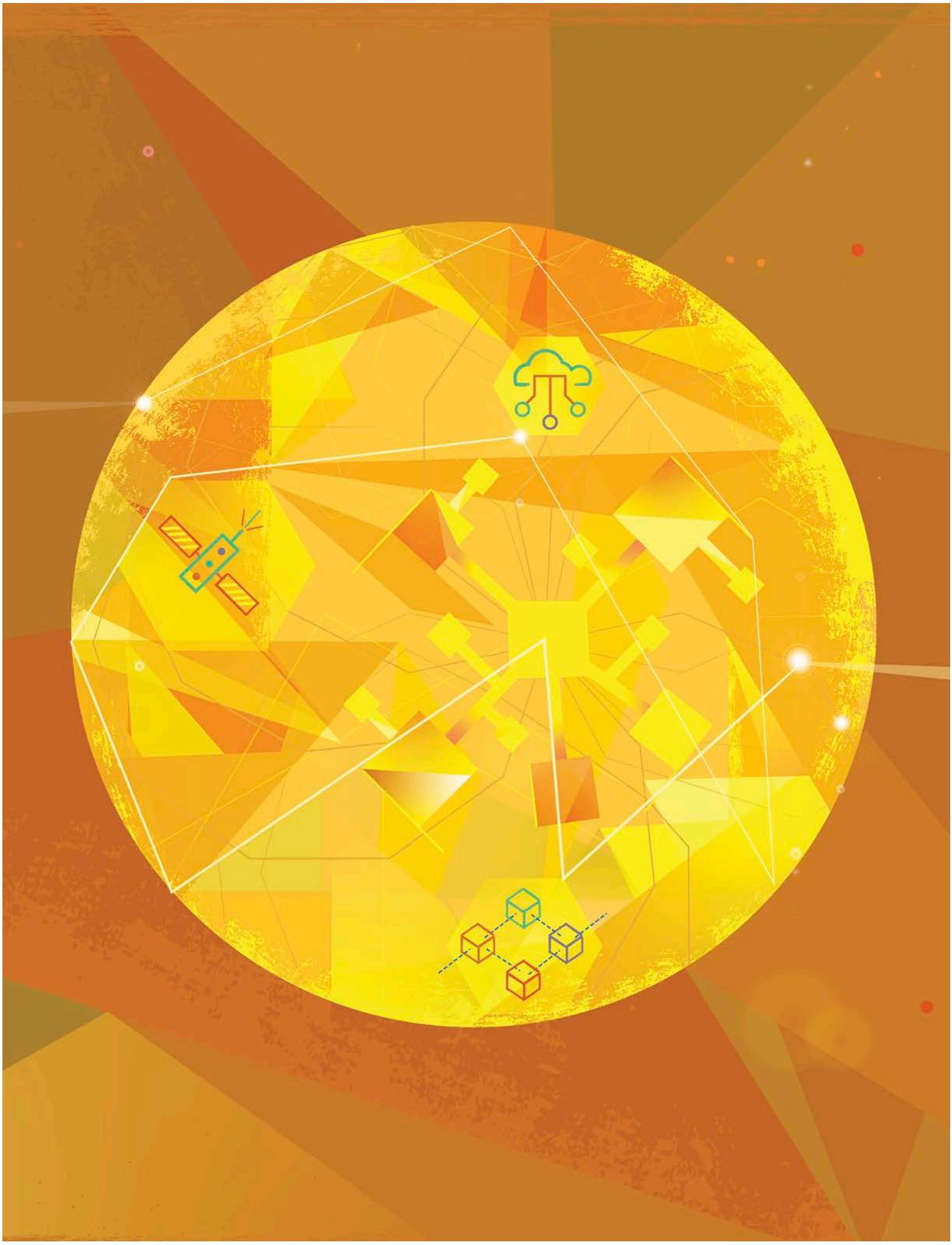


Connectivity of tomorrow

The spectrum and potential of advanced networking

ADVANCED NETWORKING IS THE UNSUNG HERO OF OUR DIGITAL future, offering a continuum of connectivity that can drive the development of new products and services or transform inefficient operating models. Increasingly, digital transformation through data- and networking-dependent technologies such as cognitive, IoT, blockchain, and advanced analytics are fueling adoption of connectivity advances. Next-generation technologies and techniques such as 5G, low Earth orbit satellites, mesh networks, edge computing, and ultra-broadband solutions promise order-of-magnitude improvements that will support reliable, high-performance communication capabilities; software-defined networking and network function virtualisation help companies manage evolving connectivity options. In the coming months, expect to see companies across sectors and geographies take advantage of advanced connectivity to configure and operate tomorrow's enterprise networks.

Traditionally, networking has lived in the shadow of high-profile disruptive enterprise technologies such as digital experiences, cognitive, and cloud that capture imaginations and headlines. Networking, though mission critical, is not particularly sexy.

This is about to change. Increasingly, technology forces dependent on networking are transforming enterprise architecture. For example, proliferating mobile devices, sensors, serverless computing, exploding volumes of shared data, and automation all require advanced connectivity and differentiated networking. Indeed, advanced connectivity is fast becoming a linchpin of digital business. In *TechTarget's* most recent IT Priorities Survey, 44 percent of respondents cited upgrading their networking foundations as a top priority for the coming year.[1] Similarly, a 2018 survey of IT leaders by Interop ITX and *InformationWeek* found that companies are increasingly focused on adding bandwidth, exploring ways to modernise their networks with software, and expanding their networking capabilities.[2]

Going forward, one of the CIO's primary responsibilities will be getting data from where it is collected, to where it is analysed, to where it is needed to drive real-time decisions and automated

operations—at scale and at speed, in a data center, in the cloud, or, increasingly, on the edge at the point where business occurs and missions are realised. As such, building and maintaining the networking capabilities required to meet this responsibility is a growing CIO priority. As part of the growing *connectivity of tomorrow* trend, CIOs have begun developing connectivity strategies that support their broader digital agendas. They are exploring opportunities to use software-defined networking (SDN), network function virtualisation (NFV), and network slicing to build controllable, secure, distributed networks that feature different kinds of devices and have the ability to utilise distributed computing power. Likewise, they are defining the roles that evolving access mechanisms such as 5G and low Earth orbit (LEO) satellites will play in their connectivity strategies. And importantly, CIOs are learning ways to maintain control over these networking components without increasing the cost of ownership.

Networking models featuring some or all of these components can transform an organisation's agility, efficiency, and competitiveness—but only to the extent that they can reliably deliver connectivity, security, and performance seamlessly to end users and applications. Often, the expectation behind every digital experience is the infinite availability and omnipresence of seamless network connectivity. And when that expectation cannot be met, the experience—and the strategy behind it—fail.

The orders-of-magnitude performance boost that 5G promises doesn't happen very often.

The orders-of-magnitude performance boost that 5G promises doesn't happen very often. Very soon, LEO satellite-based connectivity and mesh networks will deliver 5G capabilities to locations that currently have only limited coverage. During the next 18 to 24 months, expect to see more companies embrace the *connectivity of tomorrow* trend by exploring how a host of advanced networking capabilities can be used to enhance products, services, and enterprise architectures.

From a strategy perspective if you are in an industry that can benefit from greater bandwidth and more digital technology capabilities in your stores, warehouses, field operations, or across your global networks, what does this trend mean for your company's future? How will you build your connectivity of tomorrow?

Connectivity building blocks

Advanced connectivity raises the bar on network flexibility, making it possible to configure networks to fit different types of performance and availability requirements. Network management frameworks are increasingly allowing companies to dynamically configure and control network resources through software. As they develop advanced networking strategies, CIOs should start by examining how the following core capabilities may be able to advance their digital transformation agendas.

The latest advanced connectivity building blocks include:

- **5G.** The fifth generation of cellular wireless technology represents a sweeping change, far beyond being just another new wireless interface for smartphones. It offers greater speed, lower latency, and—importantly—the ability to connect massive numbers of sensors and smart devices within a network.[3] How? By breaking technology constraints. With 5G, many networking protocols can coexist to meet device and application specific requirements, and can be managed seamlessly. In *connectivity of tomorrow*, billions of connected devices will be communicating directly as machine-to-machine, and addition or subtraction of connected devices will be possible at unprecedented scale. In this environment, the ability to manage

large volumes of connected devices and the information being exchanged between them will be critical. 5G acts as a unifying technology, bringing together all the networking capabilities needed to manage the information flow and density at scale. The protocol also lowers power requirements for base communication, extending sensor battery life and viability of many IoT potential use cases.

The 5G revolution is well underway with telecom operators. Deloitte predicts that 2019 will be the year in which 5G networks arrive in scale. There were 72 operators testing 5G in 2018,[4] and by the end of 2019 we expect 25 operators will have launched 5G service in at least part of their territory (usually cities). An additional 26 operators could launch in 2020, more than doubling the total.[5]

51

operators will have launched 5G services in at least part of their territory by the end of 2020, according to predictions by Deloitte Global.

In addition, with regulatory approval for spectrum use, enterprises can deploy private local area networks with 5G technology. In some industrial settings such as factory floors, 5G can replace local area networking over Wi-Fi, significantly increasing the network's reliability, performance, and predictability. This 5G capability could be used to untether robots from fixed locations or to enable remote control of robots, thereby providing higher levels of flexibility in operations.

- **Low Earth orbit satellites.** Companies have long used large, high-altitude, geostationary satellites to connect remote areas to the outside world. These satellites have served a purpose, but they lag fiber and cable-based internet in terms of reliability and responsiveness and have potentially high cost profiles. In what some have characterised as a "new space race," SpaceX, OneWeb, and other organisations are developing small, low Earth orbit satellites that, deployed in clusters, may be able to deliver high-performance broadband anywhere on Earth. In addition to providing access to rural or isolated communities, low-orbit satellites could become essential networking infrastructure tools for industries operating in remote areas such as energy, mining, transportation, and even finance.[6]

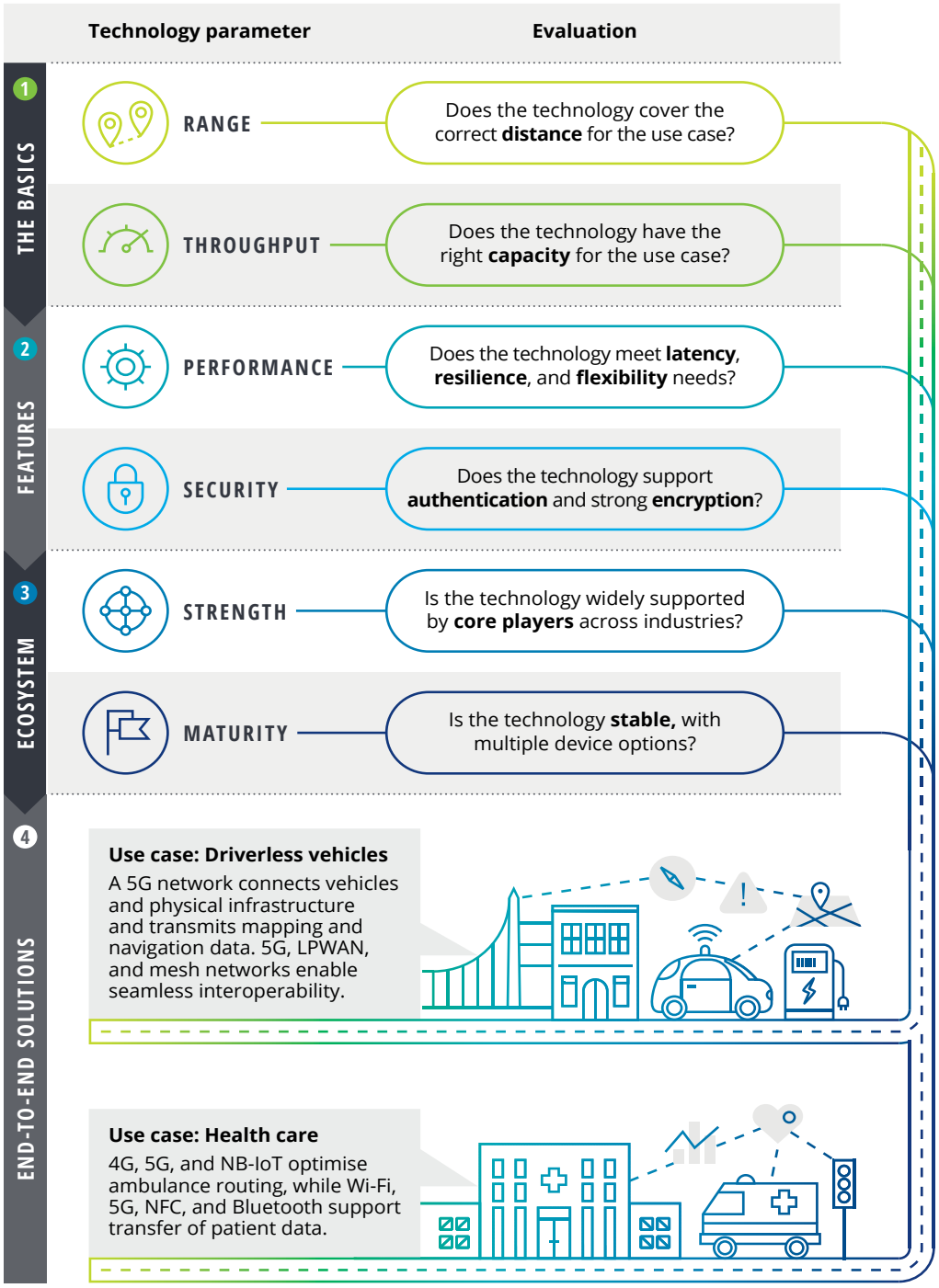
To monitor and manage evolving connectivity options that are increasingly varied, CIOs are virtualising parts of the connectivity stack using the following network management techniques:

- **Software-defined networking.** SDN is a software layer that sits atop a physical network composed of networking appliances such as switches and routers. Long restricted primarily to use within the data center, the technology is now being extended for wide area networking (SD-WAN) to connect data centers, branch banks, stores, or other multilocation applications. These physical appliances still forward data packets, but SDN software controls where these packets get forwarded. In the SDN model, software can centrally program and manage a network, potentially boosting flexibility.[7]
- **Network function virtualisation.** NFV replaces network functions such as routing, switching, encryption, firewalling, WAN acceleration, and load balancing provided by dedicated physical network appliances with virtualised software. These virtual network functions appear and behave like their physical

FIGURE 1

Considerations for connectivity technology selection

When designing end-to-end solutions, start by thinking about connectivity building blocks



Source: Deloitte analysis.

counterparts without the need for dedicated, specialised hardware. NFV deployments typically use commodity servers. Through virtualisation, these network services can scale horizontally or vertically on demand.[8] With NFV, services such as multimedia voice, evolved packet core routing, and radio access networking can now be operated completely in a cloud environment using low-cost, general-purpose computing platforms as network infrastructure.

SDN and NFV are complementary. SDN controls network functions centrally; it doesn't matter whether the network functions are provided by dedicated hardware appliances or virtualised network functions.

What does this mean for IT?

CIOs can use these advanced connectivity building blocks together with existing local area networking technologies like Ethernet, and Wi-Fi, and wide-area capabilities such as Gigabit broadband and 4G LTE to create configurable networks that can be tailored to fit a variety of enterprise needs (see Figure 1). Similar to how enterprises utilise elastic cloud computing infrastructure, with SDN and NFV they will be able to spin up, tear down, and optimise network capabilities on demand to fit specific application or end-user requirements.

As you begin developing your *connectivity of tomorrow* strategy, consider the following demand and supply factors:

- **Growing demand for real-time computation and low latency at the end device.** Applications such as industrial automation, virtual reality, and autonomous decision-making will require high computation capabilities with very low latency (round-trip time from the device to the cloud and back). In these situations, data processing can be partitioned with a portion executed in a "mini cloud" as close as possible to the device. The remaining data-processing functions can be distributed among cloud service providers or corporate data centers. This mini cloud is also known as *edge computing*—a useful model in situations where low latency connectivity to the end device is an essential component. For IoT networks that generate and move massive amounts of data, edge computing is a game-changer. It makes it possible for these IoT devices—many with minimal computing power and low-speed connectivity—to process data at the edge. This model increases efficiencies for both the telecom operator and the enterprise by reducing network backhaul traffic to central repositories.[9]
- **Proliferation of connected devices to monitor and manage.** Enabled by 5G, both the volume and variety of connected device types are expected to dramatically increase within an enterprise. These devices are likely to have a range of operating systems, computing, storage, and networking capabilities. For CIOs and their IT teams, new end-point security requirements and challenges are likely to emerge, including prevention of unauthorised devices on the corporate network, security policy management at the device level, and avoiding potential for network storms by rogue devices.
- **IT talent models evolve.** As examined in the *Reengineering technology* chapter of *Tech Trends 2018*, talent models will need to evolve as IT talent upskills and retrains to address the new normal. In the context of advanced connectivity, SDN and NFV expertise is not widely available in all regional and industry talent pools. Likewise, enterprise architects will need to address partitioning of applications between the edge and the cloud/enterprise data centers, while ensuring that data is transported efficiently and securely.

LESSONS FROM THE FRONT LINES

MINING THE POSSIBILITIES: BHP ENABLES SAFETY AND PRODUCTIVITY THROUGH CONNECTIVITY

LESSON ONE

Technology such as automated drills, self-driving haulage trucks, and real-time supply chain analytics has transformed the once-traditional mining industry to make it more efficient, more profitable, and safer. Melbourne, Australia-based BHP—which extracts and processes minerals, oil, and gas around the world—has set a path to fully integrate its use of these technologies and automate its value chain to increase productivity, gain process efficiencies, and reduce costs. This ambitious strategy relies on a robust, next-generation connectivity infrastructure.[10]

BHP is leveraging technologies such as the Industrial IoT, digital mesh, Wi-Fi, and 4G LTE to stand up its integrated remote operations centers (IROCs)—the first launched in 2013—which operate 24/7 and give the business real-time visibility into its mining processes from pit to port.[11] The IROCs enable teams that manage planning, scheduling, controlling, and analysis to perform their jobs more effectively by providing a real-time, end-to-end view of a mine's supply chain network from one central location. For the IROC to be successful, BHP had to expand its network over a 2,000-kilometer distance, launch interconnected telecommunications infrastructure, implement closed-circuit television monitoring systems, engineer downtime management systems, and enforce security measures across the entire network.

BHP's next step is to leverage its investment in enhanced connectivity to scale automation and efficiencies across its entire value chain. The organisation has installed 4G LTE, leveraged edge computing to schedule train routes, and implemented automated track signaling to control and monitor its rail systems. These measures have reduced the minimum gap between trains, allowing BHP to potentially double the capacity of its rail network. The company is also exploring ways to integrate these new capabilities with its existing, fully functional legacy systems and, at the same time, manage increased cybersecurity risks within the connectivity infrastructure.

BHP is seeing bottom-line results and process efficiencies across projects. These successes have created leadership support for the connectivity strategy, which is now integrated into BHP's overall business strategy. Moving forward, BHP plans to scale and maintain a robust connectivity infrastructure to support future innovation and functionality centrally and at the edge.

Ultimately, BHP continues to lead the transformation in the industry. Advances in connectivity will enable the acceleration of the development and deployment of remote safety systems, sensors, conveyors of the future, virtual mining with autonomous drilling and haulage fleets,[12] and predictive analytics for maintenance of its fleets and devices.[13]

SMOOTH SAILING: MSC CRUISES MAKES THE GUEST CONNECTION

LESSON TWO

More people are cruising now than ever before,[14] and as destinations grow more far-flung, staying connected at sea has never been more challenging. Today's passengers want a constant connection to their lives on shore and to their families and friends on board, as well as a way to optimise their cruising experience with instant access to facilities, entertainment, and events. To that end, MSC Cruises has been working to make its ships' connectivity fast and reliable across the seven seas as well as investing in a range of new digitally enabled services and experiences.

"It's vital that technology be at the service of the guest experience, and we're committed to investing in our fleet to develop technology and infrastructure that is capable of meeting the needs of guests for years to come," says chief business innovation officer Luca Pronzati.[15]

MSC's fleetwide digital innovation program, called MSC for Me, launched in early 2017 and debuted on board the MSC *Meraviglia* a few months later. Designed in collaboration with digital and behavioural design experts, the plan is part of a 10-year, US$10 billion investment to create a cruise experience designed around guests' preferences and behaviours.[16] To deliver a world-class customer experience at this scale, first and foremost the cruise line needed a robust and connected infrastructure.

Pronzati envisions its ships to be like smart, connected cities, but with the added complexity of being at sea and having advanced technology solutions on board that demonstrate MSC Cruises' commitment to true innovation to amplify the customer experience. MSC chose a multidimensional approach, addressing in turn connectivity for passengers and crew on board, connectivity from ship to shore, and connectivity between ships within the fleet. The company applied advanced networking techniques to make this possible, including satellites, Bluetooth beacons, edge computing, on-premises location-based services, and sensors. *Maritime Executive* reported that the entire MSC fleet connects to a dedicated cloud of bandwidth on the Marlink VSATs network, comprising 25 satellites and 32 overlapping beams.[17]

Delivering advanced connectivity to crew and passengers will require an overhaul of MSC's existing fleet, but the company is building the capability into new ships scheduled to launch by 2026. MSC Cruises announced that, on a single ship, the MSC for Me initiative is enabled by 3,000 sensors placed throughout the vessel, with 16,000 points of connectivity such as Wi-Fi and NFC beacons, 700 digital access points, 358 informative and interactive screens, and 2,244 cabins with RFID/NFC access technology. This helps guests with boarding, dynamic wayfinding, scheduling services, booking excursions, making purchases, and identifying the location of children anywhere on board the ship, while the crew is better enabled to tailor onboard operations and serve the passengers' ever-changing needs.

This advanced connectivity has paved the way for new, cutting-edge technologies and digital experiences, with new functionality coming in 2019, including facial recognition to help staff identify passengers and virtual reality capabilities for enhanced previews of excursions. Additionally, leveraging its mesh networks onboard ships, MSC is working to implement the first AI platform on a cruise ship, with a voice assistant in all staterooms. The company's proprietary digital concierge is specifically tailored to its business, supporting seven languages at launch (including Chinese) and deployed onboard to ensure seamless operations across the voyage.

"It's all about the experience for the customer," Pronzati says. "They expect speed and consistency in connection, and we want to offer that. We still have challenges in getting the right bandwidth, which is the nature of being at sea, but as the technology evolves, we will be prepared with infrastructure and services already in place to further elevate the guest experience."

MY TAKE

PROFESSOR THEODORE RAPPAPORT, NEW YORK UNIVERSITY, TANDON SCHOOL OF ENGINEERING

The amount of data consumed globally increases by 50 percent each year,[18] and I predict that four years from now our current 50 percent annual ramp will reach 70 to 80 percent. Why the jump? Because the rollout of 5G will accelerate data consumption exponentially. Organisations continually need wider pipes to accommodate ever-growing data volumes. Base stations and other 5G infrastructure will be rolling out in 2019 and 2020, and as they come online, 5G's impact will be felt around the world: in urban and rural areas, in burgeoning IoT ecosystems, on factory floors, and in corporate boardrooms.

Think about 5G's potential. For the first time, cell phones will perform as if they were connected to wireless fiber optic cables. In the arena of networking, this is a historic event, one that many doubted could ever come to pass. This bears out my longstanding argument that millimeter waves—unused bands at the top of the radio spectrum—could work better than any generation of cellular thus far.

My colleagues and I demonstrated the usage of millimeter waves in Texas and New York in 2011 and 2012.[19] Our demonstrations showed that if you use directional antennas that point the beam in specific directions, you get better coverage for the same bandwidth and the same radiated power. Moreover, you get better coverage and a better signal-to-noise ratio as you go higher in frequency. This is completely counterintuitive, but it proved to be true (neglecting the impact of heavy rain or snow, which can be compensated for with more antennas or power).

In terms of performance, 5G—which uses those high-frequency bands and the existing lower bands—exceeds 4G by several orders of magnitude. With 5G, applications traditionally dependent on cable connectivity will be able to seamlessly function on mobile devices. Think about everything right now that depends on a fiber optic or copper cable connection. Whether it be data-center functions or entire office buildings, 5G allows pretty much everything to be done wirelessly, untethering applications and networks themselves in new ways. 4G launched a wireless renaissance in which everyone (at least in urban markets) uses a cell phone for everyday activities such as banking, communication, and transportation. 5G looks to magnify this renaissance globally, with wireless pervading every part of our lives and new applications we cannot even yet envision.

There is another aspect of the global wireless renaissance that is historic. I believe that 5G can benefit rural and suburban areas that have not enjoyed the same access to wireless as cities. Throughout rural America and the world, there is a lot of aging copper wire that was installed decades ago to support voice transmission. While carriers could replace it with fiber optic cable, from a technical perspective, there is nothing preventing them from replacing it with *in-band backhaul*. Fixed point-to-point links can be easily accommodated by 5G spectrum allocations to daisy-chain base stations and small cells, and to carry traffic back to the internet and public switch networks for rural areas.

For carriers, 5G presents a ripe opportunity to become more valuable to their Fortune 500 clients by getting deeper into enterprise operations. Consider *network slicing*, a relatively new concept in which carriers spin up virtual networks using portions of 5G spectrum for particular users or use cases.[20] Let's say that a factory within a certain geographic area needs a low-latency, high-bandwidth capability to control its mobile robots. A carrier could provide this customer with a dedicated virtual network over the 5G spectrum, but with huge bandwidth pipes and the specific millimeter waves that the government is auctioning off, carriers will also be able to parse out spectrum to enterprises on demand. Moreover, large enterprises—particularly those with campus networks—may soon find millimeter wave products in the marketplace that will enable them to provision connectivity between buildings. Expect these products to quickly become so reliable and easy to install that IT personnel will have control and flexibility as they manage on-site networks. Unlicensed band products will also allow enterprises to install "instant fiber" using on-campus wireless infrastructure.

Opportunity awaits. The time to start thinking about your organisation's networking strategy is now.

RISK IMPLICATIONS

It is a herculean task for future-thinking organisations to comprehend all of the various connected networks, internal boundaries, and interactions with externally connected networks that will be possible moving forward. Already, most enterprise networks are accessed from multiple locations by employees, vendors, customers, partners, and the general public, by a variety of devices connected through different wireless technologies, mesh networks, and IoT sensors, significantly increasing threat vectors and the enterprise attack surface. But though technology has evolved dramatically in the last decade, some organisations protect their networks using the same approach they've always employed. Companies should employ new tactics to ensure ubiquitous security throughout the network, its users, and their connected devices.

- **Build it in.** Homogeneous, firewall-protected networks should be a relic in today's market; as connectivity evolves, networks will likely be a mix of 5G, Long Term Evolution (LTE), software-defined networks, multiprotocol label switching, Wi-Fi, satellite, and more. Additionally, the number and nature of devices ("things") will expand exponentially, resulting in a scope and complexity well beyond what we see today. Building security capabilities to meet the requirements of a single network model or protocol will not suffice, leaving organisations vulnerable through other channels. A solution is to build security controls so that they are embedded, inspected, and enforced at the data, device, and user identity levels.
- **Segmentation.** A large, flat network can allow malicious actors (internal or external) to move freely throughout connected systems if an actor manages to breach the external perimeter or otherwise has access to the network (for example, a "trusted" third party). Segmenting the network at both a broad level—such as separating security and administrative traffic from general user traffic from critical business application traffic—and on the device and workload-level via micro-segmentation is a key tactic in building a secure, resilient environment.
- **Zero-trust networks.** Organisations can benefit tremendously from implementing a zero-trust architecture, one in which every actor and device must be identified and authenticated, whether they appear to be within your walls or outside your network. A zero-trust approach deploys strategies such as identity and access management, multifactor authentication, encryption, risk scoring, and role-based access controls to enforce strict governance policies that allow users to access the bare minimum of applications and resources necessary to complete their tasks.[21]
- **Automation.** Automation of security processes enables an organisation to tolerate some amount of cyber risk due to the speed and agility with which it can respond to potential threats. For example, when a traditional network experiences a breach, engineers must identify that a breach has occurred, determine which segment it affects, disconnect it, and figure out how to fix the problem. If the breach occurs in the cloud or in a software-defined network environment, the fix can be accomplished in just minutes through automation before more damage can be done. Additionally, going forward, AI systems increasingly will be designed to identify breaches in the environment and contain the

Build security controls so that they are embedded, inspected, and enforced at the data, device, and user identity levels.

attack, identify the right fix, and apply it without human intervention.[22]

The upside to future connectivity is in its speed, agility, and increasingly software-driven nature. As networks become faster and grow more dynamic, their speed, flexibility, and resiliency allow their built-in security mechanisms to identify and address potential threats more quickly than ever before. Your organisation will also benefit from relationships with your ecosystem of trusted partners and vendors, who are multiplying your efforts with their own security capabilities and threat identification tools, from the cloud provider with built-in security methods to third-party API providers that are guarding their connection points diligently. Even as they embrace newer technologies and security protocols, organisations will also need to maintain their legacy infrastructure through existing cyber risk processes. As networks become more varied and complex, deliberate automation and orchestration of security and risk processes become considerably more critical.

ARE YOU READY?

As the *connectivity of tomorrow* trend gains momentum, new capabilities to support differentiated, fit-for-purpose networking for devices and applications will become available around the world. What steps can you take to lay the groundwork for new networking models in your enterprise? Step one could involve scenario planning, in which you create models that consider your business and advanced connectivity together. You can then use these models to develop strategic options within a connectivity road map aligned with your company's business strategy.

As part of this planning effort, consider the following questions:

- **In the context of our business strategy, where and how can advanced connectivity create a material impact?**

  These capabilities could be a catalyst within an enterprise to accelerate both information technology and operational technology. Knowledge of these capabilities and potential timing should serve as a key input to shape customer- and internal-facing digital transformation initiatives. Viewed through an alternate lens, digital transformation, enterprise agility, mobility, and cloud technology features such as serverless computing are all dependent on advanced connectivity. However, with advanced capabilities comes higher network complexity in the form of multiple networking protocols, proliferation of devices and device types, and edge computing. Moreover, these capabilities will likely become available and evolve at different speeds across geographies. Taking into consideration your enterprise's business and technology strategy, consider building capabilities that could be transformative to your enterprise, assess potential availability and timing, and develop strategic options and a three-year *connectivity of tomorrow* adoption road map.

- **What impact could advanced networking systems have on my enterprise architecture?**

  As capabilities such as 5G, LEO satellites, SDN, and NFV are advancing, so are compute and storage, significantly affecting enterprise compute infrastructure and data architecture. For example, sensors in the field and telemetry in applications and on mobile devices will generate increasing volumes of data to be stored, analysed, and acted upon. Enterprise architecture must consider the impact of distributed computing—between devices, edge, cloud, and data centers and where, how, and when advanced connectivity will be deployed.

As you develop strategies for connectivity and cloud, both should align with the strategic goals set forth in your digital transformation agenda. How will cloud and connectivity help your enterprise operate more efficiently? How can the ability to deliver and process enormous volumes of data where and when they are needed help your enterprise to more effectively engage customers, business partners, or your global operations? Which specific networking and cloud capabilities, deployed in tandem and managed similarly, might support new product and service offerings?

How will this trend affect my budget?

As the trend gains momentum, user expectations of networking capabilities and performance will rise. Vendors will want to recoup their significant capital investments in new products and services. Competition will likely put downward pressure on prices as technologies become more widely available. As a result, enterprise customers may have to make decisions about the capability/value requirements for advanced connectivity. Prices may be dynamic for some time, requiring enterprises to continually balance user and system demand for advanced connectivity with cost and business value. The likelihood is that CIOs will need to factor ongoing change into their networking strategy for the next several years.

How could the trend affect my IT/networking function?

Advanced connectivity can significantly raise the bar on automation. As automation levels increase, IT's primary responsibility will shift more heavily to engineering and driving the convergence of IT and operational technology. Depending on how far along you are on this path, you may need to make organisational changes to support new operational realities. Likewise, as you adopt configurable networks deployed with SDN and NFV, your connectivity service provider landscape may take on a different profile. Of course, this will depend on which capabilities you source, from where you source them, and how you integrate them into your infrastructure.

BOTTOM LINE

The *connectivity of tomorrow* trend represents a necessary and much-anticipated transformation in the way organisations move business-critical data from where it is generated to where it is needed. Across industries, this transformation will only accelerate as the total number of networked devices grows exponentially. Increasingly, technology and business leaders are recognising that when deployed as part of a well-planned connectivity strategy, building blocks such as 5G, satellites, SDN, and NFV can deliver an order-of-magnitude boost in network flexibility, efficiency, and velocity. What will your strategy be for harnessing the connectivity of tomorrow?

Contact

LUKE BAYLISS
Senior Manager, Technology Consulting
Deloitte MCS Limited
+44 20 7303 5229
lbaylis@deloitte.co.uk

Authors

DAN LITTMAN

Principal, Deloitte Consulting LLP

AJIT PRABHU

Principal, Deloitte Consulting LLP

Risk implications

KIERAN NORTON

Principal, Deloitte LLP

Endnotes

1. Kate Gerwig and Chuck Moozakis, "As 2018 budgets rise, network upgrades become a priority," *2018 TechTarget IT Priorities Survey*, February 2018.
2. Stan Gibson, *2018 State of Infrastructure*, Interop ITX and *InformationWeek*, 2018.
3. Sacha Segan, "What is 5G?", *PC Magazine*, October 2, 2018.
4. *TelecomLead*, "72 mobile operators are testing 5G," February 21, 2018.
5. Paul Lee et al., *Technology, Media, and Telecommunications Predictions 2019,* Deloitte Insights, December 11, 2018.
6. Nathan Hurst, "Why satellite internet is the new space race," *PC Magazine*, July 30, 2018.
7. Patrick Nelson, "Private 5G networks are coming," *Network World*, November 7, 2018.
8. Ibid.
9. Brandon Butler, "What is edge computing and how it's changing the network," *Network World*, September 21, 2017.
10. Input from Jacques Wannenburg, BHP VP of technology enterprise systems, and Paul Karan, BHP manager of security operations.
11. Anmar Frangoul, "How remote control centers are changing the way mining operations are carried out," CNBC, July 4, 2018.
12. Matthew Stevens, "BHP's reverse track on Rio Train robot trains," *Financial Review*, October 15, 2017.
13. Diane Jurgens, "Creating the future of mining—integration and automation," BHP, November 1, 2017.
14. Cruise Lines International Association, "CLIA 2018 cruise industry outlook," December 2017.
15. Interview with Luca Pronzati, MSC Cruises chief business innovation officer, September 28, 2018.
16. MSC Cruises, "MSC Cruises launches fleetwide, game-changing digital innovation program MSC for Me," March 8, 2017.
17. Tony Munoz, "Smarter with Marlink," *Maritime Executive*, April 21, 2018.
18. Ericsson, "Ericsson mobility report: Q2 2018," August 2018.
19. Theodore Rappaport et al., "Millimeter wave mobile communications for 5G cellular: It will work!," *IEEE Access* Vol. 1, May 10, 2013.
20. SDxCentral, "What is 5G network slicing?," accessed December 5, 2018.
21. Jon Oltsik, "Google network security sans perimeter," CSO, May 13, 2015.
22. Nitin Mittal et al., *AI-fuelled organisations*, Deloitte Insights, January 15, 2019.