” Some of these legacy companies are just discovering that the digitalization of their business operations can safeguard their core business by improving productivity and efficiency. Others are exploring or accelerating the use of digital to extend their core business and increase revenue through improved customer experiences. And a select few are much further along in their [digital transformation](#) journeys, leveraging digital to transform their business by developing new revenue streams. One such example is Nike, one of the first legacy companies to create a large-scale digital platform of goods and services. Users of the [Nike running app](#) spend almost three times as much on Nike products as the company's other customers. And Nike recently launched a [smart basketball shoe](#) that promises to improve athlete performance while also providing the company with an additional data stream about their consumers.

How can other legacy companies embark on their own digital transformations to drive business growth? A complicating factor in answering that question is that digital is not a static concept. Digital technologies began proliferating in the 1990s and advanced rapidly with the increasingly widespread use of the Internet. Current digital technologies continue to evolve even as other new technologies are emerging. Much attention has been paid, for instance, to the technologies underpinning the [Fourth Industrial Revolution](#) (4IR)—AI, [3D printing](#), advanced robotics, the Internet of Things (IoT), and augmented reality—that are reshaping production processes and therefore redefining global value chains. Digital growth and disruption, then, will increase exponentially in the coming decades. As a result, companies cannot simply “do digital” as a one-off initiative. Rather, they need to stay abreast of new digital innovations and use cases, incorporating them into their business models and operations as appropriate on a timely basis.

The environment in which digital technologies are used has also become more dynamic as a result of the digital revolution entering its second phase, which is being characterized

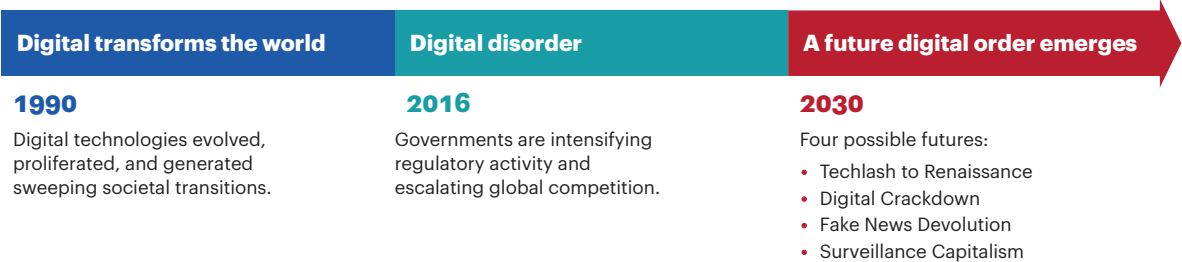
by rising action and confrontation. During the 1990s and 2000s, digital technologies evolved, proliferated, and generated sweeping societal transitions. The implications of digital for societies, economies, and political systems were, and continue to be, pervasive—in both positive and negative ways. Throughout this period, however, governments did not regulate digital in any meaningful way.

Beginning around 2016, the digital revolution entered its second phase, in which governments are taking steps on two fronts to address the growing social consequences of these technologies. First, they are designing regulations to maximize digital's upsides while mitigating its downsides. And second, they are pursuing national policies and channeling investments to take the lead in emerging digital technologies. As a result, a global [battle for technological supremacy](#) in the 21st-century digital economy is heating up, raising the risk of competing technological standards and creating the potential for an “islandized” digital environment. Altogether, these actions are creating a digital disorder that is becoming more difficult for companies to navigate.

These two forces of change will shape the future digital order, which will emerge around 2030. Its contours, however, remain an open question (see figure 1). There are various ways in which evolving digital policies and regulations and the national technological competition could play out during the digital disorder phase, creating multiple alternative futures for the global digital environment. Technology companies are already dealing with these shorter-term forces of change, but many companies in other industries have not yet taken notice. That must change. The uncertainties associated with digital disorder and its eventual resolution will affect not only technology companies, but all companies that rely on or use digital goods and services.

Figure 1
The world is in a period of digital disorder

Three stages in the digital revolution



Source: A.T. Kearney analysis

Digital Transforms the World

The effects of digital technologies have become pervasive across economies, societies, and political systems. Certainly, the effects on business have been no less important. From shopping for consumer goods to connecting with loved ones and from managing supply chains to personalizing customer relations, digital has changed the way the world works. Most often, these changes have had positive effects, including improved efficiency, reduced information asymmetry, and greater connectivity. But the downsides of the digital revolution have also become clear, including disinformation, [violations of privacy](#), and reduced competition.

Some result from digital technologies merely exacerbating or accelerating underlying human tendencies, while others are more novel phenomena associated with the digital age.

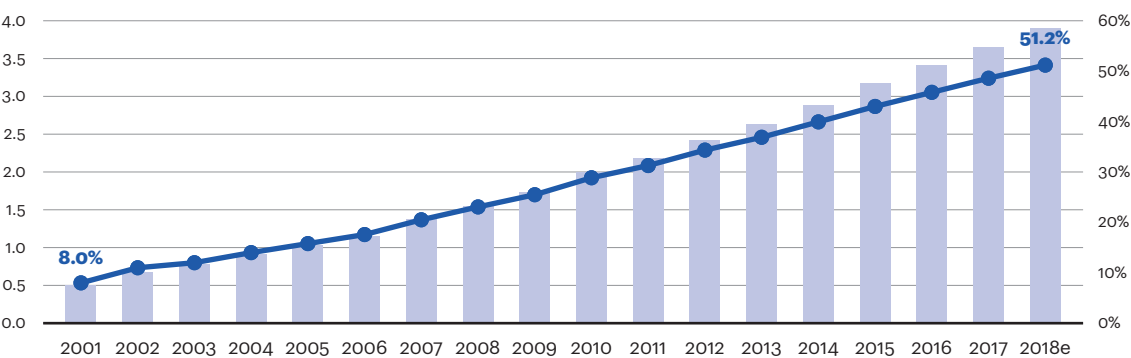
Redefining information dissemination

Global use of the Internet continues to grow dramatically. An estimated 3.9 billion people had [Internet access as of 2018](#), a nearly 400 percent increase since 2001 (see figure 2). This trend is likely to accelerate as emerging and frontier markets with comparatively low levels of Internet penetration move closer to the global average. As Internet access proliferates, so too does information dissemination—posing simultaneous opportunities and challenges for society.

Figure 2
Internet use has exploded over the past two decades

Internet users worldwide

Billions; percent of total population



Sources: International Telecommunications Union; A.T. Kearney analysis

On the positive side, greater access to the Internet has led to a proliferation of educational opportunities. For instance, enrollment in [massive open online courses](#) (MOOCs) more than doubled between 2015 and 2017, with more than 78 million people across the world taking these classes in 2017. This spread of information through digital courses has been complemented by vast troves of knowledge available on crowd-sourced knowledge repositories, such as Wikipedia. The increase in the availability of smart phones and Internet connectivity in emerging markets is also providing greater access to information needed to conduct business, participate in politics, and lead more productive lives. Mobile connectivity, for example, is being used to spread vital information about [healthcare](#), [crop pricing](#) for farmers, and e-governance functions such as [voter registration](#).

Yet digital technology proliferation has also enabled the accelerating dissemination of false or damaging information. The challenge of fake news stories is far from new, but modern digital technology has spread disinformation at an unprecedented scale and rate. Russian disinformation campaigns in both the 2016 Brexit referendum and US presidential election may be the most well-known, but other examples abound. In Sri Lanka and Myanmar, for instance, [stories targeting Muslim minority populations](#) have resulted in acts of vandalism and physical attacks. The outlook is even more troubling. Fake news attacks against businesses and political

leaders will likely grow even more sophisticated, fueled by advances in digital technology, such as [AI that produces fake news stories](#) and [DeepFake technology](#) that allows for the creation of cheap and convincing fake videos.

Remaking communication and networking

It is difficult to overstate the role that digital technology has played in connecting people globally. An estimated 3.2 billion people were [active social media users](#) in 2018, representing roughly 42 percent of the global population. Recent studies detail several [benefits from social media](#) to users, including providing alternative avenues for connection and support and adding to a sense of belonging. Communities with shared niche interests can instantly connect with one another. And online relationships have led to friendships and marriages. Social media also provides organizations with a direct line of communication to stakeholders. For instance, companies can leverage social media to reach clients, customers, employees, and partners. And social media is providing an unprecedented way for politicians to connect directly with their constituents.

While this style of [direct communication](#) may energize political supporters on both the left and the right, scholar Moisés Naím has theorized that these dynamics are [eroding traditional power centers](#) and institutions. He posits that while technology is making it easier to get power, it is also becoming harder to use it to control others and harder to keep power once it is obtained. The 2019 [Edelman Trust Barometer](#) provides evidence of such shifting power centers, finding that employers are now far more trusted than traditional government and media institutions in a wide cross-section of countries around the world.

Digital communications have also reshaped politics by creating new vectors for activities by malicious actors. According to the US [Department of Justice](#), the Russian government extensively leveraged digital communications and networking to interfere in the 2016 US presidential election through both “a social media campaign designed to provoke and amplify political and social discord in the United States” and “cyber intrusions (hacking) and releases of hacked materials.” Such methods were also employed in the [June 2016 Brexit vote](#), [2018 US midterm elections](#), and [2019 European Parliament elections](#) (subscription required). The use of digital tools for political subversion is therefore likely to continue for the foreseeable future.

Digital connectivity has also made it easier for extremist groups to gain followers and network with one another. Al-Shabaab, Boko Haram, and the Islamic State are all active on major social media platforms. Such groups use social networks not only to bring in new members, but also to share dangerous materials and machinations—such as bomb-building manuals and information on terrorism tactics—and to spread their ideologies and ideas. Similarly, alt-right groups have exploited the recommendation [algorithms on YouTube](#) to drive traffic to their videos—often linking to innocuous non-political videos that lure viewers into the extremist ecosystem.

Revolutionizing data generation and analysis

Data generation in the digital age is unprecedented. One estimate finds that [2.5 quintillion bytes of data are created every day](#) and anticipates that data production will be 44 times greater in 2020 than it was in 2009. This growth has led to the rise of big data, which refers to unprecedented data production and the increased ability to process it and rapidly generate actionable insights. When combined with predictive analytics—the use of data mining, statistics, and modelling to anticipate future outcomes—or AI, big data can improve business

operations in myriad ways. Retailers are using predictive analytics to optimize checkout wait times and improve store layout. Predictive maintenance solutions that anticipate when a machine may fail are being deployed in factories. And some manufacturers are using data monitoring to optimize the efficiency of their employees.

Massive volumes of digital data are also being used to drive new innovations. There is no understating the role that big data is playing in advancing AI (see AI section on page 19). And big data is also fueling other new and emerging technologies, including augmented reality (AR) and virtual reality (VR) systems. Moreover, there is a symbiotic relationship between big data and the IoT. The [proliferation of IoT devices](#)—projected to surpass 20 billion by 2020—has been driven by demand for big data, and big data in turn has been used to improve the abilities of IoT devices to gather, analyze, and transmit additional data as well as to communicate with other devices.

But the spread of data has also raised a host of concerns. After years of giving away personal data in exchange for convenience, many users are becoming more aware of the risks of widely sharing their information. One survey, for example, found that 78 percent of Europeans believe it is very important that [personal information](#) on their devices can only be accessed with their explicit permission. Furthermore, the ubiquity of such detailed personal data has fueled identity theft. In the United States alone, [identity fraud increased 8 percent in 2017](#), victimizing 16.7 million people and resulting in theft from consumers of \$16.8 billion. Massive data troves of all types have been targeted by cyberattacks. It is therefore no surprise that cybersecurity has consistently been the top operational challenge for global executives in our annual [Views from the C-Suite](#) survey.

Retooling finance

Digital technologies are also fundamentally disrupting finance. This is especially apparent in payment systems—the most notable of which are [mobile payment and digital wallet platforms](#). The market transaction value for this sector is expected to surge from \$4.3 trillion in 2018 to nearly \$14 trillion by 2022. Digital finance can be a boon for [financial inclusion](#), particularly in emerging economies and frontier markets. For instance, [Kenya's M-Pesa](#) is reported to have lifted 2 percent of Kenyan households out of poverty over the past decade while increasing the country's per capita consumption. But an estimated 2 billion people globally still lack [access to formal financial services](#), highlighting the opportunity to further leverage digital financial services. A recent A.T. Kearney study found that [increasing digital payments](#) by 10 percent annually could boost global economic output by up to \$1.5 trillion by 2021.

Digital technology has also enabled the rise of cryptocurrencies and a variety of other unregulated marketplaces on the so-called dark web. While proponents point to the [benefits of cryptocurrencies](#), these digital financial innovations also enable illicit financial activities such as fraud, drug trafficking, money laundering, and shell companies used as “electronic money mules.” In fact, a recent study by the European Parliament noted that the market value for misuse of digital currencies may exceed \$8 billion.

Big data is also having an effect on financial trading activities. In 2017, the [global algorithmic trading software market](#) stood at \$11.7 billion, but by 2026, it is expected to jump to more than \$26 billion. As financial markets evolve with more digital capabilities, industry executives will need to be mindful of potential risks, such as “[fat finger](#)” trading, errors in algorithmic and high-frequency trading, errant algorithms, amplification of systemic risks (such as the [2010 Flash Crash](#)), and other market distortions.

Reshaping commerce

Digital technologies are reshaping commerce on a global scale, influencing every step in the supply chain process. In planning, for instance, automated algorithms account for a range of highly specific factors—including weather, local events, and social media trends—to forecast demand for a specific good as well as potential future changes in demand. In manufacturing, machine sensors allow for greater efficiency gains and waste reduction, while new technologies, such as 3D printing, are enabling production closer to where customers are located. And in delivery, new freight matching services—effectively serving as Uber for commercial use—are proliferating. Advances in each of these parts of the supply chain provide great opportunities for efficiency gains and improved top-line growth.

The spread of digital platforms has contributed to the rising gig economy. In the United States, roughly **36 percent of the workforce is a part of the gig economy** in some capacity.

Digital technologies have also enabled the formation and rapid growth of new business models. One of the most impactful examples is e-commerce, which made up 10.2 percent of [total global retail sales](#) in 2017 and is projected to grow to as much as 17.5 percent in 2021. E-commerce platforms not only are convenient for consumers but also provide producers with better access to the marketplace. For instance, Chinese farmers are now able to sell their produce and other goods on e-commerce platforms, supporting growth in rural areas there. And globally, women entrepreneurs are benefitting from the convenience of online retail platforms to set up businesses. The user base of the craft retailer Etsy is 86 percent female, for example, and many use their Etsy storefronts as their sole source of income.

Concerns are rising, however, about whether the growing importance of network effects in the digital economy is tilting the playing field in favor of large companies. This debate is taking place across the digital landscape, from social media to search engines. The reach of the [Internet giants is pervasive](#), with many third-party services relying on codes or systems provided by the major players. Google and Facebook alone accounted for roughly 73 percent of US [online advertising sales](#) in 2017. And in 2018, Amazon alone accounted for more than 49 percent of [online retail spending](#) in the United States. Indeed, e-commerce is the biggest focus of the competition debate due to its outsized impact on both consumers and traditional retailers.

The spread of digital platforms has also contributed to the rising gig economy, with jobs characterized by short-term contracts or freelance work. In the United States, roughly 36 percent of the workforce is a part of the [gig economy](#) in some capacity—some 57 million workers. Some use gig work to supplement their incomes, while others rely on it almost exclusively. In many emerging and frontier markets, the gig economy provides a useful bridge between the formal and informal sectors. But [gig economy workers](#) rarely receive benefits, are often paid low wages, and lack the stability that traditional jobs provide.

Redistributing economic development

Greater [access to digital technologies](#) in emerging and frontier markets has accelerated economic development. For instance, sub-Saharan African farmers can access weather forecast tools, Latin America's unbanked population can access mobile banking applications, and Asian artisans can participate in the digital supply chain. Digital tools such as e-government have also helped to promote economic development by reducing red tape, increasing monitoring and evaluation capabilities, and shortening the delivery time for many services in both developed and emerging markets. One such innovation is [India's Aadhaar Program](#), whereby each resident's basic demographic and biometric data is stored digitally to reduce marginalization, facilitate more reliable public policies, determine whether government funds are allocated efficiently, and reduce the frequency of fraud and identity theft. Similar programs also exist in the [Philippines](#) to track poverty and in [Bangladesh](#) to monitor water quality.

The digital revolution has also fostered economic development globally by enabling the creation of new industries, including a global technology start-up industry in which the [volume of global venture capital deals](#) rose 58.6 percent between 2014 and 2018. US cities—particularly Silicon Valley, Boston, Los Angeles, and New York—continue to dominate the technology start-up industry from a global perspective, but [new start-up ecosystems](#) are emerging in cities around the world, including Bangalore, Beijing, Berlin, London, Shanghai, Stockholm, Tel Aviv, and Toronto.

A growing digital divide nonetheless exists. Compared with the Industrial Revolution, the digital revolution relies less on human labor and delivers the greatest gains to a smaller share of major players. As capital-producing sectors grow their efficiencies through digital technologies, firms continue to move away from labor-intensive jobs in favor of highly skilled, specialized roles. One study found that [labor's share of GDP has fallen](#) across a wide variety of developed and emerging markets—including the United States, France, Japan, China, India, and Mexico—since 1975. [Women are particularly vulnerable to the digital divide](#), as a recent IMF study found that women face a higher risk of losing their jobs to automation compared with their male counterparts.

Barriers to access and lack of adequate training exacerbate digital inequality. While 79 percent of Organization for Economic Cooperation and Development (OECD) members' citizens are [Internet users](#), these countrywide statistics hide profound intra-country variation. In the United States, for instance, nearly one-fifth of teenagers are unable to complete schoolwork because of [unreliable computer or Internet access](#)—a figure that is more acute for lower-income households. And in India and China, only 30 percent and 54 percent of citizens, respectively, are using the Internet.

The urban–rural divide is an important factor contributing to this inequality in Internet access, as broadband and mobile data coverage is a [significant challenge for rural communities](#). Many cities are also finding it difficult to keep up with their larger and more digitally oriented counterparts. For example, Hong Kong—once a hotbed of innovation—is falling in the [Global Innovation Index](#), and there is concern that it is being [left behind by the digital revolution](#). Of course, the concentration of industries in major cities is an age-old phenomenon. The winning metro areas have both the digital infrastructure and the talent pools that technology companies need to thrive, so the decision to locate operations in them is only natural. But in an increasingly digital-enabled world, this continuing concentration of talent, innovation, and economic activity risks leaving rural areas and smaller cities further and further behind. If [digital infrastructure is instead expanded](#) into smaller communities, there is an opportunity for digital technologies to reduce inequality rather than widen it.

Restructuring healthcare

A [revolution in digital healthcare](#) is under way thanks to VR and AR, advanced analytics, wearables and other IoT devices, AI, and remote connectivity for telemedicine. A surge in mobile device applications designed to support individuals suffering from both physical and mental illnesses offers consumers convenience, anonymity, low-cost access to information and education, knowledge-sharing, and around-the-clock support. The Australia-based [Black Dog Institute](#), for instance, is pioneering e-mental health in the country, focusing on the research, prevention, and treatment of various mood disorders. And the global fitness app market—which includes platforms designed to track nutrition, workouts, and weight loss and provide access to online studio classes—is [expected to grow at 23 percent compound annual growth rate](#) between 2016 and 2023.

In personalized medicine, “[digiceuticals](#)” (subscription required)—or digital therapeutics—are becoming popular vehicles for doctors to deliver diagnoses and treatment plans to patients through their smartphones. Digiceuticals companies are tackling important healthcare issues in several ways, including using digital communications platforms to connect physicians, patients—and even their employers—for more collaborative care. Other examples include the deployment of VR-based exposure psychotherapy to examine patient responses in immersive environments and the development of a sensor-equipped pill that allows clinicians to remotely monitor adherence to prescriptions.

But the digital revolution’s net effect on human health is open to debate. Some digital innovations may aggravate health issues, while still others—ironically—are created to treat problems perpetuated by digital dependency, such as anxiety and technology addiction. Researchers have identified a [correlation between excessive screen time and higher rates of obesity](#) in children, preteens, and adolescents. And for adults, there is more pressure than ever to be always “on”—connected to friends, family, the office, and the latest news cycle, which can lead to feeling overwhelmed. The overuse of digital technologies also [negatively impacts quality of sleep](#), creates difficulties in concentrating and learning, and is even correlated with lower levels of [empathy](#). In fact, addiction to digital technologies is prompting new medical classifications. In September 2018, the World Health Organization (WHO) added a new diagnosis to the International Classification of Diseases: [gaming disorder](#). Such forms of addiction have paved the way for digital detox experts and include services such as retreats and camps to disconnect. As [Netflix CEO Reed Hastings](#) puts it, the company’s greatest competitor is not its marketplace foes such as Amazon Video, HBO, or YouTube, but sleep itself.

Digital Disorder

The world now stands at a digital inflection point. As the wide-ranging impacts of this digital transformation are better understood, governments around the world are intensifying their efforts to govern and regulate digital activity. While much attention is focused on regulations relating to “[techlash](#)” (subscription required)—defined by Oxford Dictionaries as “a strong and widespread negative reaction to the growing power and influence of large technology companies, particularly those based in Silicon Valley”—many governments are in fact seeking to strike a judicious balance in policies that both maximize digital’s upsides and mitigate its downsides. These actions are motivated not only by the sweeping societal transformations that digital has brought, but also by governments’ desire to maintain international competitiveness in the 21st-century digital economy. While the global competitive landscape is intensifying across

a variety of digital technologies, two in particular stand out: 5G wireless networks and AI. The stakes could not be higher, as the winner of this escalating global competition will have an edge politically, economically, and even militarily for years to come. The overarching challenge to governments is significant. Policies that address the implications of digital technologies require leaders to understand the highly complex nature of these innovations and to craft appropriate policies on a timely basis. All too often, however, they are falling behind in their capacity to respond. In some cases, it is simply not clear whether governments can respond at all. The result of these emerging government actions both to manage and promote digital technologies is the creation of an increasingly uncertain environment in which companies must operate.

Around the world, **governments are beginning to introduce an array of rules relating to the digital economy** in an attempt to eliminate or reduce digital's downsides while maximizing its upsides.

Intensifying regulatory activity

First, governments are taking action by intensifying policy formulation and corresponding regulatory activity. Around the world, governments are beginning to introduce an array of rules relating to the digital economy in an attempt to eliminate or reduce digital's downsides while maximizing its upsides. Whether governments can strike such a balance will influence the ability of companies to use digital technologies effectively in the coming years. And debates are raging about how best to regulate digital, making it unclear how domestic and international regulatory environments will evolve. As a result, companies must navigate a complicated set of conflicting rules in key markets.

Maximizing the upsides of digital

The ongoing digital revolution is inspiring governments around the world to implement large-scale national policies to embrace new technologies and ensure their economies remain competitive in the 21st-century digital economy. One method to accomplish this is **industrial policy**—defined as government policies directed at affecting the economic structure of the economy. But both the speed and the scope of technological change add a layer of complexity to the already challenging task of developing and implementing industrial strategies that promote productivity and inclusive growth. A joint report from A.T. Kearney and the World Economic Forum offers an analysis of how well-positioned countries are to shape and benefit from the digital revolution's effect on the **changing nature of production**. The report identifies policy actions that are needed in each country to design effective modern industrial strategies. Four elements of these strategies are discussed below.

Regulatory framework. As with the traditional economy, the digital economy relies on transparent and effective government regulation of business activity. Factors such as corruption and political stability, for instance, affect economic activity in the digital age just as they did in the

industrial age. In fact, in recent years, governance and regulatory factors have topped the list of considerations that companies take into account when choosing markets for investment, according to our annual [FDI Confidence Index](#).

Another important consideration is a country's intellectual property (IP) rights framework, which enables inventors—either individuals or companies—to capture returns on their research and development (R&D) investments. IP rights are even more vital in the emerging digital economy because of the exponential gains in innovation. The World Intellectual Property Organization (WIPO) found that patent, trademark, and industrial design [IP filings hit an all-time high in 2017](#) following eight consecutive years of growth. Intangible assets, including data, algorithms, and technology, are becoming more important to business strategy and success in the digital economy. Therefore, countries that provide strong IP rights frameworks are likely to attract more innovation, investment, and economic activity than those that do not.

The regulatory environment for start-ups is also important for a digital innovation sector to thrive. Governments must make it easy to [start a business](#), obtain funding, and close a business if necessary. Also important is a culture of entrepreneurship, risk-taking, and willingness to fail. The Israeli government, for instance, has supported such a culture by offering decades-long programs to teach entrepreneurship in universities, fostering a domestic venture capital sector, and funding innovative companies. Tel Aviv is now host to the [largest number of start-ups per capita in the world](#). New Delhi is seeking to replicate this success through its [Startup India](#) initiative, which includes simplifying regulations for launching and folding a business, establishing research parks and incubators for start-ups, and providing advice and funding to entrepreneurs.

Infrastructure. Another crucial building block of the digital economy is the infrastructure to support connectivity among households, businesses, and government agencies. At its most basic level, this infrastructure includes a strong and reliable supply of electricity. More often, the focus is on the infrastructure that enables Internet connectivity, including fixed broadband and [high-speed mobile broadband](#), which now accounts for a much larger share of global Internet connections. In many emerging and frontier markets, therefore, the emphasis is on rolling out 3G or 4G mobile coverage. Developed markets are now turning to the rollout of 5G networks (see 5G section on page 18).

Some governments encourage competition between digital infrastructure providers to inspire innovation and drive down costs for customers. South Korea provides an instructive example of such an approach. Policymakers in Seoul provide [subsidies to Internet service providers \(ISPs\)](#) that serve the entire country and establish high minimum standards for connectivity in rural areas. As a result, various ISPs have nationwide networks and compete fiercely on both quality and cost. Other governments instead foster collaboration between private ISPs, which enables them to share infrastructure and investment burdens, improving efficiencies and ultimately reducing consumer prices. A [lack of competition](#) can backfire, though, as some critics argue has been the case in the European Union (EU). And still other governments pursue a more centralized digital infrastructure rollout through national champions or state-owned enterprises. The United Arab Emirates serves as one example of this model.

Some governments are also leveraging public funds to invest directly in digital infrastructure. The United Kingdom, for example, has identified more than £6.8 billion (\$8.8 billion) in both public and private [digital infrastructure investments](#) through 2021, with a specific focus on delivering high-speed fiber connectivity and 5G while reducing costs to consumers. Similarly, India announced a \$59 billion investment in infrastructure to promote a more connected economy in 2017—funds that are much needed as the country attempts to modernize its digital connectivity.

Human capital. Countries require an agile labor force that can adopt and find innovative uses for emerging technologies. But these new technologies are simultaneously reshaping the job landscape. Coordinated efforts to reskill and upskill the workforce will be required to ensure labor supply meets the demands of the emerging digital work environment. Importantly, the human capital needs of the future will not just be in technical skills. Creativity, problem identification, and flexibility will become even more highly valued as well.

One labor force strategy is to attract today's digital talent from abroad. China, through efforts such as its [Thousand Talents Plan](#), has attracted an estimated [7,000 foreign-trained Chinese scientists](#) and innovators back to the country with lucrative incentive programs, guaranteed research funding, housing and food subsidies, and relocation expenses. And Canada has begun to open its doors to [foreign technology talent](#), especially as US immigration policies have tightened in recent years. Canada's technology sector is reaping the benefits: [Toronto added far more new technology jobs](#) in 2017 than the San Francisco bay area.

Global R&D spending has steadily risen as a share of GDP since widespread use of the Internet began, growing from just 1.4 percent of global GDP in 1996 to almost 1.7 percent in 2017.

Another strategy is to focus on the educational system to build tomorrow's digital talent. Germany has emerged as a leader in 4IR technologies, driven in no small part by its emphasis on promoting advanced technical training programs through universities and apprenticeship programs. In December 2018, the United States released a national strategy to [promote science, technology, engineering, and mathematics \(STEM\) education](#). Similarly, Australia is prioritizing digital capabilities and funding STEM education initiatives as part of the country's \$1.1 billion [National Innovation and Science Agenda](#). And emerging and frontier markets are seeking to close the gap with developed markets. The Kenyan government, for instance, is focusing its [Digital Literacy Programme](#) efforts on primary schools to provide an early introduction to digital technologies.

Research and development. Investment in R&D has been a historic driver in promoting innovations in technology—and the ongoing digital revolution is no exception. It is not surprising then that global R&D spending reached a record \$1.6 trillion in 2016 (the latest year for which data is available). In fact, [global R&D spending](#) has steadily risen as a share of GDP since widespread use of the Internet began, growing from just 1.4 percent of global GDP in 1996 to almost 1.7 percent in 2017.

While the private sector provides the largest share of R&D expenditures, there continues to be a role for government as well. The OECD has found that government [funding of R&D](#) is the most common method of government support for the digital economy. Governments can fund R&D directly through public research centers or indirectly by providing grants and other funding to the private sector. The US government, for instance, played a leading role in developing semiconductors, global positioning system (GPS) technology, and the Internet through massive

R&D investments dating back to the 1950s and 1960s. After these technologies were developed, the government opened them up to private-sector use, sparking additional innovations and the creation of new business models. Other countries are now seeking to emulate this model to boost national competitiveness in the emerging digital order, particularly for technologies deemed to be crucial for future growth such as AI (see the AI section on page 19).

Minimizing the downsides of digital

At the start of the digital revolution, governments largely did not regulate digital in any meaningful way because of either a belief that regulations governing the analog economy would encompass the digital economy or a fear that regulations on emerging digital industries would stifle innovation. But with the sweeping societal implications of digital becoming clear, the world is now at an inflection point in terms of governments' willingness to regulate digital. This cycle of innovation, adoption, and then regulation is consistent with previous waves of technological change. For instance, it was almost two decades after the introduction of the automobile that the US government first established safety and other [regulatory standards for roadways](#), and it took many more decades for such regulations to be effective. Today, the intense regulatory debate regarding digital technologies is creating a high degree of uncertainty about how the digital policy environment will evolve.

Data localization. Cross-border digital data flows are on the rise, with [information and communications technology \(ICT\) services exports](#) more than doubling from just 5.2 percent of total services exports in 2000 to 10.6 percent in 2017. But data governance, the legal and regulatory framework between countries to manage these flows, has long proved divisive. While some countries have pressed for more open, globalized flows of information, other countries have erected [digital walls](#) as part of growing levels of [nationalism, protectionism, and parochialism](#). Such data localization policies either require companies to store or process data within a country's borders or restrict cross-border data flows. Cutting across both kinds of data localization is often a requirement that companies appoint [data protection officers](#) to ensure compliance with these and other data governance regulations.

Data localization regulations have proliferated in recent years, leading to concerns about a "[splinternet](#)" or the "[islandization](#)" of the global digital economy. Almost all G20 economies have some sort of data localization regulations in place. Russia has some of the widest-ranging, requiring the storage of citizens' personal data on Russian servers and establishing an official registry to punish operators that fail to comply with the law. Similarly, China not only requires many types of data to be stored domestically—including citizens' credit reports, telecommunications data, and any text, audio, or video published online—but also restricts digital imports using the so-called "Great Firewall of China." Australia has a more limited data localization regime that restricts healthcare providers from exporting personally identifiable information. And India is considering a [Data Protection Bill](#) that could require all companies to store Indians' personal data on servers within the country.

There are, however, some countervailing efforts to establish and retain open cross-border data flows. The most notable of these is the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which contains commitments to [preserve cross-border data flows](#) and limit digital protectionism among its 11 members. Several CPTPP members, including Australia, Japan, and Singapore, are at the forefront of a newly revived effort within the World Trade Organization (WTO)—after many years without any progress—to negotiate [rules governing e-commerce](#) and the cross-border flow of data. More than 70 countries are involved in these talks, but reaching agreement will become more difficult as governments continue

to implement domestic data localization requirements. The result, at least for now, is an ever-more complicated data governance regulatory environment for companies to navigate.

Data privacy. High-profile data breaches, hacks, and identity theft have brought popular awareness of data privacy to unprecedented levels. Governments are now taking steps to respond, with the European Union's General Data Protection Regulation (GDPR) leading the charge, shifting the data collection paradigm from a passive opt-out to an active opt-in approach. In addition to requiring user consent in data collection, the law includes data privacy protections, mandatory data breach notifications, and conditions for the safe handling of cross-border data transfers.

Several other countries are following suit with their own data protection efforts. Some are being incentivized to harmonize their regulations with the GDPR to secure trade agreements with the EU. The EU–Canada Comprehensive Economic and Trade Agreement (CETA), for example, includes specific chapters on protecting personal information and cross-border data flows. And as part of the EU–Japan Economic Partnership Agreement, both partners agreed to recognize each other's data protection systems. More broadly, Brazil announced plans in August 2018 to create a new National Data Protection Authority, following passage of its [General Data Privacy Law](#). Similarly, Australia's [mandatory data breach notification law](#) entered into force in February 2019.

Europe is playing a leading role in pressuring Internet companies to oversee the content on their platforms and remove objectionable material, releasing a set of guidelines for online platforms.

Steps are also being taken to enhance data protection in the world's two largest economies. China's [national standard on personal information protection](#) went into effect in May 2018, and further regulations may follow in response to growing [data privacy concerns](#) (subscription required) from Chinese citizens. In the United States, California's June 2018 privacy law requires technology companies to stop collecting and selling consumers' personal data upon their request. And at the national level, the BROWSER Act—which would establish mandatory opt-in provisions similar to the GDPR—remains under consideration. Congress is also considering an alternative approach in which platforms would be required to provide users with estimates of the overall [value of their personal data](#) to the service provider. And there is growing debate about the potential role of a government regulator in ensuring that consumers are appropriately [compensated for the use of their data](#) (subscription required).

Responsibility for platform content. Efforts to regulate platform content—specifically targeting fake news stories and hate speech—are now under way in several countries. Europe is playing a leading role in pressuring Internet companies to oversee the content on their platforms and remove objectionable material, releasing a set of [guidelines and principles for online platforms](#) in September 2017. Germany's NetzDG law, which went into effect in January 2018, goes a step further by requiring social media platforms with a large presence in Germany

to remove “obviously illegal” hate speech within 24 hours of notification—or risk fines of up to €50 million (\$56 million).

Several other countries have introduced anti-fake news legislation that either require platforms to take down offending materials or punish users posting false information. These include Malaysia, Singapore, Kenya, Vietnam, Tanzania, and France. There are efforts to coordinate the regulation of platform content internationally as well. In November 2018, legislators from several countries discussed the need for [international rules governing Facebook](#) (subscription required) and other Internet platforms in response to recent revelations of disinformation and data leaks on the platform. While the standards and requirements of these laws vary, they illustrate that regulatory requirements are likely to grow for Internet platforms in the years ahead.

The United States, in contrast, has long been reticent to police web platforms aggressively for user-generated content on free speech grounds. This position appears to be changing, however, as regulatory scrutiny of the [US Internet giants](#) is growing to a fever pitch. The Telecommunications Act of 1996 exempted websites from legal liability for user-posted materials, but the [Stop Enabling Sex Traffickers Act](#) (SESTA), which became law in April 2018, rewrote parts of the law to make it easier to prosecute sex trafficking websites for their content. Other legislation focused on improving the transparency of online political advertisements by extending existing political advertising laws to digital platforms is in process, while a comprehensive set of policy proposals for the [regulation of social media](#) and technology firms has also been proposed.

Illicit financing. The regulation of digital finance related to illicit financing, specifically anti-money laundering and counter-terrorism financing (AML/CFT), is still in its infancy but is gaining momentum. The IMF, for instance, has issued its position on [virtual currencies](#) as well as [fintech and financial services](#), but it acknowledges that a regulatory framework is still needed. The [Financial Action Task Force](#) (FATF), an intergovernmental policymaking body, amended its recommendations in late 2018 to include language on [virtual assets](#), which are not regulated uniformly on a global basis. The FATF also plans to issue its first set of rules and guidelines for cryptocurrencies by mid-2019 that could include know your customer (KYC) requirements and more uniform fraud prevention rules.

Fragmentation in AML/CFT regulations across countries, regions, and international organizations will likely persist, but some implementation of new guidelines and policies is on the horizon. The EU published its fifth [Anti-Money Laundering Directive](#) (AMLD 5) in 2018, which extends the scope to virtual currency platforms and digital wallet providers, enhances due diligence measures for financial flows from high-risk third countries, ends the anonymity of bank and savings accounts, and lowers the threshold for identifying purchasers of prepaid cards and other e-money. The US [Financial Crimes Enforcement Network](#) (FinCEN)—which has been regulating [virtual currencies](#) and [payment systems](#) since 2011 and 2014, respectively—is working with other federal government regulators to develop coordinated policy and regulatory approaches. And in countries that are eager to cement their place as global leaders in cryptocurrency deployment—such as Japan, South Korea, and Singapore—governments are taking action to ensure these sectors develop in a transparent way.

Worker rights and the social safety net. Worker rights and the social safety net, particularly for the gig economy, are evolving to the digital age. Europe is once again leading the way in the development and enforcement of labor rights in the digital economy. A Spanish court, for instance, recently found that a [Deliveroo bike delivery man](#) had de facto employee status and that his termination from the position was unlawful. The EU is also working to institutionalize social protections. Principle 12 of the new [European Pillar of Social Rights](#) declares “regardless

of the type and duration of their employment relationship, workers, and, under comparable conditions, the self-employed, have the right to adequate social protection.” And across the OECD, where on average 16 percent of workers are self-employed, some member countries—including Austria, Canada, Spain, and Sweden—also offer [voluntary protection schemes](#) to non-standard workers.

Policymakers face challenging questions about how to regulate the gig economy in markets in which the social safety net is more closely tied to employers. This is perhaps nowhere more salient than in the United States. Because gig economy workers are contractors rather than employees, certain [labor and discrimination laws](#), taxes and benefits payments, and other forms of compensation do not apply to them. In the absence of national regulations on these matters, local and state officials are stepping in. The New York City Council passed the [country’s first minimum pay rate](#) for Uber and Lyft drivers, for instance. And a [ruling by the California Supreme Court](#) in April 2018 could eventually force many California-based technology firms such as Uber to abide by minimum wage and overtime laws and pay unemployment insurance and payroll taxes.

Policymakers face questions about how to regulate the gig economy in markets in which the social safety net is closely tied to employers. This is perhaps nowhere more salient than in the US.

Taxation. The international taxation system, which is governed by the principle that a company’s physical presence in a country determines whether it is subject to taxation there, has not adapted to the rise of digital business models. Many governments have concluded that reforms are needed to align the location of taxable (digital) profits with the location where economic activities and value creation take place.

There are three primary methods of digital taxation. The first is expanding traditional withholding taxes to include digital intermediation or platform services when the company paying for the service is located in the country. South Korea serves as one example of such a tax regime, with a 10 percent value added tax (VAT) on the sales of digital services provided by foreign companies or individuals. Malaysia and Singapore are also in the process of [expanding their services taxes](#) to cover digital services. Another common method is to target the revenues from digital advertising. For instance, since 2014, Hungary has imposed a 7.5 percent tax on revenue from digital advertisements that are written or spoken in Hungarian. And as part of its Goods and Services Tax (GST) reform in 2016, India imposed a 6 percent tax on digital advertising sales. Finally, some governments are taking a wider approach to align the location of taxable profits with the location in which economic activities and value creation take place. The first significant mover in this regard was Israel, which established a “[significant digital presence](#)” test in 2016 based on web traffic within Israel, Internet platforms for Israeli customers, and other factors.

These taxes are complicating the environment for both digital companies and those that purchase digital goods and services. Almost 100 countries are therefore participating in the

effort led by the OECD to analyze the international tax challenges posed by the digital revolution. The group made a significant breakthrough in January, with several key countries coalescing behind a proposal to dramatically shift the international tax system to one based on taxing companies where they sell rather than where their assets are located. The OECD aims to present a final report with policy recommendations by 2020, which could pave the way for a more standardized global approach to [corporate taxation in the digitalized economy](#).

Antitrust. Despite the dominance of the new digital technology players, antitrust actions against them have been limited. Nowhere is this clearer than in the United States. Since the Supreme Court's 1979 ruling that the Sherman Antitrust Act of 1890 was actually designed to [protect consumer welfare](#), low prices for consumers have been prioritized above competition concerns—making it hard to argue that e-commerce giants, which generally have low prices, are violating antitrust rules. But US antitrust orthodoxy may be changing. In his January confirmation hearings to become attorney general of the United States, William Barr promised to make antitrust enforcement a priority, specifically citing concerns about the ways “[network effects](#)” were empowering the technology giants in Silicon Valley. The US Congress is also starting to explore policies that could [encourage greater technology competition](#).

While US lawmakers are still contemplating the proper approach to antitrust, the EU has taken a harder line against the giants of Silicon Valley. The European Commission (EC) has collected \$3.4 billion in fines from Microsoft in a series of antitrust cases dating back more than a decade. These cases focused primarily on Microsoft's reduction of consumer choice by bundling the company's own Internet browser and media player software within its Windows operating system. And since 2013, the EC has opened various antitrust probes to investigate Google, Amazon, Apple, and Facebook. In July 2018, for instance, Google was hit with a record \$5 billion fine for using its Android platform to drive users to its own search engine and Internet browser. And the EC launched an [antitrust probe into Amazon](#) in September 2018 over the use of merchant data on the site.

A global wave of increased antitrust scrutiny for digital technology companies is rising. In February 2018, Mexico's Federal Commission for Economic Competition announced investigations into “probable” [monopoly practices](#) by large players in the country's e-commerce market. In India, new regulations went into effect in February 2019 that require Amazon and Walmart to [stop selling merchandise in which they have an equity stake](#)—an effort aimed at bolstering local businesses. And the [Japan Fair Trade Commission](#) (JFTC) has announced plans to probe Internet giants, such as Google and Amazon, to determine if they are “preventing innovations by Japanese companies.”

Escalating global competition

Governments are also taking action by engaging in an escalating global competition to maintain and improve national competitiveness in the 21st-century digital economy. While the competitive landscape is intensifying across a variety of digital technologies, two in particular stand out: 5G wireless networks and AI. The United States and China have emerged as the two leading players in terms of the current level of domestic digital technologies and investments for the future. While such cross-border competition is by no means new, the geopolitical undertones in this battle for dominance raise the risk that the digital economy will continue to fragment, [complicating global supply chains](#) (subscription required) and the operations of international companies, and acting as a drag on economic growth.

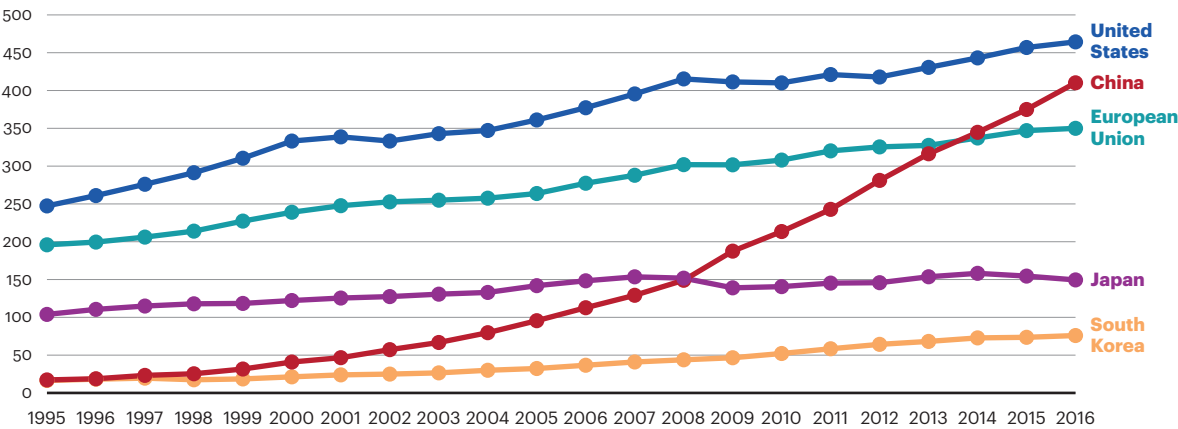
Battle for technological supremacy

The battle for technological supremacy has intensified in recent years, with China seeking to challenge the long-held dominance of the United States in this area. At the 19th Communist Party Congress in October 2017, President Xi Jinping called for China to become a “science and technology superpower ... advancing the development of big data, cloud computing, and smart cities so as to turn them into a [digital silk road](#) for the 21st century.” Specific efforts include Made in China 2025, the Next Generation AI Development Plan, and China’s 13th Five-Year Plan for Informatization (2016–2020), which prioritizes 5G mobile broadband and [quantum computing](#). Beijing is also ramping up scientific investments. Between 2000 and 2015, [Chinese spending on scientific research](#) increased by an average of 18 percent per year, compared with only 4 percent in the United States. Based on recent trajectories, China could soon surpass the United States to become the world’s largest R&D spender (see figure 3).

Figure 3
China is quickly rising among the ranks of the world’s top R&D spenders

R&D spending

\$ billion



Note: European Union data reflects all 28 member countries, including the United Kingdom.

Sources: Organisation for Economic Co-operation and Development; A.T. Kearney analysis

While China has prioritized state leadership with private-sector support, the United States is pursuing a more free-market approach to the escalating global competition in digital technologies. This approach marks a notable shift from the US government’s historic leadership role in driving new technological innovations. In recent years, however, the United States has relied more on its world-leading research universities, private-sector titans, and strong start-up culture to drive advances.

In particular, the United States has leaned heavily on the strength of its private-sector giants to win the battle for technology supremacy: Facebook, Apple, Amazon, Netflix, and Alphabet-owned Google, collectively known as the FAANGs. The FAANGs and Washington are increasingly clashing, though, as evidenced by recent [congressional hearings about Facebook](#) over privacy concerns, fake news, and consumer protections. And Chinese technology companies have rapidly emerged as formidable global competitors. Baidu, Alibaba, and Tencent—collectively known as the BATs—are just as dominant (if not more so) in their

home market as the FAANGs are in the United States. They are also tied closely to Beijing, as each of the BATs has a joint R&D lab with government entities as well as the required in-house committee of Communist Party of China members to ensure alignment with the state.

The EU is working to catch up to the United States and China in digital technology innovation and adoption. Notably, EU standards on data privacy, antitrust, and other significant regulatory questions differ in approach from both of the global technological leaders. Having indigenous technology companies that adhere to specific EU standards is thus becoming more important. The vision of a Digital Single Market is a key part of the EU's strategy to foster digital commerce within the bloc. The EC has projected that a [Digital Single Market](#) can create up to €415 billion (\$469 billion) in growth as a result of the efficiency gains of EU members coordinating on the standards for 5G network adoption, cloud computing, and other digital technologies that facilitate cross-border commerce, creating much larger consumer markets. In conjunction, the EC argues that improving the [digital skills of EU citizens](#) will be essential to the success of the society in the future, citing that an estimated 47 percent of the EU population does not yet have the requisite level of digital skills.

Another contender is Japan, which has long been a leader in technological innovation and is [leveraging automation and robotics](#) to enable greater levels of output with fewer workers amid a declining working-age population. But in terms of the digital revolution, Japan lags its competitors in important ways. For instance, [funding for Japanese start-ups](#) is only about \$1.3 billion annually, compared with \$20 billion in China and \$70 billion in the United States. The government is seeking to address such gaps through programs such as the [J-Startup program](#) that aims to establish 20 start-ups valued at more than \$1 billion by 2023. But a broadly [risk-averse regulatory environment](#) remains an obstacle to the growth of the Japanese digital economy, including digital payments and the [sharing economy](#).

South Korea is another significant player in the escalating global competition for digital technologies. It has some of the highest Internet penetration rates in the world and is expected to be a leader in deploying 5G wireless networks. In fact, several carriers coordinated the launch of live [5G service for commercial users](#) in major cities in December 2018—the first such launch globally. The country has also consistently ranked first on the [Bloomberg Innovation Index](#) in recent years. However, the OECD points out that Korean companies are not [incorporating digital technologies](#) such as cloud computing and big data into their operations at the same rate as companies in the other leading digital economies—thereby forgoing potential efficiency and competitiveness gains.

Of the [five largest economies in the world](#), India is the only one not to appear among the digital revolution leaders. As a first step to entering the digital technology race, the country is striving to catch up on digital access. The government's [Digital India](#) initiative seeks universal digital literacy and universal access to digital resources, which will require a drastic reduction in the existing rural–urban and age disparities in Internet access.

5G wireless networks

One of the central technologies in the escalating global competition is 5G wireless networks. 5G is being designed to facilitate instant, reliable connections between billions of devices dramatically faster than is possible today. Greater bandwidth will allow it to support massive machine-to-machine (M2M) communications, such as between cellphones, sensors, smart machinery and appliances, and other IoT devices. 5G will also enable a range of new and future applications in the other next-generation 4IR technologies, many of which will be the backbone of innovations in [manufacturing and production processes](#). The large-scale deployment of 5G

wireless networks will therefore be one of the most intense—and consequential—technological races of our time. [National competitiveness](#) will increasingly be determined by the level of 4IR technological adoption and innovation, which in turn will depend on the depth and breadth of national 5G wireless networks.

But 5G deployment is not without its challenges. As urban areas prepare to install 5G infrastructure, its uneven deployment is likely to become a limiting factor for the expansion of 5G-dependent technologies. For example, a fully autonomous vehicle that relies on 5G connectivity may be constrained to major cities if smaller cities and rural areas lack the necessary coverage. More broadly, disparities in 5G access could exacerbate regional inequities in digital connectivity that already exist. In the near term, therefore, the companies and individuals who benefit from the transformative elements of 4IR may remain limited to urban areas with end-to-end 5G connectivity.

One of the greatest challenges to a hyper-connected 5G future is [cybersecurity](#). According to a 2018 study conducted by Ericsson, 79 percent of business leaders across 10 industries perceive [data security and privacy as the top concern for 5G adoption](#). Such cybersecurity concerns are a matter of national security, as evidenced by some countries [blocking Chinese telecommunications giant Huawei](#) from participating in their 5G infrastructure development. And as 5G enables the explosion of IoT, so too will it provide greater opportunities for exploitation of these devices by malicious actors.

South Korea, the United States, and China appear to be the leaders in the [race to 5G](#). Meanwhile, the EU is falling behind on 5G, which the chief executive of Ericsson recently attributed to [EU regulations and high costs](#) (subscription required). Indeed, European Parliamentarian [Gunnar Hökmark](#) has warned, “Europe needs a fully developed infrastructure by the start of 2020, not a day later, in order to be able to compete for global investments. The consequences of not being up there ... will be a continuous drain of the world’s leading tech companies from Europe.”

Artificial intelligence (AI)

AI is the other primary technology on which companies are competing globally.¹ Although we are just at the start of a [long AI journey](#), 71 percent of global executives in our 2018 [Views from the C-Suite](#) survey expected that AI would have transformative effects for economic growth and competitiveness in the short term. From digital assistants and self-driving cars to [job candidate selection](#) and personalized medicine, AI-driven technologies are now more available than ever before. Data security is one of the most common business use cases, with cybersecurity companies leveraging AI to detect malware and search for anomalies in how data is processed in the cloud. AI and [deep learning](#) techniques are similarly being deployed by companies such as PayPal to identify instances of fraud and money laundering. In the healthcare industry, the technology is being deployed in [AI-assisted robotic surgery](#) and [virtual nursing assistants](#). And perhaps most commonly, AI is being extensively leveraged by retailers and entertainment providers to customize shopping, music, and movie recommendations. One recent study found that [AI-generated business value](#) reached an estimated \$1.2 trillion in 2018—a number that could reach \$4 trillion by 2022.

These advances also come with concerns. As AI becomes more capable of performing both blue- and white-collar jobs, worker displacement seems inevitable. Venture capitalist and [AI expert Kai-Fu Lee](#) recently argued that AI could displace as many as 40 percent of the world’s jobs in the next 15 years. Regardless of the precise time frame and scope of job losses, AI will

¹ There is no single definition for AI, but it is broadly understood as the capability of a machine to imitate intelligent human behavior. Machine learning, a key component of AI, is a group of techniques for machines to learn and perform cognitive functions, including, for example, algorithms that enable supervised and unsupervised learning.

certainly have a transformative effect on the global workforce. Governments, companies, and educational institutions will need to develop strategies to provide workers with the AI skills necessary to compete in the new environment.

AI also presents new ethical questions. Concerns about [bias and discrimination](#) in AI algorithms, particularly when the coders are [overwhelmingly men](#), are growing as such algorithms increasingly make real-world decisions, such as which candidates a company should hire and how much “[social credit](#)” citizens have. There are also growing worries that the ascendance of AI will result in even greater levels of [income inequality](#) as owners of AI-enabled companies are able to reduce their human workforce and keep more revenue for themselves. Security concerns also exist; the use of AI for autonomous weapons or in sophisticated cyberattacks serves as a prime example.

Despite these concerns, AI is generally acknowledged to be one of the major forces for national competitiveness in the coming decades. The [United States is the leader](#) in three of the four main drivers of AI, according to the University of Oxford: hardware, research and algorithms, and the commercial AI sector. But on the final driver, data, China is far ahead of the pack. The country’s large population and data-sharing agreements between leading Chinese technology companies and the government have enabled significant real-world AI testing. But the race is by no means won yet. Although the prevailing narrative is that China is laser-focused on dethroning US technology companies, the nascent AI market is not so binary. Many governments, including all five of the world’s largest economies, have released national—or in the case of the EU, supranational—AI strategies in recent years.

Each AI strategy is unique, but there are four common themes: investment in R&D, efforts to upgrade skills and workforce training, greater private-sector innovation, and evaluation of AI’s ethical implications. The US strategy put forward by the Obama administration, for example, establishes a framework for tracking federal R&D and identifies strategic priorities. More recently, President Trump signed an [executive order](#) calling for federal agencies to prioritize AI investments and ask for additional funding if needed as well as encouraging private institutions to invest in AI. China’s strategy is more detailed, with a sector-by-sector plan to spread AI widely across the economy. Various cities throughout China have their own AI agendas as well, with [Shanghai](#) and [Tianjin](#) each committed to spending about \$15 billion. The EU has also committed to boosting annual AI funding, although only to about \$1.7 billion through 2020.

A Future Digital Order Emerges

Governments intensifying regulatory activity of the digital economy while simultaneously engaging in an escalating global competition for digital dominance is creating a period of digital disorder. And the digital environment that will emerge once this disorderly adjustment is complete remains profoundly uncertain. To bound the uncertainty associated with envisioning the future operating environment for digital technologies, we have developed four scenarios, or alternative visions of the future. This scenario analysis is based on the two primary political uncertainties that are unfolding during the second act of the digital revolution:

- **Regulatory activity.** The extent to which governments in key markets around the world impose new regulations on technology companies and the use of digital technologies more broadly
- **Digital environment.** The extent to which the digital economy is a globalized whole, characterized by extensive cross-border digital flows, or an islandized environment, fragmented into different country-level or regional blocs

We envision these two measures as intersecting axes that allow us to identify four distinct futures for the digital operating environment in 2030 (see figure 4). In fact, some aspects of these scenarios are already playing out in various markets around the world. But the scenarios that follow here are not predictions. Rather, they are designed to be compelling and plausible visions of the future that challenge and test executives' capacity to anticipate and plan for their companies' digital strategies in the coming years.

Figure 4
Today's digital disorder could evolve in four ways

Scenarios for the future digital order



Source: A.T. Kearney analysis

Scenario 1: Techlash to Renaissance

Dramatic regulatory activity; globalized digital environment

In **Techlash to Renaissance**, the world is defined by a commonly accepted cross-border digital operating environment with strong and effective regulations. After a period of turbulence and uncertainty in the early 2020s, driven by backlash against leading technology giants, governments and the technology sector have reached a stable entente in which national policies and regulations impose commonly accepted norms and restraints on the use of digital technologies. Increased global cooperation in establishing best practices and standards for technology governance has also led to a more unified digital landscape. Global economic growth is steady, supported by new innovations, geopolitical stability, and high levels of consumer confidence.

In the early 2020s, public disapproval and distrust of the technology giants in both the United States and China continued to rise. A steady drumbeat of revelations about these companies' privacy violations, combined with successive data breaches, resulted in a growing backlash. Governments around the world responded with new digital regulations aimed at protecting citizens and combating disinformation. New data-privacy regulations, often modeled after the EU's General Data Protection Regulations, were enacted around the world. These regulations not only gave citizens the rights to their personal data, but also ensured that they would be compensated appropriately if they granted companies permission to use it. Many governments also created centralized digital data regulatory bodies to provide oversight and ensure that platforms are adhering to these new privacy and data use standards. Governments cracked down on fake news and other disinformation on digital platforms, and with less false and incendiary material flooding the Internet, public trust in both technology companies and governments recovered from lower levels a decade earlier.

In response to concerns about worker displacement by digital technologies, the United States and the EU members were the first among several countries to enact policy initiatives for worker retraining and strengthening the social safety net. As digital literacy and workforce capabilities improved, overall levels of domestic inequality in member countries began to decline.

In Techlash to Renaissance, a new generation of leadership emerged around the world as Millennials rose to political power and brought a desire for relaxed cross-border tensions.

Governments also moved forward with aggressive antitrust measures directed against the largest technology platforms. Beijing responded to concerns from citizens and government leaders that Baidu, Tencent, and Alibaba were becoming too powerful by splitting these companies into smaller components while also ramping up state oversight. And in the United States, years of successive federal court cases against Facebook, Google, Amazon, and the other technology giants set a new antitrust precedent that competition should be protected—in addition to consumer welfare. As a result, the Silicon Valley technology giants were forced to break up into smaller companies focused on a more limited set of digital services. Much as Google emerged in the aftermath of legal actions against Microsoft's dominance in the 1990s, the breakup of the technology giants during the 2020s led to the emergence of a variety of new digital players, increasing both competition and consumer choice.

One important driver of these changes was a new generation of leadership emerging around the world as Millennials rose to positions of political power. This generational cohort also brought with it a strong desire for a relaxation of cross-border tensions. US–China relations improved significantly following rigorous diplomacy as both sides saw opportunities for greater growth and innovation in a more cooperative operating environment. This paved the way for both of the world's largest economies to support the Japan-led multinational effort to define new rules for cross-border data flows and e-commerce. Data localization requirements in key markets,

including China and India, are relaxed in this more globalized digital environment. In general, the digital regulatory landscape is more harmonized across borders as states increasingly collaborate on best practices. The OECD also spearheaded the creation of a new agreement on digital taxes that target digital profits where they are generated—rather than where a company's assets are located. This move helped to further level the playing field for a variety of digital services providers and offered greater support for open cross-border digital flows.

Business implications: In **Techlash to Renaissance**, technology and non-technology companies alike thrive after a period of adjustment to the new regulatory landscape. Cross-border trade in digital goods and services has increased, creating opportunities for expansion into new markets. Competition flourishes as new entrants emerge following the breakup of the technology giants. This development ultimately benefits consumers as companies race to innovate, provide new services, and reduce costs. Business strategies focus on international growth, taking steps to ensure regulatory compliance across markets. While the regulatory changes raise short-term challenges and can require incremental course corrections, the overall harmonization of key standards across borders helps to keep these costs in check. Moreover, the favorable economic environment, combined with greater equity in wealth distribution, widens the consumer base for companies around the world.

Scenario 2: Digital Crackdown

Dramatic regulatory activity; islandized digital environment

In **Digital Crackdown**, high levels of nationalism and strict government control of digital platforms—and many other aspects of society and business—dominate the operating environment. The global economy is sputtering, and state capitalism and mercantilism are on the rise, with governments supporting national champions that serve an outsized role in providing domestic digital services and infrastructure. Governments around the world mandate that digital platforms share user data with the government, which they use to monitor citizens as well as oversee and shape platform content. Given the dominance of national champions in the digital space, the global digital operating environment is fractured. Nationalism fuels distrust of foreign goods and services, and governments construct digital walls through stringent domestic standards and localization requirements.

The continued rise of nationalism around the world throughout the 2020s was fueled by a sagging global economy, a seemingly endless string of data hacks and cyber breaches, and an uptick in small-scale terrorist attacks inspired by fringe groups that were mobilized online. Governments pinned the blame for this growing instability and human suffering squarely on immigrants, minorities, and—most of all—other countries. Isolationism asserted itself in ways unprecedented in the modern era, as international trade declined precipitously, and the cross-border exchange of people and ideas slowed to a crawl.

There was a steady rise in state capitalism, in which national capitals played a far more active role in selecting winners and losers in their domestic markets. Governments around the world increasingly followed Beijing's example in staffing the advisory boards of leading domestic technology companies with state officials. State-owned enterprises and national champions selected by governments then built digital infrastructure and provided all vital digital services. These programs have also served a darker purpose. More governments have leveraged the powers of their selected "digital champions" to exert greater levels of control over the lives of their citizens and maintain power over political opponents. Regulatory oversight of social media content has been used to crack down on expression of dissent, even in ostensibly democratic

states. Governments have also deployed AI-enabled facial recognition to monitor the movement and behavior of citizens in the physical world.

Rather than fostering international coordination to develop digital technologies and services, each country regarded the digital economy as a means to protect national security and sociopolitical stability. Digital barriers were erected, resulting in a “splinternet” in which citizens of different countries receive very different—and often government-mandated—digital news and perspectives about global developments. Governments imposed a variety of new digital regulations to achieve their digital isolation, including high value-added taxes on the sales of digital services provided by foreign companies and restrictive data localization requirements. Digital technology companies therefore found it advantageous to foster close relationships with home governments as foreign markets became more hostile to them. This regulatory environment caused the level of overseas investment to plummet, both in the technology sector and more broadly as companies across sectors were forced to rely upon the digital services provided by domestic technology firms.

In Digital Crackdown, digital barriers resulted in a “splinternet” in which **citizens of different countries receive very different digital news.**

Technological advances slowed globally as a result of the decrease in the cross-border exchange of ideas and the lack of competition within domestic economies. The state-owned or state-sponsored digital giants have been content to enjoy their monopolistic market positions, which reduced the drive to innovate. China achieved parity with the United States in many digital technologies by the mid-2020s and even pulled ahead in AI through massive infusions of state investment and successful domestic strategies to bring back foreign-trained Chinese talent. While these gains were slowed by government inefficiencies, the sheer volume of state investment drove China forward. In the United States and elsewhere, the more restrictive regulatory environment prevented dramatic innovations in these new technologies. This slower pace has a double edge, as the extent of worker displacement was much lower than initial estimates. Overall economic growth, however, was also slower as a result.

Business implications: In **Digital Crackdown**, nationalism reshapes the way business is done, for technology and non-technology companies alike. Companies are caught in the crosshairs. The digital regulatory landscape is siloed, with an array of differentiated country-specific requirements to which companies must adhere. While some multinational players aggressively move to meet these standards, many ultimately abandon international business models when digital regulations prove too arduous, instead focusing on their domestic markets. The disruption to once globally integrated supply chains dampens growth in countries around the world. The greater influence of government officials in corporate leadership creates further bureaucratic hurdles for companies, curbing their capacity for innovation, creative solutions, and agile decision-making. Consumer markets have fragmented in this more polarized atmosphere as well, with strong preferences for domestically produced goods and services.

Scenario 3: Fake News Devolution

Minimal regulatory activity; islandized digital environment

A fractured digital environment and weak regulation characterize **Fake News Devolution**. It is the digital Wild West. Fake news stories flood the Internet and sow division, resulting in rapidly fading popular trust in governments, businesses, and other traditional institutions—particularly foreign ones. Consumers around the world therefore shun foreign technologies and companies, essentially imposing islandization on the digital environment. This trend imposes limits on the size and reach of digital platform companies, as they are forced by consumers to stick primarily to their home markets. The global economy is stuck in a low-growth environment as cross-border investment dries up and rising levels of economic inequality stifle consumer spending.

Tensions grew on the world stage throughout the 2020s as digital technology poisoned the political atmosphere. Meanwhile, nationalist sentiments within countries continued to grow from their already high levels in the 2010s. This nationalism led to a variety of conspiracy theories about the motives of foreign countries and companies proliferating widely on social media networks and other digital platforms. Domestic digital service providers often helped to spread the false stories regarding the malintent of foreign competitors because they solidified consumer preferences for domestic technology companies. Consumers around the world therefore shunned foreign technology companies, creating an increasingly “islandized” digital landscape.

Fake news also ran rampant throughout domestic political environments. Elections in many large democracies were marred by a continuous and increasingly sophisticated barrage of misleading information and fake news on social media platforms that neither governments nor content providers could manage. This trend was exacerbated by the proliferation of convincing DeepFake videos and audio recordings that blurred the lines between reality and fantasy. As citizens were inundated with a dizzying amount of information and online vitriol, many simply checked out of the political process because they decided it was no longer worth the effort of figuring out what was real and what was fake. Public officials therefore lost much of their credibility and their already limited popular mandate to govern.

Compounding these government legitimacy challenges, advances in digital technologies, including most notably AI, resulted in massive worker displacement. The extensive loss of both blue- and white-collar jobs fueled historically high levels of inequality as the owners of these technologies enjoyed unprecedented growth in wealth while the rest of the population was left behind. Governments around the world proved unable or unwilling to develop adequate responses to these societal disruptions. This situation obliterated the general public’s trust in long-standing government and societal institutions. Leading digital platform companies stepped into the void by providing nominally “free” services to consumers, who were happy to give up their digital privacy in return for these services as household incomes stagnated. Large segments of the global population disengaged from politics and instead focused on ever-more immersive forms of entertainment—made available at low cost by the technology giants.

The inability of governments to cope with the spread of disinformation and other negative platform content was indicative of broader struggles to regulate digital technologies. Inadequate regulations on illicit digital financing resulted in excessive money laundering, fueling corruption and organized crime. And despite efforts to improve cybersecurity, there was a growing sense that all data could and would eventually be hacked—especially because by 2030, essentially all

information was digitized. Governments were also reticent to enact antitrust measures against existing technology giants that could negatively impact an already unsteady global economy.

An implicit understanding developed among the digital platform companies that each of them would stay in their own domestic market, avoiding direct competition with one another. Given this islandization of the digital environment, many governments continued to focus on technology investment to build domestic capabilities. Beijing remained a leader in this regard, promoting world-leading innovation in quantum, AI, and 5G technologies. And although Silicon Valley lost some of its early momentum in this space, it continued to attract young talent because digital platform companies were seen as the only viable path to a prosperous career.

Business implications: In much of the world, companies struggle to break through the din of competing information in **Fake News Devolution**. Companies are consistently forced to contend with rampant hacking, IP theft, corporate espionage, and online smear campaigns. Developing strategies to rapidly identify and respond to such attacks becomes essential. Disruptive and innovative marketing campaigns can help companies attract customers, though this does not guarantee success. Although the technology giants benefit from a largely regulation-free environment, they still must contend with low consumer demand in a slow-growth economic environment. And all companies are forced to forego global ambitions as a result of more strident consumer preferences that all foreign companies and brands are to be avoided.

Scenario 4: Surveillance Capitalism

Minimal regulatory activity; globalized digital environment

In **Surveillance Capitalism**, the leading US and Chinese technology giants supplant national governments as the most powerful institutions in the world. Following a series of strategic partnership by these companies, the digital environment is more unified and globalized than ever before. Digital platforms are able to reach more people—and influence decision-makers—on a global scale. Using these capabilities, they effectively crush any regulatory efforts that would reign in their market dominance power. Popular backlash against these technology giants is limited, however, as global economic growth is strong, and households feel increasingly flush. The global digital platforms also help to usher in a generally cooperative and stable geopolitical environment, marked by greater levels of cross-border economic flows.

Throughout the early 2020s, US and Chinese technology giants rose to unprecedented levels of economic, social, and political power—in many ways surpassing the powers of traditional nation-states. As digital platforms absorbed and became intertwined with other companies, effective antitrust regulations became near impossible to construct and enforce. In the United States, successive administrations prioritized economic growth and innovation over greater data privacy and more digital regulations. As a result, Google, Facebook, Amazon, and other technology giants doubled down on the use of consumer data to predict behavioral patterns and consolidate their market share—as [Shoshana Zuboff](#) foretold in 2019. Alibaba, Baidu, and Tencent followed a similar strategy in China and many other emerging markets, further consolidating their economic and political power.

In the mid-2020s, a stunning announcement was made: Amazon and Alibaba forged a strategic partnership at the global level—a move that effectively merged the world's two largest e-commerce platforms. Although government leaders in Washington and Beijing were blindsided by this development, they ultimately backed the plan based on the belief that

it would reduce geopolitical tensions between the two countries and result in greater economic growth and domestic stability for both countries. Other technology giants moved quickly to follow this model of global cooperation. Huawei, for example, appointed well-respected Western technology leaders to its board in an effort to reduce security concerns about the company's technologies. By 2030, such moves have paved the way for a truly global 5G network. Technology giants also invested heavily to expand global mobile payment and digital wallet platforms, making purchasing their goods as frictionless as possible. The expansion of digital finance options in emerging and frontier markets improved financial inclusion—and provided new customers for these platforms.

With global digital platforms dominating the marketplace, surveillance capitalism emerged, and personal data began being collected without recourse for citizens. In short order, these practices became normalized and broadly accepted standard practices. With these data troves, the technology giants improved their capabilities to subconsciously influence the behavior of their users in both the digital and physical world. These efforts included the use of surveillance-based micro-targeting in advertising and politics to shape popular sentiment—and even policymaking. As a result, online content was gradually homogenized in much of the world, as governments abandoned earlier efforts to erect digital firewalls. The world moved closer to one global Internet—and one global consumer base.

In Surveillance Capitalism, **the collection of personal data without recourse for citizens became normalized** and broadly accepted as standard practice.

Stifled competition on a global scale led to a slowdown in economic growth and rising levels of inequality. To stave off any popular discontent, the technology giants offered funding to support universal basic income (UBI), providing citizens with monthly payments regardless of whether they were working. Some companies even cast this as a generous *quid pro quo* for unfettered use of consumer data. While many citizens' incomes were lower than in the past, they were content to spend their time entertaining themselves using the very technology platforms that had caused their job displacement.

Business implications: In **Surveillance Capitalism**, non-technology companies must recalibrate to find roles that complement the digital giants. Any companies viewed as potential innovative competitors to these dominant players are rapidly acquired by them, creating a difficult environment for start-ups and entrepreneurs. Some companies find that the best way to survive is through strategic partnerships with the digital multinationals. For businesses willing to forgo some independence (and a portion of their profits) through such agreements, there are great opportunities for growth. Consumers welcome the ease with which they can purchase digital goods and services no matter where they are in the world. Those companies that can offer products with international appeal stand to thrive in the global marketplace where new technologies have created unlimited possibilities for digital cross-border commerce.

Recommended Actions to Prepare for the Future Digital Order

Companies cannot be passive observers of the ongoing digital revolution. Rather, they need to actively prepare for the future digital order. As highlighted by the uncertainties in our scenario analysis, companies cannot stake their futures on the possibility that a more stable digital environment will emerge. Even as the digital disorder evolves, executives will need to guide their organizations through strategic digital transformations across a variety of business functions. Specifically, companies must adapt to the emerging digital order across strategy, customer experience, operations, risk management and compliance, and employees and culture—our SCORE framework (see figure 5). Many companies may already be in the process of digital transformation in some areas of the framework but are just discovering or exploring how digital is affecting other areas. To compete in the 21st-century digital economy, though, companies must embark on end-to-end digital transformation in all SCORE areas. We outline several specific digital adaptation and transformation actions that executives should take in each of the SCORE areas below.

We also identify the scenarios in which each of these actions would be most relevant. Some SCORE actions are highly relevant across all four scenarios. Executives should therefore prioritize these actions in the near to medium term. Other SCORE actions are more relevant in some scenarios than others. Executives should monitor the evolution of the digital disorder to determine which scenario is beginning to emerge and therefore which of these actions should be taken in the coming years (see figure 6 on page 29).

Figure 5
Strategic end-to-end transformations are required to adapt to the future digital order

SCORE framework of recommended actions

S Strategy	• Redefine the company's value proposition. • Identify digital enablers vs. disruptors. • Contend with competing platforms and systems.	• Seek out markets with strong enabling environments. • Use scenario analysis in strategic planning.
C Customer experience	• Base relationships on transparency and trust. • Offer personalization whenever possible.	• Develop digital ecosystems of products. • Improve marketing algorithms.
O Operations	• Generate, analyze, and act on data. • Develop good data hygiene.	• Create a digital ecosystem of partners. • Embrace bottom-up experimentation.
R Risk management and compliance	• Improve cybersecurity strategy. • Be aware of new responsibilities and liabilities.	• Manage digital risk exposure. • Monitor emerging data privacy and localization regulations.
E Employees and culture	• Prepare the existing workforce. • Nurture the talent pipeline.	• Uphold digital ethics. • Embed digital in the company culture.

Source: A.T. Kearney analysis

Figure 6
SCORE strategies should be tailored to the digital order scenario that emerges

Mapping SCORE actions to scenarios

	Actions	Techlash to Renaissance	Digital Crackdown	Fake News Devolution	Surveillance Capitalism
S Strategy	Identify digital enablers versus disruptors.	X		X	X
	Redefine the company's value proposition.	X	X	X	X
	Use scenario analysis in strategic planning.	X	X	X	X
	Contend with competing platforms and systems.		X	X	
	Seek out markets with strong enabling environments.	X			X
C Customer experience	Offer personalization whenever possible.	X		X	X
	Base relationships on transparency and trust.	X	X		
	Improve marketing algorithms.	X	X		X
	Develop digital ecosystems of products.				X
O Operations	Generate, analyze, and act on data.	X	X		X
	Develop good data hygiene.	X	X		
	Embrace bottom-up experimentation.	X		X	
	Create a digital ecosystem of partners.				X
R Risk management and compliance	Be aware of new responsibilities and liabilities.	X	X		
	Improve the cybersecurity strategy.	X	X	X	X
	Manage digital risk exposure.	X	X	X	X
	Monitor emerging data privacy and localization regulations.	X	X		
E Employees and culture	Embed digital in the company culture.	X	X	X	X
	Prepare the existing workforce.		X	X	X
	Nurture the talent pipeline.	X		X	
	Uphold digital ethics.	X	X		

Source: A.T. Kearney analysis

Strategy

Identify digital enablers versus disruptors

In some cases, digital technologies act as enablers for a company’s core business. Optimizing back-office operations with digital technologies can improve efficiency, while leveraging digital to create new customer experiences can grow the existing business. In other cases, digital technologies act as disruptors of current business models that alter an entire sector. The effect of the confluence of smartphones, GPS, and mobile applications on the taxi industry serves as a prime example. While such digital business model innovations can cannibalize an established business model, they can also create greater and more sustainable long-term value generation. Executives need to monitor emerging digital technologies and analyze their potential applications to determine whether to apply them as enablers or disruptors.

Most relevant scenarios: Techlash to Renaissance, Fake News Devolution, and Surveillance Capitalism

Redefine the company's value proposition

Traditional business models and value propositions will continue to become irrelevant as the emerging digital order takes shape. A comprehensive assessment of the value proposition—the fundamental value the company provides to its customers—is necessary for all companies in the emerging digital order. Executives should question the company's ambition, its guiding principles, and the unique value it provides. For each of these questions, executives need to assess the effect of digital technologies on their businesses. Such assessments require big thinking and bold leadership for companies—and are necessary for their survival in both the current digital disorder and the future digital order.

Most relevant scenarios: all

Use scenario analysis in strategic planning

The accelerating pace of change in digital innovations and applications as well as the rising debates about the future domestic and international regulatory environment for digital will create new challenges for business planning over the medium to long term. Executives must not only respond to a dizzying array of current events surrounding digital, but also make long-term strategic plans to prepare for an increasingly uncertain future. Embracing this uncertainty that is inherent in the future digital environment is crucial for effective strategic planning. Executives should employ scenario planning or other [strategic foresight](#) methodologies to spot emerging digital trends, test resilience to potential digital developments, and prepare for divergent digital futures.

Most relevant scenarios: all

Contend with competing technology platforms and systems

As countries continue to “[islandize](#)” by localizing data and protecting domestic companies, the fragmentation of digital technology standards and systems will continue, creating operational and compliance challenges for global companies. The two dominant digital platforms today are those in the United States and China, and other countries may choose to follow one of these sets of standards rather than going their own way. Identifying the markets in which Chinese or US technology platforms are dominant can provide insights into which technological, regulatory, and privacy standards will be required moving forward. Recent moves by several countries, including the United States and Australia, to block Chinese telecommunications manufacturer Huawei from participating in domestic 5G mobile networks are perhaps the most high-profile examples of this competition.

Most relevant scenarios: Digital Crackdown and Fake News Devolution

Seek out markets with enabling environments for digital

Digital technologies are already pervasive in the world's most innovative and efficient companies. And embracing digital will only become more important to commercial competitiveness. Companies should therefore seek to locate their operations and sales in markets that have strong enabling environments for the use of digital technologies. Considerations should include access to high-quality broadband and mobile Internet, investments in relevant human capital and a strong digital talent pipeline, and support for R&D and a culture of innovation. Companies should also seek regulatory environments that provide significant white space to experiment with new applications of digital technologies and create new digital markets for their goods and services.

Most relevant scenarios: Techlash to Renaissance and Surveillance Capitalism

Customer experience

Offer personalization whenever possible

As explored in A.T. Kearney's [Consumers@250](#) initiative, the consumer landscape is shifting away from a mass-market model and toward one in which personalization and individualization are highly valued. Believing "I am what I do," these new consumers search out brands and retailers they can relate to, and they view commercial exchanges in terms of trust-based relationships. Executives understand this imperative, with almost two-thirds of respondents in a 2017 survey of US executives saying that [offering more personalization](#) is an urgent priority. In many ways, these forces give local companies, or those nimble enough to infuse authentic local elements into their products, an advantage. Digital technologies also offer companies opportunities to implement such personalization, whether by offering consumers the option to choose design elements of products ordered online, using 3D printing to customize consumer goods, or other methods.

Most relevant scenarios: Techlash to Renaissance, Fake News Devolution, and Surveillance Capitalism

Base relationships on transparency and trust

In an era in which people are bombarded with fake news and the [Edelman Trust Barometer](#) shows that public trust remains near all-time lows, trust has become a crucial differentiator for companies and brands. In the emerging digital order, an important component of building and maintaining trust will be the transparent use of customer data and respect for customer data privacy. High levels of trust will promote greater customer loyalty and business growth. An A.T. Kearney study found, for instance, that [banks with higher levels of customer trust](#) were rewarded with a higher share of customers' total financial services business. In contrast, some of the Internet giants serve as examples of the negative publicity and regulatory scrutiny associated with the perception of opaque behavior and the loss of trust. Executives should be proactive about identifying ways their companies can be as transparent as possible with their customers and start to build more trust.

Most relevant scenarios: Techlash to Renaissance and Digital Crackdown

Improve marketing algorithms

Digital advertising is estimated to have become the largest share of [global spending on advertising](#) in 2018, surpassing television for the first time. This shift provides an opportunity for both B2B and B2C companies to better target their marketing at their intended audiences—if they can get their algorithms right. For instance, many consumers today notice when they are targeted with Internet ads for a shirt they already purchased. A much more effective approach would be to target a consumer with ads for pants that complement a purchased shirt. Companies need to collect and leverage a wide variety of data on their customers and their purchasing patterns to build appropriate algorithms. Hiring highly skilled data scientists who can develop and refine marketing algorithms as new information becomes available is also important.

Most relevant scenarios: Techlash to Renaissance, Digital Crackdown, and Surveillance Capitalism

Develop digital ecosystems of products

In an increasingly digital economy, it will be important for companies—particularly B2C companies—to create an ecosystem of reinforcing goods and services offerings for their

customers. For instance, traditional big-box retailers are integrating their digital and physical stores to enable rapid in-store pickup of items ordered online. And a leading US health insurance provider has invested heavily in digital technologies to improve the level of communication with its members and offer them services to better manage their health. In designing such systems, executives need to start by determining what the customer wants and how they can use digital technologies to fill those needs. Similarly, with [more consumers preferring experiences](#) to traditional consumer goods, retailers and consumer goods firms should strive to design unique and memorable purchasing experiences. These experiences can include time-limited pop-up stores, retail transactions that are integrated with digital technology—such as the [cashier-free Amazon Go stores](#) and [Walmart’s use of AR](#)—and other differentiating shopping experiences.

Most relevant scenarios: Surveillance Capitalism

Operations

Generate, analyze, and act on data

Data is more readily available to global businesses than ever before, but a purposeful big data strategy is necessary to safeguard against drowning in a sea of untapped or mismanaged information. In some cases, it is likely that valuable data is not being collected, while in others, existing data generation is not being fully leveraged for analysis. For instance, an A.T. Kearney study has found that although many manufacturers measure analytics for their machines, few do so for their employees—but such “[human factory analytics](#)” could dramatically improve factory efficiency. Both of these potential pitfalls must be carefully calibrated to survive in today’s data-driven decision-making businesses. In supply chain and logistics, for instance, leading companies are using data to yield significant operational efficiencies—and a competitive edge—by optimizing delivery times, routes, and transportation methods.

Most relevant scenarios: Techlash to Renaissance, Digital Crackdown, and Surveillance Capitalism

Develop good data hygiene

Big data has made data hygiene crucial to effective operational management. Some degree of data disorganization is expected in a company because of personnel changes, mergers and acquisitions, and fluctuations in customer relationships, but an alarming [94 percent of businesses](#) believe that their customer or prospect management data is inaccurate. These inaccuracies result in negative consequences for business operations, marketing, and identification of new customer leads as well as wasted expenditures for IT and finance departments. Companies should start by identifying all data currently serving their operations, assign an organizational scheme to the data, ensure consistency in tracking data throughout the business life cycle, and be diligent about culling outdated data along the way. Ensuring that legacy data management systems can be easily accessed or upgraded to the latest software is also essential.

Most relevant scenarios: Techlash to Renaissance and Digital Crackdown

Embrace bottom-up experimentation

Rather than going through top-down enterprise resource planning (ERP) processes, companies should embrace an intentionally iterative, bottom-up experimentation process for customers or employees. Such a process is an excellent opportunity to drive innovation in ways that executives may otherwise miss because they are not on the frontlines of digital technology

adoption. Outcomes of bottom-up experimentation can include a wider customer reach, revenue growth, cost reduction and other efficiencies, and improved productivity. But it is important to be aware of potential blind spots, such as costly expenditures and time allocated to experimentation, over- or under-engineering a potential business solution, and not receiving adequate support from key stakeholders. A sound strategy to hedge against these blind spots is to participate in [digital innovation ecosystems](#) designed to support the full experimentation-to-innovation life cycle.

Most relevant scenarios: Techlash to Renaissance and Fake News Devolution

Digital ecosystems enable companies to rely on partnerships with suppliers, customers, and vendors to **control their value chain while not actually taking responsibility for each part of it.**

Create a digital ecosystem of partners

Digital ecosystems—the collection of people, organizations, hardware, services, and data connected by shared digital platforms—will soon overtake traditional physical ecosystems centered on suppliers and customers responding to conventional supply and demand market forces. Digital ecosystems enable companies to rely on partnerships with external suppliers, customers, and vendors to control their entire value chain while not actually taking responsibility for each part of it. In fact, one of the most common types of consulting engagements recently has focused on how to conduct business in a network of customers and suppliers. For instance, we have seen companies turn their legacy direct-to-customer networks into shared-use networks. Along similar lines, Ikea recently announced it is exploring an [industrywide digital platform for furniture sales](#) (subscription required). Successful companies will be those that acknowledge the significant potential revenue upside in entering digital ecosystems, embrace next-generation [shared services organizations](#), and stay nimble in their software selections to accommodate partnerships along the way.

Most relevant scenarios: Surveillance Capitalism

Risk management and compliance

Be aware of new responsibilities and liabilities

Many companies are aware of their liability for data, including intellectual property, customer data, and financial information, in the event of a cyber breach that compromises such data. But there are many other emerging responsibilities and liabilities for companies in the digital economy. A company that uses an open-source algorithm in its hiring process, for example, is likely to be legally liable if that algorithm is biased against a particular sub-set of applicants. Liability is less clear if an autonomous vehicle kills a worker at a mining site. In this case, either the mining company, the vehicle manufacturer, or the company that created the faulty algorithm

could be found responsible. Executives need to be aware of such potential liabilities and take the necessary steps where possible to protect their companies. Contract language may be able to limit the amount and types of damage for which the company is responsible. And greater investment in liability insurance may also be prudent in a fast-changing digital environment.

Most relevant scenarios: Techlash to Renaissance and Digital Crackdown

Improve cybersecurity strategy

Cyberattacks continue to increase in frequency and sophistication, yet many companies have yet to fully develop and implement a comprehensive cybersecurity strategy. Our 2018 survey of global executives found that companies with such a plan in place have disproportionate success in quickly identifying and [resolving cyber breaches](#)—and in avoiding them entirely. The benefits of implementing such a strategy are wide-ranging, affecting employees, customers, and the company's bottom line. And as digital technologies become more essential to business operations, the potential damage from a cyberattack will increase in kind. Cybersecurity should therefore be an integral part of any company's digital transformation. In developing their strategies, companies should consider opportunities for cooperation with industry consortia and public-private sector partnerships to share best practices. Companies should also consider investing in cyber insurance as a last line of defense to protect against such risks.

Most relevant scenarios: all

Manage digital risk exposure

As more business is conducted online and vital data is digitized, all companies face some degree of digital risk exposure. A thorough internal audit of each company's risk is needed. Fake news attacks against a company are one example of emerging digital risks. Executives should take measures to prevent their brand from being the target of a fake news attack and craft digital marketing strategies accordingly. And in an age of escalating social activism and a turbo-charged information environment—when a tweet or video can go viral to millions of viewers around the world in a matter of hours—executives should prepare contingency plans for widespread social mobilization against their companies or brands on digital platforms. More broadly, by assessing how the organization and its employees are using digital technologies—everything from the cloud to IoT devices—executives can strengthen risk management practices where needed. Finally, clear communication and transparency across the organization, combined with strategic agility, are essential to risk mitigation plans.

Most relevant scenarios: all

Monitor emerging data privacy and localization regulations

Companies must deal with a data governance regulatory environment that is complicated by a growing array of privacy regulations and data localization requirements. To comply with existing and monitor emerging ones, research on best practices suggests that companies should centralize their compliance teams, conduct more frequent compliance audits, and invest in corporate training programs. Appointing a chief compliance officer dedicated to staying current on global developments in this area could help many companies to ensure there is a clear chain of responsibility for complying with emerging data privacy rules, data localization requirements, and other digital regulations. A data protection officer (which is a requirement under the EU's GDPR for organizations with more than 250 employees) may also

be prudent. Companies should consider national or supranational frameworks, such as the [Privacy Shield](#) and the Asia Pacific Economic Cooperation (APEC) [Cross-Border Privacy Rules System](#), which offer the opportunity to voluntarily self-certify and commit to compliance in exchange for cost and efficiency benefits down the line in markets where privacy regulations are heavily enforced. Global companies should also consider getting involved in international efforts to create rules that foster open cross-border data flows, such as the recently launched WTO talks on cross-border electronic commerce.

Most relevant scenarios: Techlash to Renaissance and Digital Crackdown

Employees and culture

Embed digital in the company culture

Companies that successfully embed understanding and the use of digital technologies into their cultures will be best positioned to succeed over the long term. In addition to offering continuous digital learning opportunities for employees at all levels of the organization, executives should clearly define and embrace the cultural characteristics that promote end-to-end digital transformation. This stance includes constant thought about the improvements digital could provide for business processes, incentives for innovation and risk-taking, and emphasis on the upsides of digital for the company's workforce (particularly aging workers). In many cases, this work will require a fundamental shift in a company's DNA. While such a dramatic cultural change management process will likely prove challenging, it will be necessary to succeed in the emerging digital order.

Most relevant scenarios: all

Prepare the existing workforce

Companies must assess the digital skills in their workforce and then make strategic investments in training and upskilling to provide employees with the capabilities necessary to remain productive in the emerging digital order. Importantly, this process will involve helping employees deviate from the methods of work with which they are familiar. In many cases, a dramatic culture shift within the company will be necessary so employees feel comfortable experimenting with new processes and responsibilities enabled by digital technologies. At the same time, training the workforce on cybersecurity risks and good cyber hygiene is vital. And all digital training programs need to be regularly evaluated, updated, and re-administered to the workforce so employees stay current on emerging technologies.

Most relevant scenarios: Digital Crackdown, Fake News Devolution, and Surveillance Capitalism

Nurture the talent pipeline

Employers are already facing a significant skills gap, particularly for positions that require specialized digital skills. By identifying and nurturing a talent pipeline with digital skills, companies can ensure they are better equipped with the employees they need as digital continues to play a more important role in business operations. Companies should consider [partnering with local educational institutions](#) to improve the quality of their applicant pool and reduce training and turnover costs. Taking active steps to nurture prospective talent through early communication and engagement could also make a difference between landing

a prospect and losing them to the competition. Digital tools can support this process, as recruitment, customer relationship management (CRM), and marketing software now allows companies to efficiently and effectively develop and build relationships with talent prospects.

Most relevant scenarios: Techlash to Renaissance and Fake News Devolution

Companies should consider collaborating with others in their industry to **develop a common ethical code with respect to data.**

Uphold digital ethics

Companies will increasingly be expected to adhere to [digital ethics](#) to earn the trust of their stakeholders. Protecting personal data and upholding privacy standards is one aspect of digital ethics. Companies should consider collaborating with others in their industry to develop a common ethical code with respect to data. This code would enable companies to build and maintain the necessary trust with customers, partners, and employees. Executives also need to think through the ethical implications of their digital initiatives. For instance, what are the ethical implications of using AI? And do customers deserve to know whether they are talking to a chatbot or a human? More broadly, companies need to be aware of the social impact of their digital activities. Consumers, employees, communities, and investors now have greater access to information about company actions thanks to the Internet and social media—and they are more motivated to reward or punish companies based on companies' [alignment with their values](#). It will therefore be increasingly important for companies to be good corporate citizens in the digital domain.

Most relevant scenarios: Techlash to Renaissance and Digital Crackdown

Taking the Next Steps in the Digital Transformation Journey

The digital revolution continues to transform the world, and more attention is being directed at understanding digital's implications across a broad range of social, economic, and political indicators. In part as a result of this focus, there is intensifying regulatory activity for digital technologies as governments around the world are introducing an array of new rules for the digital economy. As international agreement on how to regulate digital remains elusive, however, companies are having to manage a more complex set of conflicting rules in significant markets. Further complicating the current digital environment is the escalating global competition—primarily between China and the United States—to lead the development and application of emerging digital technologies. This competition threatens to put companies in the crosshairs of geopolitics and raises the risk that competing technological standards will fragment the global digital economy into smaller “islandized” segments.

The rate of change among these forces varies across markets, industries, and consumer segments. As a result, the exact shape that the future digital order will take remains unclear. Across all four scenarios, though, two things are clear about the future digital order. The first is that digital technologies will continue to proliferate and will play a more central role in the 21st-century economy. The second is that we are on the cusp of radical change in the operation of the digital economy. Companies across all industries must therefore act now to both manage the volatility and uncertainty associated with digital disorder and simultaneously prepare for the digital order that will emerge.

Encouragingly, we are starting to see some executives question how various aspects of digital disorder will affect their business. A global financial services company, for instance, is analyzing the potential effect of data localization requirements on their costs and operations. And a telecommunications firm is exploring the impact of geopolitical risks arising from the escalating national competition in digital technologies on its access to key markets. Such efforts are certainly steps in the right direction, but all companies need to embark on an end-to-end assessment of the opportunities and risks associated with digital technologies.

Companies' digital transformations should be carried out across the SCORE framework—strategy, customer experience, operations, risk management and compliance, and employees and culture. Of course, different aspects of SCORE will be more relevant in some potential future digital environments than others. Executives should therefore monitor how digital disorder is evolving to determine the best course of action. Any future scenario for the digital order, though, will require an end-to-end digital transformation across the SCORE framework—capitalizing on the opportunities that digital provides while managing the risks it generates. And time is of the essence. The companies that adapt more quickly to the future digital order will enjoy a competitive edge in the years to come.

Authors



Paul Laudicina, chairman emeritus of A.T. Kearney and chairman of the Global Business Policy Council, Washington, D.C.
paul.laudicina@atkearney.com



Erik Peterson, partner and managing director of the Global Business Policy Council, Washington, D.C.
erik.peterson@atkearney.com



Courtney Rickert McCaffrey, manager of thought leadership for the Global Business Policy Council, Washington, D.C.
courtney.mccaffrey@atkearney.com

The authors are indebted to Stephanie Hollinger, Elena McGovern, and Terence Toland for their assistance in producing this report.

The authors also wish to thank their many A.T. Kearney colleagues for their contributions to this report, including Sameer Anand, Ramyani Basu, Wade Bjubrey, Sumit Chadha, Suketu Gandhi, Eric Gervet, John Gomes, Ajay Gupta, Todd Huseby, Bharat Kapoor, Alanna Klassen Jamjoum, Sandeep Kumar Biswas, Alex Liu, Rudolph Lohmeyer, Greg Portell, Michael Roemer, Sebastian Schoemann, Arjun Sethi, Cary Shiao, Ben Smith, and Vidisha Suman.



ATKearney

Global Business Policy Council

A.T. Kearney is a leading global management consulting firm with offices in more than 40 countries. Since 1926, we have been trusted advisors to the world's foremost organizations. A.T. Kearney is a partner-owned firm, committed to helping clients achieve immediate impact and growing advantage on their most mission-critical issues. For more information, visit www.atkearney.com.

Americas

Atlanta	Dallas	San Francisco
Bogotá	Detroit	São Paulo
Boston	Houston	Toronto
Calgary	Mexico City	Washington, D.C.
Chicago	New York	

Asia Pacific

Bangalore	Kuala Lumpur	Shanghai
Bangkok	Melbourne	Singapore
Beijing	Mumbai	Sydney
Brisbane	New Delhi	Tokyo
Hong Kong	Perth	
Jakarta	Seoul	

Europe

Amsterdam	Ljubljana	Paris
Berlin	London	Prague
Brussels	Madrid	Rome
Bucharest	Milan	Stockholm
Copenhagen	Moscow	Vienna
Düsseldorf	Munich	Warsaw
Lisbon	Oslo	Zurich

Middle East and Africa

Abu Dhabi	Dubai	Johannesburg
Doha	Istanbul	Riyadh

For more information, permission to reprint or translate this work, and all other correspondence, please email: insight@atkearney.com.

The signature of our namesake and founder, Andrew Thomas Kearney, on the cover of this document represents our pledge to live the values he instilled in our firm and uphold his commitment to ensuring “essential rightness” in all that we do.

A.T. Kearney Korea LLC is a separate and independent legal entity operating under the A.T. Kearney name in Korea.

A.T. Kearney operates in India as A.T. Kearney Limited (Branch Office), a branch office of A.T. Kearney Limited, a company organized under the laws of England and Wales.

© 2019, A.T. Kearney, Inc. All rights reserved.