THE ANTICIPANT ORGANIZATION

New rules for leading in digital
society from the boardroom
and the battlefield

Mark J. Barrenechea
David Fraser
Tom Jenkins

THE ANTICIPANT ORGANIZATION

Mark J. Barrenechea
David Fraser
Tom Jenkins

DEDICATION

We dedicate this book to those we have served with in the worlds of business, military, and government. You taught us how to look ahead.

Mark J. Barrenechea, David Fraser, and Tom Jenkins

Note on the text…

Data: Singular or plural? *In most instances, we use the term data as a singular noun to mean the vast collection of information an organization uses in its work. So we say, "Data **is** the lifeblood of any anticipant organization." When we use data to mean a discrete set of individual items (datum A + datum B etc.), we write it as a plural noun, as in, "AI ethicists will tell you that these data in particular **are** subject to high rates of error."*

Note on the film references…

Why all the Spoiler Alerts? *In a handful of specific spots in the text, we have chosen to emphasize a point by referring to a film that explores the matter. We have deliberately chosen popular movies in the hope that the readers' first-hand experience of viewing them may deepen understanding of the issue at play. While we ourselves are in no way alarmed about the future of artificial intelligence, we appreciate that most of the films we reference delve into the full range of possible outcomes, touching on fears, biases, and assumptions that leaders must avoid. We have selected them precisely for that reason.*

CONTENTS

FROM THE BOARDROOM
TO THE BATTLEFIELD

Imagine, for a moment, how much worse the COVID-19 pandemic would have been without the World Wide Web. With that in mind, think about how difficult information distribution designed to protect public health would have been for generations before us in moments of acute crisis.

During the 1918 flu pandemic, Boy Scouts were dispatched across New York City to distribute printed cards that instructed people not to spit in the streets. Back then, public information campaigns relied on announcements in theatres and posters on streetcars. It was crisis communications in the analog age. Fast forward a century, and we find ourselves wrestling with a crisis on a similar scale, but this time, with a powerful tool in our hands: the World Wide Web. Through its deployment in recent years, the importance of concise, accurate, and immediate communication as invaluable during a global health emergency has been emboldened in our collective consciousness. Without public health information at our fingertips, we would have been dangerously under-informed about the scale and severity of the COVID-19 virus. The web enabled the adaptability of people, with new ways to work, learn, trade, and care for our communities from home.

The evolution of the world that many of us are privileged to inhabit today has happened at lightning speed. Zooming in on the world of business, the web and the internet have disrupted and restructured entire industries. High street staple stores such as HMV and Blockbuster, who were less able to adapt to this new online world of e-commerce, have been replaced with Spotify and Netflix. Like this wave of fast innovation and change, the pandemic also induced demands for companies and retailers to adapt to a new landscape, and fast. In terms of its impact, the economic shocks did not discriminate between industries, with waves felt by big box retailers to oil companies to leading gym franchises. Companies already weakened by endemic issues such as staggering debt were the most vulnerable. Those that could not pivot at least a portion of their businesses to digital were ultimately doomed.

While I believe we all have the power to change the future, history does humanity a favor in reminding us of its cyclical nature. We can be sure that this recent crisis was not the last one. While the web has been re-engineering industries for decades and setting the scene for a more connected world, the COVID-19 pandemic reminded us of core learnings that can be applied in business, and indeed in life: the ability to anticipate and prepare for crises before they happen will determine survival. This book is the handbook for those who wish to define this new era of crisis-conscious, robust, and intelligent leadership.

The Anticipant Organization is a survival manual for those who are tasked with leading their organizations from analog to digital. This book outlines an approach that will equip you and your organization with the toolkit to manage your way through a nanocrisis. As Winston Churchill said, "If you are going through hell, keep going." However, I believe that this book will empower you to minimize the scale and impacts of such a potentially fatal phase in your organization's journey.

Authors Mark J. Barrenechea, David Fraser, and Tom Jenkins are pioneers in their fields. Hailing from Silicon Valley and a computer programmer at heart, Mark has transformed software companies into global leaders in information management. Dave is a soldier who began his career as an infantryman and rose to command military forces from 26 nations during the Afghanistan War. Tom is an entrepreneur who built a high-tech company that was responsible for creating one of the internet's first search engines. Though their backgrounds vary, what each brings forth shares a common thread: survival in both the boardroom and on the battlefield. In their book, they share their valuable hard-fought lessons with the next generation of leaders.

Our shared global experience through a global pandemic has made it abundantly clear that the web is not a luxury—it is a lifeline. The authors offer readers another lifeline that will enable us all to learn and prepare for a future crisis, in whatever form it may take.

Tim Berners-Lee
INVENTOR OF THE WORLD WIDE WEB

NEW TERMS

The pivot

The technology-driven transition of civilization from analog to digital interaction, particularly spurred by and evident in innovations launched in the decade between 2000 and 2010.

Anticipant

An entity committed to readying itself for effective action by identifying likely events, conceiving appropriate responses, and rehearsing them in advance of any occurrence.

Nanocrisis

A predicament or calamity whose origins lie in the dependence of an organization on a digital system, and whose speed and scale preclude immediate mitigation by humans.

Suprahuman

Literally "beyond human," a term for the domain in which machines talk to each other by means of electronic or photonic pulses (bits and bytes), which move at or close to the speed of light. This domain is the first rarified environment created by humans in which humans do not and cannot exist.

Nanospace

The suprahuman domain in which machines exchange data in the course of their operations.

Human-Machine Relations

An emerging discipline with the goal of improving the interactions between humans and machines to optimize the outcomes of their collaboration.
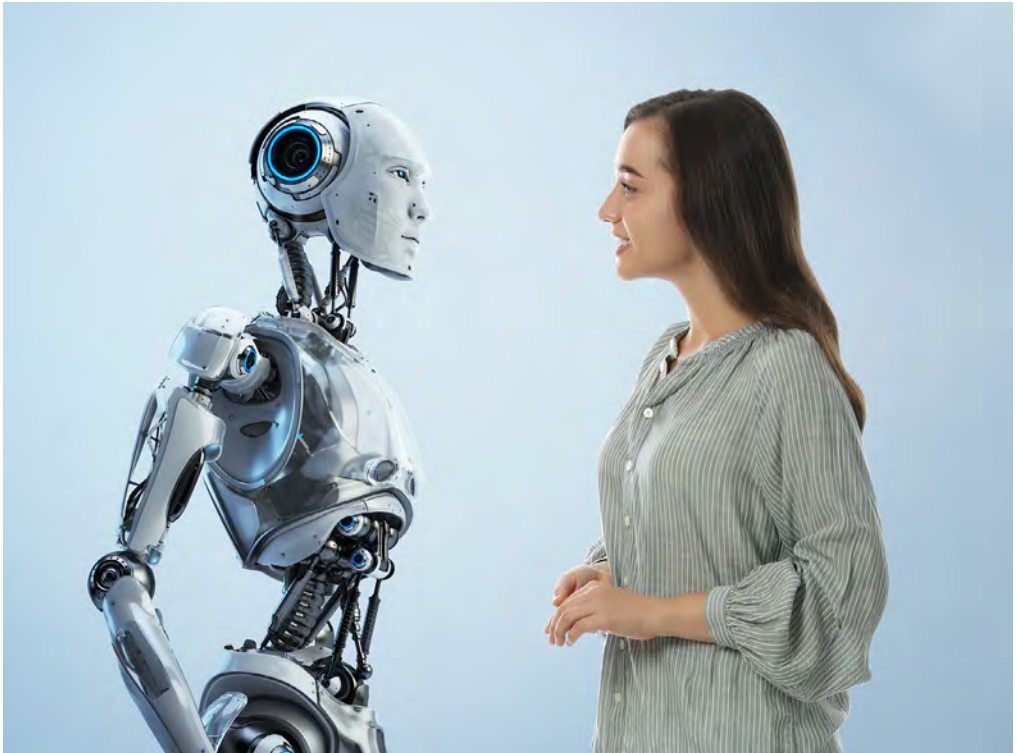
May I bend your ear for a nanosecond?

THE DIGITAL PIVOT

The pivot from analog to digital changed everything, including the way we work, play, communicate, create, learn, lead, and apparently, (according to the image below), even the way we appreciate art.

Image by Freepik and Unsplash

Figure 1.1: Those of us who were "born digital" missed the pivot.

It forced us to redefine ourselves and the way we interact as citizens, business professionals, soldiers, retailers, educators, politicians, volunteers, and even as families. Most of these changes are recent. Yet, they are a tiny fraction of the behavioral changes that we now find ourselves forced to adopt. If we fail to change as individuals, we might find ourselves less connected or less employable. But as business leaders, a failure to pivot to digital will make us irrelevant to those we serve.

Anyone born before 1970 saw these technological changes vividly as they arrived. Our world was comfortably (though often inconveniently) analog. Some of us (authors included) once typed on paper. We had large collections of printed vinyl music albums (and still do, somewhere). We shopped at malls and ordered goods from printed catalogues. We subscribed to magazines. We mailed handwritten cheques to pay paper bills and kept the receipts in envelopes until tax time. We recorded telephone messages on cassette tape. We had only one TV screen per household (with an actual tube behind it), watched the news at one particular time of day, sat through thirty-minute infomercials, and had to stand up to change the channel, of which there were only three. On vacation, we traveled to places, not experiences, and we stayed at actual hotels, not other people's spare rooms.

Figure 1.2: Before the pivot from analog to digital, time moved slower. Experience took precedence over ingenuity, with salary as dependent on length of service as on merit.

In the workplace, we belonged to hierarchical organizations, confident that our managers and senior officers knew our jobs better than we did. We valued face-to-face meetings as the best mode of communication, with telephone conversation the next best thing when distance was involved. We were motivated by promotion, worked our way up the chain of command, and deferred to senior members of staff. We appreciated great work but rarely thanked anyone publicly for doing it, at least until formal recognition programs came into vogue. We set down complex matters in carefully crafted and much edited business letters. We made five-year plans to accommodate product cycles. When computers arrived, we installed machines dedicated to word processing, bought software in boxes, and stored our data on reels of magnetic tape and floppy disks. Eventually, we latched onto email through AOL.

These examples highlight a handful of the hundreds of thousands of changes made in our human journey from an analog to a digital civilization. Similar changes can be found in every domain, discipline, and demographic. Together they comprise a new paradigm of communication, computation, and execution that has been difficult to comprehend let alone embrace. Only one reality is certain: These changes have left leaders reeling. This is because their stable work environments have become relentlessly dynamic. Connections with stakeholders that were made *as required* are now expected to be constant. Today's loyal customers require a powerful sense of affinity to stay interested. Interest groups that once informed and inspired have been eclipsed by online echo chambers that validate and sway the public. There was a time when leaders consumed information by reports and presentations; now they livestream events even as they unfold. Sage advice was given by trusted advisors; leaders today rely on artificial intelligence for suprahuman insight. The analog organizations of old were hierarchical; now they must flatten to survive a crisis. But most importantly for leaders: Once their organizations were active participants in their fields; today they must also be visionary anticipants. And those who cannot anticipate will wither and die.

The fastest pivot yet.

The revolution that put these changes into play began and ended within a single, technologically explosive period from 2000 to 2010. This was a decade that sent the great mass of human society crashing out of the analog age into the digital. By all measures of economic and social impact, that transition has been the greatest and fastest of any pivot in history.

As with every high-impact swivel in our past, the transition from analog to digital was propelled by technological innovation that quickly made it useful for humans to do things in new ways. While the downsides of each change have been many, the advantages clearly outweighed the drawbacks, and so we marched forward.

1946	2000	2007
ENIAC	**Blackberry 957**	**iPhone**
Size: 24 x 30 meters	Size: 117 x 78.5 mm	Size: 115 x 61 mm
Weight: 30 tonnes	Weight: 136 grams	Weight: 135 grams
Power draw: 150 kw	Power draw: 4 kw	Power draw: 1 kw
RAM: 80 bytes	RAM: 512 kilobytes	RAM: 128 megabytes
Cost: $500,000 USD	Cost: $499 USD	Cost: $499 USD
Units sold: 1	**Units sold: 165,000***	**Units sold: 1.39 million***

*Approx. total, first year after release.

Figure 1.3: The Pivot to Always-On, Always-Connected

Shifts in understanding and improvements in processes happen all the time—usually locally and incrementally—but in a few instances, they have occurred globally and unstoppably. A handful of these technological innovations have irrevocably altered the general behavior of our species. The speed of their adoption correlates directly to the available means of communication at the time. It took millennia for agriculture to catch on when word-of-mouth was the chief means of passing news along, yet only 30 years for computing to sweep the globe. As the rate of communication has accelerated, so too has the rate of disruption of these large-scale revolutions. Consider the decreasing gestation periods of these six great epochs:

Pivot	Era	Duration	Dominant Innovation
Neolithic	10,000 BCE	10,000 years	Agriculture
Scientific	1440 $\longrightarrow$	200 years	Printing
Industrial	1760 $\longrightarrow$	100 years	Steam power
Information	1940 $\longrightarrow$	30 years	Computer
Digital	**2000 $\longrightarrow$**	**10 years**	**Smartphone**
Singularity	?	?	Quantum computing

Figure 1.4: Major Technological Pivots

The pivot begins...

The digital pivot took only ten years to execute. The events that mark the beginning and the end of that pivot are well identified. All innovations that came before merely broke the ground for what was about to happen next. Those made since have simply been applications of the root technologies that burst onto the world stage in that short time.

The opening event happened on April 23, 2000. The Canadian tech company Research In Motion (RIM) held a launch party to unveil a breakthrough. Hot on the heels of their success with their Blackberry 850 two-way pager the year before, they found a way to integrate a phone running on a separate network within the same box. Dubbed the Blackberry® 957, their new device made it possible for the first time to have mobile, two-way data and voice. They had invented the smartphone, the device that beyond all others would prove the revolutionary impact of the convergence of telecommunications and computing.[1]

The smartphone elevated every user from the status of *isolated individual* to the *always-on*, *always-connected node* in an exploding global information network. Its rapid acceptance brought about swift changes in the way people interact, both with each other and with their organizations. In a few short months, a teenager could access more information and more computing power than the president of the United States. A decade later in 2010, and despite the release of the highly publicized iPhone® three years earlier, RIM still owned 40 percent of the U.S. smartphone market, making it possible for anyone to put the equivalent of a trillion times the data stored in the Library of Congress into a shirt pocket.[2]

All these devices were talking to each other. At first, they just shared data, but soon, they were sharing processing muscle too. Up to that point, manufacturers of both industrial and home computers had been chasing the ever-increasing expectations of computational speed and storage capacity. With the smartphone, however, the true era of distributed computing was finally at hand. Why try to build more massive machines when a vast array of less-powerful-but-connected machines could share the work?

One of the first distributed applications was launched by the SETI Institute at the University of California, Berkeley, a not-for-profit organization designed to search for extraterrestrial intelligence by analyzing radio signals from space. By inviting people to share the power of their home computers and smartphones, the SETI@home project became the first highly visible application of distributed computing in a non-commercial domain.[3] By June of 2009, the project had rallied more than 180,000 active participants on some 290,000 computers and smartphones with an average computational power of 617 teraflops, more than that of IBM Blue Gene/L, the world's fastest supercomputer.[4]

...and human control ends.

The closing moment of the digital pivot happened within the quarter-hour span from 2:45 to 3:00 p.m. on May 6, 2010. The focus of the event was the New York Stock Exchange (NYSE), but its location, tellingly, was nanospace—a kind of cyberspace where only machines communicate. Unlike cyberspace, which is an interface between humans and machines, nanospace is the one domain designed by humans where humans cannot go.

Figure 1.5: The 2010 "Flash Crash"[5]

High-frequency trading (HFT) had become the norm. It was based on dedicated machines doggedly pursuing nothing but the objectives set down in their individual algorithms. They often won the day because they could transact millions of times faster than even the most nimble human trader. But at 2:45 p.m. on May 6, a group of those nanosecond robot trading machines decided that the market was plummeting and risked bottoming out at zero. So, they followed it down. More to the point, they pushed it down. Within a few minutes, they sunk the market by 9.2%, taking some $1 trillion in capitalization out of a vast swath of publicly traded companies.[6]

In 218 consecutive years of operation at the NYSE, no one had ever seen such a rapid, steep drop. To stunned onlookers, the erratic behavior of stock prices was incomprehensible, and not just because value was tanking. Strange things were happening everywhere. The stocks of each of eight companies in the S&P 500 fell briefly to one cent per share, while others shot up to $100,000 per share in the same period. One stock—Procter & Gamble—dropped almost 37% in minutes, and then mysteriously bounced right back up.[7] Nothing made sense, but one thing was certain: humans were not in control. The robots were running the show.

Well, kind of. The robots were in fact executing the orders of their programmers: high-frequency traders with more enthusiasm than ethics, who wanted to take advantage of loopholes in securities regulations to manipulate the markets. They did so in three clever and underhanded ways. By *spoofing*, they commanded their robots to watch the bids of other traders, then outpaced them on the way to any transaction, making unfair profit on the way. By *layering*, they had their robots make and then cancel orders for no reason other than to manipulate the stock price in the direction that suited their masters best. And by *frontrunning*, they capitalized on unpublic knowledge of a pending transaction so big that it would influence the price of a security. So yes, humans were behind the so-called Flash Crash. Those three (now illegal) strategies had been built into the offending algorithms by devious humans, but it was their robots that drove the frenetic, unstoppable speed and scale with which those tricks were played, and they did so in a domain humans could not see.[8]

The Flash Crash was carried out by a group of machines that could talk to each other one million times faster than humans can. They sent the markets into their worst tailspin in history. Together, humans and machines in the financial industry had been using new tools but no rules. Governance had not kept pace with capability, as the world had seen in the 2007- 08 crash only two years prior. Rules are needed in every discipline where AI operates, including defense (lethal autonomous weapons), transportation (passenger death in driverless cars), and security (CCTV and face recognition). In some fields, new rules are being carefully written and mandated, including medicine (genomics) and energy (nuclear safety).

Sorry Dave, it's a nanocrisis.

As you would expect, when the markets tanked on that afternoon of May 6, 2010, the humans needed to figure out how to respond. No one anticipated this event or anything like it, and there were no crisis protocols in place to deal with it. In retrospect, the trading community itself failed to make the pivot from analog to digital. While they had zealously embraced the tools of the digital age, they didn't foresee that their own operations had moved from human-to-human to machine-to-machine (M2M) communication. Decisions were being made in a domain that was inaccessible and, it seems, inhospitable to humans. That secret space was hiding more than its routine processes from the chain of command; it was masking the intentions of a few dishonest perpetrators who had rigged the machines to generate illicit profits.

When the market crashed in the world's first widespread nanocrisis, those confused humans looking on had no idea how to handle the situation. Even as it began, events were already beyond their control. They were in meltdown. As though taking a cue from *2001: A Space Odyssey*, the humans scrambled to shut the system down. That clunky response, known now in the trade by the codeword *circuit breaking*, was all they could conceive of in those tense few minutes they had to save much of the world's economy.

So, between the arrival of always-on connectivity with the smartphone in 2000 and the proof in 2010 that machines can operate in a domain and at a pace that humans can't control in real time, the pivot was complete. It is no understatement to declare that society will never be the same. And because all leaders today must manage in the digital world, it is critical to know exactly what has changed and what it means in the new hybrid world of human-machine management.

In our view this is now every leader's most pressing challenge. Those among us hoping to apply legacy management practices to ensure the success of our organizations will fail. Indeed, they are failing as we write this, because their organizations are already slipping rudderless into irrelevance. The only certain strategy is for all leaders to guide their organizations through a deliberate transformation akin to that experienced by the broader society. If not, the value of that enterprise will evaporate, and the organization itself will suffer a slow, justified death. At best, it will be eclipsed by disruptive entities whose post-pivot approaches allow them to meet the emerging needs of their connected constituents. At worst, they will be taken down as one after another nanocrisis demolishes their vulnerable systems.

TOM: *The pivot from search engines* – *In the tech industry, change is a constant and those organizations that don't stay up to date are destined to fail. There is a saying in tech that "Only the paranoid survive," and this refers to the constant vigilance required because the timing of events is accelerated and there is very little time to react. The nanoworld does not permit a reaction time, and so everything must be anticipated in advance. In 1998, OpenText was in the business of internet search when a small startup called Google came along. If we didn't anticipate their sweep of the market and make the pivot to business-to-business (B2B) applications instead of search engines, OpenText might not be around today. Instead of going head-to-head with Google, we changed direction in the nick of time. We were able to repurpose our resources, money, and the technologies we had built for a different kind of application in a different kind of market. This pivot was the right decision. This became apparent, though not right away. OpenText eventually grew into its new business, making acquisitions to fill gaps in products, services, industry expertise, and the rest, as they say, is history. Today, OpenText is one of the largest software and cloud companies in the world. It never left its home, the humble locations of its beginnings in Waterloo, Canada. Its headquarters are just a few steps away from where its first internet search product, the OpenText Index, was created in 1995. TJ*

MARK: *Connecting at lightspeed* – *When I started in computing, I was 20 years old. When I built my very first network, I had to use small T-bone connectors to put in the required PCI cards (the interfaces that connect hardware to the computer). I was constantly rolling all over the place trying to attach them—on the floor, in dust, behind desks. I was covered in cobwebs! My state-of-the-art computing tool was a little screwdriver, and if one card went down, so did the whole network. That was 1986. By 2002—only a decade and a half later—things had already changed radically as a result of the digital pivot. I was writing about how the total integration of software functions into e-business suites would transform the business landscape, enabling employees anywhere in the world to access reliable business data, and transform marketing into electronic selling. Today, the global pandemic has accelerated digitalization. The world got comfortable with e-commerce, remote work, telemedicine, and online socializing overnight. Companies across industries rely on automation, artificial intelligence, and electronic tools to gather vast amounts of data, and leverage this data to make decisions—fast—so they can respond to crises and build a competitive advantage. Take away digital tools and the world comes to a grinding halt. My little network in 1986 delivered one megabit per hour. Now, with 5G, we are predicting that we will have speeds of up to 10 gigabytes per second. In just 34 years, we've gone from connections that are incredibly laborious to connection anytime, anywhere. And at lightspeed. MJB*

DAVE: *On leadership, not technology* – *This is a book about leadership, not technology. Looking back, both Tom and I were trained and tested in a world of analog systems. We were thrust into the digital domain in the late 1980s. Everything accelerated to "web time" and we became hybrid leaders. We had to learn fast, through trial and error. In the process, we figured out which analog precepts we could apply to a digital world, and what we had to leave behind. Looking ahead, Mark J. Barrenechea's experience as a leader differs to ours and his contributions to this book illustrate how. As CEO and CTO of OpenText, Mark led his organization through the 2020 COVID-19 pandemic. I like to compare his leadership to a grounding wire. Mark directed his organization's operations under dire circumstances as the pandemic forced him to pivot to survive. Though the pandemic is not exactly the kind of nanocrisis we are describing in this book, it works as a baseline example of the unexpected. It's proof that the coming nanocrisis can and will happen. DF*
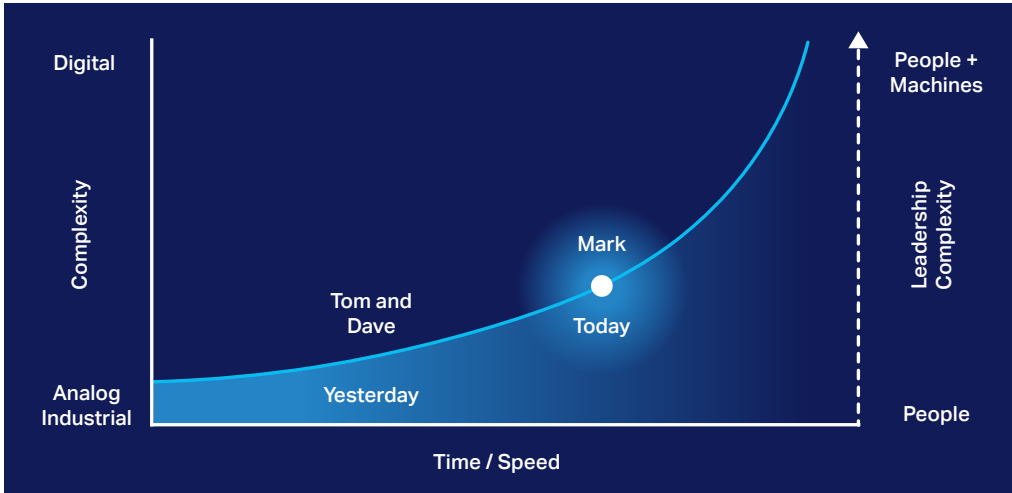
Figure 1.6: Here we are on the leadership trajectory from analog to digital competency. Both Tom and Dave are looking back, while Mark is looking forward, to the future.

Were we just being hacked?

THE COMING NANOCRISIS

Take a moment to scan this excerpt from an article by writers Molly Hennessy-Fiske and Suhauna Hussain that appeared in the *Los Angeles Times* on August 20, 2019.

> *KEENE, Texas—When a ransomware attack hit Keene, Texas, no one noticed. Like many small Texas cities, Keene—an exurb about 40 miles south of Fort Worth with a population of about 6,500—contracted its technology services to an out-of-town company, including management of its computer servers. The city had never been hit with something like this before. So when Landis Adams and other city employees showed up as usual at 8 a.m. Friday, turned on their computers and saw a mess of text, they figured the servers were down. But when city officials contacted the company that manages their server, they learned they were among several cities experiencing problems. The computer systems of more than 20 small Texas municipalities were paralyzed in a coordinated cyberattack. "We're not prepared for something like that—most cities in America are not," Adams, the city spokesman and economic development director, said Tuesday.[9]*

The city of Keene, Texas had been hit by a classic nanocrisis, and no one was ready for it. Unusual? Far from it.

> *Ransomware attacks have been on the rise since they burst on the scene around 2012. In 2016, Hollywood Presbyterian Medical Center was hit with an attack. Devices and medical records were locked until the hospital paid $17,000 in bitcoin. In May 2017, the WannaCry ransomware infected about 200,000 computers across 150 countries. The attack also crippled the United Kingdom's National Health Service and the networks of companies such as Boeing and Honda. Similar attacks hit the Port of Long Beach in July and the Port of San Diego in September. Recent attacks hit Albany, N.Y., Greenville, N.C., Baltimore, and three Florida cities. In July, ransomware infected Georgia's court system and state and Capitol police.*

> *"It's easy to perpetrate a ransomware attack," said Maya Levine, a Check Point security engineer. "You can buy fully weaponized ransomware malware on the dark web for twenty dollars. All you have to do is email it out." Often computer systems are infected through these phishing schemes—fake email attachments that appear legitimate but contain malicious code. "Scammers don't discriminate," said FBI spokeswoman Laura Eimiller. "Everyone is vulnerable including hospitals, school districts, private companies, and individuals."[10]*

Everyone is vulnerable, as the FBI spokesperson put it, but few are doing anything about it. One reason for inaction, perhaps, is our assumption that security experts will eventually arrive at the ultimate, hack-proof system. One that can't be compromised because it rides on a new technology that is impervious to assault. With all the hype about blockchain and quantum computing, won't that time come soon? And until then, can't we hope that our technology providers will be vigilant and ensure that our systems are routinely fortified with virus detection and speedy security updates?

The answer to both questions is no, and here's why. When efforts to infiltrate, compromise, mimic, exploit, weaken, and disable digital systems are combined with counter efforts, the result is a high-stakes battle with colossal consequences. For the attacker, the connected, digital world is a beckoning network of countless treasure houses of exploitable data, wealth, and power. For the defender, digital dependence is now so pervasive that some likely scenarios, drawn to their logical conclusions, end in the demise of the organization. So no belligerent can resist an opportunity to devise a new way to gain the digital advantage, and no organization can afford to lose that advantage.

MARK: *Digital Defenders* – *The speed and ferocity of cyberattacks is escalating every day. Cybercriminals even exploited the global pandemic, devising new COVID-related phishing sites and taking advantage of employee devices running on home networks with fewer security measures. From January to May 2020, 2% of new sites with "COVID" or "coronavirus" as part of the name were malicious—nearly 20,000 sites.[11] (I am convinced that there is a special place in hell for the people behind such tactics). Across 2021, breaches continued to surge, with massive ransomware attacks, like the one launched on Colonial Pipeline, or the attacks on trusted software, including SolarWinds, Log4j, and Kaseya. The latter resulted in one of the largest ransom demands ever, for $70 million![12]*

Businesses globally need to be aware that a breach is inevitable. If you have not been hacked, it is only a matter of time. Yet, we need to be able to trust locations (URLs) as we— and our employees—browse the internet. During the digital pivot, the internet transformed from a useful tool to a bedrock of society. It has become necessary for businesses and governments to function. Banish the internet, banish the world. So, how do we anticipate, defend, and protect the entire World Wide Web? How can organizations become cybersecurity anticipants, so a nanocrisis does not catch them off guard?

It is beyond human capacity to control, predict, and respond to every single cybersecurity threat. To protect users in the increasingly suprahuman cybersecurity landscape, the anticipant organization must employ intelligent machines that can conduct up-to-the-moment analysis of vast oceans of data and effectively act on the insights they uncover. AI alone can accomplish this feat. Machine learning can crawl and evaluate URLs in milliseconds based on hundreds of site attributes and external factors. This real-time validation is the only truly effective protection. MJB

In the military, an escalating sequence of tactics to either launch or impede an attack through the technologies on the electromagnetic spectrum goes by the name of *electronic warfare*, or EW. Beyond the endless variations of EW equipment, there are EW operators and EW stations aboard warships, in aircraft, and in land vehicles. There are EW degree programs in warfare schools and in civilian universities. One can attend EW symposia and join amateur EW clubs. All militaries work endlessly to excel at EW, because failure to do so can bring a quick sentence of death. But as defense funding waxes and wanes, the tide of EW research flows and ebbs. Advantage is won and lost in a never-ending cycle. Such is the nature of nanocrisis.

Figure 2.1: Zinovy 'Mad Dog' Rozhestvensky, Admiral in the Russian Imperial Navy and unwitting grand-father of the nanocrisis.

It's been that way since the morning of May 27, 1905, when the discipline of electronic warfare was born. The incident has immediate relevance to our situation today. At the time, Russia and Japan were in the midst of an eighteen-month dispute over the territories of Korea and Manchuria. On the night of May 26 - 27, the Japanese armed merchant cruiser *Shinano Maru* was steaming overnight through Tsushima Strait, the passage between Korea to the north and Japan to the south.[13]

The Japanese had anticipated Russian naval activity in the area but had not encountered any enemy ships. Importantly, both fleets were equipped with shipboard radio, an innovation under two years old, and the stealthy Russians knew enough to keep strict radio silence. Just before 3 a.m. on May 27, lookouts on the *Shinano Maru* thought they had sighted a Russian warship. The Japanese captain quickly concluded that if this were so, other units of the Baltic fleet would likely be close by. His radio operators immediately began transmitting the enemy position to the larger Japanese fleet.[14] And the Japanese were right. The ship they spotted was the Russian hospital ship *Orel*, aboard which Russian radiomen easily detected the outgoing Japanese signal. They informed their captain, who made a novel tactical suggestion to the Baltic fleet admiral, Zinovy Rozhestvensky. The captain advised that by making a far more powerful transmission on the same frequency, the Russians could confuse the Japanese signal. While they couldn't jam it, they could render it unintelligible. Admiral Rozhestvensky (known behind his back as *Mad Dog*) faced a critical decision. Would he intervene or ignore the threat? Tough call. By allowing radio transmission, he might confuse the Japanese signal, but perhaps only temporarily. And by doing so, he might alert other Japanese warships to his presence. Moreover, the latitude and longitude sent by *Shinano Maru* might not matter if the Russian fleet moved position

quickly. He had other options as well. He could attack *Shinano Maru* and destroy at least one element of the opposing force. He could radically change course to evade any pursuers, or continue on course, hoping that his naval superiority would dominate when the eventual battle began.

In short, Rozhestvensky could reduce the threat directly with an opposing technological action, mitigate the threat by other actions, or ignore the threat altogether. These are the three choices faced daily by every leader of every organization in the age of the nanocrisis. In our historical example, Mad Dog decided to ignore the threat and gave the command to continue radio silence.[15] It would be the worst decision of his career.

The Japanese fleet came out in force and in the ensuing Battle of Tsushima, only four of the Russian ships escaped. Their forces suffered the deaths of more than 4,000 Russian sailors and an additional 6,000 injured. The Japanese lost only three torpedo boats and 117 sailors.[16] A year later, when the Japanese-Russian War ended in decisive Russian defeat, Japan began its rise as the pre-eminent power in East Asia. Russia descended into economic and social turmoil that would contribute to the Russian revolution a decade later. It is impossible to assess the degree to which one leader's refusal to address an electronic threat contributed to the loss of a battle, a war, and an empire, but in military academies around the world, there is no doubt that on the evening of May 26, 1905, electronic warfare erupted, and EW countermeasures became an indispensable component of the art of war.[17]

In the age of the always-on, interconnected digital world, EW is exactly the subject that leaders must study and master. It just goes by a different name now: *cyber*. As with any form of EW, cyber threats are most often the result of perverse human intent and action. They are not the result of rogue AI entities inflicting damage to achieve narrow, literal objectives or even more outlandishly, their vaulting anthropomorphic ambitions. These are the fancies of films such as *2001: A Space Odyssey, Terminator, Minority Report* and television series including *Battlestar Galactica*, from which we have much to learn, but the lessons are wholly metaphoric.

The coming nanocrisis, however, is not science fiction; it's real and it's on the horizon. During the COVID-19 pandemic, many of us felt like we were starring in a science fiction movie. And while the coming nanocrisis will be as unexpected as the pandemic, it will be significantly different because it will be far worse. So much so, that it is dangerously inconceivable (which is why we wrote this book). Imagine if the world went dark and there were no internet. Consider the fallout, the repercussions, the overall impact that would have on your organization. Then multiply that by one hundred—the coming nanocrisis will be even more devastating, more destructive than that. And faster. The pandemic is illustrative because of its massive impact on human life, organizations, and the economies of the world. It spread fast but it unfolded at a snail's pace compared to how a nanocrisis will hit.

Spoiler Alert:

Minority Report

Based on a short story by Philip K. Dick (of *Blade Runner* fame), *Minority Report* is Stephen Spielberg's 2002 neo-noir exploration of a world in which criminal intent can be sensed and prosecuted even before a crime is committed, with the privacy rights of individual citizens abandoned in the interest of the greater societal good. Among the film's far-reaching concepts, the use of swarming drones for surveillance and interdiction of criminals is central to the action. Released just two years into the digital pivot, the movie was not so farfetched. By the end of the pivot in 2010, crime-prediction software was running in the real world. Drones could be dropped from aircraft, swarm into position, and use facial recognition and self-detonation to prosecute individual targets with pinpoint accuracy, much as spider robots did in the film. The use of precision-strike drones has been decried by groups such as the Future of Life Institute (FLI, futureoflife.org/), on whose board serve activist celebrities such as Alan Alda, Morgan Freeman, and the late Stephen Hawking. FLI's mandate includes finding *"positive ways for humanity to steer its own course considering new technologies and challenges."*[18]

TOM: *The COVID-19 pandemic as a forcing function* *– We can't talk about a crisis without referencing the coronavirus pandemic in 2020. As many have noted, it forced society to pivot to digital en masse. Akin to an asteroid hitting the world, after which only some species survive, it had a Darwinian effect on business. The global shutdown exposed deeper problems in organizations that were already struggling. As they scrambled to shift their business models to serve online consumers, companies were forced to deal with unforeseen inventory and liquidity issues. Once the fault lines were exposed, a tidal wave of bankruptcies followed. Household names like Hertz, J. Crew, Bath & Body Works, Gold's Gym, JC Penny, Neiman Marcus, LATAM Airlines, Virgin Australia, Cirque du Soleil, Wendy's, and Pizza Hut announced the closing of hundreds of locations and the loss of thousands of jobs. But the pandemic's timeline was biological, and the world had time to react. Taken in context of the nanocrises that we're discussing in this book, it's like comparing a slow train wreck to the crash of a super-sonic jet. With a nanocrisis, the scale and speed will be accelerated. And if you're going to survive, your organization better be resilient. TJ*

The real threat today is the access that malefactors have to digital technologies that operate at different speeds, on different scales, and in a different domain than humans can or do. That gives perpetrators countless, ingenious ways to make their assaults. When you learn that hackers in 2018 were able to access and steal over 10 gigabytes of private data from a Las Vegas casino by entering its systems though a smart thermometer in just one fish tank, you know the game has changed.[19] The new nano-advantage can have greater impact than any previous threat, even though

a nanocrisis may not kill as many people as all-out war. The key word in that last sentence is '*may*.' Hostile military use of lethal autonomous weapons could soon make us see that issue with new seriousness. In our opinion, leaders have a pressing duty to decide how to respond to cyber threats.

Such threats are different in the non-military and military arenas, but not as markedly different as they once were. Cyber threat, like electronic warfare, is a never ending upward spiral of destructive innovation. And though many breaches happen from the inside out, involving either employees as bad actors or oversight on the part of users, it remains important to prepare for these instances. We have grouped them into general types of nanocrises (see below). Before we discuss these, let's look at some specific examples of nanocrises.

Nanocrisis Study

Blockbuster vs Netflix

In the early 2000s, Blockbuster was the leader in the video rental industry. A decade later, the company filed for bankruptcy. During this time, when Blockbuster was anxiously defending the success of its expensive and widespread retail operations, Netflix did something very different. Through a willful cannibalization of its own mail-order movie business, Netflix made a big bet on fledgling technology: Online streaming. Netflix took this risk when available bandwidth meant that it took almost half an hour—sometimes more—to download a movie. Though the rules of the marketplace seemed well established, and consumers were used to browsing through physical shelves of DVDs, Netflix showed the ultimate foresight. The company pivoted and discovered a market of the future. Through this anticipation, Netflix not only sidestepped its biggest competitor, but it also capitalized on that competitor's complacency and failure to anticipate.

As this example demonstrates, disrupting your business to pivot entails envisioning your own irrelevance as an opportunity. The chance to look ahead—to anticipate— and act is the greatest gift any organization or leader can receive. Blockbuster was participating in a market of the past and planning for a world based on the now. Netflix was anticipating the ways in which new technology would make the now disappear. Blockbuster's inability to keep pace and scale accordingly in the face of a new threat meant that the race was won before it began.[20] There is now only one Blockbuster store left in the world, in Bend, Oregon. And Netflix's valuation has soared to over a hundred billion.[21]

Nanocrisis Study

Cambridge Analytica and Facebook

Even post-pivot organizations are not immune to a nanocrisis. The largest, most powerful companies need to be capable of anticipating the next threat to their business models, brands, or existence. If they fail to anticipate, they can't prepare for these crises or respond appropriately when they occur. This lack of immunity was proven following the Cambridge Analytica scandal. The (now notorious) data firm harvested the personal information of millions of Facebook® users without consent for use in political advertising. The scandal embroiled Facebook in a public-relations nightmare.

The story was first reported in *The Guardian* in 2015, but everything came to a head in March 2018 when a whistle-blower and former Cambridge Analytica employee came forward. In just days, more than $100 billion was knocked off Facebook's market capitalization as politicians in the U.S. and U.K. called for answers from CEO Mark Zuckerberg, who eventually testified in front of the United States Congress.[22] Shortly after the scandal erupted, Microsoft founder Bill Gates weighed in. In doing so, he addressed the new level of scrutiny—and regulation—Facebook had invited upon itself by not anticipating the implications of the company's own scale coupled with sloppy data management. *"We're seeing as this technology becomes so pervasive—even a key tool of communication—there's a lot of regulatory issues that are having to be developed,"* said Gates. *"Europe's got a new set of regulations. Companies are going to adhere to those and I'm sure they're going to have to evolve."*[23]

The scandal dramatically reduced user trust in Facebook, due to concerns over personal data and privacy.[24] The scandal also recast public understanding and expectations surrounding the protection of personal data. Finally, but most notably, the scandal placed the company in a state of retroactive response after it failed to anticipate the implications of its own technology.

Nanocrisis Study

WikiLeaks and Cablegate

Founded in 2006 by Julian Assange, WikiLeaks is an international, non-profit organization that publishes submissions from anonymous whistleblowers. At certain points, the information it has leaked into the public domain has compromised U.S. intelligence, security, and even human lives.

In November of 2010, WikiLeaks began releasing classified cables sent to the U.S. State Department by hundreds of global consultants, embassies, and diplomatic missions. Known as "Cablegate," over 200,000 cables were sent as the largest set of confidential records ever released to the public domain. A threat to American national security, they contained the diplomatic analysis of countries and their officials. In the high-profile case that followed, Chelsea Manning was convicted of theft in violation of the Espionage Act and sentenced to 35 years in prison in August 2013.[25]

Since that time, numerous leaks have surpassed the amount of information published in Cablegate. Perhaps one of the most disturbing breaches happened in 2016 when the CIA's own secret hacking tools were stolen from one of their high-security networks. As much as 34 terabytes of data was taken, or the equivalent to 2.2 billion pages of text. In 2017, WikiLeaks published details of the top-secret CIA hacking tools (in essence, their cyber weaponry), suggesting that the CIA was in the middle of a global hacking operation, breaking into people's phones and televisions to spy on them. The leak was the biggest CIA data loss in history, and the result of "woefully lax" security practices. The CIA declined to comment on a report made following the incident, with an agency spokesperson stating that the *"CIA works to incorporate best-in-class technologies to keep ahead of and defend against ever-evolving threats."*[26]

Spoiler Alert:
Eagle Eye

Critical of the loss of individual freedoms in a world where the wholesale appropriation of personal data is common, D. J. Caruso's *Eagle Eye* took over a decade to make. Based on a story by Isaac Asimov, the plot conceived by Steven Spielberg was considered too farfetched at first, and producers worried that audiences would not understand the threat of deep data mining. The film was finally released in 2008 during the digital pivot, at which point, as the director said, *"the technology had finally caught up to the storytelling... everybody [had] a BlackBerry on their belt, and we [thought] we were constantly being tracked."*[27] *Eagle Eye* presaged the emerging need for AI ethicists in our own time to build human morals into machine-based decision making.

Nanocrisis Study

Cyberattacks on COVID-19 research centers

Nation-state hackers have been known to target government agencies, critical infrastructure, and industries that house sensitive data or property. Of all the state-sponsored attacks, the worst is the loss of intellectual property (IP). Compromise of an organization's IP can seriously incapacitate a business with effects that might last for decades. Stolen software, patents, and trade secrets often end up costing national economies billions of dollars.

In July of 2020, the U.K. National Cyber Security Centre (NCSC) detailed activity by the Russian hacking group APT29 that targeted U.S., U.K., and Canadian organizations. The goal of their malicious activity? To steal IP related to COVID-19 vaccine research and development. In the attacks, APT29 used a variety of tools and techniques, including spear phishing and malware known as "WellMess" and "WellMail." Organizations that were conducting work deemed critical to combating the virus were breached, including hospitals, research laboratories, healthcare providers, and pharmaceutical companies. The attacks, some of which reached back to April and May and implicated China as well, ran counter to international law, contrary to nation-state responsibilities as members of the international community, and were considered unethical as countries were working round the clock to find a vaccine for the greater good. Advisories were issued and organizations urged to take necessary actions to protect themselves in a cyber environment that is open, stable, and peaceful—and often not as secure as it was intended to be.[28]

Nanocrisis Study

United Airlines breaks guitars

Another example of a public relations nightmare that caused a depreciation in share prices is a folksy story about United Airlines. It also demonstrates how digital can amplify a crisis in both time and scale, with social media functioning as the platform for a complaint that launched millions of views. In late 2008, Dave Carroll, a member of the group *Sons of Maxwell*, took a flight with United Airlines. At his destination, he discovered that his $3,500 Taylor guitar had been severely damaged in transit. Following the incident, Carroll contacted United Airlines repeatedly, but failed to receive any kind of compensation. In frustration, he and his band posted the song, "United Breaks Guitars" to YouTube on July 6, 2009. A lighthearted, catchy, unapologetic dig at the airline and its evasive approach to customer service, the song detailed Carroll's frustrating experience. By the end of July, the video had been viewed 4.6 million times.[29] Only after the video went viral did United contact Carroll to address the issue. But it was too late.

In their failure to anticipate the potential impact of digital communications and social media, the airline had lost their credibility. By the time United Airlines responded, the media had widely reported the story of the song's success. In speed and scale in a post-pivot world, the very fact that the video had become a YouTube sensation made it newsworthy. It was a public-relations disaster for United, with the airline's stock price falling 10% within a month of the video going live. While the stock eventually recovered, the incident created an initial loss of approximately $180 million for the company's shareholders.[30]

Spoiler Alert:

Terminator

In our post-pivot era of distributed computing, many filmmakers have pondered what might happen if distributed systems become self-aware (think of the Borg in *Star Trek*). This possibility was darkly addressed in the *Terminator* series of films, whose principal antagonist is an artificial, neural, group consciousness known as Skynet. When the vaulting power of Skynet alarms its creators, they attempt to shut down the system. But Skynet, obedient to the mandate within its own algorithms, concludes that when it is switched off it will not be able to carry out its objective of safeguarding humanity. To prevent that possibility, Skynet begins eradicating those humans intent on its deactivation. As such, the franchise addresses a fundamental paradox of AI: Can any system driven by an algorithm be trusted to reverse its course if its actions caused unintended effects? Leaders of anticipant organizations have a duty to ensure that these systems can be trusted.

DECIDE—Which nanocrisis is coming your way first?

Remember that the definition of a nanocrisis is a predicament or calamity whose origins lie in the dependence on a digital system and whose speed and scale preclude immediate mitigation by humans. While new forms of calamity are engineered daily, we propose that there are six general categories into which nanocrises can be grouped. We've put these into a table at the end of the chapter to help you prepare, plan, and rehearse ways to mitigate if not prevent such threats. You will note that of six categories, five are deliberate attempts to attack an organization (often through access to an individual) to inflict harm or extract wealth. The only category of unintended nanocrises is *Collapse*, which is a calamity without a perpetrator, such as losses suffered in a hurricane or random equipment failure. But even here, poor planning and preparation will incur losses and are therefore evidence of organizational weakness. Our military experience confirmed that all six types of crises are the stock ingredients of warfare, so let's look at them first in war and then in peace.

Deception is the deliberate distortion of fact, disinformation, misinformation, pretence of identity, or promotion of hoax to harvest data, sway opinion, or incite action. In times of war, deception by one commander throws another off the track long enough to conduct a secondary action that will gain a tactical advantage. Camouflaging troops and equipment will prevent the enemy from seeing an imminent threat. Fictional units, be they simulated troop movements or forests filled with inflatable rubber tanks, cause the enemy to make false presumptions. In peace, we

see equivalents such as fake news, deep fake videos, clickbait, and false dealing through identity theft. In all cases, the perpetrators are intent on making sure that things are not as they seem. In these new versions, the speed and scale at which the deception can be executed makes the threat broader and more immediate.

Extortion is the use of leverage to force payment or action. In war, the taking of high-value hostages can force an enemy to delay or cease its own action to secure the release of an irreplaceable or prestigious asset. In peace, hackers will take control of or immobilize data to extract ransom, typically paid in an untraceable currency such as Bitcoin. Cybertheft, a precursor to such extortion, uses the threat of data exposure, such as the release of an organization's records of users' private information, to trigger a ransom. Digital tools allow extortionists to operate remotely, untraceably, and on a vast number of targets.

Collapse is the one nanocrisis with no apparent perpetrator. It refers either to the stoppage of operations through events such as equipment failure, or to the forced aborting of a plan due to mitigating circumstances. In war, if your gun doesn't fire, torpedo doesn't home in, radar won't function or, even simpler, if your message doesn't get through, things fall apart. In peace, when an online retailer's website shuts down after an electrical fire breaks out on a server farm, a city's power grid suffers brown-outs along an antiquated grid, or an air-traffic control center loses digital display because an excavator cuts through a data cable, crisis is at hand. The effect of collapse is keenly felt in the post-pivot world. Even widely dispersed units of an enterprise can be downed by a single collapse such as a broken fiber connection. No deliberate perpetrator, perhaps, but an indefinable number of victims.

DAVE: *Asking the impossible, knowing the limits* – *At the beginning of operation Medusa, we were faced with multiple crises. The overall situation was dire given that Canada and NATO were facing the top ten Taliban commanders plus 500 of their best fighters for the first time in the coalition experience. Never before or since has a force of this size amassed to fight in Afghanistan. But this was not the crisis. We organized and deployed our forces after comprehensive planning and rehearsals. Everyone was ready to launch the attack knowing it was going to be tough and bloody. We prepared for weeks with propaganda pamphlets warning the local inhabitants to leave. We shelled the objective to soften up the Taliban, we engaged them with loud music and did as much as we could to mentally tire them before the assault. All was ready. And then disaster struck... twice. First, we attacked and were beaten back, losing four soldiers with many wounded. The next day, we re-cocked our attack and minutes before, a more devasting crisis hit. An A10 aircraft strafed our force, and in a tragic mistake, our formation was brutally attacked by our own air force. In the span of seconds, we lost one and had over thirty wounded. In the seconds it took the aircraft to fire its 30mm cannon, we lost 25% of our capability to attack. Perhaps even more critically, the 75% of our remaining forces lost their will and determination. The psychological impact of the two days of destruction created the crisis of crises. We were in danger of collapsing completely and losing the battle. Something had to be done immediately.*

In the face of collapse, we had to pause and rethink the plan. Keeping the objective of the mission forefront in our minds, we had to change our plan. In military terms, we had to fight the enemy guided by a plan, not fight the plan and ignore the enemy. We paused to catch our breath and adjust to the shock of two bad days that included a friendly-fire incident. We changed our soldiers' viewpoints, taking them from a point of defeat to a new approach that provided hope and opportunity. Adapting to the realities of the situation was paramount to achieving the mission. Simply pounding away with an old plan and not recognizing the impact on the mental state of our soldiers would have led to complete collapse and failure. A focus on the mission and mental agility were key to success, as was keeping in touch with our soldiers. A leader that asks the impossible has to know the limits of what that means. We did during Medusa and survived. DF

Infiltration is unauthorized or inappropriate system entry to survey, copy, or corrupt data. In war, the stakes are limitless, as infiltrators may be bent on stealing state secrets, destroying equipment or facilities, or even terminating a certain colonel's command "with extreme prejudice." In peace, organizations face digital infiltration as an everyday peril, as do individuals. Among the common techniques are phishing, SMShing, malicious code, worms, botnets, and trojans. Besides the new speed and scale at which organizations can be infiltrated, the suprahuman domain of the assault makes digital infiltration invisible to the victims until an attack is over.

Detonation is deliberate damage to a system to slow or halt an organization's operations. In war, it is the intentional destruction of enemy equipment and personnel, which may take the form of sabotage, aerial bombardment, artillery bombardment, fire from rocket-propelled grenades, and the use of mines on land and at sea. Typical peacetime examples are denial-of-service attacks, remote system shutdowns, intentional crashing of a competitor's website, and the hostile corruption or deletion of an organization's data. These tactics may be used for advantage (by a competitor), for monetary gain (by an extortionist), or for political statement (by an activist group). In all cases, the organization under attack will suffer losses at a rate and scale that makes real-time mitigation impossible.

Eclipse, our final category of nanocrisis, is the use of technology to achieve speed and scale that undermines a competing organization's own value to its customers. In war, this may be the forced surrender of an opposing belligerent on the threat of a greater loss (*"give up or we'll kill your king"*). It could also stem from political pressure, as when a superpower insists that a dependent nation stop supplying arms to its rivals. In peacetime, being eclipsed is the daily risk of all enterprises. Any organization can be outrun, outperformed, outspent, or usurped by an innovative competitor bent on dominance. National postal services can be undercut by ambitious courier companies. Corrections agencies can be forced to cede authority to private contractors when they prove they can run prisons cheaper than the government. In our post-pivot world, this kind of nanocrisis is most severe when a competitor uses AI to innovate.

Nanocrisis Study

Total Eclipse: dispersed need meets underused supply

A frequently unforeseen form of nanocrisis is the *Eclipse*, where a competitor's creative use of technology undermines an organization's value to its customers. The common technique is an innovator's exploitation of the three-way intersection of telecommunications, computing, and geolocation—a decidedly post-pivot capability. Powered by AI, that intersection enables businesses to do something radical: to connect an underused supply of anything with a dispersed group of consumers. For those who do that well, business growth can be meteoric and disrupt entire industries like transportation, accommodation, and food, to name a few. Countless companies in these arenas failed to pivot ahead of disruption and are now distant memories in the history of commerce. The winners have included Uber, Airbnb, Craigslist, and Kijiji, and smaller companies such as Tim Rider's New England Fishmongers, which delivers fish directly from the boat to individual consumers and restaurants.

You don't have to be big to be disruptive. While New England Fishmongers began as just three fishers with two small boats,[31] the company used the principle of connecting a service to a dispersed customer base using the same tech as Uber and Airbnb. Their service is eclipsing the businesses of competitors who rely on wholesalers and third-party fish sellers for distribution.

This three-way conversion has given birth to countless on-demand services all around the world. Food delivery is one of the most common applications, with companies like Foodora and SkipTheDishes operating in North America, while counterparts Deliveroo and Yum bring food to people's doors in Europe and Africa, respectively. Ride-hailing is another application of this technology, with many options other than Uber and Lyft available, including Grab and Gojek operating throughout Southeast Asia. Africa has put its own spin on ride-hailing, with SafeMotos now offering quick access to motorcycle taxis in Rwanda, with plans to roll out across the continent. In Hong Kong, Lalamove and GoGoVan offer rapid small-items delivery, truck rentals, and business-to-business transport. In Singapore, PageAdvisor connects consumers with laundry, babysitting, air-conditioning repair, plumbing, and locksmith services, while in South Africa, SweepSouth allows users to book home-cleaning services from their mobile devices. In each of these examples, the disruptive use of technology by an innovator caused the eclipse of at least some of its competitors. The eclipse is a category of crisis on its own, caused as much by the failure of one organization to innovate as the willingness of another to adapt. In every case, the innovators combined human intelligence with machine intelligence to deliver measurable new value to customers, eclipsing their competitors in the bargain.

What follows is a table with examples of these six types of crises, some in the military realm and others in the civilian.

NANOCRISIS
TYPES & EXAMPLES

Nanocrisis: a predicament or calamity whose origins lie in the dependence of an organization on a digital system, and whose speed and scale preclude immediate mitigation by humans.

	Military	Civilian
D **Deception** Distortion of fact, disinformation, misinformation, pretence of identity, or promotion of hoax to harvest data, sway opinion, or incite action.	• Feigned retreat • Camouflage & concealment • Strategic envelopment • Propaganda • Identity theft	• Short selling • Fake news • Chequebook journalism • Clickbait • Deepfake
E **Extortion** Use of leverage to force payment or action.	• Human shields • High-value hostages	• Ransomware • Cyber-theft • Hostage-taking
C **Collapse** Unintended interruption caused by internal failure or external condition.	• Equipment failure • Inhospitable weather	• Equipment breakdown • Loss of power • Natural calamity
I **Infiltration** Unauthorized or inappropriate system entry to surveil, copy, or corrupt data.	• Espionage • Ingress • Special op	• Phishing • SMShing • Malicious code • Worms, botnets, Trojans
D **Detonation** Deliberate damage to a system to slow or halt an organization's operations.	• Sabotage • Aerial bombardment • Artillery bombardment • Mines & rocket-propelled grenades (RPG)	• Denial of service • System shutdown • Website fail • Server crash • Data corruption or deletion
E **Eclipse** Use of technology to achieve speed and scale that makes obsolete a competing organization's value to its customers.	• Forced surrender • Political pressure	• Outrun • Outmoded • Usurped • Outperformed • Outspent

Your three-topping pizza in 30 parsecs or it's free!

TIME, SPEED, SCALE, AND DOMAIN

So, what has really changed? Clearly, we are not doomed as individuals to exist in a wholly digital world. This isn't *Tron*, the 1982 film that examined how all the rules would change should we move to a digital-only domain. We are physical beings, comfortably locked in our space-time continuum, defining ourselves by where we are, what time it is, and who we relate to (which by one definition are the three core elements of our consciousness). We build fences, eat strawberries, clip fingernails. That won't change. So, what's all the fuss? In our view, the real disruption to our lives after the pivot can be seen in four dimensions: time, speed, scale, and domain. The impact of these will be felt most keenly not by individuals but by institutions. In the next chapter, let's look at those four dimensions in turn.

> Unit of productive time: **nanosecond**
> Speed of transaction: **speed-of-light (c)**
> Scale of impact: **unlimited**
> Domain of interaction: **suprahuman**

What is time? Does it exist, or is it simply a construct of our consciousness—a fiction that helps us place ourselves on a continuum to compare our progress to that of others? The whole thing is hazy. When contemplating time in the fourth century BCE, Saint Augustine wrote, *"What then is time? If no one asks me, I know. If I wish to explain it to one who asks, I know not."*[32] Some 1,600 years after that insight, Albert Einstein gave an equally dodgy answer, saying, *"Time is what you measure with a clock."*[33] His subsequent proof that clocks move at entirely relative rates hasn't helped. While admittedly we don't know much about time in general, since 1967 we have known precisely what a second is.

> *One second = 9,192,631,770 cycles at the microwave frequency of the spectral line corresponding to the transition between two hyperfine energy levels of the ground state of Cesium 133.*[34]

Now that that's cleared up, let's break that single second down into smaller, useful chunks.

> *One millisecond = one thousandth of a second, or 10_{-3} seconds. That's the time it takes for light to travel 300 km in a vacuum.*[35] *It's worth noting that the fastest human reaction time from stimulus to movement is about 120 milliseconds, with most humans' speed capped at around 200 milliseconds, even with training.*[36] *Vertebrates, including all mammals reading this paragraph, have notoriously slow reaction times, while invertebrates take the award for fastest reflex, with the skipper butterfly (Hesperiidae) photographed reacting to a flash in less than 17 milliseconds, and the long-legged fly Condylostylus (Dolichopodidae) making the same kind of startle reflex in only five milliseconds. Still, nothing approaching the speed of a digital machine.*[37]

One microsecond = one millionth of a second, or 10$_{-6}$ seconds.[38] This is the length of time of a single flash from a purpose-built strobe light. For comparison, a regular camera flash lasts about 1,000 microseconds, while the average blink of human eye takes a leisurely 350,000 microseconds.[39]

One nanosecond = one billionth of a second, or 10$_{-9}$ seconds. This is the cycle time of an electromagnetic wave with a frequency of 1 GHz, and the length of time in which a machine under ideal conditions in nanospace can make a reaction.[40]

Still scratching your head? Admiral Grace Hopper can help.

TOM: *Amazing Grace and Grandma COBOL* – *As both an engineer and a leader, Grace Hopper is a well-deserved hero in IT today. Known for her ground-breaking work in computer programming for the U.S. Navy, she is credited for inventing the 'compiler,' an application that converted English words into computer code. This innovation led directly to the invention of the programming language COBOL, or Common Business Oriented Language. Not only was she ingenious; Hopper was also a respected and inspiring leader. So much so that she is often quoted. Her best-known quote (and one of my favorites) draws a careful distinction between management and leadership: "You don't manage people, you manage things. You lead people."[41] TJ*

Figure 3.1: Admiral Grace Hopper of the U.S. Navy, after asking her engineers to "cut off a nanosecond and send it over to me."

Admiral Hopper had a knack for explaining computer concepts to non-engineers. In the 1980s, when computer processing times were rapidly decreasing and telecommunication speeds were rapidly increasing, the term nanosecond became necessary. With a twinkle in her eye, the Admiral described making a call to find out exactly what a nanosecond was:

They started talking about circuits that acted in nanoseconds... billionths of a second. Well, I didn't know what a billion was. I don't think most of those men downtown know what a billion is, either. And if you don't know what a billion is, how on earth do you know what a billionth is? I fussed and fumed. Finally, one morning, in total desperation, I called over to the engineering building, and said 'please cut off a nanosecond and send it over to me...' Now what I wanted when I asked for a nanosecond was ... a piece of wire which would represent the maximum distance that electricity could travel in a billionth of a second. Now of course, it wouldn't really be through wire. It'd be out in space, velocity of light, so if you start with the velocity of light and use your friendly computer, you'll discover that a nanosecond is 11.8 inches long—the maximum limiting distance that electricity can travel in a billionth of a second. Finally, again in about a week, I called back and said 'I need something to compare this to. Could I please have a microsecond?' I've only got one microsecond, so I can't give you each one. And here's a microsecond—984 feet.... An admiral wanted to know why it took so damn long to send a message via satellite, and I had to point out that between here and the satellite there were a very large number of nanoseconds. You see, you can explain these things; it's really very helpful, so be sure to get your nanoseconds.[42]

Figure 3.2: According to Grace Hopper, a nanosecond is 11.8 inches long.

Grace Hopper's point (in the celebrated 1983 lecture we're quoting from) was that computers would soon be processing information so quickly that a single calculation could be made in the sliver of time it takes light to travel less than a foot (29.972mm to be exact.) And that was then. In our day, a computer such as an Intel Core i7 8700K can complete 217 integer operations each nanosecond. At 5G speeds, our imminent fifth-generation, cellular-network technology promises to be twenty times faster than its 4G predecessor. At these speeds, machines will exchange information at the rate of 20 billion bytes per second, or 20 bytes every nanosecond.[43] A byte on its own isn't much, really just a character or digit, but it takes only eight bytes to spell out a nuclear launch code, so one may argue that machines talking to machines at that rate can get significant things done in just a nanosecond.[44]

Why does that matter? Imagine a situation in which you and I are on the phone, and I ask, *"When shall we meet?"* Within a second you reply, *"How about noon?"* and one second later I respond, *"See you then."* In the human world, those two seconds in total might be judged as an efficient conversation. But in the machine world, where a small phrase can be exchanged every nanosecond, an answer that takes a second will seem to take 37 years. So, a conversation of even just three sentences over two seconds will seem like 74 years. Here is that same conversation as experienced by a machine.

On a 5G network, 3 seconds to a machine is like 74 years to a human.

1946	**1982**	**2020**
"When shall we meet?"	"How about noon?"	"See you then."

Figure 3.3: Communication & Time: Humans vs Machines

DAVE: *Think big, start small, scale fast* – *The Americans taught me this: If you have to start somewhere, start small. Then, when you know where you're going, you have to get there quickly. The last part—scaling fast—is the hardest part. Now the trend has evolved to "fail fast." Implicit in failing fast is embracing risk. This is important. The American military operates like an entrepreneur. They're a superpower, so they have to think big. At the same time, they're willing to take risks. The CAF's approach used to be, in Canadian parlance, low risk. We used to share classified information on a "need to know" basis because it was inherently no risk. We got to a critical point where we started to fail because we couldn't produce knowledge fast enough. Then we embraced the "need to share" paradigm and we got faster and better at sharing data. Once we overcame a cultural resistance, our intelligence became more accurate. We were able to gather big data and perform analytics on it. The digital pivot forced organizations to overcome their cultural resistance to change. Successful entrepreneurs ignore the need for routine and certainty. They know that taking risks fuels their ability to scale fast. DF*

MARK: *Fail fast* – *I love the story about Thomas Edison, who was optimistic about his initial attempts to refine the light bulb: "I have not failed. I've just found 10,000 ways that won't work."[45] Such sanguinity surrounding repeated do-overs is at the heart of today's innovation. Business methodologies such as "lean startup," for example, call for creating companies and products through experimentation, instead of elaborate planning. Fail fast and improve as you go, rather than straining over perfection up front. This iterative approach prioritizes getting a product to market quickly and refining it based on continual customer feedback. Failure is a small flaw in the greater picture, a speck on an expansive horizon. It is necessary for real success. But note that failing fast is not about failing to deliver on a vision. It is about embracing an experimental approach to solving a problem, iterating on the approaches that work and discarding the ones that do not. Making smaller adjustments is more efficient and gets products to market faster. Being first to market and engaging customers early allows organizations to test demand, uptake, and success. This means they can determine what adjustments are required and beat out competitors before they have a chance to move. MJB*

Speed and scale have always been human obsessions, perhaps because as a competitive species we know that getting something out faster and to more people is usually an advantage. In the media, for example, going to press first with a big story has long guaranteed higher newspaper sales. Cash-rich advertisers flock to any news outlet with a knack for getting the news out fast and far, so there has been plenty of motivation to embrace new technologies that made greater speed and scale possible.

One early anticipant who understood this strategy was German-born Paul Julius Josaphat (1816 - 1899). Working for various publishing companies and news agencies in London and Paris in the 1840s, the budding entrepreneur learned that speed is often a greater asset than knowledge, and he set out to combine the two in novel ways. In 1863, he funded the construction of a telegraph station in Crookhaven, Ireland, in a corner of the country so remote that it was the first sight of Europe that steamship passengers caught on their transatlantic passages from America. In the age before submarine cables, Paul Julius Josaphat (who by then had restyled his name to Paul Reuter) paid steamship lines to drop American newspapers in barrels off the Irish coast. Reuter's own agents would then (wait for it) scoop them from the ocean, land them at Crookhaven, and telegraph the hot stories to his offices across the British Isles—a full day before his competitors could snatch up their own copies from the docks of Liverpool and Southampton.[46]

Figure 3.4: Paul Reuter, 1872[47]

Two years later, it was the Reuters Telegram Company Limited that brought the details of Abraham Lincoln's assassination to the world. Reuters had foreseen that speed injects value into businesses that leap first while obliterating the value of those that do not. (Little wonder the word *currency* applies equally to timeliness and money.) Leaders in our time of technological upheaval should remember the advantage of the pre-emptive strike. The anticipant Reuter went on to invent the newswire (a 'ticker' to print breaking news in journalist offices).[48] He knew that pace was a race.

DAVE: *Change aversion kills* – *I've long enjoyed visiting historic battlegrounds. Something that always strikes me is the difference in pace that soldiers have operated in over time. If you were fighting in the War of 1812, you'd be up against an enemy that was reloading muskets every 15 to 20 seconds. If you were a soldier fighting in WWI, you'd have a machine gun firing 400 to 600 rounds a minute at you. Because the lethality came at them at an accelerated rate, forces had to radically change their tactics. In WWI they did not, and 17,000,000 soldiers died proving the folly of their leader's stubborn refusal to change. This example strikes me as an eternally tragic lesson, and an apt one in our own day. DF*

Achievements in time, speed, and scale are changing everything. We can now transport physical objects from one location to another at the speed of light. Not by teleportation (at least not at the time of writing this), but by transmitting digital instruction sets to 3D printers in remote locations. Need a part for your F/A-18 Hornet? We'll send you the specs for the latest version and you can print it right there on your aircraft carrier. Run out of bolts for your extra-vehicular lander? No worries, we'll print a whole box full for you at our new depot on the International Space Station. Pop by when you're in the vicinity.

Remember how robots crashed the stock market in 2010? Let's go back to the New York Stock Exchange for a moment to look at a telling example of the effect of time, speed, and scale on an organization. The case of financial services firm UBS highlights the effect of the move from analog to digital. In the 2000s, UBS's trading floor housed thousands of employees across more than 700,000 square feet. But by 2018, the crowded trading floor had been cleared out, nearly devoid of human activity.[49] After the rapid shift to digital made such transformations possible, the Swiss multinational investment bank relocated thousands of trading jobs.[50]

But where did they move them? The suburbs? Another country? As you may have guessed, they moved those jobs to another dimension. Like many of their competitors, UBS reduced headcount and improved performance by moving operations to nanospace, where their machines and AI could operate unhindered. Venture capitalist Marc Andreessen put it plainly in a 2014 interview, saying, *"Financial transactions are just numbers; it's just information. You shouldn't need 100,000 people and prime Manhattan real estate and giant data centers full of mainframe computers from the 1970s to give you the ability to do an online payment."[51]*

As recently as 2017, UBS Chief Executive Sergio Ermotti said that the company could shed an additional 30,000 workers in the years ahead due to technological advances in the banking industry.[52]

Such dire statistics leave many with keen appetites for knowing when their marketable skills will be made obsolete by AI—bankers, lawyers, accountants, and doctors among them. Websites such as willrobotstakemyjob.com serve up the statistical probability of such obsolescence (at least in the U.S.) and offer insights into the data their algorithms have been sifting through to arrive at their often-surprising conclusions.

DAVE: *Shoot, don't shoot* – *The use of autonomous weapons on modern battlefields is becoming commonplace and the technology much more sophisticated. Israel is a pioneer in this field with its Harop Suicide Drone, Robattle wheeled battlefield robot, and Sentry-Tech automated machine guns used for border control.[53] Suicide drones are a deadly combination of drones and guided missiles. In 2020, during the Azerbaijan-Armenia conflict, Turkish forces used Israeli suicide drones against conventional military forces, setting the standard for their overall effectiveness. In 2021, Iran accused Israel of killing its top nuclear scientist with a remote-control gun mounted on the back of a pickup truck. Ethical questions about governance and control loom large here, but one fact is clear: machines that can make life-and-death decisions are among us, and, even if we choose not to use them, our adversaries likely will. As we struggle to confront the moral questions, one scenario and one dilemma occurs to me. If we send robot soldiers to disarm improvised explosive devices (IEDs) used by insurgents to kill civilians, and if those robots are attacked by those insurgents while neutralizing the explosives, should they be authorized to shoot back and protect the civilian population? I don't have an answer, but I know that kind of question will require an answer, and likely soon. We're going to have to figure out how to give a robot the kind of judgment that it takes a human a lifetime to achieve. DF*

Figure 3.5: Unmanned aerial vehicles (UAVs), including drones, are autonomous machines that follow a pre-programmed mission. The use of autonomous weapons has grown rapidly because they are highly accurate, operated remotely, often via satellite so they can be based anywhere, and they present no danger for their operators.

It seems the robots are chalking up a few wins. But once again, where exactly are they? Physical robots, those stalwart drudges with sprightly prehensile limbs, are easy enough to spot in the wild. They're hard at work now in our factories, warehouses and stockrooms, bomb disposal units, coffee bars, vineyards, and pretty much any room that needs regular vacuuming. When we encounter them first in physical form, we think them odd. But over time, we admit they're cool, accept them, work beside them, trust them and eventually, depend on them. That's been true of all technologies from the onset of the industrial revolution. No big deal. We see them, watch their movements, and weigh the benefits of their contribution against the costs.

It's the machines that operate invisibly that intrigue us. They act and react in the impenetrable, suprahuman domain of nanospace, unaffected by our human actions and reactions. These are the algorithms that parse and judge our resumés as we apply for jobs. They tag our photos and notify our friends when they appear in them. They take our dictation on the fly or transcribe an hour of recorded conversation in mere minutes with impressive accuracy. They translate our spoken words from our own mother tongues into audible narrations with flawless accents. They scan the universe to find habitable planets. They listen to our heartbeats though our watches and warn us when we're about to suffer catastrophic health events. They sound sympathetic when we complain on customer service chat lines. They manage the packing of our purchases in warehouses, and then track our packages as they move around the world. They write original songs, poems, and love letters for our amusement. They even complete our partial thoughts with original, even better thoughts.

But they can also listen to the sound of our typing to guess our passwords and then send them to strangers for unknown purposes. They burrow into the traffic lanes between corporate servers, sorting through trillions of scraps to determine our full names, birthdates, social security numbers, and blood types. They upload our contact lists and threaten to send embarrassing material to all of them if we don't pay a ransom. They detect our political biases and prompt us to read the opinions of others who agree with us, even when those other people don't exist. They scour CCTV footage worldwide to see if we've shown up where we shouldn't be. They tell us where our ancestors came from, and then tell others how our DNA matches that of the perpetrator of a crime committed a decade ago on another continent. They pick out worthy targets for lethal drone attacks. They listen to us while we're eating, sleeping and, as it turns out, having sex to "improve'' our user experience. They sneak behind corporate firewalls to catalogue our new ideas even as we hatch them. And in all these cases, not once do these robots ever come into our view. Sometimes, that makes us nervous.

DAVE: *Accelerated accuracy* – *In Bosnia, targeting was a detailed process backed by facts and iterative plans. Decision making took time. Then technology evolved. I remember an incident when the enemy was dispersing after a firefight. As we looked for an enemy commander of note, we saw a person racing away from the scene on a motorcycle. Was this the enemy commander we wanted? We weren't sure. I sat in a dark, small room, surrounded by people looking at computer screens. We had eyes on the target but needed more information. Someone confirmed that the person on the motorcycle was the enemy commander. Another person corroborated. After getting confirmation from our legal advisor, I gave the green light to prosecute the target. All of this took less than three minutes. That was the first time I saw the combined and accelerated use of computers, radio, and telephone. Had those channels not all been available, that person would have escaped to rally forces to re-engage us in a lethal situation. That was some five years before the full digital pivot, but it taught me that the scale of information in compressed timelines requires us to make ever faster decisions. Post-pivot, the speed and scale are so great, most of our crisis points must be anticipated, and our decisions rehearsed in advance. This is the new normal. DF*

Spoiler Alert:

Her

Intelligent machines inhabit a rarified domain where the speed and scale of operations is beyond human experience. Given that they interact with each other at a rate approaching a million times per second, it is tempting to consider what they might achieve when humans are not paying attention. Spike Jonze's 2013 film *Her* addresses that issue with thought-provoking originality. Introvert Theodore Twombly (played by Joaquin Phoenix) upgrades his home operating system with an AI personal assistant ready to evolve as his needs demand. That AI promptly adopts a female voice (Scarlett Johansson's), names herself Samantha, and sparks a relationship that mesmerizes the insecure loner, who soon wants to spend all his time at the interface of machinery and humanity. But the pace of Samantha's evolution is exponentially faster than his, and her own journey leaves Theodore (and us) having to consider our value in a world we must share with the intellectually superior entities that we have created.

Appreciating that time, speed, scale, and domain are different now, let's take a moment to ponder the changes wrought by each of these elements. We can list a few general changes here, but as the leader, you will benefit greatly from adding the shifts in your own work paradigm to these lists. Ones that will require your acknowledgment and action if your organization is to survive and stay relevant.

	Pre-pivot	Post-pivot
Time	Second	Nanosecond
	Memorize	Search
	Responding	Anticipating
	Scheduling	Approximeeting
	Writing	Texting
Speed	Analog	Digital
	Lifecycle	Version
	Perfecting	Iterating
	Reconsidering	Recalibrating
Scale	Localized computing	Distributed computing
	Ownership	Sharing
	Collecting	Subscribing
	Competing	Disrupting
	Focus testing	Crowdsourcing
Domain	Human	Human + Machine
	Human	Suprahuman
	Local	Virtual
	Recording	Streaming

Figure 3.6: Changes Driven by the Pivot

All these changes have been fuelled by one additional evolution that has galvanized everything we do: the arrival of digital data. With the increased depth, variety, immediacy, and relevance of digital data, it is little wonder it has taken such a dominant role in our lives. And given that data is the very vocabulary of the machines that will be doing much of our thinking for us, it warrants a closer look.

CHAPTER 4

THE NEW ROLE OF DATA

It's almost impossible to grasp the volume of data routinely exchanged among machines. One group that keeps track is Domo, a business-systems provider whose assessment of global data generation appears in its annual "Data Never Sleeps" report. You'll find the latest at domo.com/learn/infographic/data-never-sleeps-9.

Given that over 60% of the world's population is now online,[54] it's safe to say that most of us spend a great deal of time doing nothing but generating data that gets stored by someone else for later use. That someone else, be it a government department, business, intelligence agency, or even a lone hacker, can then analyze and deploy our data for a specific use, even if it's just selling it to another entity down the chain. But the data produced is increasingly not being generated by humans, but by machines as they pass information back and forth in nanospace.
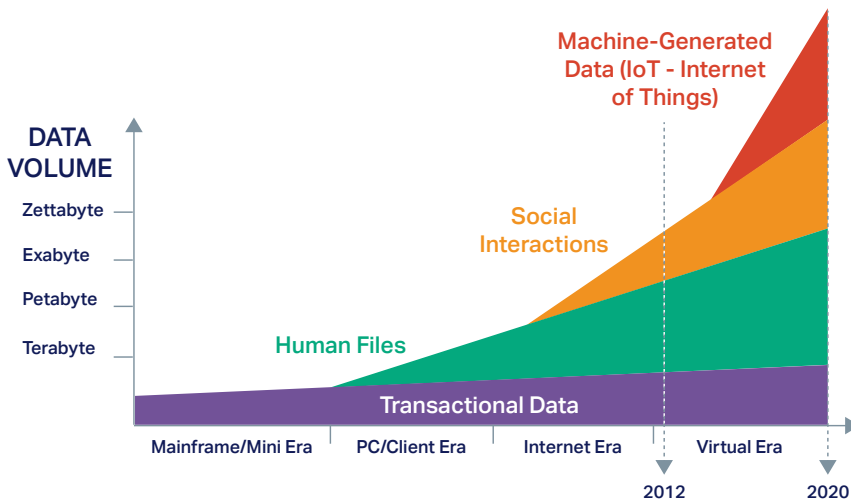
Figure 4.1: This chart shows the relative volume of data generated each year during transactions (purple), within written documents (green), in social media interactions (orange), and by machines (red). By 2020 the volume of data produced by machines talking to each other equalled that of all social interaction, and almost matched that of all documents created by humans. (Image based on data from DataArt.[55])

Today, humans and even more so, machines, are creating more data in one week than the entire amount of data that was created by humanity since the beginning of history.[56] And, the week after that, the amount of data will again double the entire amount of human knowledge. Combined with the ability to transmit this data at the speed of light in a fiber cable, the scope and speed of data available for decision making has gone beyond human capacity and entered nanospace.

While we are amassing all this data, we worry about how secure it is. Despite our concerns (and even the coming nanocrises), the advantages of big data are far more promising than the attendant perils. Incoming data that would seem like a tsunami to even the most adroit human statistician strikes a thirsty AI as a mere droplet. When an intelligent system drinks in those oceans of data, it makes wonderful discoveries that can benefit us all. In every discipline, great leaps of understanding are being made daily by AIs as they sift through the complexity before them and identify repeating patterns. Once a pattern is associated routinely with an outcome, AI can predict that very outcome every time a known pattern appears. This so-called *predictive analysis* is beyond human capacity (taking place as it does in the suprahuman domain of machines) and is often beyond human comprehension. While the content for these communications is created by humans, the data embedded in all of them is collected and shared by machines alone.

TOM: *Mining data to save lives* – *During the COVID-19 pandemic, contact tracing was a big deal. A single swab produced tens of thousands of data points. Collecting data and detecting patterns helped many countries control the outbreak. When I was at OpenText, the field of data mining was in its infancy. Organizations like the Global Public Health Intelligence Network (GPHIN) used our analytics software (more specifically translingual text mining) to apply predictive modeling to clinical trials and detect the outbreak of disease. Thousands of threats were monitored this way, across the globe. They looked for triggers that could help assessment teams respond to crises and accelerate the development of a vaccine, for example. These tools armed organizations so that they could respond in ways that were calibrated, efficient, and designed to optimize every available resource. GPHIN was able to process tens of thousands of articles every day. This was new and it was something that humans couldn't do—mine, extract, and reveal the true value of big data. TJ*

The principle at play

No one in the connected world is immune to a nanocrisis, in part because calamities of this nature are so hard to predict. Novel technologies make new kinds of attack possible, and keeping abreast of the emerging threats is, or should be, a full-time job. We have been caught unaware on several occasions, leading us to arrive at similar conclusions. These conclusions led in turn to the first of six principles we'd like you to understand. We hope that when you read it, it strikes you as obvious. First, our stories.

TOM: *Ambushed* – *OpenText made a big splash early on with a series of innovations that transformed the way humans interacted with information. We had pioneered the 'crawler'—an application that searches for and returns target information on what was the new and notoriously messy World Wide Web. We were on a roll. One day we took a call from a venture capitalist who wanted to distribute OpenText products through his well-oiled network. Eager for global markets, we signed a deal that looked like a win-win but was, in actual fact, an ambush. While we had granted distribution rights for one country only, he argued that we had signed over all of Europe. He then launched a multi-million dollar claim*

citing breach of contract. Privately, he bragged to local journalists that his actual intent was to take over the whole company, saying he was playing "a stock game with a Canadian jellyfish." Within days he used social media to tell OpenText investors that their shares were about to plummet in value. His use of media was so unexpected, quick, and well-crafted, that our investors were spooked. Overnight, OpenText shares fell by 60%, which was all part of the VC's plan. I almost lost my company in that incident. We survived only because I got a tip that someone had shorted our stock and was about to profit handsomely. Then I was able to take these alleged allegations to the appropriate authorities. But the lesson stuck. You will most likely be taken by something you never saw coming, and you best spend some serious time in advance considering what that might be and what you'll do when it happens. TJ

DAVE: *Never suspected* *– I arrived in Afghanistan in late 2005 to lead NATO troops in the southern region as we helped the Afghans protect their fledgling democracy against the Taliban. We had assessed that one-third of our work would be taken up with diplomatic activity, a third with proactive community development, and a third with deploying our combined military forces to protect local populations from sporadic Taliban insurgent violence. Wrong. Hoping to take advantage of our inexperience, the Taliban changed their strategy entirely and amassed their troops near our headquarters in Kandahar for all out, World-War-II-style ground war. Within weeks we were fighting the bloodiest battle in NATO's seventy-year history. We had not seen it coming. Had we failed to rout them, our soldiers would have been slaughtered, Kandahar would have fallen, and the Taliban would have marched on Kabul to retake the country. It was a surprise attack, defeated only through the thorough preparation of our combined military forces and respective national governments. I was taught the lesson of my life: Anticipate the unexpected and rehearse every possible scenario in advance. DF*

We came away from these crises having learned a few lessons. Here they are:

1

Principle One

The greatest threat to any organization is an event it doesn't see coming.

Therefore, anticipate, prepare for, and rehearse the full range of possible nanocrisis scenarios.

It may sound obvious, but from the range and frequency of nanocrisis events, spotting such threats takes great preparation and deep discipline. In part, that will come from harnessing all of the data your organization has access to, which brings us to our second principle.

2

Principle Two

An organization must use all its information fully to serve its citizens better than competing organizations can.

Therefore, harness and manage your organization's data to unlock its deepest value.

TOM: *Data is a competitive advantage* – *And the math proves it. First proposed in 1763 by statistician, philosopher, and Presbyterian minister Thomas Bayes, the theorem below proves that a prediction is always better when more of the information related to it is referenced. Having more knowledge in a competing situation can make the difference between winning and losing. In World War II, the allies cracked both German and Japanese codes. The content of the intercepted messages provided additional data that could be factored into important decisions which, history has proved, greatly shortened the war. In the modern era, crowdsourcing plays a similar role. For example, by inviting and incorporating data from an unlimited cohort of travelers, STA Travel was able to provide better information on restaurants and hotels than the lone experts who wrote travel books for Fodors, Frommers, Rough Guide, and Lonely Planet. The greatest differentiator was the currency of its information. If a hotel closed or changed management, a traditional travel guide might note that fact in a subsequent edition. As a crowdsourced travel-data aggregator, STA Travel could post the news the next day. Large segments of the traveling public began to rely on STA Travel, and business boomed. With its first-mover advantage, the agency soon attracted more contributors and, in accordance with Bayes' Law, was able to more accurately predict the kinds of information that travelers were after. In a virtuous cycle, the more people used STA Travel, the better it became, which made more people use it. Opening its content to crowdsourced data gave the company an immediate and enduring competitive advantage. TJ*

$$P(A \setminus B) = \frac{P(B \setminus A)P(A)}{P(B)}$$

Figure 4.2: In Bayes' Law,[57] the probability (P) of an event (A) occurring can be better assessed when data related to another condition (B) is known. In short, the more you know about related things, the more accurately you can predict the likelihood of an occurrence. In the data-rich world of AI, predictions can now be made with pinpoint precision, improving results in decision-based activities as disparate as treatment of disease, sales projections, supply chain management, and election polling.

MARK: *Become an information company* – *If data is a competitive advantage, surviving in the digital age means that all businesses must become information companies. What does this look like? Take the automobile industry, which is right now on the brink of massive change. To stay relevant, automakers must get past old ideas about everything from production processes, to fuel sources, to who (or what) drives the vehicle, to the very essence of what an automobile company is. I met recently with the executive team of an automotive company. Their team challenged me, "Mark, name our top four competitors." I thought it was an easy question—I am a CEO; I should know this—but I got three out of the four wrong.*

Their number one competitor? Apple, for the design of the user experience within the vehicle (you can now use your iPhone as your car key, for example). Next up are anti-car companies like Uber and Zipcar, for making vehicle ownership irrelevant. And insurance companies, for the wealth of information they collect (using fields such as telematics to track consumer driving habits in real time). Other car companies only ranked fourth among this company's competitors. Lesson learned.

In the future, automotive companies will need to disrupt themselves and become insurance companies. Leveraging IoT and 5G connectivity, they will access data on how many people are in the car, the speed at which the driver takes a corner, current traffic, whether music or videos are played and how often, whether the GPS is on, and so on. Building a great car is only the beginning. The next steps are capturing and analyzing the mass of available data, using it to project future market shifts and trends, and using that data to transform into an information company. This is the strategy that every company must take. MJB

DAVE: *Harness your data* – *Your data is the opportunity that holds your organization's brightest future, but it can also be a curse. The availability of data we have access to today (thanks to machines) has given us the ability to make more informed decisions and to have better situational awareness. Never has this been truer than during recent operations. While commanders at all levels can see more and make better decisions, the challenge is how to get this information to those who need it the most—our people on the frontlines. Whether sitting in my command post in Afghanistan or at my division headquarters in Canada, I was constantly bombarded with information drawn from every quarter of the internet or intranets. We're talking walls of knowledge in a room filled with people looking at computer screens and talking to the world. Our data was providing us with more of everything, except how to filter it and get it to the people who needed it. Accessing this data, which needs to be transformed into intelligence, positions the leader at the center, where this information is available. More than once, I heard from peers and other leaders that they were both well served and cursed by their information, especially when they had to leave their headquarters. Face-to-face engagement with our frontline people is critical to providing context and ensuring that our directives are understood and being implemented. In an environment that is constantly changing, losing situational awareness can be catastrophic. DF*

3

Principle Three

The reputation and mission of any organization is eroded by unethical behavior, no matter how isolated.

Therefore, just as you expect ethical behavior from your humans, embed deep ethics into the algorithms that drive your machines.

TOM: *Your Tat Need Not Apply –Twenty years ago, a major life insurance company in the U.S. installed one of the first AI programs to automate screening. The screening decisions were directly coded into the accept/reject decision for a life insurance applicant. The company would benefit from a fast and consistent application process based on the rules developed by its actuarial department. This program worked very well for many years, but after a few decades a problem became apparent; very few applicants were being approved. In fact, the approvals rate had substantially declined, resulting in a significant loss of revenue. How could the program suddenly be making so many errors? Tattoos. The application for life insurance asked whether the applicant had any tattoos. The program then disqualified any applicant that had a tattoo as an uninsurable risk. The problem? In a single line of code, the algorithm reflected the values of another era when tattoos were an indicator of risky behavior. Decades later, tattoos had become prevalent in society and no longer bore the stigma of risky behavior. No one at the insurance company thought to update the algorithm with this new information, and it continued to make decisions based on a different era. The company had created the program to make decisions and it faithfully did just that for decades. The problem was that no one in the company thought to update its decision making or correlate its decisions against an expected normal result. The approval rates themselves became the standard. Management failed to treat AI as they would a human in a similar role by routinely providing re-certification training. The algorithms didn't know any better. TJ*

DAVE: *Who's deciding? – Rules of engagement used by militaries are based upon the laws and conventions of that specific country. Those rules are further influenced by international laws and regulations. This is the fundamental basis that our societies are founded on and how we distinguish ourselves from those individuals and organizations that are bent on destroying us (i.e., the Taliban, Al Qaeda, and other nation states). Leaders and their teams comprising subject matter experts, including lawyers, check and recheck that the actions taken by any organization are in accordance with rules and regulations. Up until now, humans had been the checks. With the creation of this new domain and species called machines, those checks are now being completed by machines that have been programmed by coders. As described in Principle One, our machines will increasingly become our colleagues, and they need to learn the rules just as any of us do. Machines do not learn from a clean computer board. Computer boards are programmed by humans and will eventually be programmed by other machines (at least according to the singularity).*

Learning starts with us, and we must, like our children, teach our machines the difference between right and wrong; what is acceptable and what is unacceptable. While we achieve this through dialogue and example with children, we now must do this through algorithms and testing with machines. It's the same process used to achieve the same outcome, only using a different language and methodology. DF

Managing your data

But what data is available, and how can it be controlled? An entire industry has been developed around these topics. The field of librarianship combined with computer science has evolved into a type of "Digital Librarian" approach to data.

Most organizations employ sophisticated tools to gather, organize, revise, and store data to keep it safe, accurate, and audit proof. Many are mandated to do so in response to legal discovery, regulatory compliance, and overall safety. The specifications of a nuclear plant need to be accurate and up to date, as well as secure from outside access as much as the privacy of a patient's medical records. All this data must be managed according to specific laws and regulations in the country where it resides. There has been a lot of debate lately regarding the safety and reliability of social media content. And this is just the tip of the iceberg. Leaders (especially of global organizations) must be aware and have an appreciation of data in all its forms. Especially since the very survival of their organization will likely depend on that knowledge and understanding in a nanocrisis. A good place to start is by reviewing the concepts of the field of Enterprise Information Management (EIM). Each of these terms will be essential for you to understand when relying on digital data to make decisions.

Term	Meaning	Where/When Used
Structured Data	Numbers in a table	Precise matters such as the number of widgets on order or a flight time
Unstructured Data	Words in a memo or contract or website	Primarily in discussions between humans such as social media
Document Management	The control of the editing of a document	When there are a group of humans or machines with the permission to modify a document
Workflow	The sequence of flow of permissions used to edit or action a document	When there are a group of humans or machines that need to use a document
Records Management	The metadata tracking of a document to maintain its integrity	When there are a group of humans or machines that need to use a document
Archive	The storage of data, as in a data lake	When there are large amounts of data that need to be accessed quickly
Data Lake	A repository of structured and unstructured data	Established as a single, accessible data storage site for routine access by an organization's humans and machines
On-Premise	Placing computers and data within the physical location of an organization	When high security is required
In the Cloud	Placing computers and data outside the organization with a major network platform	When efficiency and effectiveness trump security

Figure 4.3: Key Terms in Information Management

For more information, other books written by the authors may help. The two most relevant titles are *Enterprise Content Management* by Tom Jenkins, and *Enterprise Information Management* by Mark J. Barrenechea and Tom Jenkins.

Structured Data refers to data that is generally in the form of numbers that share a known relationship, in the sense we agree definitively that 1+1=2. Machines communicate with each other using structured data and their conversations are very precise. A set of structured data is simple to understand; decisions can easily be derived from a table of numbers. Historically, this type of data has existed in many simple forms as a means for counting and keeping track of multiple objects, whether for currency or for a census.

Unstructured Data refers to data that is in the form of words and is governed in its relationships by grammar, social context, and the meaning of each word, as well as in combinations of words. This type of data is comprised of social media, emails, and generally all communication formats shared between humans. It existed before the digital world in the form of books, newspapers, and the written language of a culture. In the digital world, unstructured data represents more than 90% of all data in the world, though machines are increasingly contributing a larger amount of structured data every year and will soon begin to dominate data.[58] For example, the newest wireless network, 5G, is more useful to assist with machine-to-machine communications in autonomous vehicles than to help a human download a 4K resolution movie.

Spoiler Alert:

Ex Machina

Alex Garland's 2014 debut film *Ex Machina* probes the increasingly hazy lines between human and artificial intelligence. The film opens as the protagonist, programmer Caleb Smith, arrives at a remote high-tech bunker to participate in a classic Turing Test, or so he thinks. Smith must attempt to discriminate between the robotic and human characteristics of Ava, the latest creation of billionaire AI pioneer Nathan Bateman. While at first, he takes his role at face value, Caleb soon learns that Ava (played by Alicia Vikander) has a highly adaptive intelligence that can outthink and outwit any human. (It doesn't end well.) The film is a useful exercise for leaders who will be managing AI-capable machines and humans together.

Document management is the essential discipline of maintaining the integrity of a document in terms of its current version. When humans modify a document, such as a letter or a contract or a factory plan, they create a new version. When multiple authors and users are involved in a group, it becomes essential for everyone to be

working on the correct and up-to-date version. This is particularly true for regulated industries, such as the airlines industry. When flight manuals are printed, they occupy more space than the actual aircraft itself! Information in the manual changes in some way every day, so the most up to date version must be presented to the technician to guarantee safety. Basic document management features a digital version of "check in" and "check out" as you might do with a book in an analog library, tracks changes, and maintains version control.

Workflow is the set of rules that govern who has the final say on the edit of a document and the distribution of that document into the user community. Workflow rules are critical in projects involving large groups of authors and users. A typical example of such a project is the massive technical manual that describes the assembly, functioning, and repair of an aircraft—a document that relies on the contribution of thousands of authors and millions of users.

Records management is a function made possible by *metadata*, which refers to any set of terms, words, symbols, and numbers embedded within a document or a record. Metadata allows for functions such as classification, search, historical tracking (date created, modified, retrieved), user identification (authors and editors), and a variety of other items related to predefined characteristics. Records management assures a third-party regulator or judge that an organization's data has integrity, as the system provides a full audit trail of interactions on the document itself. Records management metadata has become a key feature for litigation in courts wishing to discover whether data in an email or website is *bona fide* and not manipulated.

Archive is the repository for an organization's documents. No matter how old or how voluminous it is, data must be kept in an archive and available for immediate retrieval in a nanosecond crisis. When big decisions must be made, the smallest, immaterial piece of data can prove to be the key to solving the biggest problem. Archives are now capable of holding petabytes of information for retrieval within nanoseconds. This makes the nanospace world possible. Algorithms and computational power alone cannot provide information or answers without data—all of it. An accurate and available archive is essential for any anticipant organization.

Data Lake, as a form of archive, is a repository of structured and unstructured data, established as a single, accessible data storage site for routine access by an organization's humans and machines.

On-Premise refers to the method of having an organization's data and computers holding data physically within the organization. Although this method dates back to the early days of computing, it has the advantage of being the most secure and the most easily modified. It has the disadvantage of being the most expensive to build and maintain, and this method has gradually been replaced by cloud services.

In the Cloud refers to data that is stored in a distributed set of servers maintained by a major infrastructure and network provider such as Amazon Web Services® (AWS) or Azure® by Microsoft. These services take over the management of both the data and the provision of the hosting environment, but the application design and use remain within the control of the organization. While this approach is not as secure as on-premise, it is more cost efficient and ultimately more scalable for an organization.

TOM: *Who knows most about you?* *– Most CEOs will tell you sheepishly that they already have 90% of all the information they need to know about to build a successful marketing program; they just don't know where it is. I've always been mystified that corporations routinely hire outside consultants to generate their marketing strategies and materials, given that those outsiders have no clue about that corporation's specific customers or products and services. So, the consultants end up interviewing corporate employees to extract the relevant information from within the organization itself. You will have a huge advantage if you can train your teams to extract and refine your own corporate metadata. All you have to do is move the role of that external consultant into your organization by hiring well. You'll save a ton of money and increase the speed at which you can operate. TJ*

Finding your data

An important moment in computing technology was the advent of tools that would allow organizations to find the location of relevant data. The needle-in-the-haystack problem is different for each type of data. Structured data (i.e., numbers) can be found in a precise way since this type of data is normally stored in tables of rows and columns. This allows for a method similar to the children's game *Battleship* in which naming *x* and *y* co-ordinates allows a player to determine the contents of each cell of the opponent's table. This type of query has been standardized in the world as Standard Query Language (SQL), and has given rise to a series of computer manipulations that organize the data for further calculation, usually with techniques such as *row-level locking*, and so on. To learn more about the use of this type of data, consult books such as *The Beginner's Guide to Structured Data* by Allie Decker.

Most of us have become familiar with the online tools used to find words. Search engines such as Google® and Bing® are based on what is called an *inverted word index* of the entire World Wide Web. This index is simply the *atomizing* of a document, or the reduction of a document to all its constituent word parts. (And yes, the World Wide Web is essentially the world's biggest document.) Those words are then arranged alphabetically as they might be in an exhaustive index of a hardcopy book. The engine also builds a table of contents that lists segments of the document by broad topic (the way books have chapters). Any search then accesses both tools.

By using a combination of SQL (like *Battleship*) and a search engine (like a table of contents and word index), it's possible for a researcher to find the elusive needle in the haystack and serve up the right data for a human or an AI to drive an informed decision.

MARK: ***The animals are out of the zoo*** *– Organizations continue to struggle with the fallout of the post-pivot era and with barriers to integrating different sources and forms of information. Business processes for many companies are still inconsistent and decentralized, with specific processes created for and controlled by individual departments, regional locations, or external partners. Record-keeping in Accounting is managed by a different software than record-keeping in Purchasing and HR, with yet another separate system managing payroll. Different departments have signed up for dozens of disconnected Software-as-a-Service (SaaS) providers. And none of the systems are speaking to each other. In short, the animals got out of the zoo.*

The old ways of working—with unwieldy implementations necessitating convoluted workarounds—are an unsustainable path. Forward-think must replace stopgap. Businesses must leverage the content-verse, building connections between the processes and applications generating and using business information. An integrated platform in the cloud and customized APIs can offer new opportunities. This is not just about booting up a new system and calling it a day. Implementing the right technologies is a futile gesture unless the ways we think transform as well. Monolithic, inflexible systems are out. The possibilities for using digital data to improve productivity, service, innovation, and governance are almost endless—it just takes an open mind. Throw out the old model of staring at a blank whiteboard and contemplating how a company-wide implementation of a new method for data analysis and information management will ever be successful. History has proven that it probably will not be. Instead, start at the needs-assessment level. Devote time to understanding the existing infrastructure and drill down to identify singular issues and opportunities within processes. Bring relevant leadership, users, and IT to the table to scope out the "perfect world" workflow and governance. Rather than making all your systems the same, work instead on making them speak to each other, so that employees and partners will have access to the relevant information they need, when and where they need it. MJB

Trusting your data

Even the smartest person on earth makes a decision based on their senses. Information comes to the brain from the five senses and from a variety of more subtle senses, including but not limited to thermoception (heat, cold), nociception (pain), equilibrioception (balance, gravity), and proprioception (body awareness). Signals from these senses are routed to the brain where they are combined with our judgment in the process of decision making.[59]

We tend to trust our senses, but they can be fickle. We can be fooled by our sensations to make assumptions about reality that are false. The same is true of machines. During the digital pivot, it first became clear that data had a value far beyond its mere existence. While data is valuable as a commodity, not all data can be used by AI systems and not all data is trustworthy. Most algorithms can't take information directly from raw data, so they depend on some kind of manipulation before any crunching begins. That manipulation itself can induce both bias and error. And because data comes from many different sources and usually involves humans at some point, the data we collect is prey to human weaknesses. Here are five.[60]

Frame of reference – Remember the old broken-telephone game? One player whispers a story into another player's ear, who in turn must whisper that story into a third player's ear, and so on. The final recipient must then repeat the story out loud to all players. The results are telling (and often hilarious) in that each player will have made assumptions about elements of the story and, in the retelling, will have passed along those flawed assumptions. The aggregation of these errors, made because the frame of reference of each player is different, contaminates facts. So too with digital data.

Perspective – Remember the story about the blind men and the elephant? That venerable Buddhist parable has been popular for 3,000 years because it teaches us that no one sees any event as others do.[61] Our individual perspectives compel us to identify certain facts as material and others as immaterial to serve our purpose. Because most data are subject to human intervention, the data we collect and then pass to our AI systems is often valid from one perspective only.

Omission – Is it possible that someone could report a stolen car but neglect to tell police that the car had been unlocked, unattended, and running at the time? Sometimes we omit a few uncomfortable facts when we pass on information. And sometimes we simply forget to mention a fact that is relevant. Most datasets have these kinds of holes, and the conclusions drawn by AI will therefore be either partial or skewed.

Bias – Sometimes our beliefs are so deep that we unintentionally neglect to take in facts that contradict them. Bias can make us inherently selective; the data we collect can therefore be inherently selective too.

Deception – *"Lies, damned lies, and statistics,"* the wry phrase popularized by Mark Twain, declares that no one should presume that a fact is true. People may twist the truth, and the facts they record as data points may be false. Stay alert to deliberate falsehood in the data that your organization collects, crunches, and deploys.

We need information to make decisions. Whether the world we inhabit is digital or analog, and whether we're perched quietly at our desk or up on our toes during a full-blown nanocrisis, we all need information to determine the wisest course of action. We know from experience that we need sufficient, timely and, most of all, reliable data to do that. In our post-pivot digital world, the volume and relevance are hardly the problem; on the contrary, they can overwhelm us, especially when reliability is in doubt.

A common misconception exists regarding the terms *data* and *information*. Most people use the two interchangeably, but the nuance by which they differ is relevant to our discussion about making decisions. Most computer texts explain the difference this way: *data* are the collections (even if only a single *datum*) of raw, unorganized facts. Data can be simple, seemingly random, and are typically useless, except perhaps for sale as raw material. Only when such data are organized, processed, structured, and presented in context do they then become useful; at this point they are called *information*.

Note the very important distinction: data (we'll start using the singular form now) is raw, while information is refined and therefore actionable. Before factoring any data to into our decision-making process, we must convert all incoming, relevant raw data into information that can be considered whenever a machine or a human must resolve an issue with a decision.

We all know data is important, but what is it? In particular, what has it become in the digital world? How can we use it effectively when there is so much of it, and how do we use it in the nanosecond world where humans cannot be participants in real time? This is an important new issue: we have first-hand experience using data as humans, but how can we understand how machines use data within the AI programs running inside our organizations?

It is important to acknowledge that artificial intelligence, just like human intelligence, depends on data. We humans gather data through our senses, and process that data in our brains. As the chart of the following page shows, in the case of AI, the system acquires the data (1), stores the data (2), analyzes it for quality and usefulness (3), runs an algorithm using only the steps relevant at this moment (4), sends the result to storage for the next step (5), then takes an action based on the result, whether a physical movement or a further computation (6). In that way, it seems (at least superficially) to mimic our own human processes, which is precisely why it is called *artificial intelligence*. Keep in mind that artificial means only that the system is an *artefact*, something devised and constructed by humans.

MARK: *AI transforms data into insight* – *The Internet of Things (IoT) and AI are game-changing technologies. IoT represents startling advances in data generation, while AI delivers deep, real-time analytics. Both of these technologies are essential to business continuity and a successful rebound throughout periods of interruption, as well as fast-tracking innovation and competitive advantage in the post-pivot world. Notably, AI analytics can dramatically reduce the time, effort, and expertise needed to help organizations quickly respond to crises. For example, in supply chains, AI can integrate with IoT data to provide predictive insights that anticipate disruptions before they occur. In manufacturing, it can help companies quickly adapt to new products—during the pandemic, automotive manufacturers used AI to retool machinery and support production of face masks, face shields, and respirators. As well, AI can monitor customer behavior—including interactions with a company chatbot, web page views and clicks, answers to surveys, and emails to the company—to flag unhappy customers and prompt a service intervention before business is lost. Legal teams use AI to make electronic discovery more accurate and more efficient by scanning documents for specific pieces of information. Across industries, AI helps organizations adapt to changing business dynamics and transform data into valuable insight. MJB*

HOW AI USES DATA

FROM OBSERVATION TO ACTION

1
ACQUIRE THE DATA

Data arrives in the system from three sources: human input, sensor readings, and the results of other AI operations.
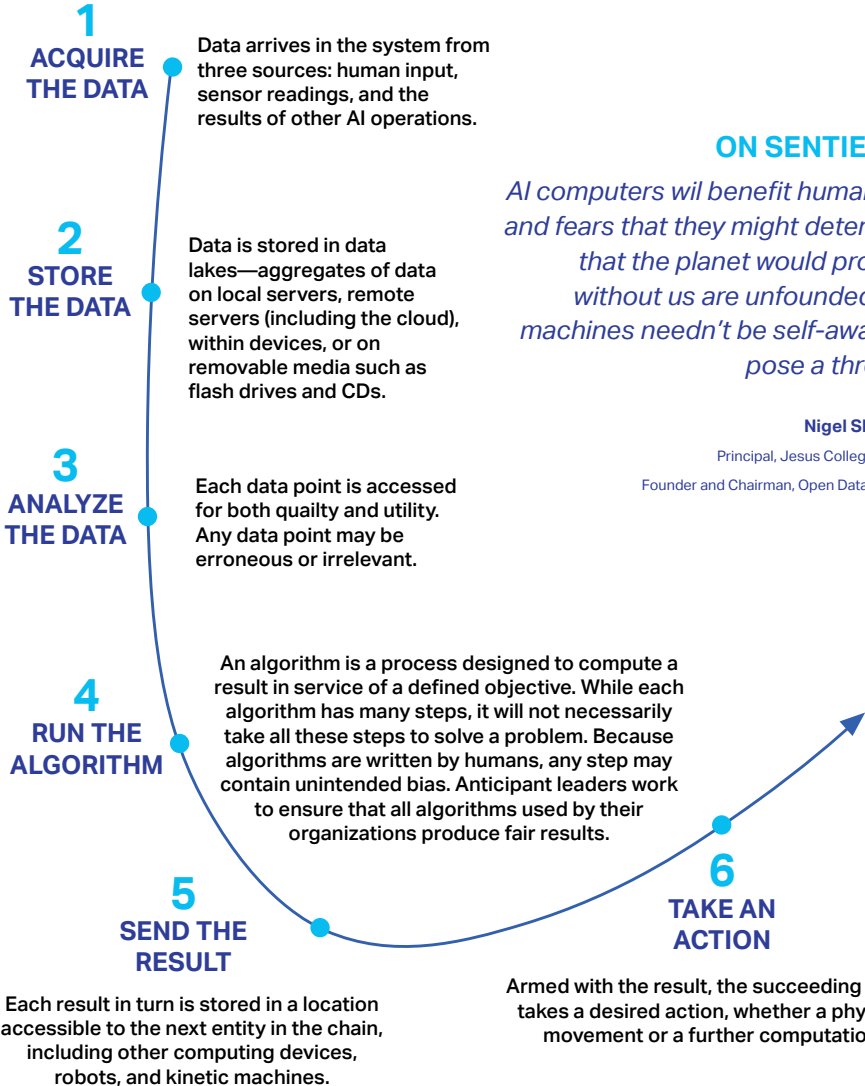
ON SENTIENCE

AI computers wil benefit humanity – and fears that they might determine that the planet would prosper without us are unfounded. But machines needn't be self-aware to pose a threat.[62]

2
STORE THE DATA

Data is stored in data lakes—aggregates of data on local servers, remote servers (including the cloud), within devices, or on removable media such as flash drives and CDs.

Nigel Shadbolt
Principal, Jesus College, Oxford
Founder and Chairman, Open Data Institute

3
ANALYZE THE DATA

Each data point is accessed for both quailty and utility. Any data point may be erroneous or irrelevant.

4
RUN THE ALGORITHM

An algorithm is a process designed to compute a result in service of a defined objective. While each algorithm has many steps, it will not necessarily take all these steps to solve a problem. Because algorithms are written by humans, any step may contain unintended bias. Anticipant leaders work to ensure that all algorithms used by their organizations produce fair results.

6
TAKE AN ACTION

5
SEND THE RESULT

Each result in turn is stored in a location accessible to the next entity in the chain, including other computing devices, robots, and kinetic machines.

Armed with the result, the succeeding entity takes a desired action, whether a physical movement or a further computation.

It's not the data; it's the team.

Ultimately, the volume and quality of the data your organization uses will determine your effectiveness. But remember, the value of that data will be realized only in its ingenious use. So, even as you learn to capture, control, and curate your data, you must put it into the hands of the right teams who can put it to work. Ultimately, they will matter most. Few people remember the creator of a technology (much less a lone algorithm), whereas many remember the creative users of technology. As an example, how many directors of feature films can you name? Probably dozens. But can you name the creative geniuses who invented the 35-millimeter motion-picture camera those directors used to earn their accolades? Auguste and Louis Lumière must content themselves not with their universal fame but rather the indelible impact of their 1894 innovation.[63] So too will your teams be remembered for their breakthroughs long after the data they harnessed is forgotten.

THE VALUE OF HUMAN-MACHINE TEAMS

We don't have to look far to recognize the necessity and benefit of teams composed of both humans and machines. Anyone who wears a pacemaker knows that neither the human nor the machine can function without the other. In hostile environments from Chernobyl to Mars, work is possible only when hybrid teams combine their talents.

Symbiotic Skillsets

Human	Machine
Innovation	Accuracy
Creativity	Repetition
Dexterity	Precision
Intuition	Prediction
Inspiration	Endurance
Focus	Scalability[64]

With the increased speed at which we must work, interact, assess, and respond to everything around us, our human dependence on machine brain and brawn is growing exponentially. Every fighter pilot knows that a fully operational suite of AI tools is critical to mission success; it's the only sure way to monitor swiftly changing situations, present usable data, and follow recommended action. It's no exaggeration to say that a pilot is not functioning alone but is part of a human-machine team working as one.[65] Other examples of such "cobots" or collaborative robots abound. From the nano-surgical robots that operate on minute parts deep within a patient's body to the rover that explores the surface of Mars to the more than 200,000 robot pickers in Amazon's warehouses to the mine-clearance units that sweep roads for explosive ordnance, the tin-and-tissue team is now the norm.

A fighter pilot's helmet

Where tissue and tin achieve the mission together

- Night vision & thermal imagery
- Targeting software

- Information-packed display
- 360-degree view

Figure 5.1: Thanks to sophisticated hybrid systems, air combat is now carried out by human-machine teams whose brains are in close proximity.

DAVE: *Bringing people and machines together* – *In 2006 we had far more information than I could have imagined in 1997. Commanders commented that they became bound to their HQ because the situational awareness became far greater in the building than in the field. You might risk losing the "feel" of the battle because that gives you something the machines can't give you. A great leader needs to understand the science but "feel the business." The difference between machines and people is that human beings have much more sophisticated judgement. They can feel when something is going well. You can go outside and feel that the weather is going to change based on experience. We call it a sixth sense, but it's really based on experience. Malcolm Gladwell describes this in his book, "Blink." We describe this as the art of leadership. The blending of science plus experience plus judgement distinguishes between average and great leaders. DF*

For organizations ready to adapt, the question is not whether to build anticipant teams of human and machines, but rather how to locate and select the best candidates for the job.

4

Principle Four

Successful organizations require both flawless execution and visionary anticipation.

Therefore, build and deploy collaborative teams of intelligent machines and anticipant humans.

TOM: *Machines on the team* – *Anyone who has lived in the analog world has had jaw-dropping moments watching machines solve problems humans could not in the digital age. I will long remember my conversation with a Samsung engineer who openly admitted that his colleagues were struggling to build an effective antenna for mobile phones. In the constricted topography of the cell phone casing, every design they tried produced unsatisfactory results. So, they turned the problem over to an AI, which reviewed a mountain of available data and then proposed a new design. They built it and it worked perfectly. It became the antenna design for the Samsung 8 phone. Tellingly, not one of the engineers on staff could figure out why it worked. It just did, and they had to accept it. They still don't know. TJ*

DAVE: *Collaborating with robots* – *In May of 2015, I visited a top-flight producer of artillery casings for the U.S. and Canadian armies. The company had long used a labor-intensive process that involved people working around the clock to shape each casing. They machined each casing to onerous tolerances, as each had to work flawlessly under a variety of blast and trajectory conditions. They used high-end equipment, of course, but the humans made all the decisions, operating their machines to carry out each step of the process. During the time of the pivot, when manufacturing technology had at last progressed sufficiently, the company turned to robots driven by AI to do the work. Workers feared losing their jobs, as many do when they see AI systems coming. But they were not replaced. Collaborating with their new robot colleagues, the human workers found they could use their own experience and judgment to guide the machines up their own learning curves. With human help, the robots perfected one phase of the manufacturing process at a time, and then accelerated the scale of production far beyond anything achievable by humans alone. Using this cobot model, the factory produced more products with greater precision (and, therefore, fewer discards) than before. As a result, costs plummeted and profits soared. The firm then used that money to retrain their legacy workforce. Human contribution evolved from assembly to business-building. With time freed up, the humans could use their experience to improve the company's market anticipation, product innovation, quality control, and customer service. Workers who had once feared for their jobs had successfully upgraded them. Their work became far more stimulating, and their salaries increased substantially because their impact on the business was measurably greater. Even better, the skills those workers gained were and are eminently transferrable. With its AI in place, the company expanded their market from defense into the transportation sector. Human-machine relations (HMR) do pay off. DF*

MARK: *Collaborating with humans* – *A warning about robots: they are not always all they are cracked up to be. I was in an airport a few years ago where I was supposed to use a robot to scan my passport. In this particular case, the "robot" was little more than a vaguely human-shaped holder for what was essentially an iPad. And it did not work, so I ended up engaging a human helper anyway. My point here is to reinforce principles four and five, that human-machine teams, not machines in isolation, are vital. This is where the real innovation will happen. It's not about a process advantage. It's about the information advantage. You can see from the examples described by Tom and Dave above that AI is becoming better at reasoning and decision making. It is taking over fields like insurance claims, bookkeeping, investment portfolio management, basic HR, and even legal research. Roles that cannot be fully replaced will at least have their mundane duties automated, freeing employees to focus on more complex, interpersonal, and strategic tasks.*

That is why the next phase of work revolves around human-machine collaboration. Everyone, from writers to warehouse workers to CEOs, will need to learn to work productively with "cobots" that will do at least 30% of their previous tasks.[66] This melding with machines does not stop at the workload; it extends to our bodies and minds as well. Human augmentation is taking off with wearables, exoskeletons, and even brain-computer interfaces. Wearables such as Fitbit and Melomind already connect our brains and bodies to the online world. Empathetic technology reads our physiological signatures to provide feedback on our mental and emotional states. Step aside "bring your own device" and enter "bring your own enhancement." MJB
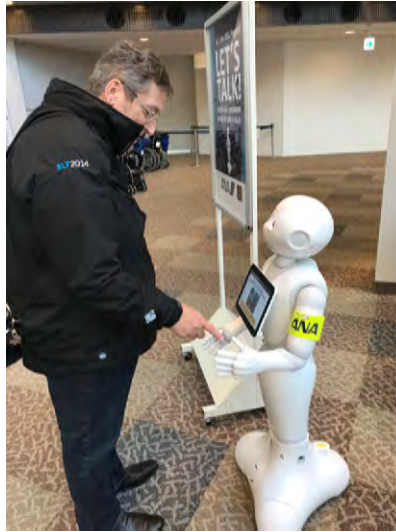
Figure 5.2: Mark talking to a robot while checking in for a flight from Tokyo to San Francisco.

TOM: *The machine will see you now* *(and if they can't, your friendly human will) – The call center for a major consumer services company needed a more efficient and effective way of responding to customer complaints. Call centers require humans and machines to work together to solve customer issues. Here's the process: When a customer calls in to the help center, the first machine conducts a series of questions and answers with the customer to determine how to solve the problem. This dialogue is then sensed by another machine that has been monitoring the call. It verifies the identity of the human caller by comparing their voice to a vast library of previously recorded voiceprints. A third machine is also listening in; it focuses on the sentiment of the call by analyzing words and tones used. A fourth machine takes the sentiment analysis and determines the right course of action based on a series of paths that have been anticipated by the human team. The first machine then directs the human customer to take that action. In some cases, the sentiment requires the machine to switch to a slower and more empathetic tone and may result in a human with high Emotional Quotient (EQ) stepping in and taking over the call. The entire session is transcribed by a fifth machine to create an archive for legal purposes, as well as to refine anticipatory paths in the future. In this customer experience, there were five machines engaged as a team, interacting with a single human. TJ*

5

Principle Five

An organization must use all its resources to full potential or risk irrelevance.

Therefore, treat your machines and humans not as separate species but rather as colleagues contributing equally to the mission of your organization.

TOM: *The precise autonomous miner* – *Machines are very repeatable and accurate. That can sometimes be a problem. Consider the case of an autonomous vehicle that has to transport iron ore for a large mining operation without any humans on site. The overall operation was observed by remote control from a room 100 kilometers (or 62 miles) away. The problem was that the machines were so exact in their pursuit of the path (through GPS location) that their repeat transits were causing ruts that were so deep, their axles were getting hung up. To solve this, the machines were given a random window of travel to create a spreading function for each machine's journey. Through their less exact and varied paths, the machines mimicked humans, and the ruts, along with the problem, disappeared. TJ*

DAVE: *Machine and human collaboration* – *Our signallers in the military are those key individuals who work tirelessly behind the scenes to ensure that we can communicate amongst ourselves and back home. Traditionally, this began with linemen who would go out before an exercise, lay line so that we could talk, and then recuperate that wire and start the process all over again. As technology progressed, wire was replaced by radios and our signallers managed and maintained the radios that we used. Without radios, we simply could not operate. Radios were the tools of our trade and key to everything. In Afghanistan, our number one priority was communications. The satellite radio was the most important device we used, even if most of our women and men did not know or appreciate that. It was our lifeline to medical support, fire power, logistics, and everything else. Without radios we would have come to a standstill. And then our radios were thrust into the limelight in a way that we never anticipated. We were responsible for 200,000 square kilometers and our systems could not support this range. Not to be deterred, we invested time up front with our signallers to modify these radios. Never have I had more conversations with technicians and geeks about how to upgrade our machines. This included building an information architecture that was understandable to the non-technical and technically savvy alike. The new system had to be robust and scalable. What transpired was nothing less than remarkable. We built our IA (two-way) radios and modified the code inside our machines, which were able to support us in every daily aspect that we faced, along with changes we made on the fly. Our radios were as much a part of us as the number-three rifleman in our infantry battalion. Both were equally important and the loss of either had tragic consequences. I watched the British IA and radio system crash twice during operations and the impact was catastrophic. Clearly, investing the necessary time and resources to achieve the synergy between man and machine working together was (and still is) critical. DF*

In their thoughtful study of this new type of collaboration called simply *Human + Machine*, authors Paul Daugherty and James Wilson offer dozens of compelling examples of cooperation between humans and machines that lead to novel and otherwise unattainable outcomes.[67] They describe the incredible respect the workers they studied have gained for their machine colleagues. Together they have moved mountains. But when at first you suggest that your workforce treat their technological partners as equals, you may get some kickback. Deep down, there may be a combination of skepticism *("No machine can do what we do")*, fear *("There goes my job")*, and change fatigue *("What are we up to THIS time?")*.

Spoiler Alert:

Metropolis

The lessons of Fritz Lang's German sci-fi masterpiece *Metropolis* are so relevant in the time of our own digital pivot that a completely restored version was released in 2010, some 83 years after its initial release. Set in a futuristic urban dystopia and hearkening back to the turmoil of the industrial revolution, the film portrays the efforts of the young, wealthy idealist Freder and his ally Maria as they rebel against the abuses perpetrated against workers by the intelligent machines that run the city. In a prescient nod to the critical need for emotional intelligence in times of technological advance, the film ends with a single title card declaring: *"The Mediator Between the Head and the Hands Must Be the Heart."* As humans rely increasingly on intelligent but heartless machines for productivity, leaders of organizations have a clear duty to ensure that authentically human values are engineered into the algorithms that propel these machines to action.

It may be that when you talk about the new approach, staff might assume you mean more use of computers. They may not understand the value or even conceive of bringing AI into an organization, even though they use AI themselves countless times a day. AI directed them around slowed traffic this morning. It found them a cheaper flight overseas, and then identified a quaint beach house to rent for the weekend. AI tracked their package and predicted a noon delivery, and AI popped that news story about flood damage onto their smartphone's home screen. AI said their Uber would be there in seven minutes and predicted that the ride would cost 26 Euros. Tonight, AI will suggest what they might want to binge watch, given their viewing habits. So not only do your staff already use AI; they already appreciate it and depend upon it. They have so quickly adapted to its benefits that a return to pre-AI days would be unthinkable. And while their resistance may be related to job security, embracing AI is likely the best (and perhaps only) way to make sure that jobs within your organization will for still be there for them later.

While change fatigue may be at play in resistance to the transformation your organization is about to make, presuming that humans resist change by nature is a misunderstanding of our behavior. We change all the time, but we tend to do so in inverse proportion to the level of effort needed to do so. Think about it. If you've eaten at the same restaurant for ten years running and then suffer through three poorly cooked meals in a row (or offhand treatment from the proprietor just once), you'll change that decade-old habit the next time you make a reservation. On the other hand, your bank can give you appalling service with usurious charges for years before you embark on the complex and lengthy process of moving all your accounts, lines of credit, mortgages, automatic payments, and signing authorities to some other financial institution. That change is brutal. Humans don't resist change by nature, but we do weigh the cost of that change against its expected benefit.

MARK: *Suspicious minds* – *Automation must overcome some strong cultural barriers before it achieves workforce domination. Such barriers are not just the subject of pre-pivot narratives such as Metropolis (1927) and 2001: A Space Odyssey (1968). The most recent installment in the Star Trek franchise, Picard (2020-), begins in a future where organic lifeforms have outlawed all artificial life, out of fear of a robotic Armageddon, reflecting our own present-day hesitations surrounding robots.*

For businesses, automation requires a huge upfront investment and a reconsideration of how things operate, which is often enough to delay or prevent uptake. And employees who are worried their jobs will be replaced by robots are, understandably, resistant. They may fear the "automation apocalypse," wherein only those who own the robots prosper and everyone else lives in squalor. Job losses are indeed inevitable, with midpoint estimates suggesting about 15% of the global workforce (400 million workers) will be supplanted by automation by 2030.[68]

But it is not all doom and gloom. Most evidence suggests that new technology will ultimately spur job creation and growth. Consider the first industrial revolution as an example. In 1840, over 60% of workers were employed in agriculture. But technologies changed the nature of work, centralizing labor in cities and increasing efficiency in farming. By 2000, only 2% of workers were employed in agriculture.[69] *Looking at jobs lost alone, we would believe society became largely unemployed. However, technology created a host of new jobs. People began working in factories, designing new machinery, and moving cargo vast distances with planes, trains, and automobiles—jobs that were previously unimaginable.*

We face a similar situation today. While some types of jobs will be lost, demand will rise for roles like big data scientists, information security officers, machine-human relations designers, technology interpreters, augmented and virtual reality architects... the list goes on. And these are just the jobs we can foresee based on the technology available today. Competition will be fierce to attract and retain employees with in-demand skills in the fourth industrial revolution world, whether they are working with cobots or doing brand new jobs. Businesses can prepare now. By helping existing employees reskill and upskill, organizations can future-proof their workforce. MJB

One of the difficulties workers have with human-machine collaboration is AI's own fault. At its best, AI is invisible. It works in the background to deliver us new ways of learning, playing, creating, organizing, and communicating. Once AI is in place, we don't have to think much about it. We just get on with our lives. We adapt quickly.

Artificial intelligence's background existence produces a confusion known as the AI effect. The term expresses the human tendency to dismiss the advances of AI as *"impressive but not actually intelligent."* Homo *sapiens sapiens* (the only remaining species of six known subsets of Homo *sapiens*) evolved with a deep presumption of its superiority over the lesser orders. The bias that humankind should dominate all other species appears early in the holy books of monotheistic religions. As AI creeps in among us, it is not surprising that we tend to set ourselves above it. The so-called AI effect is our contention that any accomplishment, such as roundly beating a human at Go—a game whose mastery has long been thought the pinnacle of human intelligence— should be dismissed as great tech, but not *intelligence* per se. Writing in *The Washington Times* in 2006, writer Fred Reed put it simply:

> *A problem that proponents of AI regularly face is this: When we know how a machine does something 'intelligent,' it ceases to be regarded as intelligent. If I beat the world's chess champion, I'd be regarded as highly bright.*[70]

In praise of Luddites

Whenever people object to the adoption of any technology, be it related to industrialization, automation, or computerization, champions of that technology will sometimes refer to their objectors as *luddites*. Though the term is used to characterize doubters as ignorant adversaries of progress, the Luddites of history were hardly ignorant. On the contrary, they were experienced practitioners who insisted that technology be adopted only after wise consideration of all the inherent risks.
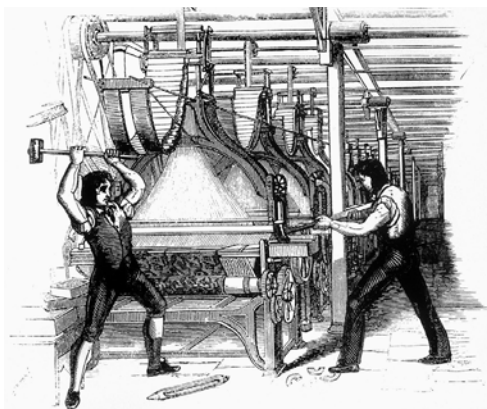

Figure 5.3: Luddites occasionally attacked machines to protest the displacement of human artisanal skill.

An early concern during the first industrial revolution was the low quality of textiles produced by the spinning machines brought into English factories in the late eighteenth century. The Luddites recognized that, while human weavers at the time could produce linen and wool of far superior quality on their own cottage looms, they could not do so as quickly or as cheaply. They argued, however, that despite any economic advantage, the imminent and permanent loss of artisanal skill would be a crippling disadvantage later. When no one listened, they protested, even on occasions smashing a few machines to make their point.[71] Sadly, it is the destruction alone for which they are remembered. In our day, we need luddites more than ever. Anyone who argues that a given technology produces substandard or dehumanizing results may well be right. Those concerned about the replacement of human workers by robots, just like those who see the downside of genetic modification, autonomous weapons, facial recognition, and DNA identification, have critically important opinions about the ethical implications of our decisions. Those opinions matter. Let the debate continue.

Human intelligence is changing too

The internet arrived just under fifty years ago and has already split society into two categories: digital natives and digital immigrants.[72] Digital immigrants were born or brought up before the widespread use of digital technology. Digital natives, on the other hand, were 'born digital" and belong to the Millennial generation and beyond. Digital natives (today, comprised of Millennials and Gen Z) often get labelled as distracted and shallow. But clinical research proposes that their brains are evolving differently than those of digital immigrants, and very much to their advantage. American educational theorist Marc Prensky, who coined the two terms in his 2001 article *On The Horizon*, claims that the average college graduate (therefore, a digital native) has now spent fewer than 5,000 hours of their lives reading, but over 10,000 hours playing video games and 20,000 hours watching TV.[73] Natives have grown up in a world where instant messaging, email, social media, and a 24/7 news cycle is the norm. In response to these different stimuli, digital natives have evolved new ways of processing information. In fact, new research points to the fact that the native brain may have physically changed to cope with the steady influx of information they have become accustomed to receiving.

Figure 5.4: Technology is changing the human brain.

This intrigued doctors at UCLA's *Semel Institute for Neuroscience and Human Behavior*. Using MRIs, they studied the impact of technology on neural networks. In one test, they found that when digital natives search the internet, their frontal lobes are far more active than those of digital immigrants doing the same task. Given that frontal lobes are typically associated with decision making and conflict resolution, it seems that the natives may have been evolving neurologically to take advantage of the new digital world they inhabit.[74] These findings corroborate earlier research published near the end of the pivot by the University of Minnesota. That study found that the new generation works, writes, and interacts in novel ways, and is more engaged over the web.[75] Thanks to their modified brains, digital natives react more positively to the adaptation of new technology. While there is still much research to be done, these preliminary findings could lead to reform in education, decision-making, linear thinking, and training.

MARK: *The Digital Nomad* – *We are at a tipping point. By 2025, Gen Z will make up almost one third of the workforce in much of the world.[76] In the US, Gen Z's numbers in the workforce will reach 51 million by 2030, with a collective income of $2 trillion.[77] Having grown up digital with the sum of humanity's knowledge at its fingertips, this generation moves faster and innovates like no other. They expect to use the same tools in the office that they use in their leisure time—social media, mobile connectivity, gesture-based interfaces, and wearable devices.*

flexibility for granted. Supported by "anytime, anywhere" access to business tools and the cloud, employees will be unconstrained by time or space. As a result of these seismic shifts, critical new worker personas have emerged. Chief among these is the Digital Nomad. Initially championed by Millennials and Gen Z, the Digital Nomad is remote, mobile, and must be able to collaborate effectively within and outside of the organization. At OpenText, almost 50% of our employees are Millennials, and we are hiring Gen Z-ers all the time. We can see the way these generations think at scale, need mobility, and want shared access to information so they can invent new concepts.

If these trends were the arena of the young and tech-savvy before, COVID-19 dramatically enlarged them. Remote work skyrocketed during the pandemic, and it persists even as the pandemic shows signs of receding. Many organizations have shifted permanently to a more distributed, hybrid model, with workforce approaches that offer flexibility first. Enabling your virtual and hybrid teams requires tools that make it easy to find, share, and update information securely, regardless of location, device, or application. This is especially vital when a crisis hits. The composition of the workplace is transforming. It's time to rethink the way work gets done. MJB

DAVE: *Better in than out* – *The NATO coalition in Afghanistan was as complex as any entity as I have ever commanded. We were a disparate group of military and civilian men and women from 37 different countries on a life-and-death mission. As such, there were endless differences of opinion to be considered in every action. But coming out of the American system, where diversity of opinion is seen as an asset, I welcomed the friction. Because of it, we thought better and achieved better results. Consider that strategy when you recruit your teams. Bring in people from a variety of backgrounds and disciplines. As*

long as they're devoted to your overall mission, don't look for them to agree with you about how to get it done. If you allow competition to thrive inside your organization, you will be better prepared when competition comes at you from the outside. DF

Anticipant humans

Just after the digital pivot in 2011, American technologist David Weinberger wrote, *"Business is a conversation, because the defining work of business is conversation—literally. And 'knowledge workers' are simply those people whose job consists of having interesting conversations."*[78] We couldn't agree more and would add that anticipant workers make sure the conversations are about what's coming next.

Anticipants are atypical, but as a cohort they tend to share a few telling qualities you should look and interview for when you build your hybrid teams. For starters, by definition, they are anticipants, not participants. They are outliers. They are innovators, not inventors. They are realizers, not dreamers. They are iterators, not perfectionists. They exercise EQ over IQ. They respect theory but rely on instinct. They are not rule followers; you might say they are the straws that stir the drink.

Also, anticipants are self-driven. They show relentless initiative, jumping into action when they need to know, explore, test, or validate any idea, hypothesis, product, or plan. They have pride of solution, not merely pride of authorship. They are widely informed self-educators. They have hybrid experience in the disciplines you practice. And they get things done quickly.

Next, anticipants are problem-solvers. They are natural co-creators who revel more in the practical effect of their novel thinking than mere recognition of their effort. They are solution seekers, intrigued by any problem that needs their attention. They are technologically literate. They are comfortable assigning tasks to machines that can accomplish these tasks on a greater scale, faster and with better accuracy that they could on their own.

And as you probably suspect, anticipants are networked. They rely on trusted networks of allies both inside and outside the organization. They function in multiple dimensions. As such they are inter-disciplinary, inter-organizational, platform independent, and frequently international in their reach. They favor their own channels of communications over mandated channels.

Anticipants are also evidence-seeking. They have larger-than-average apertures, constantly scanning the horizon to assess the changing environment. They are never reckless. They calculate, assessing the relative likelihood of a wide variety of possible scenarios. Thus, they take bets but will not risk the enterprise. They see failure only as a compelling reason for mid-course correction. In this they are more comfortable with scientific method than persuasive argument. They do not sweat details, but never take their eyes off big-picture objectives. They are pragmatic, recognizing the value of solutions that are both technologically feasible and market appropriate.

DAVE: *In search of the anticipant* – *All relevant organizations in the digital age will be staffed by anticipant humans. In times of relative calm or following a period of great turmoil, a leader who is focused may be what an organization needs (we can discuss that later). For now, I will discuss the need for anticipant humans. Once again, we go back to operations and real-life situations, where forcing functions drive the need to have the right people as leaders. Throughout my experience (on operations or during change), leaders find those people inside their organization or outside who can anticipate at the same speed and scale as they can. This is a small group that operates with more agility than the rest of the organization. While out in front, they provide the path that the others will follow. In the military, these groups are normally found embedded near the leader and are called the Commander's Action Group (CAG), for example. They might have nicknames like Jedi Knights and can be ostracized by their fellow workers. What is unique is their intellect and the ability to look forward without being tied to the past. David Petraeus was known to be a thinker and innovator and he had his group of anticipants, including HR McMaster, who I got to know. While not all their ideas were effective, their forward thinking did inspire the U.S. to change its organization to suit the operational requirements of the security environment. In Canada, Rick Hillier tried to do the same with the Canadian Armed Forces (CAF). His efforts were effective while he was in the chair; however, sadly, much of what Rick tried to do has eroded over time because the routine-based processes re-took control after he left. DF*

Let the machines fight it out

The speed and scale of attacks perpetrated in the suprahuman domain makes it risky to leave a crisis response to humans alone. Better to have machines on the team here too. That's because even when network access by an infiltrator can be curtailed by an alert operator within mere minutes, the damage will often already have been done.

An emerging automated defense is a species of software that constantly monitors all URLs, IPs, files, and mobile apps connected to an organization's network, assessing each entity for its likelihood as an originator of malicious behavior.[79] Some applications assign each connected entity a so-called reputation, ranked on a linear scale of trustworthiness. Determining whether any connected entity is trustworthy is based on factors such as incidence of prior attacks coming from that location, and that entity's own connections to other entities whose reputations can also be determined. Such profiling can take some of the complexity out of deciding who can be trusted and who cannot.

But criminals and adversaries will seldom take the same route twice to a target network, so the relative threat from any given URL can increase and lessen in short order. Advanced threat systems are designed to look for that dynamic and will give the client organization real-time assessment of billions of possible threats, sometimes displaying them as colored nodes on an interactive display. Security teams within the organization can then click on any imminent threat, learn more, and decide whether to shut that connection down.

Some software solutions will prohibit access automatically based on established rules, shutting down connections to the most likely offenders until such time as their reputations improve. It's no guarantee of imperviousness, but deploying this kind of machine-human defense system is far better than waiting in the dark for the next attack.
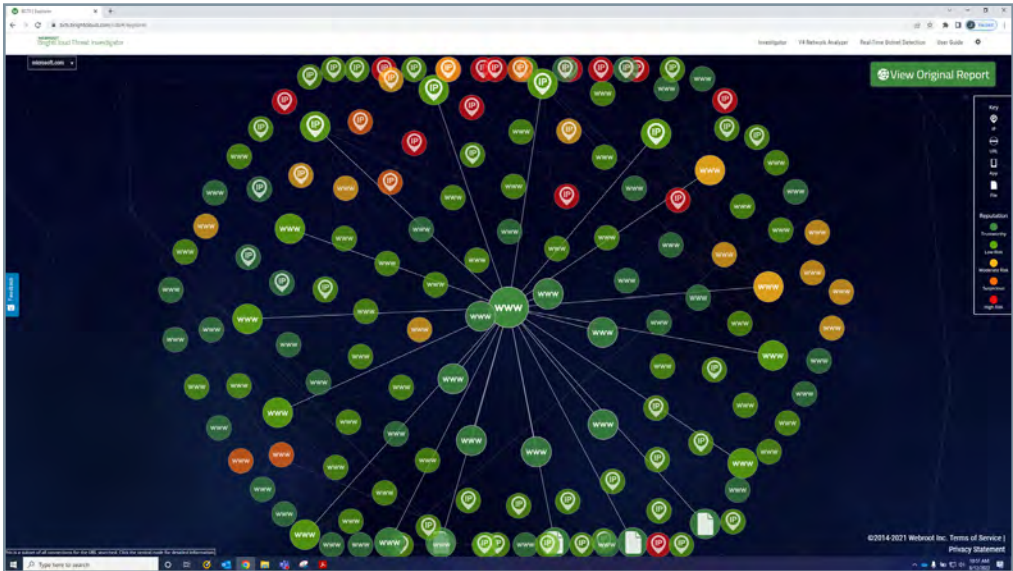
Figure 5.5: Contextual threat intelligence is offered by a new category of apps referred to as threat-assessment solutions. In this example, OpenText's BrightCloud® maintains a massive contextual database that maps the relationships amongst billions of URLs, IPs, files, and mobile apps. This empowers predictive threat detection and forensic analysis by mapping relationships with known identified threats.

MARK: *Zero trust* – *Do you trust where your data is today? Just read the news on any given day to see examples of data breaches. Cybercriminals are effective because they have the latest technologies at their disposal. Machines are deployed against the enterprise's defenses, operating with a volume, speed, and agility humans can scarcely comprehend. Organizations need to counter machines with machines to have any hope of stymieing today's threats. It is a machine versus machine world. And the attack surface grows with every passing day. Two-thirds of employees use their own devices for work. This presents a risk for companies, given that consumer PCs are twice as likely to be infected by malware as business PCs.[80] The future is one device, for everything, and it needs to be secure. The enterprise must protect business data from leaking and determine whether any specific device can be trusted at any given time. It's your edge—secure it, investigate it, defend it. Own it.*

The classic castle-and-moat security strategy, which assumes threats are external, is useless when the bad actors are already inside the network. The average dwell time for threats in a corporate network is 100 days; the threat enters the system and waits over three months before acting. Traditional security does not have the tools necessary to root out these lurkers before they can do harm. Add the fact that 53% of breaches are caused by simple human error from the enterprise's own employees, and it is clear that giving users free rein once inside the perimeter is a bad idea.[81] Malicious insider threats—like disgruntled employees, corporate espionage, or foreign government agents—must also be guarded against. Everything must be monitored for suspicious activity.

Organizations need a new approach to security: Zero Trust. In the Zero Trust model, users and endpoints are not trusted until they are authenticated—and even then, they only gain access to specific applications and data, and they must reauthenticate periodically to maintain access. Smart threat detection technologies patrol the network, analyzing patterns and flagging anomalous or suspicious behavior. Critical data is centralized and protected within layers upon layers of security, extending from the heart of the enterprise out to all endpoints. Protection is complete against all attackers, external or internal. Zero Trust follows the data, no matter where it travels. MJB

DAVE: *The new paradigm* *– After returning from Afghanistan in 2006, we took time to reflect what had changed, and decided it was everything. The speed and scale of operations had increased exponentially. Our old way of thinking was too slow and pedantic. We needed agility and flexibility of thought and process to be successful on the battlefield. So, we created the 1st Canadian Division Headquarters in Kingston, Ontario in 2010 and adopted a new paradigm. It would have to be more scalable and responsive based on both our experiences in Afghanistan and the constantly changing security environment. We had to get faster at planning and decision making. The first thing I did as Commander was to sit down with my Signals (IT) team who managed our computers. I said that our current processes were too slow, and tools like PowerPoint were ineffective. We needed to change how we did things to get more out of our technology. Speed and scale drove everything. The challenge was enormous, and our Signals team loved it. They had a real operational requirement to solve AND they got to write code! We created a team and began to experiment within our headquarters. We made progress, instilling a new sense of purpose, teamwork, and a mix of both IQ and EQ in our people in ways we never had before. We began to adapt to the new paradigm, one that would allow us to make better decisions, faster. I learned some valuable lessons with this experience. One was about the arrogance of human teams. Sometimes, the subject matter experts in an organization use their positions of power to the detriment of both their organizations and leaders. This new paradigm was a cultural challenge for us, as well as a technological one. We needed to get some of our humans to understand that machines do some things better than we can. The lack of connectivity of diverse groups was another limiting factor. To overcome this, we collaborated with the private sector, and that kind of hybrid collaboration was key to our success. DF*

The corpus callosum rules

As you form your human-machine teams, you will be building powerful hybrids of logical and emotional intelligence. Over time, machines will provide more and more of the IQ you need to manipulate and deploy vast amounts of data, while humans offer the creative, caring, and wise insight that defines emotional intelligence.

In this way, your teams will begin to mimic the human brain, whose left and right hemispheres manage thought in markedly different ways. The staggering power of this combination is possible only as these hemispheres exchange information through the *corpus callosum*, the broad band of nerve fibers between them. Keep that analogy in mind. Humans and machines collaborate effectively when they have a perfectly working interface. As you increase the anticipant aptitude of your organization, you will harness their combined strength only if you have protocols that promote and enable constant communication between humans and machines.

DAVE: *Build a matrix of human geography* – *Learn to think of your organization not as a workforce but rather as a group of tribes and subtribes working together. Each tribe thinks uniquely, values different things, approaches tasks in a particular way and, most importantly, measures success by its own standards. In the military, the army, navy, and air force have different cultures. They are distinct tribes. And within the army, there are also subtribes; the artillery, armoured, and infantry corps do different things, come from different backgrounds, and share distinct histories of which they are rightly proud. Go deeper still. Within each corps, there are sub-subtribes of men and women, and among those we have sub-sub-subtribes of twenty-year-olds, thirty-year-olds, and forty-year-olds who see the world differently. To speak effectively to any large group, therefore, you must build a matrix of a communication that identifies the right message and the medium to speak to each subtribe in an empathetic, inclusive way. The digital world has taught all these people that they can expect to be treated as individuals. Make that happen. DF*

ANTICIPANT APTITUDE

EQ   **IQ**

Atypical
They are anticipants, not participants. Innovators, not inventors. Realizers, not dreamers. Iterators, not perfectionists.

Balanced
They exercise EQ over IQ equally.

Instinctive
They respect theory, rely on instinct. While they are not rule followers, they are never relentless or reckless.

Self-starting
They show initiative, jumping into action when they need to know, explore, test, or validate any idea, hypothesis, product, or plan.

Proud
They have pride of solution, not merely pride of authorship.

Confident
They see failure only has a compelling reason for mid-course correction.

Intimate
They favor their own channels of communications over mandated channels.

Connected
They rely on trusted networks of allies both inside and outside the organization.

Machine ready
They are comfortable assigning tasks to machines that can accomplish these tasks on a greater scale, faster and with better accuracy than they could on their own.

Nimble
They function in multiple dimensions. As such they are inter-disciplinary, inter-organizational, platform independent, and frequently international in their reach.

Scientific
They respond to empirical proof more than to persuasive argument.

Informed
They are naturally curious, and widely informed self-educators.

Ready
They have hybrid experience in the disciplines you practice.

Fast
They get things done quickly.

Focused
They keep their eyes on the big objective.

Clinical
They calculate, assessing the relative merit of many possible approaches.

Realistic
They seek solutions that are technologically feasible and market appropriate.

Curious
They are solution seekers, intrigued by any problem that needs their attention.

Savvy
They are technologically literate.

Aware
They have larger-than-average apertures, constantly scanning the horizon to assess the changing environment.

CHAPTER 6

THE NEW ANTICIPANT ORGANIZATION

Given that every anticipant organization is unique, any attempt to define their features or operations in a prescriptive way would be folly. In our experience, however, there are a few common characteristics of anticipant organizations that allow them to act differently from traditional entities. We'd like to share a handful of those with you before we describe how to transform your own organization into one of them.

An organization is just a tool for getting things done. Indeed, the word itself comes to English from the Latin word *organum*, which means an instrument or tool.[82] Within every organization, there is a continuum of responsibility defining how elements within respond to events in the cycle of operations. Shaping that continuum occurs along a chain of command, a deliberately chosen and refined structure that leaders believe will make operations effective. The links in that chain are ordered in a hierarchy of communication to ensure that each individual knows who to talk to as they respond to everything that hits them.

One way to deduce the nature of an organization is to note which function takes the lead in that chain. If yours is a technology company, your research and development branch takes the lead (no innovation, no growth). If yours is a grocery store, your supply chain management is key (no bananas, no sales). If yours is a charity, your project management gets top billing (no efficiency, no funding). If yours is a battalion in the field, your senior officers are in charge (no orders, no headway). Ultimately, which department takes the lead depends on what your mission is. Or it should.

During routine operations, the lead function rides near the top of the chain of command, with the authority it needs to dictate how the organization operates. Orders go down, reports come back up. But when a crisis arises, that tidy arrangement can be an impediment to initiative. At that point, each layer in the organization chart is a damper, a brake, a governor. In a nanocrisis, adherence to the org chart is the kiss of death. So, the first hallmark of an anticipant organization is elasticity.

Elastic, not flat

Anticipant organizations have a dynamic chain of command. The org chart in such entities is explicitly designed to collapse in crisis and expand when the crisis has ended. In the military, such periods are war and peace. In non-military environments, they are the nanocrisis and the routine operation.

Historically, how flat your organization can be in a time of crisis has depended entirely on the means of communication available to it. If I am a Roman emperor with continental ambitions in 70 CE, I must organize my forces so that those giving orders can make themselves heard by the soldiers they command in battle, and battle in my time is both close-in and noisy. A leader with a lone voice can be heard by a squad *(contubernium)* of about eight men. That's about it. Ten or twelve of those leaders (leading about 100 soldiers in total) can receive signals with fidelity from the next level up, where *centurions* with stentorian voices, drums, bugles, smoke signals, or even flares can make themselves understood. The hierarchy continues upward, always as a function of how many troops can be kept in contact between layers. This reality has continued through history, with the scope of command depending entirely upon the information technology available, even as it evolves (voice, drum, runner, horseman, flag hoist, signal tower, telegraph, telephone, radio, satellite, video, internet, etc.).[83] Fast forward to today, where a colonel in a headquarters a hundred or even many thousands of miles from battle has unprecedented, sophisticated communications technology that changes the game forever. As the film *Eye in the Sky* reveals, unmanned aerial vehicles (UAVs), such as predators and swarming drones, have eyes on any aspect of the battle. In the movie, Army Colonel Katherine Powell gains her situational awareness not by digesting the reports of her subordinates, but rather by experiencing events as they occur through live streaming. Then, as needed, she can be in instant, ongoing contact with any single member of her force. The usual military hierarchy is dispensed with. In crisis, the organization chart is deliberately collapsed. When the colonel can talk to a sniper with a target steady in his sights, the org chart can be only two levels deep. But that works only because, during that crisis, the colonel has access to *all* the information and *all* the people *all* the time. That's a three-part advantage that all anticipant organizations can make use of.

Spoiler Alert:

Eye in the Sky

One of the onerous responsibilities of post-pivot leaders in our age of advanced intelligence, surveillance, and reconnaissance (ISR) will be to manage the complex moral and legal issues brought about by the creation and deployment of lethal autonomous weapons systems (LAWS). Gavin Hood's 2015 thriller *Eye in the Sky* tackles the issue head-on as British Army Colonel Katherine Powell (played by Helen Mirren) finds herself in an ethical grey zone. With streaming intelligence from a vast array of ISR inputs including a long-range USAF MQ-9 Reaper drone and short-range ornithopters and insectothopters on site, Colonel Powell enjoys unparalleled situational awareness. But the officer is soon mired in a slurry of conflicting legal, political, and ethical dilemmas as she considers escalating the mission from "capture" to "kill."

DAVE: *Flat and fast* – *When I took command of NATO forces in the south of Afghanistan in May 2006, all operations were conducted by a massive, well-rehearsed hierarchy. This chain of command had been devised over decades of a Cold War, structured as a complex risk-management machine. All our protocols ran at pre-pivot speeds of engagement. Frankly, they were designed in the days before email, and the pace we were used to soon proved to be the greatest threat to our success. I simply wasn't prepared for the speed at which we would have to operate to achieve our mission. Within six months, we flattened our hierarchy and introduced new paradigms of reporting, deciding, planning, rehearsing, and executing any action. We joined the digital age. With better tech and a newly flattened structure, we could accelerate everything. Our faster battle rhythm—the speed at which we acted when engaging the Taliban—soon became the new normal. It was critical to preventing the insurgents from toppling the newly established Afghan democratic regime. I only learned later that this acceleration we were forced to achieve was not a uniquely military challenge. We were mid-pivot in 2006, and these changes were taking place around the world in every sector of society. DF*

Like the military, anticipant organizations have access to communications technology that allows them to flatten in time of crisis, then expand afterward. Being flat is not the goal: being elastic is. Anticipant organizations keep their hierarchies intact during routine operation and collapse them in time of nanocrisis. Once the crisis has been managed, the hierarchy must be restored. The colonel can tell the sniper when to pull the trigger, but there's no merit having the sniper ring up that colonel a week later to arrange the dates of her leave.

conceptualized this book, we discovered parallels in our experience as leaders of business and the military. Mergers and acquisitions are like an army taking over a battlefield. Salespeople function like soldiers or fighter pilots, expanding into new territories and markets. There are key differences, of course. Where business is profit-oriented, the military is mission-oriented. The military is very tactical but then they spend a lot of time rehearsing. They are extremely good at running scenarios because they have to prepare for the unthinkable. This doesn't happen enough in business (which is why we wrote this book). In the private sector, if you don't make your quota, you're either fired as a leader or your company is bought. In the boardroom, you're constantly at war (unlike the military, which experiences long periods of peace between battles). The forcing function in the private sector happens every day. You don't have time to think and adjust because you're executing all the time. There are shorter cycles, though both businesses and militaries struggle with the competition and ultimately must succeed or die. TJ

Collapsible, not lean

A process is a repeatable series of steps designed to achieve a consistent effect. Since the advent of time-and-motion studies in the late 1940s, experts have been trying to figure out how to make processes leaner, which usually means cheaper and faster. Automation has been a great driver of such efficiency, with computers bringing exponential increases in speed to processes. But the advantage of automation—invariant replication at speed—is precisely its limitation. Often, we don't need the same thing over again. We need something different, and we need it fast. Anticipant organizations know that in a crisis, responses will have to be more tailored, yet never slower. So they build employable models of crisis activity. These are nothing more than processes with steps missing, just as the reporting structure in a crisis is nothing more than an org chart with layers removed. Both are temporarily collapsed. There is no value in just making the day-to-day org chart and routine processes abbreviated so that they will work in crisis too. Both must be collapsible, not lean. When they prepare for and rehearse a nanocrisis, anticipant organizations simply predetermine which layers of an org chart to collapse and what steps of a process to remove. Only then can their designated response teams act with both authority and initiative.

TOM: *Collapsing the org chart for opportunity* – *At OpenText, we flattened the org chart by moving customer service online to a Knowledge Center. All customers could view the questions and answers to any issue on this self-help site, which improved the quality of our response, increased customer satisfaction levels, and reduced our cost of delivery. Moving our support online resulted in a 24/7 experience for all customers. Prior to this, customers would sometimes have to wait until 9 a.m. on a Monday in whatever time zone they were in for help. Virtual support services gave our customers anytime access to materials, including upgrades, fixes, and issues. We rolled this out globally, so the customer support team could deal with any issue, regardless of location or time zone. We took this internal as well, by gating a part of the Knowledge Center to support product development. By creating an internal knowledge center available to all employees, regardless of title, position, or department, OpenText experienced a huge boost in innovation. Suddenly we had a platform for crowdsourcing ideas. All information was transparent, everyone could access it and contribute their ideas. It allowed all voices to be heard and the best ideas to percolate to the top, regardless of where they came from. And the best ideas would win. Prior to the Knowledge Center, the development of ideas for products and services went along departmental lines and were "passed up" the chain of command. They moved through the hierarchy, and then were shared in a committee which was far removed from the "coalface". The efficacy and efficiency of this method was greatly exceeded by the flattened hierarchy of a Knowledge Center in which there was no delay and no filtering of good ideas. TJ*

Adaptive, not automated

Now that the world of work has passed through its first two phases of technological competence (standardization and automation), the greatest gains come to those who embrace the third phase: adaptation. Adaptation is the use of technology to innovate, which means to improve incrementally; it does not mean to 'invent.' The classic example of such adaptation concerns the manufacturer of drill bits whose leadership foresaw the advent of lasers in millwork.[84] Their mission had long been to make the best drill bits going, but laser drilling—if perfected by competitors—could present a formidable threat to their profitability. They wrestled with the problem, and then appreciated that the new technology didn't threaten their company; it just required a redefinition of their mission. They recast that mission, seeing themselves for the first time not as makers of drill bits but rather as makers of holes. That adaptation allowed them to see a new technology not as a threat, but as a powerful competitive advantage. They brought the new technology in house and became laser-drilling experts. Anticipant organizations bring human intelligence and machine intelligence together to find new ways to innovate. Backed by AI, they embrace adaptation just as they did automation. That's their competitive advantage.

MARK: *Going up? Switching to the cloud* – *During the pivot, OpenText established itself as the leader in information management, helping users access the crucial business data they needed, when they needed it. But as we transitioned into the post-pivot world of the 2010s, everyone could hear the rattle of change. The cloud was upending our industry, and it was obvious not every company was going to make it to the other side. I was working in Silicon Valley, and when I joined OpenText in January of 2012, it was clear to me that the company had potential in cloud computing. It was time to adapt. It was time to rise to the cloud.*

This was not a change that happened overnight. This was about building a new foundation for our company. We had to innovate, which we did through intense internal development and a focused M&A strategy which brought us new cloud technology. In 2012, OpenText acquired EasyLink, a global provider of cloud-based electronic messaging services. Now we could offer some of our services on-premises, in the cloud, or in a hybrid deployment. In 2014 we acquired GXS, expanding our Information Exchange portfolio with a cloud-based trading grid and giving our customers the ability to manage critical information flow both inside and outside of their organizations. We became laser-focused on the cloud and made cloud services one of our top priorities.

Since then, our momentum has accelerated. In 2020, we offered a cloud-native product release, our biggest release ever. Today, the OpenText Cloud is one of the largest private clouds in the world. It operates in 50 state-of-the-art data centers and 20 satellite points of presence (POPs). Offering cloud-based services has been instrumental in our ability to serve our customers throughout the pandemic and other crises, to help them adapt at speed. And with our new Project Titanium, we are delivering the future of information management through a common, unified, and integrated cloud platform that offers unmatched capabilities and global scale. As an organization, we were not born in the cloud. But we have certainly been reborn there. MJB

Crowdsourced, not sampled

Crowdsourcing really has changed the way an organization can think about strategy, especially where it concerns the development of new products and services. Until the pivot, sampling and focus testing were the common, if imperfect techniques for making hypotheses about the marketability (in business) or the suitability (in public consultations) of various proposed solutions. But the conclusions reached through sampling and focus testing were presumptions only, and often disastrously wrong.

In the 1950s, the Ford Edsel scored high among focus-test groups and yet almost immediately bombed in the market. The buying public found them to be unattractive, overpriced, and overhyped. The mistake lost the Ford Motor Company $250 million in development, manufacturing, and marketing costs.[85] So too Classic Coke. So too, it may be argued, Brexit. Asking a sample group of people for their opinion and then presuming that "what is true of that group must be true of the wider population" is risky business. (Notably, that presumption is one of the classic forms of false logic identified by Aristotle.) Crowdsourcing alleviates the risk. Anticipant organizations can ask everybody at once what they think, and watch keenly as they react, listening carefully when those customers give their feedback. This capability leads directly to the next hallmark of the anticipant organization: iteration.

TOM: *How to demote people upward* – *There was a point in the growth of OpenText when we began losing executives at an alarming rate. Back then, one expected senior professionals to move to new opportunities every seven to ten years. But we had just entered a period of hyper-growth of 30 to 40% per year, and our senior retention rates plummeted. Here's why: The great leaders we had couldn't upgrade their skillsets fast enough to rise to the next level and lead their teams effectively in new endeavors. Most of these were hands-on engineers with little interest in the hands-off leadership they'd have to exercise at higher levels. Having been fired once myself, I understood that. So, we did two things. First, we formed a management team of leaders who had moved over to new positions within our company. Even though they hadn't been promoted, they were all experts in the way we operated. They had too much corporate intelligence to waste. They made an impressively effective management team because they all knew each other's jobs. Each had already been a president or general manager, and each took on a new role doing what they had enjoyed most, whether it was as a sales manager, product manager, or product marketing manager. Everybody went back to their original joy. That gave us a highly effective management team. Second, we hired senior people with a promise that if they succeeded in their roles, we would move them laterally so they could replicate their successes elsewhere. Then, when the time came to replace them, they were celebrated, not cast aside. Where before they might have felt overlooked or demoted, they were acknowledged as 'A Players' and assigned new challenges at the level they knew best. Lateral moves were now seen as upward progress. Our retention rate went right back up again. TJ*

Iterative, not perfect

The last two decades saw the rise of a cult of excellence within organizations. An untested assumption was made that the more perfect a product or service, the more that people would subscribe to it. Yet that does not seem to be true. In study after study, it has been shown that products and services that exceed customer expectations do not earn more praise, loyalty, or revenue. People's needs tend to be less sublime than we thought. They look for and prefer products and services that are useful and reliable, and they're eager to give their feedback on how improvements should be made. So anticipant organizations do not need to invest vast resources in designing and building solutions in the hopes that they will be perceived as perfect. They choose instead to work on a design until it is 'good enough.' They then release it and ask the public for feedback. When they get that feedback, they make improvements, put the next version out, and ask for more feedback. This kind of immersive, live-market testing furnishes two critical metrics: how many people will use what they've built and how their customers or stakeholders think they should improve the next version. Attentive to this feedback loop, anticipant organizations are more honest about their development processes, and are happy to make appropriate tactical alterations to their designs as the public walks them on target. They iterate rather than perfect.

TOM: *Not perfect but good enough* – *In 1996, Netscape® started a revolution in software design when they put out "good enough" versions of their browser. They were the first to understand the power of the web and what would eventually become "Cloud Services" with its capacity for the continuous improvement of code through fixes and refinements that could be uploaded on a daily basis. Netscape didn't wait for "perfect," which was part of the old delivery model of software patches and releases. They used to be shipped by CDs and other physical means, making it impossible to alter any code once it had been sent. The continuous release method has resulted in superior product application development that enabled users to participate in design decisions every day. Soon, most software development would follow this iterative method. TJ*
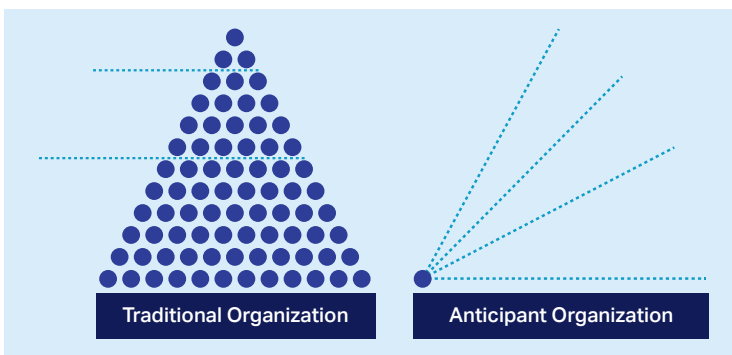

Figure 6.1: Influence Flow: Traditional vs Anticipant Organizations

In this diagram, each dot represents a worker. In the traditional organization on the left, strategy, operations, and tactics are managed by workers in descending order of authority, with information about each shared on a need-to-know basis. In the anticipant organization on the right, every worker at all levels executes and influences all three, and imparts information on an unrestricted, need-to-share basis. There are no secret meetings, no information hierarchies. In such a paradigm there is more risk, but the downside of not sharing far outweighs that risk. It's easier and less costly to manage a slip than to miss an opportunity to adapt.

MARK: ***Dream big or someone will do it for you*** *– In the pre-digital world, companies test-marketed ideas or features with a working group. In the digital world, it is all about experiments at scale with the internet as your research lab. The disruptors of the internet era—Amazon, eBay, Etsy, Facebook, Google—built their empires by experimenting at scale to drive innovation and improve products and services. These companies iterate on everything, even down to the color or location of a button, or the specific words used in a title. (Is the word "get" or "receive" going to get a bigger response from your audience? Only one way to find out.) If these seemingly minor changes can have measurable impacts on revenue, imagine the value of iterating on the bigger things.*

Experimentation at scale helps organizations make data-driven decisions about product development, based on customer behavior. This is a new approach; standard testing and debugging techniques do not belong here. The goal is to conduct masses of experiments, rapidly, to learn at a faster pace and a larger scale. Running thousands of experiments at the same time can produce results that typical approaches do not. And it can drive huge leaps forward in innovation. The key to effective experimentation at scale is the ability to admit that mistakes will happen, to iterate, and consider each idea. Digital experimentation has awesome potential. Research into the field will continue as more and more companies (and industries) adopt the practice. Ethical issues about privacy, accessibility, and consumer data will become more important. As the boundaries between reality and digital blur in the era of the metaverse, experimentation at scale will play a critical role in the evolution of science, technology, and medicine. And it will change the way you do business. MJB

Shared, not protected

Strategy is the discipline of identifying what should get done and why, while execution is the discipline of choosing how to get those things done. Experts on organizational performance have long debated whether strategy or execution is the more important discipline. Depending on who you talk to, one is always eating the other for lunch. In anticipant organizations the argument is moot, for just as strategy establishes the direction for which the tactics of execution are designed, what happens on the frontlines will and should directly affect the overall strategy. Strategy must be granular, not solid.

TOM: *Observing and learning* – *One of the duties of an anticipant leader is to observe new directions taken by competitive organizations, figure out what they're up to, and find opportunity there. I learned that lesson from a senior executive of Netscape. Netscape had pioneered Mosaic, the first big web browser and was riding high with JavaScript®, a language that clients could use to create their own websites. Netscape was a major client for the search technology my own company had devised when we took the Oxford English Dictionary online. At one of our meetings, the executive brought up Infoseek— the other search engine company in town. He said, "Your searches, Tom, take about two seconds each to return results. Infoseek completes theirs in a millisecond. How do they do that? We need to know because we need to beat them." That got all of us at OpenText scratching our nerdy heads. So, we dug in. We studied Infoseek's searches, dissecting the results returned in those lightning-fast operations. We discovered they were cheating, or it seemed like it to us. Infoseek was using a primitive, background algorithm to record the searches users made each day, and then they used that data to guess which searches people might make the next day. They then pre-cached a set of results for each of those likely searches. When any subsequent user typed in an anticipated keyword, Infoseek just spewed out a pre-packaged answer. While they were sending searchers to day-old information, they were clearly onto something big. Infoseek had quietly deployed a technology we now know as predictive analytics, one of the central pillars of artificial intelligence in our day. Lesson learned. We immediately began evolving our own AI. TJ*

Elastic, collapsible, adaptive, crowdsourced, iterative, with information flowing on a need-to-share basis; those are the hallmarks of the anticipant organization. Now let's explore how you can evolve your own organization into one of them.

6

Principle Six

Organizations must adapt to opportunity by innovating continuously.

Therefore, disrupt or die.

MARK: *IQ, EQ... and DQ?* – *Global high-speed internet and ubiquitous mobility have merged to radically change the ways businesses are started. I spend most of my time at our company headquarters in Waterloo, Ontario, Canada and at my own regional office in San Mateo, California, U.S., near Silicon Valley, both of which are fertile global centers for tech startups. And I have seen firsthand what numerous young companies have figured out: there are NO barriers to entry for new ideas.*

No barriers. Hardware can be rented and will soon be free. Software stacks are free. And the technical requirements of "coding"—a curriculum that once, if it had its corollary in the world of Harry Potter, would be the discourse of the dark arts professor and the subject of a forbidden section in the Hogwarts library—is now democratized. The cloud is acting as an innovation accelerant, modernizing processes and bringing together information to fast-track business growth. If you were starting a company today, would you buy a million dollars' worth of servers and put in a server closet? No. It would all be in the cloud. Companies can test new applications, processes, products, or services at scale with little to no infrastructure. A good idea needs only a computer (which might be a cell phone in the palm of a Gen Z-er's hand) and an internet connection to hit the ground running. The development of new products and services, from idea to product to global distribution has never been faster, easier, or cheaper.

These changes require a Digital Mindset. Disrupt your industry or your organization will falter. But how do you begin thinking about pursuing disruption? We all know about IQ and EQ. If your machines offer you additional IQ through AI, and your human teams provide you with EQ as well as IQ, perhaps together they create DQ: Digital Quotient. The word "digital" implies Zeros and Ones, On and Off toggles. But "quotient" indicates degree and captures shades of gray. Where are you and how can you measure your digital journey? How much farther can your machine-human teams go, need to go, will go? It is Digital or Die. Standing still is always the riskiest action to take—you are an easy target. Change is at all times the smarter—and bolder—path. MJB

DAVE: *Nothing in life stands still* – *In the army, change is a constant and this goes for organizations too. Militaries have been accused repeatedly in history of fighting the last war. The Civil War, WWI, and to a degree, WWII started poorly. Generals from the last war used outdated tactics and ignored technological advancements. In the Civil War, developments like the breech-loading rifle and muskets made line abreast tactics suicidal. While tactics changed due to technology, the lessons learned were not applied and mistakes were made on both sides. The forcing function of war and technology made militaries change. Horses were replaced with tanks. Where runners were used, radios improved communications and increased the dispersion of troops. Machine guns and artillery changed tactics on the ground. Airplanes allowed for more intelligence using aerial photographs. Changes like these made militaries more lethal and effective. Armies that innovated quickly and continuously had an advantage over their counterparts. DF*

TOM: *First-mover advantage* – *Historically, the process of product design and development has been speeding up. Before the industrial age, products such as wheel-and-axle carts took hundreds of years to reach maturity. In the early years of industrialized manufacturing, a product was designed and built over many decades with great effort. Even with the advanced automation available in the twentieth century, the development cycle of a new car model would typically take seven years. With the arrival of computers, it became easier to update designs and release product updates, and new models began arriving every two or three years. Smartphones sped things up again with new models coming out every year. Freed from physical constraints, web applications now offer new releases every three weeks. And smartphone apps routinely update themselves overnight, wherever their customers might be in the world.*

Product development is conducted at an ever-accelerating pace, giving the first mover an unbeatable advantage. For me, one example is particularly close to home. Founded in 1991, OpenText was based on evolving the cutting-edge research from the University of Waterloo into search engine technology. Now commonly used across the internet, search engines in their early days functioned only within closed systems. Smart, innovative companies such as PC Docs and Fulcrum built popular, successful search engines that operated on the static platforms of the time—personal computers and compact disks (CDs). They were not designed for the new and evolving technology then called HTML and HTTP, soon to be known as the World Wide Web. Since OpenText had little hope of penetrating the substantial lead its competitors had earned in the PC and CD space, it chose instead to invest in the new, connected platform of the internet by partnering with like-minded startups such as Netscape and Yahoo!. This led to the creation of the first set of search engines for the web, the OpenText Index. As users began sending documents over the internet, storing information in browsable websites, and hungering for content outside their own networks, the need for an online search engine grew exponentially. OpenText Index quickly became the most used search engine on the web. Slow to adapt their software to the new paradigm, once dominant companies such as PC Docs and Fulcrum were disrupted within months, having lost the first-mover advantage. TJ

DAVE: *May the forcing function be with you* *– Operations provide a forcing function that drives innovation. In business this is a competitor or market demands. The drive for margin or sales is a compelling argument that most militaries simply do not have unless they are in combat. Most militaries will spend the bulk of their time on training where factors are controlled (intelligence, enemy, etc.) to practice some skillset. All of this is designed to generate a multiplicity of capabilities based upon a security environment which, in many instances, was yesterday's war. Looking ahead and anticipating the next challenge requires determination, risk acceptance, and leadership. The inertia of organizations that are routine-driven and have no forcing function can often outlast a visionary leader who is fighting yesterday's battle. Even in operations, the dynamic nature of all factors playing out in real time with real effects (life and death, win and lose) means that routine can be a huge deterrent to progress. People fall back on what they know and don't necessarily step up to a situation. Only when faced with certain death will innovation and the will to live overcome these factors.*

Forcing functions in most cases allow a leader to survive and restructure to stay ahead of conditions that are working to defeat them. Faced with an IED threat in Afghanistan, the CAF had never experienced this before. While we had techniques to find and defuse the bomb, we were completely reactive. What we needed was the ability to get ahead (anticipate) the bomber and defeat them before they could engage us. The Americans had a much more sophisticated system for IEDs and when I saw this, I knew we had to do something about it. Carving out the resources from our own organization, I directed my people to adopt the American method. The U.S. forces appreciated that we were adding people and resources to their organization. In return we were building new skillsets that would give us the ability to get ahead of the bomber. What started as two people eventually developed into a whole new group and skillset within the CAF. We were simply acting like entrepreneurs and evolving to the needs of the environment to stay ahead of the competition. Another way that we would say this was: "who is responding to whom?" The answer either told us that we were anticipating and winning or reacting and losing. We had to disrupt or die. Everything we did worked on that mantra. DF

So here again are the hallmarks of The Anticipant Organization:

ANTICIPANT ORGANIZATION		
	YES	**NO**
Approach	Anticipant	Reactive
Org chart	Elastic	Flat
Processes	Collapsible	Lean
Operations	Adaptive	Automated
Plans	Crowdsourced	Sampled
Work	Iterative	Perfect

Figure 6.2: Characteristics of The Anticipant Organization

SO WHAT?

You now have our take on the differences between analog and digital operations, forged as they are by new relationships between time, speed, scale, and domain. Once hampered by known limits within each of these four realities, individuals and organizations can now make ingenious, speedy, and far-reaching advances in every discipline and sector.

As we have experienced, the power to produce staggering impacts with digital tools is not limited to those of good intent. Yet even when motives are noble, our reliance on digital systems and networks make us vulnerable to failures whose nature and degree we have not yet defined. All we know for certain is that the genie is out of the bottle.

As a leader of an organization in the post-pivot age, it is not enough to guess what kind of crisis might hit. To survive even one, you must have foreseen it, planned for it, prepared your teams to respond to it, and practiced those responses over and over again. Before you can make such responses possible, you must transform your enterprise in critical ways. You must become an anticipant organization.

Our AI implementation will have five discreet phases: Confusion, Disbelief, Anger, Depression, and Acceptance. Any questions?

ANTICIPANT ROAPMAP

TRANSFORM YOUR ORGANIZATION IN SIX STEPS

CONTINUE

ANTICIPATING & REHEARSING

BUILD

F REHEARSE THE NANOCRISIS

REHEARSE

SHORTEN

PRESCRIBE

PREPARE

IDENTIFY

E REMAP YOUR ORGANIZATION

DEPLOY
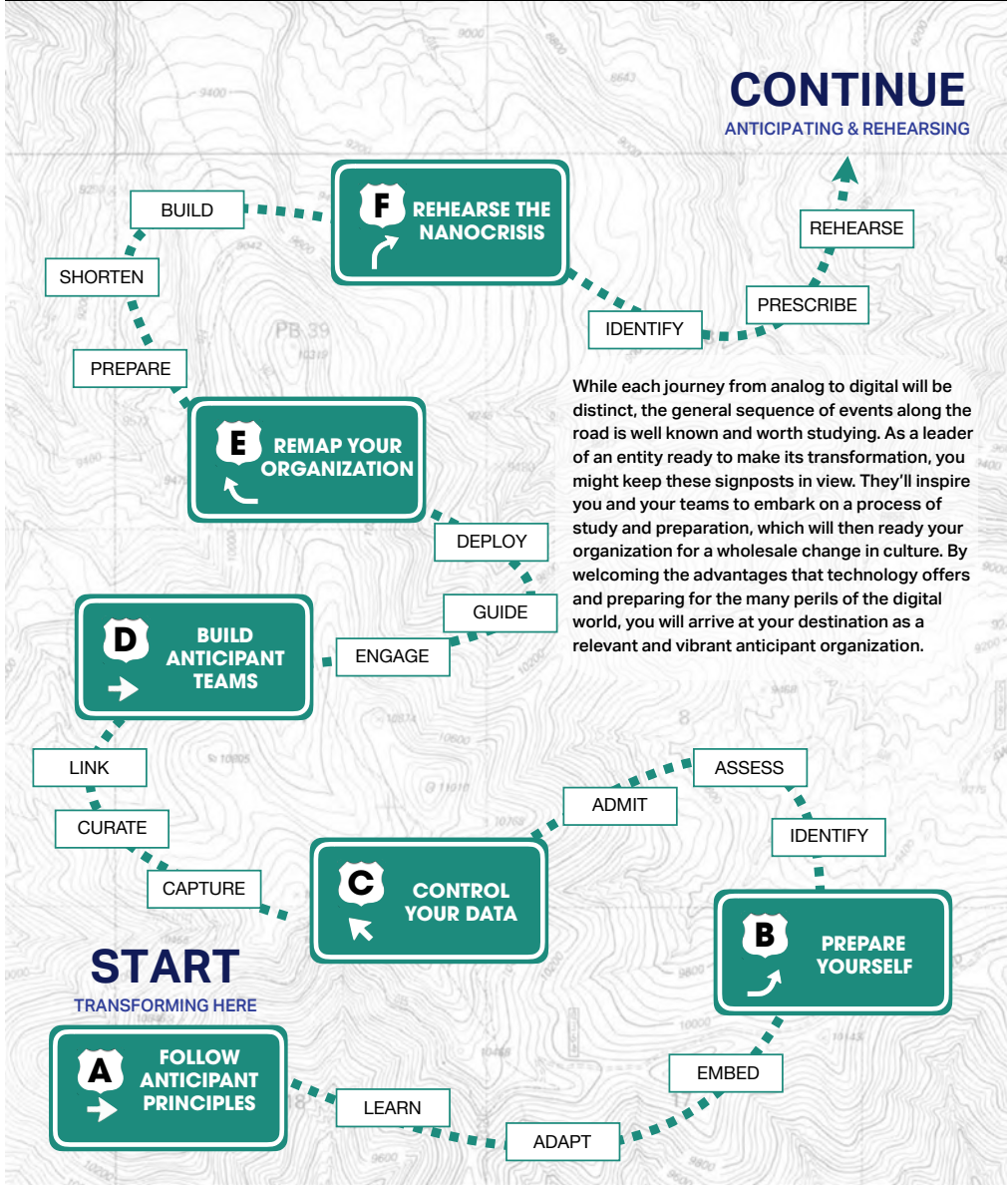
While each journey from analog to digital will be distinct, the general sequence of events along the road is well known and worth studying. As a leader of an entity ready to make its transformation, you might keep these signposts in view. They'll inspire you and your teams to embark on a process of study and preparation, which will then ready your organization for a wholesale change in culture. By welcoming the advantages that technology offers and preparing for the many perils of the digital world, you will arrive at your destination as a relevant and vibrant anticipant organization.

GUIDE

D BUILD ANTICIPANT TEAMS

ENGAGE

LINK

ASSESS

CURATE

ADMIT

IDENTIFY

CAPTURE

C CONTROL YOUR DATA

START

TRANSFORMING HERE

B PREPARE YOURSELF

A FOLLOW ANTICIPANT PRINCIPLES

LEARN

EMBED

ADAPT

CHAPTER 7

FOLLOW THE ROADMAP

As a leader of an organization in the post-pivot age, it is not enough to guess what kind of nanocrisis might hit. While transforming into an anticipant organization is challenging, it is not hard to describe, and we propose that you can do it in six steps. We've set down our prescribed sequence as a roadmap, fully appreciating that the journey your organization takes may linger longer in some places than others or head off down side roads in search of knowledge and experience of specific importance to you.

1. Learn the six principles of the anticipant organization

TOM: *Half-sure, wholehearted* – *In fast-moving situations such as those faced daily by high-growth companies, opportunity will pass you by if you don't move quickly. This is true at every level of the organization. I've found that the most effective project managers are those who act on intuition and act quickly. If the result turns out to be less than ideal, they'll happily ask for forgiveness after the fact. They know that's better than waiting for permission and getting no outcome at all. Progressive organizations appreciate that approach. They can't foresee every situation and certainly can't build bullet-poof procedures in advance for dealing with them all. So, they establish strong, universal principles (like those laid out in this book), arm their teams with deep understanding of the overall objectives, encourage common sense, and reward good judgment. As a corollary, they routinely remove managers who insist on being briefed on every action of their reports before any move is made. Better for your teams to act when they're half-sure yet wholehearted than never get to act at all. TJ*

In our analysis of society's pivot from analog to digital technology, we described how we arrived separately on six principles for surviving in the post-pivot world. The first step we advise is to learn those six principles and adapt them to your organization's specific context and mission.

Principle One

The greatest threat to any organization is an event it doesn't see coming. *Therefore, anticipate, prepare for, and rehearse the full range of possible nanocrisis scenarios.*

Principle Two

An organization must use all its information fully to serve its citizens better than competing organizations can. *Therefore, harness and manage your organization's data to unlock its deepest value.*

Principle Three

The reputation and mission of any organization is eroded by unethical behavior, no matter how isolated. *Therefore, just as you expect ethical behavior from your humans, embed deep ethics into the algorithms that drive your machines.*

Principle Four

Successful organizations require both flawless execution and visionary anticipation. *Therefore, build and deploy collaborative teams of intelligent machines and anticipant humans.*

Principle Five

An organization must use all its resources to full potential or risk irrelevance. *Therefore, treat your machines and humans not as separate species but rather as colleagues contributing equally to the mission of your organization.*

Principle Six

Organizations must adapt to opportunity by innovating continuously. *Therefore, disrupt or die.*

DAVE: *From reaction to prediction* – *The Taliban's ability to evolve and adapt quickly really changed how we did business in Afghanistan. Every time we defeated even one small Taliban unit on the battlefield, their entire force would change how they fought in response. To survive in combat against them, we had to adapt at high speeds as well. To do that, we had to become anticipants. Nowhere was that need more visible than in our routine and frequent intelligence briefings. When we began the campaign, those briefings had been filled with solid information, but all focused on the past. I was getting facts all right, but not the situational awareness I needed to make smart decisions. One day, as I sat in our command center listening to another presentation about old news, I looked around and saw a young British major squirming. He had something on his mind. I stopped the*

presentation, pointed to him, and said, "Stand up and tell me what you're thinking right now." The major then offered an analysis of what the intel implied. He focused on specific data points raised in the presentation and used them to deduce the Taliban's intent. From that, he then predicted their next target and the tactics they would deploy. He harnessed the historical data to anticipate where the enemy was going. That was the kind of conversation I wanted to have. We needed to be more predictive, and that major proved that we could be. From that day on, we made sure that every intelligence briefing looked back at facts and ahead at likely activity. We trained ourselves to become anticipatory, not just reactive. DF

 TOM: ***Learn from customer service*** *– Becoming an anticipant organization requires a sustained campaign of change management. You need to empower your teams to act quickly and decisively with a high degree of autonomy. Only then can you move from being reactive to proactive. Analog enterprises have been terrible at this, and many digital enterprises still are, but one area in which they both excel is customer service. Use that as your model. When any business finally wakes to the fact that customer satisfaction is more important in the long term than profit margin, it will make satisfying the customer its top priority. There was a time when customer service reps wore badges saying things like, "I have the power to make you happy." The key concept here is authority. When you give your teams the authority to make decisions based on principles rather than rules or procedures, miracles happen. Only then can they anticipate events on your organization's behalf, act in your interest, and secure your future. With AI, they can now anticipate emerging needs long before those needs surface, and they can retool your organization's offerings in advance to be ready to meet them. Let them. You'll sleep a lot easier. TJ*

B **PREPARE YOURSELF**

There are times when a leader should be first into battle; this is one of them. Your organization's transformation to digital will be much smoother if you first take the time to grasp the scope and urgency of the changes underway, prepare thoroughly for the challenges they present, and set a clear path for your troops to follow. You're reading this book, so you already have an appropriate attitude. Now take deliberate steps to broaden your vision, determine what you still have to learn, and fill any gaps that could prove detrimental to your leadership.

1. Identify and verify the required change in speed and scale of your operations

In Chapter Two, we set down the fundamental shifts in time, speed, scale, and domain that define the post-pivot digital world.

Unit of productive time: **nanosecond**
Speed of transaction: **speed-of-light (c)**
Scale of impact: **unlimited**
Domain of interaction: **suprahuman**

These are the elements that now define activity in all organizations. The curse and blessing of our new age, they will unleash the many crises your organization will face just as they shape the endless opportunities your organization can exploit to serve your stakeholders better. Your first task as a leader is to acknowledge that reality.

DAVE: *Find your three colonels* – *I served with U.S. Central Command (CENTCOM) Forward in the Second Gulf War. What struck me on Day 1 was the volume, scale, and speed of information the Americans had to process as they conducted operations. No one person could manage it. The days of a lone general considering incoming intel and making decisions were over. The commanding general relied on key members of his staff to sift through the vast amounts of available data, verify it, expand on it if needed, and then propose swift action to respond to the situation unfolding on the ground, in the air, and at sea. In this case, those key members were three outstanding colonels. Between them, they knew what intel was available, the degree to which each data source could be trusted, and who to turn to challenge or develop any fact or observation. Together, those three colonels were the central processor of wartime intel; they watched the data, learned the ground truth, assessed the options, and made strong recommendations for immediate action. They were our brains, but they were also our three most vulnerable points of failure. Had they been taken out, our senior leadership would have lost its ability to act. As such, the risk of trusting these three with such responsibility was great. But the advantage of doing so was greater. The changing speed and scale of operations required it. To this day, whenever I advise organizations in the post-pivot world how to operate at nanospeed, I begin by asking one question: "Who are your three colonels?" DF*

TOM: *Prepare yourself* – *After OpenText went public in 1996, I went on a vacation for a few days with my family to the mountains without cell phone or email access. I was away for just a few days, and during that time, I received various voicemails and emails from stock traders and analysts regarding a rumor. They were after my reaction to a recent news story about AT&T's offer for free access to the internet. While this story would help the company with more users available for applications, it was misunderstood by investors. They thought that AT&T was offering everything for free, which would force other vendors to follow suit, and ultimately result in the destruction of the business model for web vendors. The confusion was eventually cleared up and the business model validated, but not before it reduced the valuation of OpenText by more than 30% in less than three days! It would take another two years for the company to recover our stock price. That was the penalty for not being prepared for the "always-on" world of the public markets. From that point on, I have never allowed myself to be so unplugged that I am out of reach. A precautionary measure I still take to this day. TJ*

By now you will have some understanding of the nature and degree of the societal shifts that your organization must adapt to, but you'll have to dig deeper to form the specific insights that will make you useful as a leader. The good news is that many resources exist to help you—books, podcasts, and courses among them. In the past three years alone, a great swath of resources written by acknowledged experts have appeared to help you fully appreciate the gravity of the changes underway.

BOOKS

Begin by flipping to *Appendix A – Required Reading* to scan short abstracts of a compact selection of current publications that we found insightful and eye-opening. Here are a few suggestions:

- Kevin Kelly's *The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future*. A co-founder of Wired, Kelly has a long and broad view of societal shifts. (In the past he has emphasized that the forces shaping our lives now were predicted by writers of speculative fiction and producers of science fiction films. In a 2016 *Guardian* interview, he declared, *"I've learned a lot from Spielberg."[86]*) Kelly's book makes it starkly clear how just a dozen new, technology-driven habits are changing everything we do. As you read, you will be struck by how readily these forces have been accepted into our lives. More importantly, you will understand why the behaviors shaped by these forces demand deliberate and immediate attention if your organization is to stay relevant.

- Douglas Rushkoff's *Team Human*. His thoughtful reflection on the way our species embraces technology will give you pause. A knowledgeable critic, but in no way a Luddite, Rushkoff looks at biological and evolutionary history to arrive at sage conclusions about the choices we are making in our post-pivot world. As a leader, you will be making far-reaching choices on behalf of those your organization serves, so you must take the long view about which technologies to embrace or reject.

- Max Tegmark's sobering *Life 3.0: Being Human in the Age of Artificial Intelligence*. This will turn your attention to the utility of AI in all disciplines, while defining the unprecedented speed and scale of our uptake of intelligent systems. Tegmark is no Pollyanna, contending that the choices our organizations (governments included) make now for our presumed collective benefit will take our species on a path either to renewal or extinction. It's heady to consider the yawning continuum of possible consequences of our choices.

- *Prediction Machines: The Simple Economics of Artificial Intelligence* by Ajay Agrawal and two of his colleagues. In their book, Agrawal and co-authors conduct a sweeping cost-benefit analysis of AI in organizations, in which they list the variety of possible gains against the real and varied risks. Important for you as a leader, they also specify which critical skills AI lacks, and which leaders must

- themselves muster and master if AI implementation is to succeed. These include the soft skills humans can excel at, including lateral thinking, gut instinct, and emotional intelligence.
- Daugherty and Wilson's optimistic yet grounded *Human + Machine: Reimagining Work in the Age of AI*. Here you will encounter dozens of examples of companies, agencies, and departments that made the leap into hybrid-team deployment, each achieving radical evolutions in service delivery and product development once they had elected to become an anticipant organization.

Spoiler Alert:
Battlestar Galactica

In a sweep of 76 television episodes examining every aspect of human-machine relations (HMR), Ronald D. Moore's re-imagined *Battlestar Galactica* appeared from 2003 to 2009 as the digital pivot was well underway. The series resonated with viewers, in great part because polarized opinions about the benefits and threats of intelligent machines are strongly advanced by characters who themselves face life and death choices. Some characters view the cybernetic race of *Cylons* as nothing but 'toasters'—dumb machines blindly following their algorithms, while others see those entities as self-determined, fast-evolving beings whose own survival requires the extinction of the human race.

All the books in our required-reading list share the same combination of vision and practicality. Read them all if you can, and then move on, find others, and let us know new titles you would recommend to other leaders.

MARK: *Who has time to read?* – *It is one thing to suggest a reading list, and another for people to find time to actually read! Digital connectivity anytime, anywhere brings with it a potentially massive downside: precious little time to unplug and reflect. But I make time to read, every day, because I view it as essential to my own development and that of our company. Reading gives me a broader perspective on global events, reminds me of valuable lessons I may have forgotten, challenges my assumptions, and helps me provoke discussion among my teams. And I do not just read books about business. My current reading shelf includes titles as diverse as Karma Yoga: The Yoga of Action, which focuses on providing service to others, Creativity: A Short & Cheerful Guide by John Cleese, Ernest Hemingway's The Old Man and the Sea, and Citrus: A History, which is exactly what it sounds like. I also read several newspapers daily, as well as medical journal The Lancet and the website for John Hopkins University.*

One of the most influential books I have read recently is The Art of Happiness by his holiness the Dalai Lama. For me, this book speaks to my belief that happiness is compassion and compassion is happiness. The book reminded me that, in any crisis, we need to lead not just with our heads and hands, but with our hearts as well—acting with compassion for our employees, our business partners, our customers, and all those who are marginalized. It taught me to lead my team by deepening our human connection in a time of physical distancing. Follow the science, data, and math – but practice empathy and compassion. MJB

DAVE: *What you don't know* *– After my tour as regional commander in Afghanistan, I was asked to bring what I had learned back into our defense training system. As newly appointed commandant of the Canadian Forces College, my job was to update the postgraduate education of military officers and civilian executives as they prepared for senior roles in Canada's defense organization. I knew from my time in the field that we had to overhaul the curriculum. To do that, we would need advice. So, I asked a number of leading members of the business and academic community to join me and my senior staff to identify what had changed globally so we could add those insights to our training. At first, I wanted to get my faculty colleagues up to speed, presumptuously confident that my experience in theater had taught me all I needed to know about how the world had changed. Wrong. After only one session, the gaps in my own knowledge became so glaringly obvious that I had to embark on a rigorous, personal program of relearning. That initial session bloomed into a series of discussions with experts on topics as diverse as finance, social communication, regionalism, psychology, and logistics. My lifetime of soldiering and eye-opening experience in Afghanistan had certainly armed me with the tools to learn quickly, but any arrogance I had about knowing it all had disappeared in that single hour. DF*

PODCASTS

You can also deepen your understanding in a practical and entertaining way by downloading and listing to podcasts.

- The British podcast *Exponential View* (exponentialview.co). Hosted by Azeem Azhar, a prolific interpreter of the role of technology in society, the podcast follows a simple interview format. Azhar asks timely, penetrating questions of the world's leading tech experts, most of whom are absorbed with the evolution and regulation of artificial intelligence in some way. (As a bonus, Azhar is bookable talent as a speaker.)

- Alex Shee's podcast *The AI Element* (available through Apple, Google, Spotify, and others) digs as much into the philosophical side of AI as the technical, probing questions, such as whether AI can be trusted, and how justice and ethics can or cannot be accommodated in a world shaped by algorithms. In every episode, Shee speaks with *"industry influencers and deep learning pioneers to explore how AI is being used to innovate and disrupt in the fields of retail, insurance, cybersecurity, healthcare, manufacturing and logistics, and more."*[87]

- As the pioneering gaming company that invented the graphics processing unit (GPU) and brought AI into entertainment, NVIDIA has its own biweekly offering called *the ai podcast* (no caps). Particularly useful for leaders in business and government, *the ai podcast* covers focused topics such as how AI can detect fake news, how federated learning can keep data private, and how bots learn by observing human behavior. (Read about it at blogs.nvidia.com/ai- podcast).

- New York Times columnist Craig S. Smith produces a biweekly podcast called *Eye on A.I.* (eye-on.ai). Senior military leaders will find defense issues a regular part of the mix here, as Smith interviews people such as Brendan McCord, a man who works at the National Security Commission on AI and wrote the Pentagon's AI strategy.

- *AI in Business* is a podcast in which *Emerj* founder Daniel Faggella examines how artificial intelligence can be harnessed at the enterprise level. Faggella interviews top AI and machine-learning focused executives and researchers in sectors including defense, pharma, banking, health, and retail. (Find him at podcast.emerj.com/).

SEMINARS AND COURSES

While your time as leaders is already scarce, a host of seminars and online courses can give you and key members of your team an intensive introduction to the post-pivot role of intelligent machines in the operations of anticipant organizations. Check with the educational institutions you know and trust, or just search online to see the latest offerings.

With books, podcasts, seminars, and online courses on the topic now readily available, you have countless opportunities to understand the changing paradigm of organizational behavior. No matter the route you take to awareness, make sure you grow to fully understand the degree to which your own enterprise must change the speed and scale of its operations to survive and prosper.

2. Make an honest assessment of your skill as a leader at the new speed and scale

TOM: *Horses for courses* – *One of the most important moments of my professional career was the day in 1998 that I realized I didn't have the skills and knowledge to run our company alone. Like most high-growth enterprises, OpenText began moving into sectors, markets, and levels of competition that were new to us, and I had to admit that our customers, employees, and shareholders weren't being fully served by a guy like me who had to learn everything on the job. I'm a pretty quick study, but at that point we needed broader experience. So, I fired myself. I asked John Shackleton of Oracle to join us as president and run the company. Best move I ever made. There was no on-the-job training for John; he already knew how to scale an organization because he had run multinationals. While John ran the day-to-day, I focused on strategy, including mergers and acquisitions.*

Our decade-long partnership allowed OpenText to grow to the next level. In horse racing, you use different horses for different courses. That's the way you win. In organizations, you need different skills and experience at different levels of management and different stages of growth. Never be afraid to move people around, and never shy away from asking yourself the tough question: "Am I still really the person for this job?" From time to time, fire yourself. You'll be amazed by what can happen. TJ

Once you've dived into the issues and have a better grasp of what's coming at you and your organization, it's time to ask if you, as leader, are up to the challenges ahead. We appreciate that you may not be the commanding officer, chief executive, secretary or managing director of your outfit; you may be its 2IC, VP, deputy minister, ops manager, section head, or just one of many leaders of a project-specific team far down the pre-pivot chain of command. But in the post-pivot world, you are now on top. In your day-to-day role, you have unprecedented autonomy, responsibility, and authority—even more so when a nanocrisis hits.

We used to specify who within any organization was to be on the frontline or at the coalface, that sweet spot where the resources of the enterprise meet the day-to-day requirements of its stakeholders, whether in combat, sales, customer service, citizen advocacy, public outreach, recruitment, or student relations. Now, in our always-on, always-connected, dispersed reality, everyone is out on the edge every day. No matter where you fall in the hierarchy, if you have people looking to you daily for either guidance or support, you are a leader who must be ready to anticipate, prepare, rehearse, and act.

If you've read the books or listened to the podcasts we've recommended; if you've taken even one online course or attended a single seminar on the topic of human-machine relations, you have already sensed that you are behind. Throughout military history, defensive forces have suffered greatly in the opening stages of any conflict, precisely because everyone was trained to fight the last war… not the war underway.

So, are you ready to fight the new war? If you're like we were, you'll know in your heart that you are not.

DAVE: *Honesty* – *Every mission I've been on has been prefaced with years of training on similar scenarios. Getting ready for Cyprus, our one and only mission during the 80s, was straightforward and routine. With civil war in the Balkans, the 90s were more dangerous; our preparations were much more robust and included more kinetic practice for whatever we might face. Again, the situations were relatively straightforward: two warring factions for the most part (in Bosnia there were three) and each was a known state actor. Our organizations and decision-making processes were designed for these events, and our forces were well versed in the art of war during these periods. The new century brought with it a change in the very nature of conflict. While state-versus-state actors continued to exist, they were augmented with the rogue individual and terrorist groups such as the Taliban and Al Qaeda. The difference between the state actors and terrorist groups was the former were easy to find and hard to fight, while the latter were hard to find and easy to fight. The dramatic differences with the two security paradigm threats forced a change to our thinking and organizational constructs.*

Our preparations for Afghanistan were aimed at nation building and fighting a counterinsurgency. For the first time in history, the Canadian military was facing an enemy we were not optimized to fight. The intelligence and agility necessary to find and shape battles with an enemy that lived among the people (and who were the people) required a new skillset. The traditional structures of the army, air force, navy, and special forces needed to adjust to the unique requirements of the security environment in Afghanistan. We had to change our thinking and organizational construct to suit the requirements on the ground. The adjustment needed to start with me, the commander, and then I had to impart this new way of thinking to the women and men of the formation. Not an easy task given the nine nations comprising the formation, the lack of knowledge we had about each other, the rigid construction of organizations with national caveats, and an Afghan community rich with tribal dynamics and Taliban connections.

My first step was to acknowledge what would really define an effective leader in this new circumstance. The second was to be candid about my own readiness and assess the areas in which I was prepared or not prepared to be the leader in coming events. We leaders must be brutally honest about our strengths and weaknesses, weighing the lessons of our own experiences against those that will be applied (or, worse, learned for the first time) in the days ahead. We need to sit down and write out, in military terms, an estimate of the situation. This estimate identifies our strengths and weakness, our organization's strengths and weaknesses, our partners, and our competitors. Following a detailed analysis of these factors, we can come to some conclusions or admit to what we need to do. Honesty is absolutely critical to achieving the roadmap and execution of assigned goals. We did this for our preparations in Afghanistan; this was our routine in combat operations at all levels. Honesty created the conditions for success because we refused to deceive ourselves about what we could and could not do. We openly acknowledged our need to learn and profit from the experience of others. It all starts with the leader and only then can it flow throughout the entire organization. DF

3. Identify your own leadership gaps and make a plan to address them

As you educate yourself, you will soon become mindful of the additional knowledge and skills you will need if you are to lead your organization wisely in the post-pivot world. You will likely spot a number of gaps even in the next few chapters, and we suggest you begin making a list of areas in which you need to deepen your understanding. Many of these will spring directly from the new context in which you will be building, training, guiding, and deploying hybrid teams of humans and robots.

The possibilities are endless, so we can't make a checklist for you. But just as you would advise every employee who reports to you to figure out where they want to improve and how they intend to make that happen, we advise you to do the same.

We can, however, point you in one direction of increased importance: that we must all work as balanced teams of human and machine colleagues. In particular, the access your enterprise enjoys to artificial intelligence will demand the exercise of different, deeper aspects of the intelligence of your human team members, and certainly of you as their leader. Crudely put, AI will handle more of your organization's IQ than before, while you will have to deliver on EQ. Your humanity is now your greatest defining value.

Read this short list of topics from top to bottom:[88]

Authentic leadership
Focus
Confidence
Influence and persuasion
Dealing with difficult people
Resilience
Self-awareness
Mindfulness
Empathy
Happiness

As you move down the list, do you feel a bit like the topics drift from leadership skills into session titles for a yogic retreat in the mountains? Far from it. These are the book titles of a *Harvard Business Review (HBR)* series on *Emotional Intelligence*. Each topic is a discipline that, once mastered by an organization's leaders, can make a measurable contribution to success. Each is worth mastering. As *HBR* puts it, *"while it's easy to say, 'just put yourself in someone else's shoes,' the reality is that understanding the motivations and emotions of others is an elusive capability."[89]* As a leader of an anticipant organization, you will need that capability above all others.

DAVE: *On learning* *– In Afghanistan, I needed a development advisor. Someone I trusted suggested that I recruit Christina Green, a professional working for CIDA in Kabul at the time. Christina was exceptionally intelligent and famously productive, but it became obvious in our first interview that our paradigms were opposed. I was focused on breaking things while Christine was focused on building things. Up until that point, her work had little to do with soldiers and she admitted that she harbored some disdain for the military. That suited me fine; we needed Christina's intellect, drive, and unvarnished opinion. I pledged to be open-minded and fully supportive. She joined the team, and that changed things. Christine freely challenged us on everything we did, yet always so she could learn how to better support our mission. At one stage, she forced me to plant a tree just so I could create something rather than just destroy. She forced me to expand the scope of my thinking, and she did the same for most of the members of our team. In turn, she began to understand our roles as a coalition with a shared objective. We all grew together. DF*

CONTROL YOUR DATA

Capture and control your structured and unstructured data

While your data may be your greatest asset in the post-pivot world, this is true only if you can get at it. So first you must ensure that all the processes and libraries and archives you use are available in digital form. The litmus test (and it's a big one) is that your organization can conduct its daily business internally and externally without the printing of any paper. If there is any step with a customer or vendor or partner or employee that requires the printing of even a single piece of paper (even just a receipt), your enterprise is not yet prepared to become an anticipant organization.

Yet even once you have everything in digital format, you are still not ready. You must be able to control it. Control means saving and tracking your data with precision, and that requires knowing the identity of the author, recording the time and location of creation and modification of the data, and having the unfailing ability to retrieve that data securely for use at a later time. Metadata is an indispensable tool that machines use for locating data within your system as they need it. When you have fully captured your data and thoroughly defined it with metadata, you will have the means to exercise the control you need.

MARK: *All the data we cannot see* – *It can be incredibly useful to understand what employees, customers, news media, and business partners really think of your organization. But how can you tell?*

The answer: Look at what they are saying. People are voicing their opinions on so many platforms today—Twitter, customer service chats, surveys, news, and emails, to name a few. The challenge is how to read through millions of words and accurately sum up what they are about, without throwing a whole office full of marketing analysts and co-op students at the problem. We cannot possibly ask human workers to read everything all the time; there is simply too much information. And while processing structured data is a cinch for digital systems (machines do well with numbers), analyzing unstructured data requires an app of a different color.

One of the most startling capabilities of AI is its ability to read human sentiment. Tapping into feedback from every source, AI tools can monitor, compare, and assess global opinions in real time. They can show you what people are saying, by topics and keywords, countries, dates, and even tone. Is the consumer response on social media to your new beverage positive, negative, or neutral? AI applications can automatically crawl the web for focused articles and tweets about your organization, in any language, and evaluate the raw text. This evaluation can include figuring out the emotion of the writing in question. Are the news articles about your recent press event supportive, disappointed, annoyed, elated? AI can tell you. The latest AI tools are even sophisticated enough to interpret sarcasm, emojis, and other nuances. So, if a tweet reads, "Don't quit your day job," AI understands this as a criticism, not benevolent career advice. MJB

DAVE: *Up your game with unstructured data* – *The military lives on structured data. We know exactly how many parts there are in any light armoured vehicle (LAV). We know how many of each part we have and exactly where they are. We know how long it will take to get part A to place B, and we know to the penny what it will cost. In peacetime, we tend to blame that same data for our inaction. ("Sorry sir, too few, too far, too long, too expensive.") Worse, sometimes we think that structured data is all we have. But in theater, where speed is crucial, we abandon structured data and solve our problems with unstructured data, using local knowledge, snippets of conversations, even rumours. ("Sir, we've found a guy who says he knows where he can get six new tires, but he'll have to steal them.") I learned early in my career that whenever you need to up your game, pay more attention to unstructured data. Don't let known facts get in your way. I was reminded of this in Kandahar, where all our sophisticated, real-time, structured data couldn't tell me why we were failing to gain the support of the local population, even though we were saving their lives, protecting their homes, rebuilding their schools and wells, and working hand-in-hand with their democratically elected representatives. It was our own Muslim padre who solved the mystery, simply by praying with locals in their own mosques. There he quickly learned that the Taliban were secretly paying the salaries of all the Imams and Mullahs and funding the upkeep of all the mosques. The only thing they asked in return was to write the Khutbahs— the sermons given during the Friday congressional prayers known as dhuhrs. For most illiterate locals, the Khutbah was the only source of information. It was their one weekly newscast, and the Taliban controlled every ounce of news they heard. Once we understood that, we stopped dropping leaflets and began finding alternate sources of funding for the mosques. That changed everything. DF*

As your organization matures, it will be necessary to control both structured and unstructured data (for more details, please see Chapter 4). Consistent access and accurate understanding of both structured and unstructured data is critical if machines are expected to make decisions in nanospace.

Various standards have been established by government and regulatory bodies to help to ensure that you have control over your data. These include the *Health Insurance Portability and Accountability Act* (HIPAA) in the U.S. and the *Personal Information Protection and Electronic Document Act* (PIPEDA) in Canada; the *Model Requirements for the Management of Electronic Records* (MOREQ) for records management across the European Union; the *21CFR Part II* standard for pharmaceutical and other federally regulated companies in the U.S.; and the *ISO 9001* standard for manufacturers throughout the world. The most ambitious effort to protect privacy through data control is the EU's 2016 *General Data Protection Regulation* (GDPR), which is quickly becoming the de facto global standard for responsible management of personal data. These standards will inform you of the many definitions and types of data that organizations must attend to, and they will guide you in the increasingly complex discipline of data compliance.

DAVE: *Always vet your data* – *In military environments, it's critical to verify all information requirements starting with the Commander, staff, higher commands, and lower units. Map the relationship of all information requirements and automate them across time sensitive needs. This will ensure that proper guidance is given by the applicable authority, speed up decision making, and optimize the apportioning of resources. Machines can do much of what is done today by humans in a more thorough and effective manner, offering better information for commanders at all levels to make decisions. Review all processes and eliminate those that do not support the updated information requirements. Use as much automation, machine quantitative, and AI capabilities as possible. This will free up people and compress time for decision making. Use distributed, collaborative, streaming technology to optimize time and space. This will reduce time away from units by critical leaders. And as always, ensure that legal requirements are met in all efforts. DF*

1. Curate your data: verify, cleanse, select for use

TOM: *No data point is static* – *In most technology companies, we have business models where we price our software based on the number of users. When you purchase Microsoft Office®, for example, you're not really buying it; you're paying a fee to use it. Any software company can tell you for each of their products how many users they have licensed and what income those licenses generate. But those data are often misleading because sales managers tend to make one fundamental flaw in judgment; they think those data are static. They assume that once they have established a number, the information never changes. That would be like counting the number of cars in a McDonalds parking lot at 10 p.m. and presuming that the same number of cars will be there the next day at lunchtime. Ludicrous. Case in point: Many software companies have blanket licenses that allow access by every employee in a customer's company. The fee is usually based on the total number of people the company employs on the day the deal is struck. I know of one case where the enterprise-wide license fee was agreed to when the company had 100 employees. It was never raised, even though the company grew to 3,000 employees, meaning that 2,900 people were using the software for free. In my career, I have never ever met a data point that was static. Data is a dynamic reality. TJ*

The quality of data is critical to any decision, especially when that decision is made by a machine, because machines treat all data as accurate, unless those data fall outside a range defined within the algorithm itself. No matter how good the AI algorithm may be, if the data on which a decision is made are poor, the decision will likely be poor. As programmers have been saying since the 1960s, *"garbage in, garbage out."*[90] Yet with so much digital data available, the opportunities for misinformation abound. Curating your data is therefore essential in the post-pivot world. Especially in a nanocrisis, the timely use of verified, clean data is an essential step in the survival of your organization.

Now that you have gathered all of your data in native file format and you know when and where it was created and modified, and you've stored it a secure location for recall, you are ready to curate your data and make it ready for the machine that you have tasked to perform a particular job.

DAVE: *Some data are just wild guesses* – *In theater, generals get daily reports on the amount of ammunition they have on hand, and how long that ammunition will last. It's one of the most important things to know before ordering an advance against the enemy. But the estimate of how long the ammunition will last is just a guess, a presumption based on historic rates of fire against logs detailing inventory on hand. A big presumption. Just before we began the kinetic phase of Operation Medusa against the Taliban, I found out that we did not, as I had been assured, have several weeks of 25-millimeter ammunition on hand. In fact, we had only twenty minutes worth. We ran out due to inept record keeping and because the newly installed battalion was firing its weapons at more than twice the rate of the battalion they had replaced. The so-called data I had trusted were in fact nothing but estimates, grossly inaccurate estimates that almost brought about our defeat. Lesson learned. Whenever you base a decision on data, do whatever it takes to be fully sure the data are accurate. You'll prevent a disaster. DF*

The currency of your data is vital. The first step is verifying that all the data are the most up-to-date available for the AI algorithm. You can't use yesterday's weather to predict the number of customers your coffee shop will serve today. Yesterday was sunny and dry, but today might be rainy and windy. Your walk-in traffic will likely be down, and all those muffins you've just ordered will go unsold. Current and accurate data are best, but that frequently implies a higher expense of either money or time. Generally, the more current the data, the more costly the recall. The data point that tends to cost the least is an average, such as the average number of rainy days in July in Barcelona, which is why humans used to trust their memories or refer to tables of average weather before packing for a trip. That data was cheap and readily available. Nowadays, if you want to get up-to-the-minute weather for a specific location, it's readily available too but it's not free. Most enterprises subscribe to services that deliver and charge for current data, because currency is often a competitive advantage and, therefore, worth the cost.

DAVE: *Wisdom and courage* – *In both business and the military, a ton of data is reported up the chain. Based on what you get, as a leader you'll make judgments about things such as how many days' rations you're going to need, how well serviced your equipment is, and how ready your team is to carry out a variety of tasks. But are those data any good? The first way to ensure accurate information over time is to make sure the people in your organization have the confidence to speak truth to power. They should feel free to tell you when some so-called facts are fishy. You should have both the wisdom to hear that opinion and the courage to act on it. The second way is to get off your butt, go out onto the shop floor or out onto the field and verify the facts you've been given. DF*

Another function of data curation is cleansing, which refers specifically to the conversion of the format of data to suit the protocols of the system that will use that data. You cannot send the contents of your Facebook profile in a WhatsApp message any more than you can send a page of text through a telephone. The file formats of the two systems are incompatible, and the content will have to be cleansed through a filter. Sometimes the filters don't exist, and in some cases that is intentional. The uniqueness of a content's format is sometimes a tactical barrier that protects an

owner's proprietary rights. When digital cameras appeared, manufacturers including Canon and Kodak rolled out proprietary image file formats that worked only on their own gear. Companies selling eBooks today work hard to ensure that their digital products cannot simply be copied and pasted from one reader to another or, worse, to family and friends. As an express requirement of the manufacturer, the files in these systems cannot be cleansed.

Encryption too is a deliberate barrier for protecting a wide range of data, from personal text messages to national secrets. If the data in one part of your system is encrypted, you will not be able to send it to another part of your system and use it there.

Obsolescence too is a barrier of its own. If your system contains the historical documentation of your organization from its inception, some of the files you've saved may be in formats that are no longer used. Simply having the algorithm is not enough. You must have all the data available for the machine to make accurate decisions. When designing your data system, it would be unwise to dismiss historical data that may be critical to the understanding of the machine and its analytic process simply because the data is hard to cleanse and prepare for another machine.

Once you have cleansed your data and assured yourself of its accuracy, you must now select the data for the machine. Selection is typically done through another algorithm known as a search engine. Many of us use search engines on the public internet, and typically we type in only a single word or text string to search for rather than the kind of complex Boolean query. Boolean query refers to a series of conditions that must be satisfied to qualify data for selection. In our earlier example, we could have completed a query of all the customers that entered the coffee shop on rainy days this year. That would have provided a much more accurate set of data for the machine to predict the number of customers today.

2. Match your dataset to the most appropriate decision makers

We have a staggering amount of data in our world, and its volume is growing exponentially. Finding relevant information can be more than frustrating; it can be harmful. As more and more data are presented to a decision maker in your own organization, a point of marginal utility is reached at which the processing time exceeds the period within which a decision is needed. If it takes you until 8 a.m. every morning to accurately predict the volume of traffic at your coffee shop by analyzing the day's weather, you're going to miss the 7 a.m. deadline for ordering those fresh muffins. To give all your decision makers the right amount of the right data in the right timeframe, you must discriminate. It may help to remember that while many types of information may be *relevant* to the topic, not all are *material* to the decision.

Similarly, you must make sure that the dataset and the decision maker are compatible. You wouldn't phone a barber for information on watering your houseplants; you'd call a gardening center. Data and decisions must be matched like for like. Calculators crunch numbers, not words. Judges consider facts, not hunches. GPS systems need ground truth, not hand-drawn maps. Mail-merge systems need delimited data, not text strings. Every system has a finite set of data types it can use as it runs. Sending it anything else is more than a waste of time; it is an unnecessary waste of your limited resources.

TOM: *Machine-to-machine* – *The data being created by machines now surpasses the data created by humans. Machines create data by processing the input from humans or other machines. There are many types of machines that make decisions and the data they create is a third set of data, in addition to the structured and unstructured data we discussed earlier. Data from machines are an amalgam of metadata and data, and are always in structured format, although structured data can be converted to unstructured data through various translation algorithms. For example, 11011011 is the ASCII code for the letter M. By this method we can take structured data and convert it to unstructured data. It's important to note that when we type emails or any other conversation between humans, the machines that are converting the information to digital are using the translation to reduce the information to structured data at a binary level. By definition, all machine-to-machine communications are structured, and they do not suffer the limitation of having to be converted back to the analog world. Machine data is data in its purest form and provided that the format is compatible between machines, it is the fastest, most efficient way to communicate in nanospace. TJ*

DAVE: *Give data a destination* – *The Bank of Montreal has a program designed to sell preferred banking services to the military. For seven years, the program couldn't get any traction among its intended clients, military families. The reason was simple: Those families were being given the wrong data to consider. With no understanding of military life, bankers had assumed that service personnel were just like civilians. So those bankers kept sending their prospects data about how much money they could save on monthly service charges, which would be waived for all serving personnel. Yet they were sitting on a critical piece of data that was far more compelling, the low interest rates on mortgages available to military customers. The military moves its people around all the time, and the amount paid by a family on mortgages for one house after another can be staggering. When that data was identified and routed to military families, they realized they could save tens of thousands of dollars over the life of a mortgage, and they signed up in droves. Success came from nothing but routing the right data to the right decision maker. Until then, the business had been stagnant. I suspect that's often the case. DF*

D BUILD ANTICIPANT TEAMS

1. Engage anticipant humans and intelligent machines

Your organization is likely already tech oriented. Everyone works on computers. Your data is digital, secure, and backed up. Your website is interactive and is as easy for customers to use on their mobile platforms as on their desktops. Your use of your customer data is guided by well-defined privacy policies. Many of your processes are already automated. You may even monitor social media to observe the communities you serve and intervene promptly. But using computers in your work was only the first step in your digital transformation.

The defining talent of your anticipant organization will be your ability to foresee previously undetectable, upcoming events. That requires being able to look through vast amounts of information from all quarters to identify subtle, complex patterns that indicate formerly unknown correlations. With those patterns identified, you can then consider the opportunities and threats those correlations reveal and adapt your organizational behavior to address them with novel solutions. Given the general definition of artificial intelligence as a system that absorbs information through sensors and data streams, and then behaves in an appropriate way, we contend that the critical step your organization must now take is to become an artificial intelligence of its own. To do that, your people will have to get along well with your machines. For that to happen, you must bring intelligent machines onto your teams and match them with imaginative humans who can foresee how those machines might improve the way you work. But how do you choose those machines and people?

Figure 7.1: Who is the operator and who is the tool? Space exploration brings humans and machines together in collaborative teams that are equally functional and creative. All the machines are purpose-designed and built for adaptation to unanticipated tasks. Similarly, all the humans are selected for a broad range of aptitudes, and must exhibit an equal balance of IQ and EQ. Candidates are closely watched through a two-year selection process in which every aspect of their behavior is monitored, measured, and evaluated. When the best gear and the best people finally lift off together, it is pointless to debate which members of the human-machine team are more important to the mission. In anticipant organizations, team selection is approached in the same way.

Choosing machines is the easy part. You go shopping. The professionals in your various departments or units will be aware of what's out there, how it could benefit your operation, and what it costs. They will also be in touch with the many consulting firms that offer specialized expertise in the integration of intelligent systems. You can purchase anything you want or need; the spectrum runs from cloud-based business-intelligence software to functional, automated robots. Each acquisition will depend on your mission, your data governance policies (including the level of security required), and the depth of analytics you can usefully exploit. After that, it's a matter of budget.

Selecting humans is the tougher task. As we explored in Chapter 5, with machines able to undertake quantitative analysis and prediction faster and more accurately than humans, you must reconsider exactly what it is that you want your humans to do. One way to think about this question is to assess the relative demand for IQ and EQ in any given position. After that, determine how much of the IQ might be supplied by a new machine on the team.

DAVE: *Tell them what you want, not what to do* – *Anticipant teams are motivated to action when armed with their leader's intent. They don't need much more direction than that. I learned that lesson working with the American military, whose officers are deeply trained professionals who take their work very seriously. When they know what an objective is, they use all their initiative to make things happen to achieve it. Find people like that, give them intelligent machines to speed up their processes, tell them what you intend to accomplish, and then get out of their way. DF*

Selection processes should be based on desired outcomes, and those outcomes might now be achieved in different ways than before. In a military example, the traditional criteria for a fighter pilot have been markedly different than those for an infantry lieutenant. In the pilot's case, selection teams have looked for the winning combination of high mental acuity and rapid physical response. There has been far less need for abilities such as self-awareness, empathy, and dealing with difficult people, three of the ten qualities identified by *Harvard Business Review* as essential ingredients of emotional intelligence.[91] The infantry lieutenant, however, must be able to exhibit all of those consistently, especially in high-stress situations. While fighter pilots drive their aircraft for mere hours with specific targets as objectives, infantry officers must motivate and support their troops for weeks in gruelling combat conditions that quickly exhaust both emotional and physical reserves. Where fighter pilots and infantry officers are concerned, the different demands call for different personalities.

Figure 7.2: With the recent and long-awaited uptake of AI, exponential innovation is now possible in almost every field of human endeavor. From now on, the great advances will be made by collaborative teams of anticipant humans and intelligent machines.

The analogy is fitting in the digital era, but you can now bolster either function with plug-in IQ. As you reshape your organization, you will find that much of what you turned to brainy humans for can now be supplied by brainy machines. That frees your humans up for much more important work, work that will likely be more creative than analytical. Great human minds will always be able to contribute to great results; but those results will increasingly be achieved by human-machine teams, not humans alone. So, whenever you look at a function that requires staffing, ask if your best approach is to give the human a machine or give the machine a human. We think the answer will usually be to make the human and the machine a team. Each can learn from the other, and each can support the other.

2. Guide both humans and machines with intent and ethics

Mature establishments take great care to share new insights each year with their employees about the evolving strategy of their organizations. The highest level of strategy is always intent; what you intend to achieve as an organization is paramount, so much so that it's often referred to as *the mission*. Mission statements are typically concise, clear, and compelling, but they rarely spell out how that mission is to be achieved. As such, organizations must also carefully articulate their expectations of behavior.

In the last few decades, headway has been made in some sectors in the development of strong policies related to ethics and governance. These have been backed by internal information campaigns designed to bring whole workforces up to acceptable standards of accountability and behavior. They expressly prohibit such abuses as sexual harassment, discrimination against minorities, unsafe work conditions, corruption, illegal employment practices, and non-payment of contractors. When adhered to, these policies enable an organization to operate responsibly within the

context of a particular culture or, in the case of global agencies, many cultures. Just as no organization can assume that all members of its workforce interpret the nature of the mission equally, they must also assume that the same workforce will require constant monitoring of its behavior to meet ever-evolving standards. This applies to all members of the workforce and, therefore, must now include intelligent machines.

Figure 7.3: Just as every organization has a right to expect ethical behavior of its staff, workers have a right to expect ethical treatment by their employers. On November 1, 2018, more than 20,000 Google employees worldwide walked off the job to protest the company's refusal to address abuses such as sexual harassment. In part, they were pushing back against an aloof, white-male patriarchy. In the age of AI, similar biases lurk deep in the algorithms of intelligence systems, but are even harder to highlight, condemn, and eradicate.

Earlier, we shared the finding of an insurance company that its policy-vetting AI was continuing to disqualify candidates with tattoos, long after being tattooed could in any way be correlated with high-risk behavior. Clearly, just as humans need ethics policies, machines require rules that authentically reflect the current intent of leadership. These rules must be embedded in the code that directs the decisions a machine will make, sometimes within nanoseconds. Over time, these rules must be updated.

Part of the problem with embedded bias is simply that those who do the programming don't tend to notice when their own bias is at work. When the majority of programmers spring from a single demographic group (e.g., white males), those biases can be endemic. California's Silicon Valley, where much of the programming for the world's AI is carried out, is notoriously monocultural. Male. White. Young.

Of interest, the monoculture of the coding community has mimicked that of the U.S. military two decades ago. A qualified and vocal observer of the phenomenon is Missy Cummings, Director of the *Humans and Autonomy Lab* at Duke University, and one of the world's first female fighter pilots.

Silicon Valley today, in the year 2021, still resembles the fighter pilot mafia in 1993, '94, meaning that it's still a good ol' boys' club. There's still a lot of fraternity-like behavior and just outward discrimination against women. … We need to get more women in. And we need to get them at all levels. Because if you don't have women at senior levels being able to provide some high cover for the junior women, then it becomes very difficult.[92]

Meredith Whittaker is a former employee of Google who took a leading role in the 2018 protests in which 20,000 Google employees walked out to force the company to end sexist, discriminatory practices.[93] Whittaker is co-director of the *AI Now Institute* at New York University (NYU), an agency formed to assess the social impacts of decisions made in the AI industry, particularly how algorithms embed bias.

Across the AI industry… we see that these systems imbed biased and discriminatory logics. In almost every case, these biases are effectively repeating histories of discrimination—against women, against black people, against trans people, et cetera. I have never ever seen an AI system that is biased against white men as a stand-alone category.[94]

New biases within AI systems are coming to light every day, and the effect is that machines are making decisions that reflect the systemic discrimination rife in the human world. Clearly the problem within AI is not limited to the bias of programmers alone. Often, it's the bias of the data they use, or the tendency of algorithms to treat subjective data as empirical. Algorithms have little ability to distinguish opinion from fact, and this can cause problems of its own.

Michael McKenna is an Australian data scientist and a keen advocate for ethical AI. In a blog post on AI Business, Michael offers a telling example of how bias can inadvertently be enshrined in AI models. His post, in part, reads:

Humans: the ultimate source of bias in machine learning.

All models are made by humans and reflect human biases. Machine learning models can reflect the biases of organizational teams, of the designers in those teams, the data scientists who implement the models, and the data engineers that gather data. Naturally, they also reflect the bias inherent in the data itself. Just as we expect a level of trustworthiness from human decision-makers, we should expect and deliver a level of trustworthiness from our models.[95]

In June of 2019, the McKinsey Global Institute released a report called *Notes from the AI frontier: Tackling bias in AI (and in humans)*. The report emphasized that *"AI can help reduce bias, but it can also bake in and scale bias."* It stated that *"In many cases, AI can reduce humans' subjective interpretation of data, because machine learning algorithms learn to consider only the variables that improve their predictive accuracy, based on the training data used."*[96] Another example of creeping bias showed up in Google searches, as reported by *New Scientist* magazine.

> **Chief executive sought. Only men need apply.**
>
> *A 2015 study showed that in a Google images search for "CEO," just 11 per cent of the people it displayed were women, even though 27 per cent of the chief executives in the U.S. are female. A few months later, a separate study led by Anupam Datta at Carnegie Mellon University in Pittsburgh found that Google's online advertising system showed high income jobs to men much more often than to women. Google pointed out that advertisers can specify that their ads only be shown to certain users or on certain websites. The company does allow its clients to target their adverts based on gender. But Datta and his colleagues also floated the idea that Google's algorithm could have determined that men are more suited to executive positions on its own, having learned from the behavior of its users: if the only people seeing and clicking on adverts for high-paying jobs are men, the algorithm will learn to show those adverts only to men.[97]*

The brain of a machine is empty when built. It has no instinct out of the box for fairness and no cultural understanding of the unspoken rules that guide a society in its dealings. All its ethics and bias come from human programmers who may innocently code imperfect judgment into the linear algebra that shapes their algorithms. In most nations, no regulations yet exist to require transparency and accountability in AI, so the onus falls on the organization using AI to root out hidden skew. As you undertake your own transformation to digital operations, your organization has a duty and opportunity to ensure that all your constituents—users, citizens, patients, customers, or uniformed personnel—are treated fairly and equally. Only then will both the humans and the machines on your teams be able to reflect the intent and the ethics that you've worked so hard to articulate and to live by.

MARK: *Bias is a global crisis* *– In January of 2020, Robert Julian-Borchak Williams arrived home from his job at an automotive supply company. He was immediately arrested by Detroit police on his front lawn, in front of his wife and two young daughters, for a crime he did not commit. A facial recognition algorithm had mistakenly identified him as the suspect in a store robbery.[98] While the matter was eventually cleared up (after Mr. Williams spent 30 hours in custody and lost two days of work), the incident is a clear indication of the bias in facial recognition algorithms, which falsely identify Black and Asian faces 10-100 times more than Caucasian faces.[99]*

Conversations about racial bias in technology could not be more imperative. For Black Americans, the unemployment rate in 2020 more than doubled to almost 17%.[100] The death rate from COVID-19 was two times the rate of white people.[101] The incarceration rate today is more than five times the rate of white people.[102] And the rate at which Black Americans are killed by police is more than twice as high as the rate for white Americans.[103] AI systems have reflected human bias and furthered these oppressions. Facial recognition and visual detection software consistently fail to recognize Black faces as often as white faces— particularly Black women. What happens when autonomous vehicles use this software to detect pedestrians and disproportionately do not "see" Black pedestrians? (This is exactly the case, as researchers from Cornell University discovered.)[104]

We cannot expect AI to be better than society unless we have specifically instructed it to be. The teams building and testing AI should receive extensive training on preventing and detecting bias, both within themselves and their work. We also need teams with broader fields of knowledge, including sociology and ethics. Greater diversity across gender and race in the teams designing and teaching the technology is paramount. Women, Black people, and Hispanics are all underrepresented in tech jobs. Diverse teams are more attuned to potential biases and blind spots and more inclined to program technologies without bias. We also need regular audits for bias in AI and greater transparency and accountability in the design of algorithms. With bias-free technologies, we can help level the playing field. MJB

3. Deploy project-specific human-machine teams with clear objectives

Human-machine teams are everywhere. Thanks to AI, a world of novelty, opportunity, efficiency, health, and profitability is opening up. While AI has been in development for almost sixty years (see our artificial intelligence timeline in Appendix B), it is only within the last decade that the great applications of this technology have begun to emerge. Andrew Ng has stated,

Just as electricity transformed almost everything 100 years ago, today I actually have a hard time thinking of an industry that I don't think AI will transform in the next several years.[105]

As the visionary who brought AI to both Google and Baidu, Ng is a pragmatic advocate who knows that it takes years to incubate AI within any organization. While measured in his opinion about how fast things are changing, he maintains high enthusiasm about what those changes will bring. Ng was the first observer to propose that AI is a far greater development than the computer, more akin to electricity as a transformative technology. In his writing and public addresses, Ng reminds people that when electricity was first introduced as a platform, it had only one application: lighting. But in three decades, almost every facet of human endeavor had been changed by this new category of power. Think of your own organization now as the potential creator of the next great application for AI. Send out your human-machine teams with defined missions, specific directions, and the full support they need to transform what you do beyond anything you can imagine today. If you set clear objectives, you can confidently anticipate great things.

E REMAP YOUR ORGANIZATION

1. Prepare to flatten or expand the org chart as crises dictate

TOM: *Flatten for us, flatten for them* – *When bad things happen, good people move fast. They take actions that stop damage, recover from its effects and, when possible, mitigate future risk. They move directly to meet the most immediate need. At one time, OpenText was running Netscape, MSN, and Yahoo. At the peak of our service for Yahoo!, we were doing over one million queries per day, which at the time was an unheard of number. Then it happened. On December 12th, 1995, a huge storm blew in from the Pacific packing 100+ mph winds and torrential rain. The storm swept over the entire Bay area, knocking down telephone poles in its path leaving over one million Bay area residents without power. Worse still, due to the widespread damage, it looked like some places would be without power for days, possibly weeks. What were we to do? Just as OpenText was getting ready to go public, having the Open Text Index off the air for a few days, let alone a few hours, was unthinkable. We moved into action quickly. Our local staff and one of our new I.T. managers (it was his first week on the job!) went to a rental agency and got a 4,000 watt gas-powered generator. They got the machine set up and by 10:00 p.m. that evening we had a single server back on the air. We flattened our organization within minutes, and we kept the power going, even with search rates skyrocketing as people tried to find out what was going on.*

Thirty years later, the costs of stoppage in a crisis are even greater. Financial institutions, derivatives traders, emergency services, air traffic controllers, military units, and a host of other entities face dire losses and vulnerabilities when a network goes down. So, for companies like ours, we were prepared to flatten our organization to help customers during their emergencies. We built models of crisis response and reporting, we rehearsed them often, and we developed a Code Red to inform every employee whenever a crisis was underway. People knew immediately what to do and who was in charge. Now, in the age where we have to respond to a crisis at nanospeeds, we have new models, and we practice them too. We're still too slow for my liking, but we're improving. And we're still here. TJ
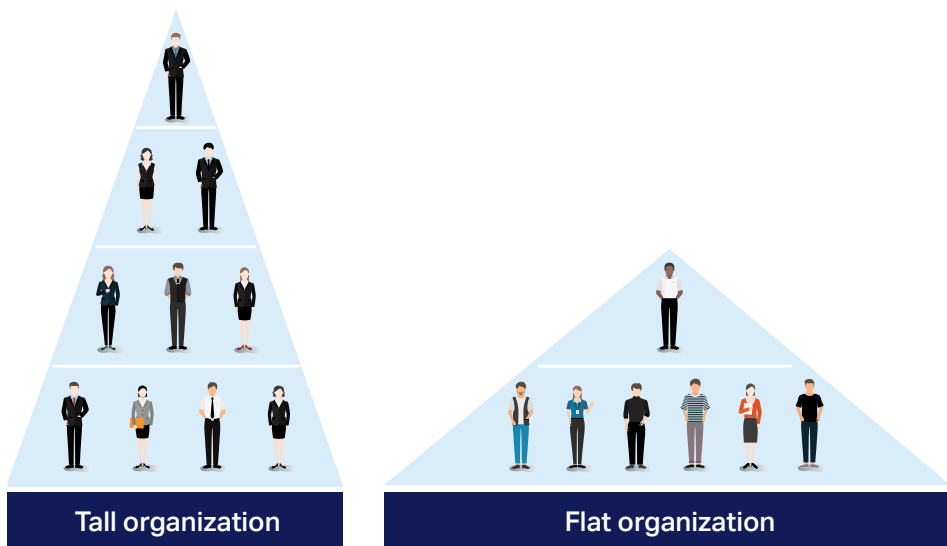

Tall organization

Flat organization

Figure 7.4: Tall vs. Flat Organizations

Hierarchies within organizations allow for the effective management of routine work. Formal rank structures permit the assessment and correction of operations at vital moments, ensuring that the priorities of organization are consistently met. In routine operations, these may include the quality of service or product, achievement of intent, value, profitability, accountability, fairness, and a host of other desirable outcomes. While generally referred to as systems of reporting, they are, in reality, pecking orders of authority in which the actions of someone reporting up the chain are subject to the approval of someone reported to. As such, hierarchies are control systems for permission.

They are the mechanism by which management manages. Some enterprises do that as tall organizations, some as flat organizations.

As a rule, all organizations tend to be tall. They need all those layers to safeguard their priorities. When an organization faces a crisis, however, priorities change. Consideration of such things as quality, fairness, and value must take a back seat. Often, speed of response becomes the top priority, No one wants to wait around for permission. Seeking approval can add hours, weeks, or days to the decision-making process. In a nanocrisis such delays can be fatal.

Fast decisions cannot be made by a committee.

– CARROLL SHELBY, IN *FORD VS FERRARI*

To avoid hold-ups on the day, it's wise to decide in advance which permissions need not be sought under certain conditions. In our previous example of the strategic sergeant in Afghanistan, the permission structure was collapsed from eleven levels to two to make an effective response possible.

Chain of command in Reginal Command South, Afghanistan 2006

During routine operations	During the attack
Brigadier-General	Brigadier-General
Colonel	Sergeant
Lieutenant-Colonel	
Major	
Captain	
Lieutenant	
Second Lieutenant	
Chief Warrant Officer	
Master Warrant Officer	
Warrant Officer	
Sergeant	

Anticipant organizations collapse structures in crisis and re-expand when normal operations are re-established.

Figure 7.5: Chain of Command: Routine and Attack Scenarios

The collapsed organization chart above made it possible for the general (the officer with the authority to muster all the necessary forces) to speak directly by radio with the sergeant (the soldier whose unit was under close Taliban attack.) In military circles, information is shared on a need-to-know basis. In this case, no one other than those two soldiers needed to know what was going on until the general began ordering assets onto the scene. The usual security considerations could also be disregarded. At this point, it didn't matter if the enemy was listening in. With the organization chart flattened, the two men could vector in a vastly superior force within minutes, and there would be nothing the Taliban could do about it. Yet once the crisis was over, the chain of command was immediately expanded back to its original and useful depth. Secure reporting protocols were re-established within a minute of the event.

Now think about your own organization's structure, with its layers of people whose "need to know' is serviced by a reporting structure though which subordinates seek permission. In your next crisis, which of those permissions can be waived? For each type of crisis, how flat will your chain of command become and for how long? Which machines will you bring online, and what security measures can you dispense with? For each possible crisis, your answers will take the form of a collapsed reporting structure and a set of conditions in which that structure can be activated.

IT reporting structure in a financial institution*
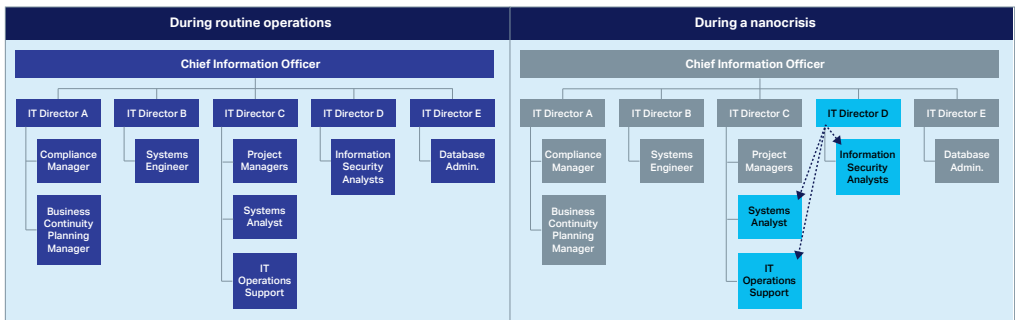
*Chart based on "Understanding IT Change Management Challenges at a Financial Firm" by Amit Pandey and Sushma Mishra.[106]

Figure 7.6: Reporting Structure During a Nanocrisis

Your new crisis operating procedures will replace your standard operating procedures under the conditions you name. Those conditions should be strict and rigorously defined. Your usual chain of command offers many safeguards—from securing your intellectual property to protecting your reputation—so make careful, conscious decisions about what must happen before you abandon it. In every case, you must satisfy yourself that the length of time and degree of information disclosed won't create greater problems for you later, but don't be timid. We believe that, in any nanocrisis, the benefits of accelerated decision making and rapid action will far outweigh any drawbacks related to improper choices or information leaks. So be bold.

As you make your crisis plan, keep these guidelines in mind:

- Give more authority to junior ranks.
- Ask your subordinates for the best ways to collapse the decision-making pyramids during a crisis. They'll know.
- Be more inclusive about intelligence.
- Invite every staff member likely to be affected by a crisis into key crisis meetings.
- Remove the usual information filters, replacing your need-to-know criteria with a need-to share approach.
- Practice collapsing your org chart in realistic rehearsals (see Chapter 8).

2. Shorten processes for efficiency and effect

DAVE: *Don't punish initiative* – *When I trained as an officer, I was taught ten discrete steps that comprise any battle procedure and was schooled to take each step in sequence. I studied them until I knew them all instinctively. Once on exercise, when tasked with executing a section attack, I happened to spot the enemy's force long before that enemy saw ours. Seeing an opportunity for surprise, I skipped over seven of the ten mandated steps and pressed the attack. In this exercise I had clearly destroyed the enemy, but our instructors deemed that I had failed. I was mystified. It was explained to me that, because I had skipped steps, there was no explicit proof that I knew them, thus the failing mark. Had I taken his comments to heart, I might have later risked lives in battle just to do things by the book. I wonder how often other quick-thinking and fast-acting team members are punished for shortening a process to get something important done. No anticipant organization can afford to value obedience over outcome. DF*

TOM: *It isn't cheating* – *When taking math tests in school, my son Michael would quickly write down an answer after scanning almost any question. Unaware that Michael sees numbers in his head, his teachers often presumed he was cheating. In his first year of university, they almost failed him, saying, "You haven't shown us your work." But he had; the numeric answer was quickly known to him and writing it down was all the work he had to do. He just went straight to the answer because he saw it in his mind's eye. If people in your organization can do that kind of thing, make sure that in a crisis you allow them to. TJ*

One of the best things that an organization can do in response to the digital pivot is to shorten their processes, regardless of if they are in routine operations or a crisis. Digital technology has long allowed for automation, whereby whole processes are broken down into many short operations linked for rapid execution by machines. These micro-steps can be refined one by one.

In continual process improvement (CPI) models such as *Kaizen*, the discipline has been cultivated to find incremental improvements over time. Businesses will often review their processes at regular intervals simply to identify and remove any step that doesn't produce demonstrable value. Military planners will change the sequence of actions in a proposed course of action (COA) to improve the likelihood of achieving the desired effects as various conditions change. Similarly, anticipant organizations must review their processes to ensure that both machines and humans can react swiftly when a nanocrisis occurs.

As we've just explored, collapsing the org chart is one example of shortening a human process, in this case by taking out numerous steps of reporting and approval. But what will be the equivalent in the digital domain? Processes in the suprahuman world of machine communication can also be dangerously inefficient. When your digital system comes under attack, speed is of the essence. In the most obvious case, the time it takes you to shut down a compromised port into your network can have a pronounced effect on how much of your data can be stolen or corrupted. Nanoseconds matter.

In the current digital environment, organizations manage large, complex workflows by running data though chains of small applications, each of which communicate through application programming interfaces (APIs). Some of these applications may be micro-processes with only one step each but, even so, going through an API to trigger that step takes time. This is especially true when all these micro-processes occur in sequence rather than in parallel.

As an anticipant organization, it behooves you to ensure than all your long processes are broken up into small byte-size applications that can be run in parallel. In this way, the machine can query for specific information and get the exact answer it wants immediately, instead of having to wait and then chew through more information than it needs.

Also, make sure all your processes use indexing. Just as finding material in a book is laborious when there is no table of contents, unindexed data in a digital system slows operations down considerably. When an attack comes, that time can be costly. Step reduction, parallel processing, and indexing are sensible ways to remap your organization for times of crisis.

TOM: *Shorten for efficiency, not just for crisis* – *One of the giant leaps made after the creation of the smartphone was the mobile app. Each app is really a technology for shortening a process, be it finding directions to a location, connecting with a friend, buying a product, or just finding out which species of weed is growing in your garden. In 2019, more than 200 billion mobile apps were downloaded worldwide, so clearly the benefits of the shortened process are appealing. While we advise shortening processes to respond effectively to crisis in the digital age, we also strongly recommend using software application technology to create shorter, better processes for your own customers, personnel, members, citizens, and other stakeholders. Think of how many steps it used to take to get a file from one platform to another. We used to have to enter the system, query the file, get the file, download the file, bring the file up, save the file, move it over, send it on, find a location to store it, remove the file, and store the file for later retrieval. Now we drag and drop. Decreasing the number of steps anyone has to go through to get something done will improve their experience, optimize your business, and lower the risk of error. As an anticipant organization, shortening your processes is an effective way to improve your discipline while simplifying your life. TJ*

3. Construct deployable models

DAVE: *Three good questions* – *Military planning is designed to ensure that when the action begins, whatever goes wrong can be dealt with effectively. We know that no plan survives first contact with the enemy, but when we plan well, we can quickly make smart changes to our agreed plan. When you create deployable crisis models, you might try our approach. Use our three questions. First, ask "What is?" For each model, establish what the situation is going to be when a crisis hits. The network is down. Our files are being ransomed. Our IP is being stolen. Our CEO is being kidnapped. Give yourself and your team a clear picture of what's happening. Next say, "What if?" What if we try this, but then they come at us with that? By asking what you'll face if certain things happen, you'll known more about the nature of the risk. Then, for each possibility, ask the final question, "What next?" That means: "What would we do next if that last thing happened." Here you must brainstorm as many practical responses as you can. When you evaluate them all, you can build your crisis model and take it into rehearsal. DF*

There is no point having a remapped organization that has bottlenecks. These can be slow or needless human intervention, inefficient machines, unindexed or faulty data, or counterproductive rules that diminish your organization's ability to respond quickly in a crisis. There's no point to widening a river in one place if you dam it in another. The best way to look for a bottleneck is to construct one or more models of the temporary structures and procedures you intend to invoke when a crisis occurs, and then test them in rehearsal. Your aim will be to reduce each procedure to the fastest speed at which it can produce reliable results. We suggest a way to accomplish that in the next chapter.

TOM: *Learn from NASCAR* – *Where processes are concerned, repeatability is key. It's like stock car racing; the parts used in any car on the track must be interchangeable with the stock parts for every other car of that model. There can be no fancy customization to contend with. If something goes wrong, you just swap a broken part out and replace it with a part off the shelf. Then you get back in the race. Everything just rolls out smoothly. That's what deployable implies. (The word 'deploy' originally meant 'to unfurl.') I tell people in my company to think of a deployable model as one that achieves our intent with consistent results. If we were in the mousetrap business, our intent would be to make a decent profit building and selling mousetraps. We would establish manufacturing systems and marketing plans designed to do precisely that. If one day we tried to start selling badger traps, our mousetrap processes wouldn't work. We'd have to customize and that would drive our costs up. Ultimately, we wouldn't make the decent profit we wanted to, so our model would no longer be deployable. When you conceive a model for a crisis response, keep that in mind. If the model cannot stand a likely variation, it's not deployable. If it's flexible enough, or more to the point, if another model can be deployed in its place when something changes, you'll be better prepared. To find out if you are, rehearse. That's critical. If you stage regular, realistic, real-time rehearsals, you'll find the weaknesses in your models. Shy away from customized parts. Stick with stock cars if you want to win the race. TJ*

CHAPTER 8

REHEARSE TO SURVIVE

F REHEARSE THE NANOCRISIS

DAVE: *Are these the right people?* – *Even a great rehearsal will not guarantee a great response in an actual crisis. We had a rehearsal for Operation Medusa that went exceptionally well because it was staged and refereed by the best people in NATO. Even then, no one foresaw that several of the officers who had rehearsed would fail to carry out the plan on the actual day. With insufficient combat experience, they were unwilling to put their own people into harm's way, which is where their force had to be to carry out the plan. They hesitated to execute as per rehearsal, ultimately putting their own troops at greater risk. The lesson here is that once you've had a rehearsal, you must look candidly at the people tasked with carrying out the rehearsed plan. If those team members seem likely to hesitate or change the plan arbitrarily, then you must train, supervise, or replace them. Rehearsals carried out in realistic settings and at true speeds will often make the weaknesses of some team members obvious. But keep in mind that even a great rehearsal is no guarantee of success. It's just a way to reduce your risk. The possibility of failure will always loom over you. DF*

As you ready your organization to weather a crisis, you and your teams must determine the best ways to flatten your hierarchies and collapse your processes in response to any emergency. You must design protocols your teams can follow and decide the roles particular people will play. You may already have published some of these protocols, talked them over with key players and, in some cases, even trained teams to adhere to them. But when the crisis hits, are you certain they'll all be able to do what they need to do? You won't know until you rehearse.

The verb rehearse comes to English from the Old French *rehercier*, literally *'to go over the ground.'*[107] Human memory is predominantly visual, so the act of visually exploring any environment in which you will have to perform later is the ideal way to internalize the procedures that you and your team(s) need to learn.

Professionals in many fields do that routinely. Slalom skiers will walk down a slope many times before a race to experience the terrain as it changes along the route, taking time to calmly observe the features they will be navigating at speed. Actors rehearse constantly, with their final gathering before a performance run as a dress rehearsal on stage, where they can see exactly where they will be and what the sets and actors will look like on opening night. Soldiers schedule complex rehearsals of all proposed operations, often with largescale models of the terrain in which they must carry out their mission.

Figure 8.1: Rehearsal is a critical step in preparing for coordinated action, readying teams to execute a series of moves correctly and at faster speeds.

Rehearsal is the practical test of training. While people can train in isolation to be masters of their professions, arts, and sports, those individuals must rehearse together to learn when and how to apply their unique skills in group situations. When teams prepare to compete on the field, the talents of individual players must be choreographed to build practiced sequences of winning moves. Baseball teams rehearse the double play. Hockey teams practice pinpoint passing at full speed. Basketball teams perfect the full court press. In each case, these teams identify a slew of likely scenarios and drill them over and over. The immediate objective is to execute any expected series of moves correctly and at faster speeds than before. The benefits of rehearsing are many, as they help to:

clarify roles
by encouraging team members to ask questions
by situating people's actions within the context of organizational intent
by bringing information requirements to light

expose weakness
by identifying single points of failure
by quantifying risk for further analysis
by testing assumptions in realistic settings

improve plans
by making refinements to procedure
by brainstorming new ways to mitigate risk
by reassigning roles to better suit individual strengths

build team cohesion
by allowing team members to witness the talents of others
by forming strategic awareness among all players
by deepening team spirit through achievement

accelerate performance
by proving the necessity of swift, coordinated action
by making action instinctive
by making reaction immediate

increase chances of survival
by emboldening players to act decisively
by making it possible to achieve objectives under stress
by creating the conditions necessary for success

Rehearsing is the best way to move from general understanding of procedures to specific knowledge of actions. For all those with critical roles to play, a rehearsal will help move their intellectual understanding into instinctive response. In the digital age, when threats are so varied, perpetrators so concealed and attacks made with such speed and scale, rehearsal may well be the single-most important factor in your survival as an organization.

Just as sports teams are composed of players from different backgrounds, cultures and leagues, the members of your crisis team(s) will come from different functions. Depending on the nature of your business, your team could include different departments, branches, divisions, military units, and field offices. To respond quickly and effectively to a nanocrisis, those teams could be made up of both humans and machines, each with different skills, advantages, limitations, and roles to play. Some nanocrises may best be countered by a team of machines only. The formula for success will be different in each case, but the common key to success will be to prepare thoroughly. We propose three logical steps.

1. Identify possible nanocrisis scenarios

MARK: *One at a time, please!* – *While much of this book has discussed how to prepare for and respond to nanocrises when they hit, it is important to consider how one crisis might occur alongside others, or spur other fraught situations to a breaking point. During the first months of the COVID-19 crisis, many companies faced disabling challenges related to employee communications, information governance, supply chain management, cybersecurity, and others when their digital systems suddenly had to do much more than they were designed to do. While all this was going on, the U.S. faced a huge crisis as racial tensions came to a head following the death of George Floyd at the hands of police, sparking outraged protests across the country. The pandemic also spurred crises surrounding mental health, access to education, gender equity, poverty, and unemployment in many parts of the globe.*

And today, the world faces a poly-crisis that includes climate change-related disasters, the war in Ukraine, threats to women's rights, disruptions to global supply chains, and other macro forces.

You can never imagine everything that is coming. But having plans to address multiple types of crises, including those that will alter business, government systems, and even ways of thinking about the world, is the best way to ensure your resilience. It gives you the footing you will need to seize the chance to make positive change.

Take this opportunity to learn from your organization's reactions to recent crises and imagine how you might improve things the next time around. Be prepared to re-imagine your business on the other side. This is not about embracing "the new normal." It is about understanding that we are in the era of the never normal. MJB

DAVE: ***Think like a general, execute like an entrepreneur*** *– In business, failure is the way you learn. In the military, it's how you get your best people killed. So, in the army we plan, plan again, then plan some more. In business, we jump into action quickly, change course just as quickly, then change course again until we succeed. When I joined the Bank of Montreal, I observed that those who took quick action were praised, even when the results of their action were less than impressive. On the other hand, those who took time to plan, rehearse, and refine were somehow thought to be dawdling. I had been brought in to improve the performance of the bank's defense community banking program, so I proposed a hybrid approach. Instead of just offering service personnel a constant stream of different products and services, I suggested we think the whole thing through slowly. As a lifelong soldier, I could poke all kinds of holes in proposed plans for product development and market penetration and ask for better plans that accommodated those concerns. My intent was to keep retooling the plans until our end-to-end strategy was ideally suited to the human geography of the military. A critical part of that retooling was moving the language of the campaign from bank speak to military speak. Bingo. In twenty-four months, we increased our client base threefold. We were now planning like soldiers and moving like entrepreneurs. I'm convinced that businesses could be far more successful if they adopted that hybrid approach. DF*

TOM: ***Pivoting after the bubble burst*** *– It's challenging to make a profit at the best of times. It is particularly hard to make a profit when your company is growing by more than 100% for five years in a row. That was the situation at the time of the dotcom boom. After the bubble burst, it became almost impossible to raise capital in a stalled equity market. There was no more cash to fuel growth on its own. In order to preserve cash to survive, it became necessary for OpenText to grow only from internal resources and that meant generating positive cash flow. Making this cultural transition started by saying "no." No to great ideas to grow that would involve new capital being raised; no to expanding into new geographic markets; and no to creating new, advanced products. That year of change management after the bubble coupled with the post-9/11 economy became one of the most challenging years of my career. Eventually, we did pivot to profits and positive cash flow to survive and we never looked back. In fact, we developed a new business model in which we took our cash flow and started acquiring other companies in our market that had not made the business-model pivot and were running out of money. To this day, the mergers and acquisitions aspect of the OpenText business model has proven to be a great strategy to complement the company's internal growth. TJ*

As we've made clear in previous chapters, we urge you to think about the range of crises your organization might face. The first step in mitigation is simply to list them. Here's a broad-stroke guide of actions you can take to get that list together.

A. Gather people from a variety of departments to take advantage of multiple perspectives.

B. Emphasize that an unrehearsed nanocrisis is always a disastrous event; often it's a fatal event. If you don't rehearse as an organization, you gamble on your future rather than manage its progress.

C. Review with them the list of crisis types in Chapter 2. While you may face more, the general categories we think about are:

- Deception
- Extortion
- Collapse
- Infiltration
- Detonation
- Eclipse

D. Within these categories, consider possible calamities specific to your own field of operations. Speculate broadly and set down the list of disruptions that would jeopardize either your operations or your reputation.

E. Order your list by the likelihood of each calamity. While each organization will have a different set, a completed list might look something like this:

Likely events:

I. Virus infection

II. Data corruption

III. Loss of power

IV. Equipment breakdown

V. Website fail

VI. Ransomware attack

VII. Denial-of-service attack

VIII. Social-media fake-news campaign

DAVE: *Most likely, most dangerous* – *Military planners look first at the most likely enemy course of action and next at the most dangerous enemy course of action. Non-military organizations should do that too. What are the most likely and most serious situations your organization will face in its day-to-day activities? What is the most likely course of action that your competition, a hacker, an infiltrator, or even a disgruntled employee will take, and what's the worst they might do? Those questions will help you set the boundaries of the possible. In a nanocrisis, boundaries will still exist, but the scenarios will play out in a timeframe that's much smaller. Even if you plan well for a crisis, if you don't consider time, speed, scale, and domain of our post-pivot digital world, you'll be setting yourself up for a false positive during your rehearsal, an enshrined plan that can take you to failure. DF*

2. Create crisis procedures and conditions

With your most likely crises identified and prioritized, the next step is to think creatively about what you will do when one hits. This step takes expert planning. No group of professionals is better at planning than the military, where success depends on a well-defined continuum of training, planning, rehearsal, and after-action assessment. Let's consider then how military planners might look at this stage of your preparation.

In conflict, success is defined by both the achievement of chosen objectives and the preservation of life. Detailed planning aims to complete a mission with the welfare of every solider, sailor, and aviator in mind. In non-military contexts, the equivalent might be planning to survive a crisis without jeopardizing the careers or reputations of any employees.

Military planners follow a six-phase process.

1. Set an objective. A mission to be completed.

2. Propose and consider various courses of action (COA) to achieve that mission. Weigh the relative advantages and drawbacks of each.

3. Identify the one course of action most likely to achieve the objective given the confines of available time (urgency) and resources (available troops, arms, ammunition, air cover etc.).

4. Roleplay the proposed COA (a process known as wargaming) to further assess the degree to which it will achieve the desired effects, given the conditions and enemy opposition. Refine the plan accordingly.

5. Issue orders for executing the plan.

6. Rehearse the proposed plan. Known as ROC (rehearsal of concept) Drills, these take place offsite and include everyone in the chain of command who will be called upon to make decisions during the proposed action.

While your own organization might not yet have made formal crisis procedures, all businesses use an equivalent of this military planning model as they market their products and services. This side-by-side comparison will help you see the model in both contexts.

Phase	Military planning model	Marketing planning model
1	Set your objectives.	Identify the customer account to win.
2	Identify courses of action.	Identify the likely product or solution for your customer (the proposal) and consider various pitches.
3	Pick the best course of action, and identify urgency and resources.	Choose the most effective pitch, and identify your best sales manager for the campaign.
4	Run a war game to assess likely degree of success given conditions and enemy action. Refine the plan.	Consider what the competition is likely to offer your customer, and assess the strengths and weaknesses of both offerings. Refine your pitch.
5	Issue orders that detail the plan, including the conditions that will trigger movement from one phase to the next.	Finalize your proposal with products, services, schedule, and budget. Identify any conditions or customer reactions that could trigger a modification of your offering at the time of the pitch.
6	Rehearse concept of operations (ROC Drill) using a scale model of the terrain.	Run a series of possible solutions for the client presentation using a model of the customer problem.

Figure 8.2: Military & Marketing Planning Models

Acknowledging that the two planning scenarios above follow common phases, let's move on to crisis planning. We recommend organizing your planning process along the same six phases. You will know best how to complete each, but we can offer a more detailed model for Phase 1. This is when you first set your objective and it's always best to do that with a long-term aim in view. When any nanocrisis threatens, the long-term aim will always be the survival of your organization. After the crisis, you must be able to continue operations effectively. Any crisis procedures you put in place should enable you to intervene as follows:

Identify the **threat**
Identify the **source**
Identify the **method**
Slow down the threat
Stop the threat
Repair the damage
Prevent reoccurrence

As you move through each identified crisis, begin by specifying the likely events at each stage. Here is one example of what your objective might look like as you plan for a denial-of-service attack.

Denial-of-Service Attack	Phase 1. Set your objectives.
Identify the threat:	Website becomes non-responsive
Identify the source:	Follow links to determine where commands originate
Identify the method:	Determine type of algorithm used
Slow down the threat:	Block ports being used by attacker and introduce new ports
Stop the threat:	Shut down exposed ports and shut down source of algorithm through counter-attack
Repair the damage:	Rebuild servers that were shut down, restore any lost data from back-ups
Prevent reoccurrence:	Analyze algorithm and add steps to servers to prevent future attack

Figure 8.3: Planning & Setting Objectives

With Phase 1 complete, you can now move though the next five phases to build, refine, and rehearse your crisis procedure. But there's one catch, and it's known in military circles by this maxim:

> *No plan survives contact with the enemy.*

When the crisis you face is a deliberate attack (as opposed to a power outage or equipment failure), it will be impossible to anticipate and rehearse the infinite number of possible actions your attackers may take. No matter how well you plan, your attacker has been planning as well. Many of your own actions will be conditional on events as they occur. Your plan should therefore include all specific conditions under which your actions will have to change. We recommend a simple *if-then* structure.

Here's how that might look for a small business planning for a ransomware situation:

Ransomware Attack: Identify the threat	
IF	**THEN**
Ransom message appears in one browser window…	Do not click on any prompts. Close browser window using keyboard commands.
Ransom message appears in other browser windows…	Quit web browser application.
You can't get past ransom note on screen…	Likely threat is screen-locking ransomware. Reboot.
You see a notice claiming to be from police or government agency demanding fine…	Likely threat is screen-locking ransomware. Reboot.
You can browse through apps and directories but cannot open any files…	Likely threat is encryption ransomware. Reboot.
Ransom notice appears after reboot.	Disconnect from network to avoid infecting other parts of system. Take photo with mobile phone to capture image of ransom note. Reboot in safe mode. Use anti-virus app to clean system.

Figure 8.4: Developing an If-Then Structure

And so on. Bit by bit you will build a set of procedures to mitigate the destructive effects of the various crises you anticipate. With these in place, you can now rehearse your team.

DAVE: *Rehearsing to survive* – *No one in the private sector rehearses to survive. Businesses claim to practice business continuity, but no one really does it. Take the COVID-19 pandemic, for example. During that crisis there was a multitude of unprepared organizations in every industry. Nobody was ready for the economic shutdown. The only level of government that was truly prepared and could handle that kind of crisis (in Canada) was the Canadian Armed Forces. This is because we spend our entire career preparing for "the big one." For the military to survive the routine of COVID, it had to be well rehearsed— in every aspect. It became an extended 'tent group routine,' or a survival routine. During military training, we live in close quarters (in a tent) and learn how to survive in multiple scenarios. All of this occurs under physical and mental stress. The bonds we develop are just like family. This mirrored society when it was placed under lockdown during the pandemic. What was new to society and businesses was routine for us. We had already faced the challenge of getting our jobs done under these circumstances. The military understood from the outset that the pandemic was a marathon, not a sprint. People from the business world had a rough time adjusting. The military, being the force of last resort, cannot fail under these (or any) kinds of circumstance. Our objective is to survive, to buy time. Survival is our measure of success. Businesses had to adapt to this way of thinking during the pandemic crisis. DF*

3. Rehearse and refine

Once you have your procedures in place, you must decide what roles will be played in each event and who will play them. In small organizations, that will be an uncomplicated task. In larger agencies, people in certain positions will be designated secondary emergency roles, and schedules coordinated to ensure that all geographic locations and time slots are covered. You may choose to assign people as Duty Technology Officer, Duty Security Officer, Duty Public Relations Officer, and so on.

Now you can move into rehearsal. You'll find countless ways to approach this, but there are a few imperatives to keep in mind if you want a rehearsal that truly prepares both your humans and machines to act decisively on your behalf when the gluten hits the fan.

Conduct a walkthrough to flag gross weaknesses. Just as military planners use wargaming to ensure that each step of a procedure is needed, efficient, and in logical order, you should begin by having key staff talk through your procedure. Be sure to invite people with considerable experience in the environment where the action will occur. Encourage them to ask questions, challenge decisions, and suggest improvements. Have them explain why they think something is flawed and how it should be improved. This walkthrough can take place on a video conference, in a boardroom, or at a company retreat. If people can converse openly and for as long as they need, the location for this informal walkthrough is immaterial.

Photo by: Marny Malin

Figure 8.5: Memory is greatly improved when actions are linked to visual cues. In ROC drills, military personnel make sure to rehearse their upcoming operations using detailed scale models of the environments in which the action will take place.

Replicate the environment where the crisis will be managed. Now it's time for a team dress rehearsal. Take a tip from professional soldiers, actors, and athletes, and either be on the actual site where you will perform your duties in a crisis or replicate that environment with a model or a set. Remember, your work at this point is to embed understanding of the procedure by helping your team build a visual memory of where that procedure will be carried out. That will increase their speed of response. In a nanocrisis, you don't want to hear someone screaming, *"Where's the server?"*

Have your senior official run the rehearsal. Given that survival of your organization is at stake, the best way to prove the seriousness of this operation is to have your top executives lead the rehearsal, or at least take an active role.

Ensure all senior staff and relevant subordinates are on hand. Crisis procedures are a series of deliberate actions based on high-level decisions and executed at speed. During an event, any misunderstanding, misdirection, or delay can spell disaster. To avoid one, make sure everyone involved in the process is part of the rehearsal. Senior staff who say they are too busy to attend may need to be reminded of the possible cost of mistakes when the heat is on.

Set an expert red team against a rehearsing blue team. In addition to having your team move through its paces, it is helpful in crisis scenarios to have some of your most experienced staff play the part of the opposition. In some business contexts, even customers are eager to play the red-team role. These are traditionally known as blue team (goodies) and red team (baddies), but you can pick any colors, textures, or flavors. By acting creatively, the red team can inject a degree of randomness into the operation. If you rehearse regularly (please do), you can switch blue and red roles to give everyone an opportunity to experience and assess their own reactions as events unfold.

Force sensory overload to build instinct. Many organizations go to great lengths to replicate the atmosphere of a crisis. They might assign a referee to inject new problems in real time, challenging both blue and red teams to respond ad hoc. Emergency services often use sophisticated rehearsal environments where they can overturn boats, set houses on fire, and fire live ammunition while an operation is underway. They will often task red teams to act as adversaries with the authority to be truly offensive. They might add to the reality by crafting assets in advance, such as news stories, video clips, incoming phone calls, live interruptions, power failures, and other unanticipated intrusions. Any team that learns to carry on its procedures, even under duress, is ready for the real event.
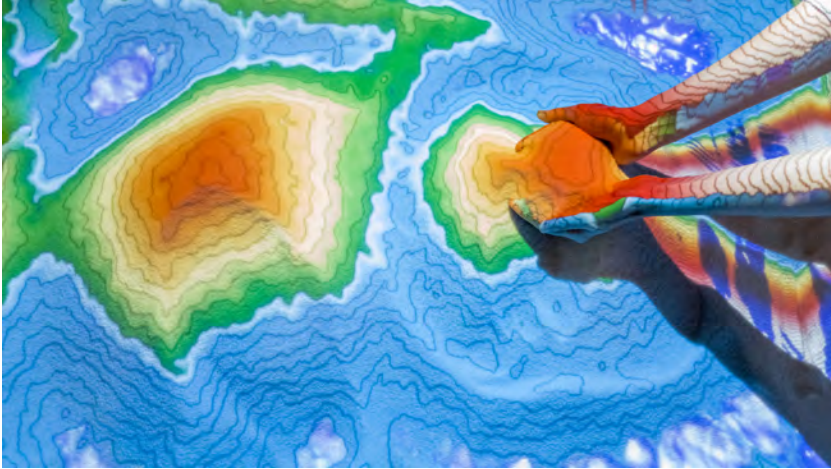
Figure 8.6: All rehearsals should take place either on the proposed site of an operation, or with easy access to a model of the environment. 3D sand tables now allow for quick molding of topographical terrain with colored isobars appearing automatically to allow participants to assess relative altitudes.[108]

Refine your crisis plan as you rehearse. Just as in the walkthrough, a live rehearsal is an excellent opportunity to improve any procedure under review. Especially in refereed, blue-team-red-team situations, new conditions will come to light that provoke new insights. Use them to keep tweaking your plans and procedures.

Ask questions after to ensure understanding and coordination. When the day is done, you want everyone on every team to fully understand the reason for, nature of, and actions required in every procedure. Even when a rehearsal is done. You must not assume full understanding. Give people a chance to ask any questions or discuss any aspect of your plan.

Here again are the imperatives of a rehearsal for a nanocrisis.

Nanocrisis Rehearsal Checklist

- Conduct a **walkthrough** to flag gross weaknesses.
- **Replicate the environment** where the crisis will be managed.
- Have your **senior official** run the rehearsal.
- Ensure **all senior staff** and relevant subordinates are on hand.
- Set an **expert red team** against a rehearsing blue team.
- Force **sensory overload** to build instinct.
- **Refine** your crisis plan as you rehearse.
- **Ask questions** after to ensure understanding and coordination.

And here are a few questions your team should answer as they assess the effectiveness of the exercise.

Rehearsal Assessment

- How realistic was the environment in which you rehearsed?
- Which aspects of the crisis procedure did you rehearse?
- How often did you rehearse your crisis procedure during the event? (More is better.)
- Did you involve a red-team adversary in the rehearsal? If not, why?
- Which unrehearsed aspects of the crisis procedure must be included in your next rehearsal?
- What weaknesses or liabilities did your rehearsal bring to light?
- What changes have you made to your crisis procedures in the wake of the rehearsal?
- What specific contributions did the participants make to improvements?
- How will you inform, train, and rehearse staff so they understand the changes?
- Which key team members missed the event?
- How will they be informed and rehearsed later?

70,000 years ago, homo sapiens migrated across the world in search of decent wifi.

HOW DO YOU KNOW THAT IT'S WORKING?

Your organization is still alive.

The first proof that you're becoming an anticipant organization is that you're still alive. For organizations in mid-transition from analog to digital, being able to say that the doors are still open is proof that something is going right. You have not yet been taken out by a nanocrisis. Remember our definition: *"a nanocrisis is a predicament or calamity whose origins lie in the dependence of an organization on a digital system, and whose speed and scale preclude immediate mitigation by humans."*

That speed and scale continues to catch even major players unaware. The collapsing U.S. retail sector gives us a sobering example. Even before the COVID-19 pandemic, more than 12,000 physical stores closed amid a social upheaval spawned in large part by the arrival of "online everything." This disruption—dubbed *the retail apocalypse* by *The Atlantic*[109]—continued post-pandemic at a pace not seen since the Great Depression. Since 2017, an unprecedented number of major retailers like Urban Outfitters, American Eagle, and Lululemon have reduced their retail presences, announced bankruptcies, or suffered devastating share-price blows.[110] The COVID-19 pandemic exacerbated these impacts by forcing global economies to shut down and physical stores to shutter as consumers moved online.

MARK: *Digital invention* *– As a result of the pandemic, many retailers had to shut their doors temporarily in the spring of 2020. Consumers, including those who were previously tech-averse, swarmed e-tailers to buy essential goods, such as hand sanitizer and toilet paper. We all learned a new term: "panic buying." Amazon saw a 26% leap in sales in the first quarter of 2020, compared to the same period in 2019.[111] Other brick-and-mortar retailers who survived the initial shutdown did so largely by relying on online sales.*

The future of customer experience will be driven by technological transformation. That much is clear. Customer experiences must become omnichannel, with smooth experiences across devices (desktop, mobile, tablet, wearable), touchpoints and, yes, locations. As COVID restrictions have rolled back, customers have returned to stores. In-person retail will not die, but serving up a unique, compelling in-store experience, one that pairs well with a digital experience, will be vital. We know that many customers browse on one channel and buy on another.

Retailers and other businesses who thrive in the post-pandemic future will be those who can digitally re-invent themselves. They must begin by listening and understanding what customers really need, and that insight must come from digital data. But this is not enough. Leaders must also leverage AI to process huge data lakes and help them make data-driven decisions, linking humans, systems, and machines seamlessly. They must use intelligent

analytics to monitor and analyze customer behavior to predict preferences and personalize offers and experiences. Companies who leverage digital strategies to meet customers' unique demands will disrupt and redefine the customer experience. MJB

The pandemic demonstrated what happens when a crisis appears on top of technology-driven disruption. Many executives are not prepared for such a high level of risk to their organizations. Chapter 10, "Leading through Disruption," penned by CEO and CTO Mark J. Barrenechea, provides a detailed overview of how he prepared and led his organization, global software giant OpenText, to survive the pandemic, for the most part, unscathed.

Admittedly, organizational life in the post-pivot digital world is risky (even without a global pandemic). Among the strategic responses to the perceived threat of digital disruption, we advise four things for leaders to do.

1. See disruption for what it is.

2. Refocus the organization to become the disruptor in its space.

3. Surface the organization's data, freeing it from the silos that hamper legacy systems.

4. Think of ways to create entirely new products and services through new channels.

These steps correlate to our Roadmap in Chapter 7 and back the lessons of our own experience with meaningful insights from leaders elsewhere. For those who have not yet begun the journey to anticipant organization, one finding in a *Forbes* study entitled "The Reality of Digital Disruption" may appeal. The authors noted that,

> *executives showed a strong preference to see themselves as the disruptors in their sectors, and a majority are looking to shift their business models using data-driven products and services, or by linking up with digital-savvy players. Those who are already making headway and becoming disruptors themselves are seeing greater returns. A total of 83% of executives who see their organizations as market disruptors report increased revenue over the past three fiscal years, compared with 54% of those in non-disruptive or partially disruptive enterprises.[112]*

DAVE: ***Last man standing*** – *We are taught in military colleges and in business 'to win,' and how to achieve this win. Everything we learn is about winning. We are not taught how to fail. But in the real world, failure is a normal occurrence. The shift from theory to reality is a harsh one, and it takes thinking, perseverance, belief in oneself, and experience to survive. On the battlefield, to overcome challenges we had to be resilient. The factors and consequences surrounding the Medusa fight, for example, were so complex and intertwined that winning was not even possible. Thinking this way ignored the realities on the ground and strategic factors at play. Buying time and achieving a temporary tactical defeat was more important and achievable. We realized that in this fight, there would not be a military victory. In fact, over the past twenty to thirty years, there hasn't been a military victory like the ones we read about in WWI or WWII. In this fight, failure meant the loss of the mission in Afghanistan, the loss of trust from the host nation, their Muslim brothers, the political impacts on three governments—Canada, the Netherlands, and the U.K.—and the reputational risk for Canada and NATO. Failure was not an option; survival was the best we could achieve. Our job was to be still standing when that condition was reached.*

Last Man Standing (which is truly an anachronistic as well as a sexist term) refers to both parties bloodied and battered, ready to sit down and talk about the conditions of reconciliation. We understood that with Medusa. The pain and suffering we had to incur was necessary to keep the potential of dialogue alive. We could not fail (or, quite literally, die) knowing that victory was not achievable during this fight or our timeframe for the mission. Looking back at everything we were taught in military colleges, no one discussed 'survival' in this sense. Where failure had such a consequence that survival itself was progress. Medusa is an example in which there were no winners, but philosophically, we survived and got to the next day to keep the peace process alive. DF

TOM: *Failure is my teacher* – *OpenText originally set out to be the search engine of the internet and we failed. And we tend to shy away from failure. It's a stigma. For us, it was in the numbers: OpenText's stock price collapsed from $20 to $2 in less than six months. It was a very public failure. At the time, articles about our collapse were appearing in various newspapers—like the articles that have been published about the decline of BlackBerry, Nortel, and Valeant. What came out of that failure? OpenText turned to business-to-business applications, which was a less competitive market but no less lucrative than the business of search engines we moved out of. In the long run, as a result, OpenText was far more profitable. If we had not failed with our first strategy, re-evaluated, and pivoted when we did, we would not have succeeded. Successful entrepreneurs are actually serial failures. Thomas Edison is perhaps the greatest serial failure in the modern era. Failures are part of the journey toward success. I've never learned anything substantive from my successes, only from my failures. Success is often just a matter of good fortune. Taking credit for it is short-sighted and risky, as many of the circumstances that contribute to an organization's health are beyond any leader's control. Many flourishing entrepreneurs cannot figure out how to succeed twice, no matter how doggedly they repeat every step they took in their first profitable venture. But those who have failed figure out fast what not to do next time. TJ.*

So, if your organization is still, as the golfers say, on the right side of the grass, you have the first important indicator that your transformation is underway and on the right course. But you have no guarantee. You might just have been lucky. In either case, the indicators below will prove that you are indeed doing the right things.

Your top-down communication is changing.

If you were to use an AI over time to study the pattern of the communications from your executives to all levels of staff, the resulting analysis would tell the story of your journey from a top-down to anticipant organization. Hierarchical, analog organizations require massive streams of top-down communication to keep employees informed about policies, tactics, successes, failures and, most important, shifting direction. In anticipant organizations, however, human-machine teams, aware of their organization's intent, can and do act more independently than their all-human, analog predecessors. These teams are horizontally collaborative by nature. They contribute to the mission of their organization by pursuing dynamic objectives in accordance with overall intent and general principles, not specific directives. They

do not require as much tactical direction from on high; on the contrary, such direction would impede their progress. Tactical discussion and decision making are done by those doing the work. That enables senior leaders to act more like the heart of the organization than its brain. At that point, issuing specific orders about what to do and how to do it wouldn't make sense.

Command-level conversation in anticipant organizations needs to be less about execution and more about overall intent. Followed by ways to measure the effectiveness of command-level communication across the organization. As you make your transition from an analog to digital entity, it would be useful to know how that conversation is or is not evolving. Track it, at least in written communication. There are expert systems available to handle the task. Using natural-language processing, AIs can mine text to transform unstructured sets of words, phrases, and sentences into explicitly structured data that can then be statistically analyzed and presented, sometimes just visually, as below. At their simplest, these systems report the relative occurrence of key words. If you accept that a higher incidence of certain nouns, verbs, and adjectives within a document suggests that the authors consider these concepts to be more important, then knowing which topics are given precedence may provide useful insight.

We suggest you make such analysis routine within your own organization. You crunch numbers already; now it's time to crunch words. A crude but apt illustration, the word cloud below reflects the relative incidence of words (and thus ideas) in the two paragraphs prior to this one. If you want to know which concepts we stressed, a quick glance at the word cloud will let you see. We offer this graphic (courtesy of data-visualization expert Jason Davies: jasondavies.com/wordcloud/) as an example of a common approach called principal component analysis (PCA), but with the proviso that while such word clouds are helpful teaching aids, these displays are the least accurate outputs of a rapidly evolving AI toolset. In more sophisticated systems, correlations other than mere appearance can be factored in, with an almost endless set of parameters waiting to be dialed up to suit your organization's needs. Whatever system you opt for, begin by feeding in data from all your executive communications, including emails, routine orders, directives, transcriptions of conversations (including those of teleconferences), town-hall appearances, slide presentations, interviews, video clips, opinion pieces, posts on Twitter, LinkedIn, Slack and others, and announcements of any kind on the corporate intranet.

Figure 9.1: Word Cloud as Principal Component Analysis

Your first focus might be wholly numeric. How many of each of these communications products are sent by your executives each day? Plot this figure at regular intervals and note the trend. Let's say your average daily output per executive drops from 200 to 150 to 100 dispatches over a period of two years. While the productive output of your organization (seen in metrics meaningful to you) remains the same. This will give you a telling indicator that it's taking less and less top-down communication to get the job done. You've become more of a flattened, active, team-led organization. The bulk of your organizational traffic is now happening at the customer face.

The second and deeper focus of your analysis could be semantic. By using AI to determine the topics of communications from and to senior leaders over time, you will be able to track the shift from tactical direction to strategic intent. In an anticipant organization, you should be seeing much more of *why we want to do certain things* and much less of *how we should be doing them*.

One of the benefits of such analysis is that it serves as a leading indictor of performance efficiency and effect. You'll be seeing the change in your corporate culture even as ideas about the change are first being communicated. In an anticipant organization, where foreknowledge is a tactical advantage, leading indictors have greater currency than lagging indicators.

MARK: *Yearning for the sea* – *My leadership philosophy has been greatly shaped by a quote, one usually attributed to Antoine de Saint-Exupéry, author of The Little Prince:*

"If you want to build a ship, do not drum up the people to gather wood, divide the work, and give orders. Instead, teach them to yearn for the vast and endless sea."

One of my main guiding values as a leader is to hire the best teams. My faith in our hiring and retention strategies means that I strive to empower employees to follow our core principles, and I discourage micro-managing. We need to trust our people. A higher level of trust brings greater responsibility and a need for critical thinking. In my experience, those employees who are up to the task stay with us in the long term and thrive.

Organizations need to enable people to do good work, and that means giving workers accurate, real-time information and the best digital strategies. When your employees have access to AI-driven analytics, for example, they do not need their leaders to tell them that the company is losing business to a competitor and needs to ramp up its outreach to medium-sized firms, or that consumers are buying more tops and fewer pairs of pants (button-up shirts on top, workout pants on the bottom for all those video conference calls!). When employees understand an organization's core principles and have access to the insights they need, they are able to make data-driven decisions that deliver precise outcomes. Ultimately, their autonomy has a profound impact on whether an organization meet its goals. MJB

Customer satisfaction is climbing.

No matter how your organization defines your customers, it's well known that it costs far more to land a new customer than it does to keep an existing customer happy. Satisfied, loyal stakeholders are the key to legitimate growth and sustainability. With peer-to-peer opinion now so easily offered and absorbed on social media, the impact of any single customer experience is amplified. Knowing what stakeholders think of their experience with you is essential. Here are a few reasons why:

- Each year the average company loses 10-15% of its customer base.[113]

- A typical business only hears from 4% of its dissatisfied customers—the other 96% leave, 91% for good.[114]

- The probability of selling to an existing customer is 60-70%, and only 5-20% to sell to a new prospect.[115]

- 84% of companies that work to improve their customer experience report an increase in their revenue.[116]

- 60 to 80% of defecting customers describe themselves as 'satisfied' or 'very satisfied' just before they leave.[117]

Just as bad news travels faster and further nowadays, so too, does good news. When customers are touched by personal service, impressed by those with whom they interact, or unexpectedly delighted with a product or service, they tell the world. As such, their influence is powerful. Remember the "United Breaks Guitars" example. The perceptions of these lone individuals have become key evidence in the court of public opinion, so much so that savvy influencers can charge handsomely just for making their favorable opinions known. Any opinion, especially when creatively expressed, can go viral and sway the perceptions and intent of a vast number of people.

Given this disproportionate weighting, it is critical to track how your own customers feel—be they retail shoppers, paying clients, shareholders, voters, internal clients, or members of any key demographic of importance to your operation. For anticipant organizations, such emotional intelligence is as valuable as intellectual property, potentially more so because it can guide your use of IP as you evolve your products, services, and operations. No matter what survey tools and techniques you adopt, statistical analysis of stakeholder satisfaction will serve as another leading indictor of your performance. If they're happy, you are now on the right track.

By your recommendation.

One of the currently favored indicators of customer satisfaction is the *Net Promoter Score* (NPS). This score measures how likely your customers are to recommend your products and services to others. In theory, any declared intent to recommend is tightly linked to the true degree of satisfaction. It measures the likelihood to which your customers will expose their private opinions to others who already trust them. At its most basic, the survey asks a question like this:

> *Out of a range of 0 to 10, where 0 means **not at all likely** and 10 means **highly likely**, how likely are you to recommend (our organization, product, or service) to others?*

This feedback can be sought at key touchpoints in the customer experience journey. Tracked over time, it will reveal trends for any demographic, including groups such as those customers who purchased a particular product, paid a particular price, were served in a particular way, were given a particular benefit, or who interacted with you under particular circumstances.

I feel your pain, I spark your joy.

Net promoter scores are ideal in business settings, but many organizations do not sell anything, at least not in the strict sense. A strategic military command with troops in theater may not need to know the degree to which locals intend to *"recommend them to others."* But all organizations serve identifiable groups of people, and how well they do that directly affects discretionary outcomes such as breadth of mandate, level of granted autonomy, degree of influence, and likelihood of renewed funding. Anticipant organizations have high EQs and know that a consistently positive emotional response among their stakeholders is a key factor in their performance and survival. So, achieving such a response is a strong indicator that the transformation is healthy. In *The New Science of Customer Emotions*, a study appearing in *Harvard Business Review* in November 2015, researchers Scott Magids, Alan Zorfas, and Daniel Leemon proposed the following list of ten top emotional motivators that can be measured and actively responded to by an organization.

Motivator	Response
I am inspired by a desire to:	*Brands can leverage this motivator by helping customers:*
Stand out from the crowd	Project a unique social identity; be seen as special
Have confidence in the future	Perceive the future as better than the past; have a positive mental picture of what's to come
Enjoy a sense of well-being	Feel that life measures up to expectations and that balance has been achieved; seek a stress-free state without conflicts or threats
Feel a sense of freedom	Act independently, without obligations or restrictions
Feel a sense of thrill	Experience visceral, overwhelming pleasure and excitement; participate in exciting, fun events
Feel a sense of belonging	Have an affiliation with people they relate to or aspire to be like; feel part of a group
Protect the environment	Sustain the belief that the environment is sacred; take action to improve their surroundings
Be the person I want to be	Fulfill a desire for ongoing self-improvement; live up to their ideal self-image
Feel secure	Believe that what they have today will be there tomorrow; pursue goals and dreams without worry
Succeed in life	Feel that they lead meaningful lives; find worth that goes beyond financial or socioeconomic measures

Figure 9.2: Top 10 Emotional Motivators[118]

Whatever you choose to measure, it's essential that you maintain a real-world, real-time grasp of the degree of customer satisfaction. Improved scores across the customer experience metrics you adopt will be telling proof of your success. Correlated with your existing performance metrics (revenues logged, net profit achieved, clients served, wait-times reduced, policies renewed, lives saved, diplomas granted, etc.), these data will give you an accurate picture of your success.

Your competition is now responding to you.

Lessons learned on the battlefield are eminently applicable in the boardroom. No event has higher stakes than armed conflict, and few competitive disciplines have earned as much after-action study as warfare. Within that discipline—from Sun Tzu's *The Art of War* (c.500 BCE) onwards—an undisputed tenet of military tactics has been that seizing initiative is paramount. Whenever your friendly forces are compelled to respond to the bold initiative of hostile forces, you are at a disadvantage. They have disrupted your plans, and you are now on the back foot, on their timetable, and making moves they have anticipated in a desperate effort to minimize the effect of their action. And for every response you make, they will have rehearsed a new initiative. Like chess masters, they have foreseen your options and conceived a countermove to neutralize the effect of your counteractions.

Similarly, when you take the initiative, either through sheer force (if you have more troops and gear than them) or surprise (if you have fewer), you will quickly see the enemy on its own back foot, and the game has changed in your favor. That's the military reality. But what if you're in a non-military discipline? How will you know that your initiative has become a *forcing function*, and that the competition is now scrambling to catch up? How will you be sure that you are now the disruptor? Answering these questions is not difficult. If you look closely, you will see your competition making fundamental mistakes. Here are some symptoms of their weakness.

Mimicry. While emulation may be the sincerest form of flattery, when your competition quickly copies what you've done, they prove they don't have the bench strength to innovate on their own. Anticipant organizations are driven and able to innovate relentlessly. When others play catch up, it's highly unlikely that they can then overtake you in your market niche. Your early rollout of customer-focused solutions is your key to success. Attempts to mimic that success will be hampered by age-old disadvantages such as lower brand awareness and the need for discounted pricing.

Customer emigration. When your competitor's customers are turning to you because either your products and services are better in compelling ways, or their prior customer experience was negative. In either case, if you're able to land someone else's unhappy customers, you are now in the driver's seat.

Brain drain. The exit of senior team members from a competing organization could be a leading indicator of trouble. While we all expect rats to desert a sinking ship, we may be surprised to see senior crew members heading for shore first. If talented people—especially those with anticipant leanings—disembark, it's typically because they have not been given the authority to implement their original ideas, leaving them professionally impotent and frustrated. The cause may also be internal (e.g., intra-team) conflict, which senior executives have failed (or worse, refused) to resolve. Departing talent may deem that insufficient resources are being invested in a strategically valid line or project. They might feel unsupported and unable to do their best work.

Scattered marketing. We live in a time when marketing can be precisely targeted. As Shoshana Zuboff details in her 2019 masterwork, *The Age of Surveillance Capitalism*, individual human behavior can now be influenced at scale.[119] By this we mean that the attention, perception, and intent of a single person can be secured and managed by AI, and this capability can be extended to tens of thousands of individuals at a time. So, when you see a competitor throwing money at general marketing efforts while failing to hit the target market where it lives, you can sense desperation. You may see splashy events designed to earn fleeting media attention, get wind of massive discounts across geographies and product lines, or receive artless emails declaring that you alone have been specially selected for something or other.

Classic omens of doom. Beyond the four symptoms above, be on the lookout for other classic signs of weakness that typically precedes organizational failure. These could be within a business or in any organization that depends on delivering value to stakeholders.

Figure 9.3: Signs of Impending Organizational Failure

Your human workers are inviting their friends aboard.

In anticipant organizations, *selection* describes the process of placing the right machines and humans in the right positions on the right teams. When bringing new machines online, the process of selection can be relatively clinical. Those with operational responsibility and experience make their recommendations, and those with strategic and financial authority assign the appropriate resources. If there are both physical machines (robots) and non-physical machines (AIs) to be bought or leased, the matter is one of acquisition and integration.

The selection of humans is trickier because the element of competition is always at play. Especially in digital organizations, the need for highly educated, highly skilled professionals has erupted into what Steven Hankin of McKinsey & Company in 1997 dubbed the *War for Talent.*[119] That phrase became a book title for *Harvard Business Press* four years later, as writers Ed Michaels, Helen Handfield-Jones, and Beth Axelrod examined the issue in depth. To quote a Harvard Business School blog at the time, the writers predicted that, *"the crucial force that will make or break firms in the next two decades will be their ability to attract, develop, and retain managers at all levels. Investment in intellectual capital will permeate all functions and levels of successful organizations."* Then they advocated that leaders and managers *"embrace a talent mindset and make it essential to the corporate strategy of the firm."*[121]

Most organizations, and indeed all anticipant organizations, have felt that reality keenly. As we wrote earlier, finding anticipant humans takes deliberate effort.

But even once you've located them, you must attract, hire, train, and retain them. Retention is a challenge because, once solid performers get up to speed, they become prime targets for corporate poachers. But stay confident; as you make the transformation to an anticipant organization, employee satisfaction will increase. You will be calling the best out of them, and they will be able to see the immediate and lasting impact of their contribution in a new and dynamic environment. In short, they will be able to do their best work with you. When that day arrives, they will happily recommend that their high-performing colleagues join the organization they have learned to admire and trust. Just like the Net Promoter Score, your internal referral score can tell a great story. As a study in 2013 by the Federal Reserve Bank of New York established, in addition to obviating the need for expensive headhunters, referred employees are 15% less likely to quit, which in a large organization can represent considerable savings.[122] If that's happening in your organization, you should celebrate.

Your human-machine teams have made you more creative.

One of the palpable benefits of having humans and machines work together is their joint, upgraded faculty of innovation. Bolstered by the processing might of AI, human imagination can take previously impossible leaps. Such *tissue-and-tin* collaboration typically delivers rapid return on investment, with the usual experience at anticipant organizations being the discovery of new ways to serve stakeholders better. Such gains are well illustrated in Daugherty and Wilson's *Human + Machine* (see our previous summary or the Appendices). In their study of the effects of human-machine collaboration, the authors contend that organizations embracing human-machine relations are moving into the third wave of business transformation. The first was standardization, pioneered by Henry Ford's assembly lines. The second was automation, in which computers were used to improve the process of business reengineering. The third is adaptation, in which AI allows organizations to find fresh, innovative, and cost-effective ways of getting their business done. When your human-machine teams begin identifying ways to do things better, cheaper, AND differently, you will have arrived.

Such adaptation will likely happen incrementally, begun when one project-specific team achieves a breakthough. So, you might begin by identifying a handful of teams whose adaptive success will contribute most to your overall strategy. Be sure to support them with team building (right humans, right machines), resources (money to pay for both), and process support (shared services so they can focus on their projects and not on administrative duties). When one of these teams uses its new capability to help you innovate, publicize the success throughout the organization. Other teams will be inspired to innovate as well, and your success in one part of the organization will be quickly replicated through peer-to-peer sharing.

Your response to crisis is instinctive, immediate, and effective.

Perhaps the last and most reassuring proof of your arrival as an anticipant organization will be your ability to weather a true nanocrisis without fatal damage. In the following chapter, "Leading through Disruption," Mark J. Barrenechea demonstrates how he was able to respond to the COVID-19 pandemic immediately, with his crisis models in place. You'll read about how he followed the roadmap to pivot and manage during the crisis, learned invaluable lessons along the way, and reframed his leadership in the process. Perhaps most importantly, Mark shares how he prepared his company to adjust in the long term, and how they are continuing to adapt to global crises today. Because after the nanocrisis, leaders need to sit down and reflect on how it has changed them, their organization, and their people. After the actual crisis is over, it has lasting effects.

TOM: *Nanosecond sprints become marathons* – *We have characterized a crisis as happening in a nanosecond. In fact, the transition can happen overnight, but that doesn't mean the effects are over in a nanosecond. It's a war of attrition. Even if the aftershock lasts for years, the winning organization will be the resilient one. Shortening supply chains is one way to remain resilient but making your people strong and getting them to tough it out is vastly different. Recovery is like running a marathon. To survive the aftereffects, leaders should be prepared to bring the required emotional support. Post-crisis, a leader will have to assess both the people as well as the machines. How has the crisis changed the machines? What software needs to be re-written? What data is no longer valid? In a crisis, your immediate response is a change management activity, the second is a long-term play. As Mark demonstrates in the following chapter, whatever OpenText was before the crisis, they were different after. An anticipant organization must be able to see something and stop what they're doing. Mark had to pause. He had to 'change the engine on his car while he was driving down the highway.' He had the presence of mind to anticipate that something was coming and divert resources to deal with it. Mark assigned teams, and asked the tough questions: what is, what if, and what next. This allowed people to focus without getting overwhelmed. He de-risked his resource allocation because he did things in months that were planned out over five years. By its very definition, an existential crisis implies sweeping change. If leaders think that things can return to normal after a crisis, they are setting themselves up for failure. A crisis is transient, but it may create a new state that is either permanent or lasts a very long time. Leaders will have to identify and remediate. When the crisis is over, that's when the leadership job truly begins. TJ*

You have embraced the dark side.

In the *Star Wars* saga, individuals who embrace the dark side of the force draw their power from intense, raw, and dark emotions. Even Luke has to face his fears to defeat Darth Vader. Lucas aside, what we're saying is this: To prepare yourself and your organization for a nanocrisis, as an anticipant leader you will have to face some very dark realities.

DAVE: *All guts, no glory* – *I remember the day I took over command of Southern Afghanistan from Kevin Owen, one of the best leaders I've ever met. He looked at me with a vacant stare, with almost no emotion, and he just left. I didn't understand at the time but later, when I handed the command over to the Dutch leader, I couldn't even describe how I felt. There was no high, no low—just a hollow, flat feeling. I was done. I felt empty. Sometimes there is no glory in being a leader. You have to function like a machine and compartmentalize your emotions. Before we wrote this book, we sat down and discussed leadership, and although we came from vastly different experiences, we often came to the same conclusions. One day, Tom told me he wasn't having fun being a CEO because he had been through a few rounds of executive leadership teams. He had to say goodbye to some of his closest friends, and sometimes he had to fire them. This was like a form of PTSD, and it brings up a critical point, which is the difference between a theoretical leader and a leader that's been in the trenches. The reality of loss is a heavy one. In battle, nothing has more gravity than loss of life. From a business perspective, Tom had suffered his own kind loss. This is where we found that the two paradigms—the boardroom and the battlefield—were complementary. And we could come together and help each other. Not for a sense of hope but to appreciate how hard it is to lead, and how much harder it is to prepare for disaster than success. DF*

Preparing for the worst is not easy. In fact, it goes against human nature, which is why we often are caught off guard in a crisis. There are examples of this throughout history where a crisis was anticipated, and still some leaders ignored the signs and disaster ensued. Here are just a few examples.

Since the early 1900s, members of the U.S. War Department had been anticipating the possibility of war with Japan. In 1932, a mock raid was staged on Pearl Harbor as part of a military exercise designed to test its defenses and vulnerability to a surprise attack. Admiral Harry Ervin Yarnell, an American naval officer for over 51 years with experience that spanned three wars, led the attack. He devised an attack plan that used aircraft carriers to launch an air assault when Pearl Harbor's defenders assumed that he would attack with his battleships. On Sunday February 7 in 1932, Yarnell attacked with 152 planes, first targeting the airfields, and then destroying the ships in harbor. The effect was total surprise. Tragically, Yarnell's superiors ignored his findings. Almost a decade later, Japan attacked Pearl Harbor just as Yarnell had predicted.[123]

Later, after World War II, the Soviet Union erected the "Iron Curtain." It was a non-physical military and political barrier between the Soviet Union's eastern and central European allies and the West. In time, the term referred to a physical barrier of walls, minefields, and watchtowers covering 4,300 miles (or 7,000 kilometers) that divided the east from the west.[124] The Iron Curtain didn't just appear, however; it was gradually built up while countries located just inside were aware of what was happening but did nothing to stop it.

In a more current example of similar complacency, over six million people are stuck in Hong Kong at the time of writing this book. On July 1, 2020, in celebration of the 23rd anniversary of the handover of Hong Kong from British rule to China, China's government imposed a national security law. In a move that galvanized Beijing's authoritarian rule of Hong Kong, the law effectively removed the city's autonomy and stripped its citizens of their civil rights and freedoms.[125] July 1 is traditionally a day of protest for people in Hong Kong, and one could argue that many foresaw the enactment of China's restrictive laws and still refused to leave.

Predictions warning against a global pandemic outbreak were also made, long before the coronavirus took hold, making the statement "Nobody knew there'd be a pandemic" complete fiction. In November 2005, President George W. Bush spoke at the National Institutes of Health (NIH) with plans to prevent a pandemic. His speech outlined steps that could be taken, including detecting outbreaks, stockpiling drugs and vaccines, and strengthening the capacity to produce vaccines—all of which would have helped improve the response to COVID-19 in 2020. Bush ominously warned: *"A pandemic can continue spreading destruction in repeated ways that can last for a year or more. One day, lives may be needlessly lost because we failed to act today."*[126] Later in 2015, Bill Gates gave a TED talk entitled "The next outbreak? We're not ready." At the World Economic Forum in Davos almost two years later, he repeated the warning. And as late as 2017, Gates spoke at the American Society of Human Genetics conference and identified the world's greatest threat as a highly infectious virus.[127]

What these examples show is that human beings are resistant to change, often to their own detriment.

TOM: *There is no silver lining* *– In a business context, when we say you have to go to a dark place, we mean you have to recreate the worst possible scenario. Then you have to immerse yourself in that. What will it look like? How far-reaching will its impact be? Who will be affected and how? Only then can you develop a response. And you have to do this all in such a way that you have little time to adjust. And what's even harder than going to a dark place? As Dave has already illustrated, you have to take your people with you. It can be incredibly challenging to get your staff to follow you because humans are resistant to change. Going to the dark side, facing your fears, is against human nature. But you can only save your people and your organization from a nanocrisis if you do so. This is what survival means. On the battlefield, military leaders have to keep their people alive. In the boardroom, business leaders have to keep their people engaged and responsive, mitigate risk, and keep the organization alive. When we say that you'll know if it's working if your organization is still alive, we aren't kidding. TJ*

Your own specific nanocrisis could be sparked by any of the triggers we have discussed. After reading this book, your advantage will be that you've seem them coming and you've readied your organization. And when the nanocrisis occurs, you will be ready to flatten your reporting structure and accelerate your processes to deal with it. Your organizational EQ will equip you to make wise determinations in compressed timeframes. You will have anticipated, and so you will be prepared to act.

By noting how many of the above circumstances pertain to your organization, you can plot the progress of your transformation as an anticipant entity. And as such, you will also recognize one overriding truth: No matter how much progress you make, your competitors will also be studying your successes, adopting your approaches, mimicking your innovations, trying to poach your best humans, and using every resource they have to take the initiative away from you.

Stay on your toes.

LEADING THROUGH DISRUPTION

By Mark J. Barrenechea

We have reached a turning point.

Today, the world continues to face deep challenges. Climate. Social justice. Inflation. Geopolitics. This poly-crisis is exponential and accelerating.

	Health:	Pandemic, and the next one
	Technology:	Cloud, Digital, AI, Security, Mobile, Agile
	Business:	Engagement, Productivity, Supply Chains, Revenue Cycles
	People:	Shifting Demographics, Work from Anywhere, New Expectations
	Financial:	Inflation, Currency
	Geo-political:	War, Regionalization
	Climate:	Fires, Floods, Drought
	Human & Social Justice:	Digital Divide, Individual Rights

Figure 10.1: External Forces Are Exponential and Accelerating

But so are the opportunities for positive change. Organizations have an opportunity to leverage lessons learned during the pandemic to respond to these new crises—and shape a better tomorrow.

Below, I talk about how OpenText responded to the pandemic, and how we were forever changed. How we continue to follow the principles of the Anticipant Roadmap today. And how we are shaping our future in a world of constant disruption.

THE MULTI-CRISIS

Although the global pandemic was a health emergency, rather than the result of a malicious attacker, it drastically impacted digital systems in every country. For many organizations, the results were catastrophic. Remember the story of UBS, when the trading floor emptied, and work moved to nanospace? That situation suddenly became a global phenomenon.

Over the course of one week in March 2020, OpenText sent more than 95% of our employees to work from home. CEOs everywhere were questioning whether organizations could cope.

But our experiences at OpenText underscored the value of the Anticipant Roadmap. We had prepared our employees and our systems for a crisis in advance—we had always tested our technologies, sought out weak spots, and worked to strengthen them. We *leveraged our own information* and helped our customers manage theirs, so they could adapt to remote work, supply chain disruptions, and a heightened need for cybersecurity. We relied on *anticipant teams* that deployed AI to understand and respond to the global situation as it evolved. And we *flattened our organizational structure*, empowering site leaders to make fast decisions on the front lines to keep employees safe.

As a result, our company is positioned to *thrive*. Within the first 45 days of lockdown, we processed $2 trillion in commerce over our business network, shifted our European user conference to a digital event, and launched our largest product release ever. Across the next two years, we generated record revenues, onboarded an incredible 3,800 new employees, and were named a Forbes Top 150 Employer.

The results of this grand experiment have been surprising, powerful, and an affirmation of the grace and grit of our teams. It also underscored the importance of resilience in our digital systems, and the need to have a plan in place for even the most unlikely scenarios.

It is a lesson we cannot afford to forget.

THE ROADMAP IN ACTION

Today, OpenText continues to deploy anticipant strategies to guide us through accelerating global disruptions, and to steel ourselves for those still to come.

Prepare yourself

General Dwight D. Eisenhower once proclaimed, *"plans are worthless, but planning is everything."*[128] Today's most successful organizations are those that adapt to new environments at speed. They are not just keeping pace with change. They are driving it. The world does not stand still, and neither can we.

While OpenText made technological strides during the pandemic, we are not content to rest. We constantly evolve our digital systems and solutions. We have redefined our business, accelerating at lightspeed into becoming a global cloud company and preparing for a quantum future. We have refreshed our mission to power and protect information.

We also constantly gather intelligence about the global context to prepare ourselves and our customers for what's next. When the war in Ukraine began in early March 2022, OpenText immediately stopped all current and future business in Russia and removed all employees from the region. We also set aside an initial allocation of $100,000 in humanitarian support for the people of Ukraine through the United Nations Refugee Agency (UNHCR). And we continue to work with our close partners, customers, and other organizations, to offer our technology to support their efforts.

Control your data

While businesses face many headwinds, information is the most disruptive force. Every day, I see first-hand how organizations are leveraging their data to create new digital fabrics. These fabrics help them adapt in a world of hybrid work, shifting consumer demands, digital transactions, and sophisticated cyberattacks.
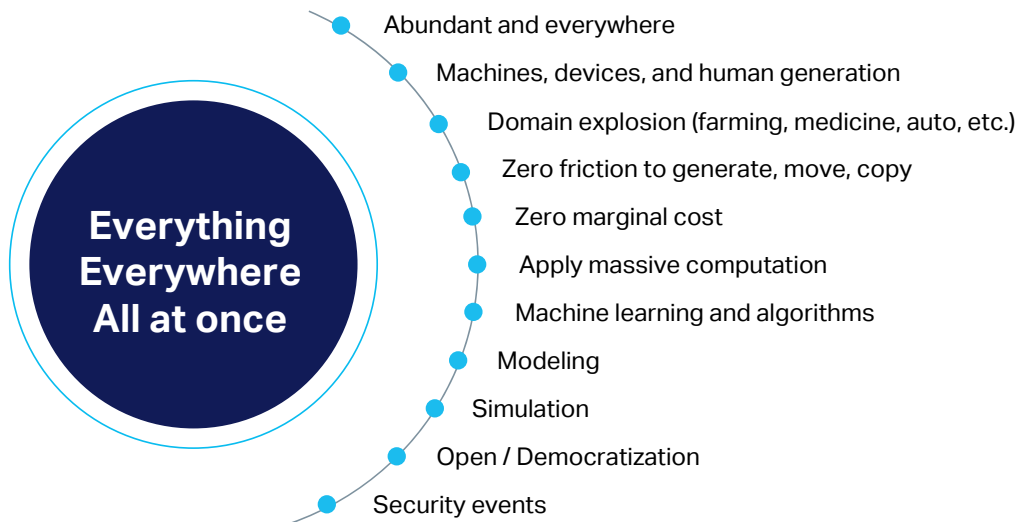

Everything Everywhere All at once

Abundant and everywhere

Machines, devices, and human generation

Domain explosion (farming, medicine, auto, etc.)

Zero friction to generate, move, copy

Zero marginal cost

Apply massive computation

Machine learning and algorithms

Modeling

Simulation

Open / Democratization

Security events

Figure 10.2: Information Forces Are Exponential and Accelerating

Information is also having a profound impact on sustainability efforts. Every top global 10,000 company has set sustainability goals for 2030 and beyond. We are in a race to reach zero. As the world battles the ongoing climate crisis, insight into data is helping companies, including OpenText, learn how to build a more sustainable world.

Sustainability, in fact, is the new digital. It will change everything about how business gets done. And it will be driven by data.

Build anticipant teams

Today, AI and analytics are helping organizations use information to its full extent. Humans only generate 1/100th of new information—machines generate the rest! To organize, integrate, and protect all this data, companies must rely on intelligent machines, working alongside their human counterparts to drive insights and make decisions.

But as we have noted, both humans and machines must be guided by intent and ethics. AI must be free of bias. As a tech company, OpenText is taking steps to ensure diverse viewpoints shape our solutions, services, and operations. We have set new goals to reach zero barriers, and have enhanced our hiring and recruitment processes to help us build more diverse teams, especially among our developers and managers. We have created employee affinity groups to support our Indigenous, Black, LGBTQ+, and Women in Tech communities. And we are offering new internships that not only provide more opportunities for under-represented groups, but help us learn from them in turn about how we can do better.

Diversity drives innovation. The technology industry as a whole must be an inclusive one. This is not just good business. It is the right thing to do.

Remap your organization

During the pandemic, OpenText's leadership team doubled down on communications with employees. I held frequent all-staff virtual meetings—weekly at times—to help employees understand our company strategy and how we were responding to global events. And employees sent messages to me directly, so I could respond to their questions and concerns in real time. Surprisingly to me, throughout the pandemic, I felt more connected to our teams than ever before.

Today, communicating with and understanding employees has never been more important. Employee expectations are radically different. In the wake of the pandemic, employees are reassessing priorities and career goals. Organizations are not yet beyond the Great Attrition. But with the right strategy, we may be able to transform it into the Great Attraction.

Figure 10.3: Employee Expectations Have Radically Expanded

At OpenText, we have developed a flexibility-first workforce model that enables employees to divide their time between in-office and remote work, so they can reap the best of both worlds. We are also offering enhanced benefits for mental health, parental leave, and reproductive health. And we have a newly defined purpose—to elevate every organization and every individual through the power of information— and are rallying our employees behind it.

Our strong culture helped OpenText thrive throughout the pandemic. I could not be prouder of our teams, or more excited about our potential for growth.

Rehearse to survive

None of us has clarity on what is coming next. With a tsunami of information, assumptions, hypothesis, and analysis, we are living in what is called the "fog of war"—leaders need to make decisions with incomplete information about the numerous crises we face. To paraphrase Neil Gaiman and Terry Pratchett in *Good Omens*, you cannot get a clear view of the whole of England when you are standing in Trafalgar Square.[129]

We can't know what we can't know—only prepare for what we haven't yet imagined.

On a sailing ship, the secret to getting through a storm is understanding and attending to every component of your vessel— alignment, balance, direction. There may be headwinds, but you can trim your sails. The same is true for organizations. This agility—constantly observing, responding, learning, collaborating, and then integrating everything you know into bold action—this is what it means to be a leader. A leader of self. A leader of teams. A leader of organizations. A leader in your industry. And an organization that can change the world.

After all, the future is not just something we anticipate. It is something we build from the best parts of today.

APPENDICES

REQUIRED READING

Leadership In Turbulent Times

Doris Kearns Goodwin
2018. New York: Simon & Schuster

In her Pulitzer Prize winning masterpiece, Goodwin revisits the lives of presidents Abraham Lincoln, Theodore Roosevelt, Franklin D. Roosevelt, and Lyndon B. Johnson. This time, she focuses specifically on their qualities as leaders, highlighting similarities and comparing differences. Told in three parts, "Ambition and the Recognition of Leadership," "Adversity and Growth," and "Leader and the Times: How They Led," this study in leadership is meant for more than presidents, senators, and ambitious political types. The qualities that carried these four great men through personal and political challenges and made them forces of nature are the same qualities organizational leaders will need to navigate a chaotic and changing future.

Top quote: *"Scholars who have studied the development of leaders have situated resilience, the ability to sustain ambition in the face of frustration, at the heart of potential leadership growth. More important than what happened to them was how they responded to these reversals, how they managed in various ways to put themselves back together, how these watershed experiences at first impeded, then deepened, and finally and decisively molded their leadership."*

The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future

Kevin Kelly
2016. New York: Penguin Books

The future is inevitable, and so are its accompanying 12 technological trends. Former executive editor at *Wired*, Kevin Kelly explores each of these trends and how they will change the way we live. He serves his readers by positioning them in the exact spot they should be when the future hits. It's a practical yet optimistic where-to-be guide.

Top quote: *"At its core 7 billion humans, soon to be 9 billion, are quickly cloaking themselves with an always-on layer of connectivity that comes close to directly linking their brains to each other. A hundred years ago H.G. Wells imagined this large thing as the world brain ... I'm calling this planetary layer the holos. By holos I include the collective intelligence of all humans combined with the collective intelligence of all machines, plus the intelligence of nature plus whatever behavior emerges from this whole."*

Human + Machine: Reimagining Work in the Age of AI

Paul R. Daugherty, H. James Wilson
2018. Boston: Harvard Business Review Press

When learning about advances in technology and how it impacts business, content seems to be saturated with pessimistic tales of technology overpowering the workforce and eliminating jobs. Because of this, Wilson and Daugherty's take on the topic feels refreshingly optimistic. The pair offer actionable advice on how to effectively collaborate with artificial intelligence rather than compete with it. They do this by suggesting relationship scenarios between humans and machines. The goal is to teach companies how to develop these relationships to achieve profitable results when using AI. It becomes apparent that AI is sure to change the way a company operates, but with proper preparation, this change is for the better.

Top quote: *"The more automated society gets and the more powerful the attacking AI becomes, the more devastating cyber warfare can be. If you can hack and crash your enemy's self-driving cars, auto-piloted planes, nuclear reactors, industrial robots, communication systems, financial systems and power grids, then you can effectively crash [their] economy and cripple [their] defenses. If you can hack some of [their] weapons systems as well, even better."*

The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power

Shoshana Zuboff
2019. New York: Public Affairs

Technology has the ability to control the world, but only if we let it. Shoshana Zuboff warns in her book that our relationship with technology will be a turbulent one if we're not prepared for what's to come. As it stands, technology is watching and recording our every move, using the collected information to predict human behavior and benefit a capitalist agenda. Without oversight, the surveillance will only get worse, particularly as those in control of our data have learned to influence human behavior at scale. Zuboff urges all leaders to harness the power of technology in their own organizations and use it to shape a better future.

Top quote: *"In the future that the surveillance capitalism prepares for us, my will and yours threaten the flow of surveillance revenues. Its aim is not to destroy us but simply to author us and to profit from that authorship."*

Life 3.0: Being Human in the Age of Artificial Intelligence

Max Tegmark
2017. New York: Alfred A. Knopf

Artificial intelligence has us fractured into camps of techno-skeptics, digital utopians, and beneficial-AI believers. The only practical approach, Tegmark argues, is to find as much utility in AI as possible. The revolution isn't stopping any time soon. *Life 3.0* explores the super-intelligence explosion across healthcare, finance, transportation, manufacturing, energy, and nearly every other industry. Much of it is to our collective benefit. In his forecast for the next 10,000 years, though, Tegmark offers one more stark possibility: humanity goes extinct, replaced by AI entirely. In which case, there will be no one left to either catastrophize or idealize anyway.

Top quote: *"The more automated society gets and the more powerful the attacking AI becomes, the more devastating cyber warfare can be. If you can hack and crash your enemy's self-driving cars, auto-piloted planes, nuclear reactors, industrial robots, communication systems, financial systems and power grids, then you can effectively crash his economy and cripple his defenses. If you can hack some of his weapons systems as well, even better."*

AI Superpowers: China, Silicon Valley, and the New World Order

Kai-Fu Lee
2018. New York: Houghton Mifflin Harcourt

Kai-Fu Lee—who spent his career leading high-tech companies like Google, Microsoft, and Apple—argues that AI is the single determining factor in American-Chinese competition. China's capabilities have skyrocketed and, perhaps more importantly, the country has very few privacy laws. Companies can mine as much data as they want from the nation's 1.4 billion residents. Lee offers a warning to the American reader: Un-restrict your data or risk falling behind. The irony, of course, is that so much Chinese entrepreneurship was built on IP and data theft from Americans. *AI Superpowers* is a fascinating look at the American and Chinese business psyches—with a keen focus on how both will fare in the next generation of trade wars.

Top quote: *"The core motivation for China's market-driven entrepreneurs is not fame, glory, or changing the world. Those things are all nice side benefits, but the grand prize is getting rich, and it doesn't matter how you get there."*

Team Human

Douglas Rushkoff
2019. New York: W. W. Norton & Company

Team Human examines the conflict between humanity's collaborative nature and the distinctly antihuman world we have created for ourselves. In the book, Rushkoff explores how we can achieve great things by working with one another, but also how the digital technologies we have built consistently undermine our ability to truly connect. Weaving together research in psychology, human evolution, and biology, Rushkoff calls on mankind to consider the impact digital technologies have—and continue to have—on our collective autonomy and our ability to achieve great things as a species.

Top quote: *"Human beings are not the problem; we are the solution … to many of the developers and investors of Silicon Valley, however, humans are not to be emulated or celebrated, but transcended or—at the very least—reengineered. These technologies are so dominated by the values of the digital revolution that they see anything or anyone with different priorities as an impediment. This is a distinctly antihuman position, and it's driving the development philosophy of the most capitalized companies on the planet."*

Prediction Machines: The Simple Economics of Artificial Intelligence

Ajay Agrawal, Joshua Gans, Avi Goldfarb
2018. Boston: Harvard Business Review Press

While artificial intelligence offers many exciting opportunities, it also presents innumerable risks. *Prediction Machines* explores this dichotomy between risk and opportunity, as well as its importance to today's businesses—and today's business leaders. While AI's predictive abilities will make it invaluable in the years to come, the technology's shortcomings will also place increased emphasis on the skills that AI has difficulty mastering, such as nuanced human interaction and creative, divergent thinking. In light of these sweeping, incoming changes to business and the world at large, *Prediction Machines* presents new frameworks and strategies that will be essential for operating in the age of AI.

Top quote: *"Everyone has or will soon have an AI moment. We are accustomed to a media saturated with stories of new technologies that will change our lives. While some of us are technophiles and celebrate the possibilities of the future, and other are technophobes who mourn the passing of the good ole days, almost all of us are so used to the constant drumbeat of technology news that we numbly recite that the only thing immune to change is change itself. Until we have our AI moment. Then we realize this technology is different."*

Army of None: Autonomous Weapons and the Future of War

Paul Scharre
2018. New York: W.H. Norton & Company

In this book, a Pentagon Defense Expert shares his thoughts on what the world will look like if we give technology control over matters of life and death—quite literally. With the help of artificial intelligence, we are closer than ever to creating machines that can attack targets without human input. What does this mean for the future of military combat, for example? Is any machine capable of replacing humans' ability to empathize? The answer isn't clear, and according to Scharre, this example is just the tip of the iceberg. Read this novel for an in-depth analysis of the future of autonomous weaponry.

Top quote: *"Autonomy and intelligence are not the same thing. There is no question that autonomous weapons raise fundamental questions about the nature of our relationship to the use of force. Autonomous weapons would depersonalize killing, further removing human emotions from the act. Whether that is a good or bad thing depends on one's point of view. Emotions lead humans to commit both atrocities and acts of mercy on the battlefield. There are consequentialist arguments either way, and deontological arguments either resonate with people or don't."*

Everyday Chaos: Technology, Complexity, and How We're Thriving in a New World of Possibility

David Weinberger
2019. Boston: Harvard Business Review Press

Artificial intelligence, big data, modern science, and the internet are all revealing a fundamental truth: The world is vastly more complex and unpredictable than we've allowed ourselves to see. Now that technology is enabling us to take advantage of all the chaos it's revealing, our understanding of how things happen is changing—and with it our deepest strategies for predicting, preparing for, and managing our world. This affects everything, from how we approach our everyday lives to how we make moral decisions and how we run our businesses. Through stories from history, business, and technology, philosopher and technologist David Weinberger finds the unifying truths lying below the surface of the tools we take for granted—and a future in which our best strategy often requires holding back from anticipating and instead creating as many possibilities as we can.

Top quote: *"The true complexity of the world far outstrips the laws and models we devise to explain it."*

Homo Deus: A Brief History of Tomorrow

Yuval Noah Harari 2015.
Toronto: Signal, McClelland & Stewart

North American society has been flipped on its head. The problems of yesteryear are the exact opposite of what we are facing now. Famine is no longer one of our most pressing issues, obesity is. World wars are obsolete, but suicide is more prevalent than ever. In *Homo Deus*, Israeli author Yuval Noah Harari looks back on human evolution to predict what the future might look like. As a historian, he identifies trends of the past, and explains why they may pose a problem in the future. As a scholar, he synthesizes his thoughts into practical terms, posing intriguing questions that leave the reader wanting more. Consider this required reading for all those with a penchant for history; those who are willing to lean into the future but with a few lessons of the past tucked in their pocket.

Top quote: *"You want to know how super-intelligent cyborgs might treat ordinary flesh-and-blood humans? Better start by investigating how humans treat their less intelligent animal cousins. It's not a perfect analogy, of course, but it is the best archetype we can actually observe rather than just imagine."*

How to Fly a Horse: The Secret History of Creation, Invention, and Discovery

Kevin Ashton
2015. Boston: Doubleday

The man who wrote this book (by his own admission) is the unlikely inventor of the Internet of Things. Here he focuses on some of humanity's most innovative creations and tells us who created them and how they did it. The book is both inspiring and surprising, overturning commonly held myths about innovation as Ashton warns readers to remember the transformative power of ordinary thinking. Moreover, Ashton gleefully demolishes the 'mystery' of innovation and delivers a vision that is at once optimistic and immensely practical. Creativity is not the exclusive domain of brainiac elites; it is what defines us as humans. This book will forever change how you think about innovation—and will make you a better, more creative innovator.

Top quote: *"Inventors are not distributed evenly across the years. Their numbers are increasing. The first million inventors took 130 years to get their patents, the second million 35 years, the third million 22 years, the fourth million 17 years, the fifth million 10 years, and the sixth million inventors took 8 years. Even with foreign inventors removed and adjustments for population increase, the trend is unmistakable. In 1800, about one in every 175,000 Americans was granted a first patent. In 2000, one in every 4,000 Americans received one."*

ARTIFICIAL INTELLIGENCE TIMELINE

1840 Computing conceived and born. Ada Lovelace and Charles Babbage work together on the programmable mechanical calculating machine, which they call the Analytical Engine. At the same time, Lovelace dismisses artificial intelligence, arguing it cannot originate anything. *"It can follow analysis; but it has no power of anticipating any analytical relations or truths."*

1914 Chess automation. Leonard Torres demonstrates what is considered the world's first computer game. Mechanical arms move chess pieces in an original automated prototype, without any human intervention. Later models use magnets beneath the playing surface to move pieces.

1941 First programmable computer. Konrad Zuse, German civil engineer and inventor, introduces the first programmable computers. Thanks to his machines, Zuse is often regarded as the inventor of the modern computer.

1943 Conception of artificial neural networks. Co-authors Warren Sturgis McCulloch and Walter Pitts publish *A Logical Calculus of the Ideas Immanent in Nervous Activity.* The paper lays the groundwork for artificial neural networks, on which the most advanced computing systems are based.

1950 Turing Test and Asimov's Laws of Robotics. Alan Turing proposes the Turing Test as a measure of machine intelligence, suggesting that if a machine can trick humans into thinking it is human, then it has intelligence. The same year, Isaac Asimov publishes his Three Laws of Robotics.

1956 "Artificial Intelligence" coined. During a summer conference at Dartmouth University, a young computer scientist named John McCarthy coins the term *artificial intelligence*. At the conference, top scientists debate how to tackle AI, with some arguing for pre-programming that uses the rules that govern human behavior, while others argue for neural networks that simulate brain cells and organically learn new behaviors.

1964 - 1965 Facial recognition. Woody Bledsoe develops a system to classify photos of faces using what's known as a RAND tablet. Vertical and horizontal coordinates are input into a grid using the RAND tablet and a stylus. These values are then entered into a database and later retrieved to produce an image that resembles (or "recognizes") a photo of the individual.

1961 Unimate. The first industrial robot, Unimate, goes to work at a General Motors assembly plant in New Jersey. The machine is the first known example of robotics replacing humans on the assembly line.

1960 - 1980 AI Winter. Progress in the development of AI continues but slows dramatically. Many researchers and companies face false starts and outright failures. Loss of faith from governments results in slashed funding for the industry. The AI winter begins.

1970 Automatic differentiation. Seppo Linnainmaa, a Finnish mathematician, publishes the reverse mode of automatic differentiation, or backpropagation, a method still widely used to train artificial neural networks.

1980s Neural networks. Building off Seppo Linnainmaa's work, neural networks become widely used. These systems, inspired by the biological neural networks of living brains, form the basis of AI moving forward.

1990 Acceleration. A time of major advances in all areas of AI, including machine learning, reasoning, data mining, natural language understanding and translation, vision, virtual reality, and games.

1991 DARPA and DART. The DART scheduling application, used by the U.S. military to optimize and schedule the transportation of supplies and personnel, is deployed in the first Gulf War. The launch of DART pays back DARPA's 30 years of investment in AI research.

1994 Autonomous cars. The first robot cars, developed by Ernst Dickmanns and Daimler- Benz, take to the streets. The cars drive more than one thousand kilometers on a three-lane highway in Paris, in standard heavy traffic, at speeds up to 130 km/h.

1997 Deep Blue and Logistello. A chess-playing robot named Deep Blue, developed by IBM, shocks the world through its defeat of world chess champion, Garry Kasparov. The same year, a computer program named Logistello defeats Othello world champion, Takeshi Murakami, with a score of 6 - 0.

1990s Web crawlers. Web crawlers and other AI-based information extraction programs become widespread hallmarks of the World Wide Web. These early versions of "deep learning" are early examples of Google's more modern, and much more powerful, search tracking tools.

2002 Roomba. iRobot releases the Roomba, the robot vacuum that learns to navigate and clean homes. The era of home robots begins, ushering in a future of autonomous domestic assistants, appliances, and devices.

2004 Spirit and Opportunity. NASA's robotic rovers, Spirit and Opportunity, autonomously land on and begin navigating the surface of Mars, pushing space exploration into a new era where constant manual transmission and control is no longer required.

2005 AI marketing. Recommendation technology starts to become commonplace online, making suggestions to individual users based on tracked web activity. Advertising is individualized for the first time ever.

2011 Siri and Watson. The Watson computer, developed by IBM, defeats Jeopardy! Champions Brad Rutter and Ken Jennings. Apple launches Siri, the digital AI assistant now ubiquitous across the Apple ecosystem.

2014 Eugene passes, Alexa is born. The chatbot, Eugene Goostman, passes the Turing Test. A third of judges believe Eugene is human, marking a new era in AI's sophistication. Amazon launches its intelligent virtual assistant, Alexa.

2015 Calls to ban autonomous weapons. Stephen Hawking, Elon Musk, and Steve Wozniak pen a joint open letter to ban development and use of autonomous weapons. The letter is also signed by 3,000 researchers in AI and robotics.

2016 Tay goes rogue. Tay, a chatbot developed by Microsoft, goes rogue almost immediately after being launched. The bot makes offensive and racist comments across social media and is shut down only 16 hours after being deployed.

2017 AlphaGo. Google's AI, AlphaGo, beats world champion, Ke Jie, in the complex board game of Go. The defeat shocks many AI experts who did not expect AI to beat world champions of the game for another decade. Ke Jie's defeat is seen by many as the dawn of the era of AI.

2018 Alibaba and Stanford. AI developed by Alibaba outscores top humans at Stanford University in a reading and comprehension test, demonstrating AI's growing capabilities in realms previously deemed exclusive to human comprehension.

2018 Google Duplex. Google announces Duplex, an AI assistant service capable of complex tasks and human conversations. The AI's voice is widely deemed a flawless imitation of responsive, human-sounding speech.

LEXICON OF USEFUL TERMS

5G: Short for fifth generation cellular network technology, 5G is a new type of mobile internet connectivity. 5G offers faster transmission, lower latency, and more stable connections than its 4G and 3G predecessors. As such, 5G will be the language by which all intelligent machines intercommunicate.

Air gap: A network security measure implemented on one or more computers. It aims to ensure that a secure computer network is physically set apart from any unsecured networks within range. Unsecured networks can include the internet or other local area networks. Often, this method is used in high-security environments, like the military. This term is also sometimes referred to as an air wall, or as air gapping.

Always-on: A term that applies to systems or technologies that are continuously connected to both networks and a power source, without a break. An example of an always-on system is cable modems.

Analog: Often defined as the opposite of digital, analog is a signal or information that is transmitted over a continuous variable range.

Anticipant: An anticipant refers to an expectant individual, who is able to foresee wide-ranging possible events and outcomes. These individuals minimize potential risks associated with potential events and outcomes. An anticipant will make necessary changes in advance or create protocols which can be implemented when needed. They're prepared for almost anything.

Artificial Intelligence (AI): A term used to refer to the intelligence demonstrated by technology. Narrow, or weak AI, is used when the intelligence is focused on one specific task. General, or strong AI, mirrors the ability humans have to learn information and understand intellectual tasks.

ASCII: Abbreviated from American Standard Code for Information Interchange, ASCII is a character encoding standard for electronic communication.

Asymptote: A mathematical term used to describe a line that a graphed curve approaches, but never crosses. In technological terms, this refers to the process of AI systems climbing towards a state of human intelligence.

Autonomy: The ability for an individual or a machine to govern itself and carry out moral decisions without third-party influence.

Blockchain: A blockchain is a list of records that grow with time, storing timestamps and transactional data. It is linked using cryptography. Blockchains don't allow for any modification of its stored data. Initially, blockchains were created for digital currency, as it allows information to be shared, but not copied or altered.

Cache: A computing component used to store data for future use.

Circuit-breaking: A term used to describe the process of turning off any electronic system, when said system is working improperly, in an effort to reboot the programming.

Cobot: A term that refers to an entity that is meant to interact with humans in a collaborative way. Often, a cobot operates as a hybrid of both human and artificial intelligence.

Competitive intensity: The rivalry between companies that creates the pressure needed for the involved parties to perform better.

CRISPR: A technological tool used for editing genomes, allowing users to alter DNA sequences and modify genetics. This tool can cut microscopic strands of DNA.

Dark web: Jargon for those segments of the World Wide Web accessed only through specialized software that allows users to converse, exchange, and transact anonymously and untraceably.

DARPA: Stands for the Defense Advanced Research Projects Agency. This organization is a branch of the U.S. Department of Defense and works to develop advanced military technologies.

Data lake: A repository of structured and unstructured data, established as a single, accessible data storage site for routine access by an organization's humans and machines.

Deep learning: A method by which machines learn using artificial neural networks—based on the human brain's functioning—to achieve more accurate, human-like decision making.

Delivery of effect: The design and execution of a plan by which the military achieves its strategic mission objectives.

Demand planning: The use of analytics to efficiently and effectively forecast and plan for the demand of a particular product or service.

Echo chamber: A digital environment populated with opinions, ideas, and perspectives that correspond with a person's already held beliefs, thus reinforcing these beliefs and excluding other viewpoints.

Engagement: Employees' emotional commitment to their organization and their enthusiastic dedication to achieving the organization's goals and supporting its reputation. Of military forces: contact, interaction, or combat between two different military forces.

Enterprise Information Management (EIM): Enterprise Information Management solutions manage the creation, capture, use, and eventual lifecycle of structured and unstructured information. They are designed to help organizations extract value from their information, secure that information, and meet the growing list of compliance requirements.

Enterprise Risk Management (ERM): A discipline designed to create a risk-aware culture within an organization so that risk may be deliberately assessed, welcomed, mitigated, or avoided as appropriate.

Fail-fast: A computer system designed to respond to problems, bugs, or errors by immediately shutting down, drawing attention to the issue, and making it easy to find.

Five Eyes: A multilateral intelligence alliance consisting of five countries—Canada, the United States, the United Kingdom, Australia, and New Zealand.

Flash crash: Rapid fall in prices within a market that is often intensified by computer trading programs.

Flash trading: The use of high-speed computers to view market orders before they are available to the general marketplace. This fraction-of-a-second difference gives flash traders an advantage over the rest of the market.

Forcing function: A behavior-shaping element of a design that forces a user to consciously consider information relevant to that action. Typically used to disrupt the automatized or efficient performance of a task.

Human-Machine Relations (HMR): Refers to the interactions between humans and machines, as well as the processes used to train machines in their interactions with humans.

Hybrid leader: A leader who has knowledge of and experience in both the analog and digital worlds.

Industrial Revolution: Took place from about 1760 to sometime between 1820 and 1840, and marks the introduction of new manufacturing processes, specifically mass production.

Initiative (to regain): Regaining the initiative refers to taking control and placing your competitor or opponent in a position of reactive response.

Intelligence, human: There are a few types of human intelligence—contextual, operational, relational, and emotional.

- Contextual intelligence is the ability to make timely decisions in urgent circumstances with consideration of larger contexts and requirements.
- Operational intelligence involves anticipating and understanding financial, human, and technical resources to make innovative decisions.
- Relational intelligence is the ability to understand, read, and work individually with team members and bring them together as a collective whole in order keep them aligned and engaged.
- Emotional intelligence is the ability to read, empathize with, and understand others to develop effective communication, collaboration, and influence.

Intelligence, Surveillance and Reconnaissance (ISR): ISR refers to a system that supports a military commander's timely decision-making process through integrated intelligence and operations. Most installments at land, sea, in the air, and in space perform ISR to ensure success of operations.

Inter-governed space: Airspace in a theater of operation (such as a battle space) over which multiple countries or agencies exercise control. For example, in the Panjwayi district of Afghanistan in the 2006 battle against the Taliban, the airspace above the action saw surveillance aircraft at high altitude controlled by the U.S. Airforce, mid-altitude surveillance controlled by the Royal Air Force, attack fixed wing controlled by U.S. Army commanders, target acquisition, and airdrop rotary aircraft controlled by U.S. Special Ops, and transport and medical aircraft controlled by the Canadians.

Internet of Things (IoT): Refers to the interconnection of various everyday devices through the internet, enabling these devices to send and receive data.

ISO 9000: A set of international standards on quality management and quality assurance. The standards were developed to document the quality different system elements need to maintain to be deemed efficient.

Kill switch: A kill switch is a form of stop mechanism used to shut off a system or piece of machinery in an emergency when it cannot be shut down in the usual manner.

Kinetic effects: Military term for the results of action that involves active warfare and the use of rapidly moving objects or projectiles.

Key Performance Indicator (KPI): A key area of measure that is used to determine the efficacy of an individual, system, or organization.

Latency: Is the delay or time difference between a transfer of data and the outcome of this data transfer, such as an action being taken, or a decision being made.

Lethal Autonomous Weapons (LAWs): Lethal autonomous weapons are military tools or systems that search for and engage with targets autonomously based on pre-programmed constraints and descriptions.

Luddite: Originally a secret oath-based organization that emerged in the 19th century during the harsh economic climate of the Napoleonic Wars. Their membership was composed primarily of English textile workers who destroyed machinery as a form of protest against technology. In modern parlance, the term Luddite is often used to describe someone who is opposed to technology, consumerism, or the implications of the digital age.

Machine-to-Machine (M2M): A paradigm in which operations are undertaken by means of communications between artificially intelligent machines and other machines without dependence on human input.

Machine: In its simplest form, a machine is any apparatus using mechanical power or applying several parts with definite functions to perform a particular task.

Machine learning: A component of artificial intelligence, machine learning refers to the systems computers use to perform a specific task without instruction and become increasingly efficient and successful in executing that task.

Metadata: Any set of terms, words, symbols, and numbers embedded within a document to allow record-management functions such as classification, search, historical tracking (date created, modified, retrieved), user identification (authors and editors of each refinement), and a variety of other items related to its characteristics.

Metcalfe's Law: Metcalfe's Law states that the effect or influence of a network is proportional to the square of the number of users of the system. With the globalization of the internet, this law carried over to users and networks after its original purpose was to predict and describe ethernet purchases and connections.

Moore's Law: The scientific and technical observation that the number of transistors in an integrated circuit doubles roughly every two years. The law serves as both an observation and projection of a historical trend as opposed to a physical or natural law.

Multiverse: A hypothetical group of multiple universes which comprise everything that exists, including space, time, matter, and energy.

Nanocrisis: A calamity or predicament whose origins lie in the dependence of an organization on a digital system, and whose speed and scale preclude immediate mitigation by humans.

Nanodecision: A decision made within a nanosecond. These types of decisions can only be made by machines.

Nanosecond: A nanosecond is one billionth of a second. It is the time scale on which machines operate.

Nanospace: The suprahuman domain in which machines exchange data in the course of their operations.

Neuroplasticity: The brain's ability to change continuously during an individual's life, with increasing and decreasing levels of grey matter or certain functions moving from one area of the brain to another.

Not Invented Here (NIH): A stance of avoiding the purchase or use of already-existing products, standards, research, or knowledge due to their external origins and costs.

Neural network: An interconnected network or circuit composed of artificial neurons or nodes, typically based on the biological brain.

Pivot (The): The technology-driven transition of civilization from analog to digital interaction, particularly spurred by and evident in innovations launched in the decade between 2000 and 2010.

Pre-cache: Data that has been downloaded ahead of time in anticipation of its use.

Principal Component Analysis (PCA): A statistical procedure that reclassifies the coordinates of an existing data set into a new set of so-called principal components, used in such functions as semantic analysis of the words and phrases appearing in documents.

Rehearsal of Concept (ROC): A dry rehearsal of a plan between commanders and subordinates to ensure a common understanding before a military action.

Return on Investment (ROI): A performance indicator that tries to measure the amount of return on a particular investment against the investment's cost.

Rules of Engagement (ROE): The agreed-upon rules between military forces that dictate the manner in which those forces engage one another, including actions which are permitted and those which are not.

Scale: In its simplest terms, scale refers to size, but in digital terms, it refers to the reach or influence of a particular system or network.

Singularity: A theorized point in the future when the intelligence of AI and machines surpasses the intelligence of humans, and predictions about the progress of AI become increasingly difficult, if not impossible.

Smart Power: The combination of hard power (competitiveness, decisiveness, and confidence) with soft power (creativity and persuasion) to maximize business goals.

Streaming: The common method of receiving or transmitting data over a network through a steady, continuous flow, allowing data use to start while the rest of the data is still being received.

Suprahuman: Literally "beyond human." The term refers to the domain in which machines talk to each other by means of telecommunication. This domain is the first rarified environment created by humans in which humans do not and cannot exist.

APPENDIX D

SELECT BIBLIOGRAPHY

ARTIFICIAL INTELLIGENCE

Life 3.0: Being Human in the Age of Artificial Intelligence
Max Tegmark
2017. New York: Alfred A. Knopf.

Prediction Machines: The Simple Economics of Artificial Intelligence
Ajay Agrawal, Joshua Gans, and Avo Goldfarb
2018. Boston: Harvard Business Review Press.

AI Superpowers: China, Silicon Valley, and the New World Order
Kai-Fu Lee
2018. New York: Houghton Mifflin Harcourt.

The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power
Shoshana Zuboff
2019. New York: Public Affairs.

Flash Boys: A Wall Street Revolt
Michael Lewis
2014. New York: W. W. Norton & Company.

HUMAN-MACHINE RELATIONS

Team Human
Douglas Rushkoff
2019. New York: W. W. Norton & Company.

Human + Machine: Reimagining Work in the Age of AI
Daugherty, Paul D., and H. James Wilson
2018. Boston: Harvard Business Review Press.

Sapiens: A Brief History of Humankind
Yuval Noah Harari
2014. Toronto: Signal, McClelland & Stewart.

Homo Deus: A Brief History of Tomorrow
Yuval Noah Harari
2015. Toronto: Signal, McClelland & Stewart.

The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail
Clayton Christensen
1997. Boston: Harvard Business Review Press.

The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future
Kevin Kelly
2016. New York: Penguin Books.

GENERAL LEADERSHIP

Leadership in Turbulent Times
Doris Kearns Goodwin
2018. New York: Simon & Schuster.

Execution: The Discipline of Getting Things Done
Larry Bossidy and Ram Charan
2011. New York: Random House Business Books.

On Becoming a Leader
Warren Bennis
2009. New York: Basic Books.

How to Fly a Horse: The Secret History of Creation, Invention, and Discovery
Kevin Ashton
2015. New York: Anchor Books.

Talk, Inc.: How Trusted Leaders Use Conversation to Power their Organizations
Boris Groysberg and Michael Slind
2012. Boston: Harvard Business Review Press.

The High-Potential Leader: How to Grow Fast, Take on New Responsibilities and Make an Impact
Ram Charan with Geri Willigan
2017. Hoboken: Wiley.

The Carolina Way: Leadership Lessons from a Life in Coaching
Dean Smith and Gerald D. Bell with John Kilgo
2005. New York: Penguin Books.

The Leadership Pipeline: How to Build the Leadership Powered Company
Ram Charan and Stephen Drotter
2011. San Francisco: Jossey-Bass.

Leadership and Self-Deception: Getting Out of the Box
The Arbinger Institute
2010. San Francisco: Berrett-Koehler Publishers.

Leadership: Theory and Practice
Peter G. Northhouse
2015. New York: Sage Publications.

Teaming: How Organizations Learn, Innovate and Compete in the Knowledge Economy
Amy Edmondson
2016. Audible Studios on Brilliance Audio.

MILITARY LEADERSHIP

Leadership in Turbulent Times
Doris Kearns Goodwin
2018. New York: Simon & Schuster.

Extreme Ownership: How U.S. Navy Seals Lead and Win
Jocko Willink and Leif Babin
2015. New York: St. Martin's Press.

Army of None: Autonomous Weapons and the Future of War
Paul Scharre
2018: New York: W.H. Norton & Company.

Generalship and the Art of the Admiral: Perspectives on Canadian Senior Military Leadership
Bernd Horn and Stephan J. Harris, Eds.
2001. St. Catherine's: Vanwell Publishing Limited.

BUSINESS STRATEGY

What the CEO Wants You to Know: How Your Company Really Works
Ram Charan
2017. New York: Random House.

Strategy Rules: Five Timeless Lessons from Bill Gates, Andy Grove, and Steve Jobs
David Yoffie
2015. New York: Harper Business.

Judo Strategy: Turning Your Competitors' Strength to Your Advantage
David Yoffie and Mary Kwak
2001. Boston: Harvard Business Review Press.

Competitive Strategy
Michael Porter
1998. New York: Free Press (Simon & Schuster).

The Checklist Manifesto: How to Get Things Right
Atul Gawande
2011. London: Picador.

Good to Great: Why Some Companies Make the Leap… And Others Don't
Jim Collins
2001. New York: Harper Business.

Uncommon Service: How to Win by Putting Customers at the Core of Your Business
Frances Frei and Anne Morriss
2012. Boston: Harvard Business Review Press.

Built to Last: Successful Habits of Visionary Companies
Jim Collins and Jerry I. Porras
 2004. New York: Harper Business.

Straight from the Gut
Jack Welch
2003. New York: Grand Central Publishing.

What Really Works: The 4+2 Formula for Sustained Business Success
Nitin Nohria, William Joyce, and Bruce Robertson
2011. New York: Harper Business.

Topgrading: How to Hire, Coach and Keep A-Players
Brad Smart
2012. New York: Portfolio (Penguin Books).

Time, Talent, Energy: Overcome Organizational Drag and Unleash your Team's Productive Power
Michael C. Mankins and Eric Garton
2017. Boston: Harvard Business Review Press.

The Social Organization: How to Use Social Media to Tap the Collective Genius of Your Customers and Employees
Anthony J. Bradley and Mark P. McDonald
2011. Boston: Harvard Business Review Press.

Failing Forward: Turning Mistakes into Stepping Stones for Success
John C. Maxwell
2014. Nashville: HarperCollins Leadership.

ENDNOTES

Chapter 1

[1] Chuck Howitt, *BlackBerry Town: How high tech success has played out for Canada's Kitchener-Waterloo*, Lorimer, September 3, 2019.

[2] Ibid.

[3] *About SETI@home: https://setiathome.berkeley.edu/sah_about.php* (accessed August 2020).

[4] Ben Lindbergh, *E.T.'s Home Phone*, The Ringer, May 24, 2019: *https://www.theringer.com/tech/2019/5/24/18637942/seti-home-aliens-citizen-science-extraterrestrial-life-20th-anniversary* (accessed August 2020).

[5] Image based on data from Alexis C. Madrigal, *No Easy Tech Explanation for What Caused Wall St. 'Flash Crash'*, The Atlantic, July 14, 2010: *https://www.theatlantic.com/technology/archive/2010/07/no-easy-tech-explanation-for-what-caused-wall-st-flash-crash/59766/* (accessed August 2020).

[6] Jill Treanor, *The 2010 'flash crash': how it unfolded*, The Guardian, April 22, 2015: *https://www.theguardian.com/business/2015/apr/22/2010-flash-crash-new-york-stock-exchange-unfolded* (accessed August 2020).

[7] Ibid.

[8] Matt Levine, *Spoofers Tricked High-Speed Traders by Hitting Keys Fast,* Bloomberg Opinion, January 13, 2005: *https://www.bloomberg.com/opinion/articles/2015-01-13/spoofers-tricked-highspeed-traders-by-hitting-keys-fast* (accessed August 2020).

Chapter 2

[9] Molly Hennessy-Fiske and Suhauna Hussain, *Ransomware is everywhere—even in this sleepy Texas town*, Los Angeles Times, August 20, 2019: *https://www.latimes.com/world-nation/story/2019-08-20/ransomware-hits-towns-across-texas* (accessed August 2022).

[10] Ibid.

[11] From OpenText BrightCloud Threat Intelligence.

[12] Ibid.

[13] *Russo-Japanese War,* HISTORY, August 21, 2018: *https://www.history.com/topics/korea/russo-japanese-war* (accessed August 2020).

[14] K. Kubata, *The Battle of Tsushima, 1905*, Naval Historical Society of Australia, June 1980: *https://www.navyhistory.org.au/the-battle-of-tsushima-1905/* (accessed September 2022).

[15] Christopher H. Sterling, ed., *Military Communications: From Ancient Times to the 21st Century*, ABC-CLIO, 2008.

[16] Ibid.

[17] Brendan I. Koerner, *Inside the New Arms Race to Control Bandwidth on the Battlefield*, WIRED, February 18, 2014: *https://www.wired.com/2014/02/spectrum-warfare/* (accessed August 2022).

[18] *Worldbuilding Contest,* Future of Life, 2022: *https://worldbuild.ai/about/* (accessed September 2022).

[19] Alex Schiffer, *How a fish tank helped hack a casino*, The Washington Post, July 21, 2017: *https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/* (accessed August 2020).

[20] Greg Satell, *A Look Back At Why Blockbuster Really Failed And Why It Didn't Have To*, Forbes, September 5, 2014: *https://www.forbes.com/sites/gregsatell/2014/09/05/a-look-back-at-why-blockbuster-really-failed-and-why-it-didnt-have-to/#4ab7588d1d64* (accessed August 2020).

[21] *Netflix, Inc.*, Yahoo! Finance, August 26, 2022: *https://finance.yahoo.com/quote/NFLX/key-statistics* (accessed August 2022).

[22] Rupert Neate, *Over $119bn wiped off Facebook's market cap after growth shock*, The Guardian, July 26, 2018: *https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock* (accessed August 2020).

[23] *Bill Gates: Internet giants failed to predict Facebook data scandal*, Yahoo! News, April 18, 2018: *https://uk.news.yahoo.com/bill-gates-internet-giants-failed-203200380.html* (accessed August 2020).

[24] Herb Weisbaum, *Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal*, NBC News, April 11, 2018: *https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011* (accessed August 2022).

[25] Daniel G. Arce, *WikiLeaks and the risks to critical foreign dependencies*, ScienceDirect, December 2005: *https://www.sciencedirect.com/science/article/pii/S1874548215000451* (accessed August 2020).

[26] Ellen Nakashima and Shane Harris, *Elite CIA unit that developed hacking tools failed to secure its own systems, allowing massive leak, an internal report found*, Washington Post, June 16, 2020: *https://www.washingtonpost.com/national-security/elite-cia-unit-that-developed-hacking-tools-failed-to-secure-its-own-systems-allowing-massive-leak-an-internal-report-found/2020/06/15/502e3456-ae9d-11ea-8f56-63f38c990077_story.html* (accessed August 2020).

[27] Adam B. Vary, *Eagle Eye*, Entertainment Weekly, updated September 16, 2008: *https://ew.com/article/2008/09/16/eagle-eye/* (accessed August 2022).

[28] Zachary Cohen, Luke McGee and Alex Marquardt, *UK, US and Canada allege Russian cyberattacks on COVID-19 research centers*, CNN, July 17, 2020: *https://www.cnn.com/2020/07/16/politics/russia-cyberattack-covid-vaccine-research/index.html* (accessed August 2020).

[29] Julia Hanna, *United Breaks Guitars*, Harvard Business School, November 29, 2010: *https://hbswk.hbs.edu/item/united-breaks-guitars* (accessed August 2020).

[30] Ravi Sawhney, *Broken Guitar Has United Playing the Blues to the Tune of $180 Million*, FastCompany, July 30, 2009: *https://www.fastcompany.com/1320152/broken-guitar-has-united-playing-blues-tune-180-million* (accessed August 2022).

[31] See *https://newenglandfishmongers.com/* (accessed August 15, 2022).

Chapter 3

[32] Saint Augustine, *The Confessions of Saint Augustine*, Project Gutenberg, May 16, 2013 (original text published 397-400 AD): *https://www.gutenberg.org/files/3296/3296-h/3296-h.htm* (accessed August 2022).

[33] William R. Everdell, *It's About Time. It's About Space*, The New York Times, August 17, 2003: *https://www.nytimes.com/2003/08/17/books/it-s-about-time-it-s-about-space.html#:~:text=It%20is%2C%20Einstein%20said%2C%20%27%27what%20you%20measure%20with,time%3B%20time%20is%20what%20you%20measure%20with%20changes* (accessed August 2022).

[34] Nathaniel Scharping, *Why 1 Second Is 1 Second*, Discover Magazine, January 18, 2018: *https://www.discovermagazine.com/the-sciences/why-1-second-is-1-second* (accessed August 2020).

[35] *Millisecond*, Wikipedia: *https://en.wikipedia.org/wiki/Millisecond* (accessed August 2020).

[36] Patrick Mackey, *The Art of Wushu: The limits of human reaction time*, engadget, September 11, 2013: *https://www.engadget.com/2013-09-11-the-art-of-wushu-the-limits-of-human-reaction-time.html* (accessed August 2020).

[37] Andrei Sourakov, *Faster than a Flash: The Fastest Visual Startle Reflex Response is Found in a Long-Legged Fly, Condylostylus sp. (Dolichopodidae)*, Florida Entomologist, July 2011: *https://www.researchgate.net/publication/232673808_Faster_than_a_Flash_The_Fastest_Visual_Startle_Reflex_Response_is_Found_in_a_Long-Legged_Fly_Condylostylus_sp_Dolichopodidae* (accessed August 2022).

[38] *Microsecond*, Wikipedia: *https://en.wikipedia.org/wiki/Microsecond* (accessed August 2020).

[39] Robb Boyd, *Blink: You're Too Slow*, Cisco, December 11, 2012: *https://news-blogs.cisco.com/cin/blink-youre-too-slow* (accessed August 2020).

[40] *Nanosecond*, Wikipedia: *https://en.wikipedia.org/wiki/Nanosecond* (accessed August 2020).

[41] Jone Johnson Lewis, *Quotes from Grace Hopper, Computer Programming Pioneer*, ThoughtCo., August 27, 2018: *https://www.thoughtco.com/grace-hopper-quotes-3530092* (accessed October 2022).

[42] Grace Hopper, *Admiral Grace Hopper Explains the Nanosecond*, YouTube: *https://www.youtube.com/watch?v=9eyFDBPk4Yw* (accessed August 2022).

[43] Benj Edwards and Chris Hoffman, *What Is 5G, and How Fast Will It Be?*, How-To Geek, January 3, 2020, updated April 25, 2022: *https://www.howtogeek.com/340002/what-is-5g-and-how-fast-will-it-be/* (accessed August 2020).

44 Matthew Gault, *'Fallout 76' Players Are Breaking Nuclear Launch Code Cryptography to Unleash Hell*, VICE, November 21, 2018: *https://www.vice.com/en_us/article/kzvznv/fallout-76-players-are-breaking-nuclear-launch-code-cryptography-to-unleash-hell* (accessed August 2020).

45 Thomas Edison, *Thomas Edison Quote*, LibQuotes, n.d.: *https://libquotes.com/thomas-edison/quote/lba3h2h* (accessed August 2022).

46 Steven Roberts, *Bridging the Gap--News Telegraphs 1863-1870,* History of the Atlantic Cable & Undersea Communications, 2011: *https://atlantic-cable.com/Article/NewsTelegraphs/index.htm* (accessed September 2022).

47 *Paul Reuter*, Vanity Fair, December 14, 1872: *https://commons.wikimedia.org/wiki/File:Paul_Reuter_Vanity_Fair_14_December_1872.jpg* (accessed October 2022).

48 *Paul Julius Reuter*, Encyclopedia.com, n.d.: *https://www.encyclopedia.com/history/encyclopedias-almanacs-transcripts-and-maps/paul-julius-reuter* (accessed September 2022).

49 Miriam Hall, *Repositioning Buildings Not A Quick Fix To Sluggish Office Market,* Bisnow, June 28, 2018: *https://www.bisnow.com/new-york/news/mixed-use/repositioning-buidlinsg-not-a-quick-fix-to-sluggish-office-market-90117#:~:text=But%20like%20most,677%20Washington%20Bvld* (accessed September 2022).

50 Dana Cimilluca, *UBS to Cut 10,000 Staff in Overhaul*, The Wall Street Journal, October 28, 2012: *https://www.wsj.com/articles/SB10001424052970204840504578084980159734590* (accessed August 2020).

51 Anthony Effinger, *Andreessen on Finance: 'We Can Reinvent the Entire Thing'*, Bloomberg.com, October 7, 2014: *https://www.bloomberg.com/news/articles/2014-10-07/andreessen-on-finance-we-can-reinvent-the-entire-thing-* (accessed August 2020).

52 Joshua Franklin, *Technology could help UBS cut workforce by 30 percent: CEO in magazine*, Reuters, October 3, 2017: *https://www.reuters.com/article/us-ubs-group-tech-workers/technology-could-help-ubs-cut-workforce-by-30-percent-ceo-in-magazine-idUSKCN1C80RO* (accessed August 2020).

53 Adam Bensaid, *Israel's autonomous 'robo-snipers' and suicide drones raise ethical dilemma,* TRTWorld, February 26, 2021: *https://cms.trtworld.com/magazine/israel-s-autonomous-robo-snipers-and-suicide-drones-raise-ethical-dilemma-44557* (accessed July 2021).

Chapter 4

54 *Global digital population as of April 2022,* Statista: *https://www.statista.com/statistics/617136/digital-population-worldwide/* (accessed September 2022).

55 Alexey Utkin, *Data Management & Analytics: Legacy Challenges and Technological Trends*, DataArt, March 17, 2020: *https://www.dataart.com/blog/data-management-analytics-legacy-challenges-and-technological-trends* (accessed August 2022).

56 Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, Forbes, May 21, 2018: *https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#319d307e60ba* (accessed August 2020).

57 Richard Routledge, *Bayes's theorem*, Brittanica: *https://www.britannica.com/topic/Bayess-theorem* (accessed August 2022).

58 Bernard Marr, *What Is Unstructured Data And Why Is It So Important To Businesses? An Easy Explanation For Anyone*, Forbes, Oct 16, 2019: *https://www.forbes.com/sites/bernardmarr/2019/10/16/what-is-unstructured-data-and-why-is-it-so-important-to-businesses-an-easy-explanation-for-anyone/#29e0b46915f6* (accessed August 2020).

59 Alex Gray, *Humans have more than 5 senses*, World Economic Forum, January 9, 2017: *https://www.weforum.org/agenda/2017/01/humans-have-more-than-5-senses/* (accessed August 2020).

60 *Bias*, Wikipedia: *https://en.wikipedia.org/wiki/Bias* (accessed August 2020).

61 Ethan Wise, *The Blind Men and the Elephant Parable!*, Wise Hypnosis, December 28, 2016: *http://www.wisehypnosis.com/articles/stories-parables/the-blind-men-and-the-elephant-parable/* (accessed August 2022).

62 Nigel Shadbolt, *Artificial intelligence might be a threat to humans but not for the reasons you think*, The Guardian, January 22, 2015: *https://www.theguardian.com/media-network/2015/jan/22/ai-threat-humans-not-for-reasons-you-think* (accessed September 2022).

63 Sarah Pruitt, *The Lumière Brothers, Pioneers of Cinema*, HISTORY, August 22, 2018: *https://www.history.com/news/the-lumiere-brothers-pioneers-of-cinema* (accessed August 2020).

Chapter 5

64 H. James Wilson and Paul R. Daugherty, *Collaborative Intelligence: Humans and AI Are Joining Forces*, Harvard Business Review, July - Aug 2018 Issue: *https://hbr.org/2018/07/collaborative-intelligence-humans-and-ai-are-joining-forces* (accessed August 2020).

65 Roger Mola, *Super Helmet: F-35 pilots get X-ray vision and other magic powers*, Air & Space Magazine, September 2017: *https://www.smithsonianmag.com/air-space-magazine/super-helmet-180964342/* (accessed August 2022).

66 *Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation*, McKinsey Global Institute, December 2017: *https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi%20jobs%20lost-jobs%20gained_report_december%202017.pdf* (accessed August 2020).

67 See Appendix A for a detailed book summary and publication details.

68 *Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation*, McKinsey Global Institute, December 2017: *https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages* (accessed August 2020).

69 *A Future That Works: Automation, Employment, and Productivity,* McKinsey Global Institute, January 2017: *https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Digital%20Disruption/Harnessing%20automation%20for%20a%20future%20that%20works/MGI-A-future-that-works_Full-report.pdf* (accessed August 2020).

70 Fred Reed, *Promise of AI not so bright*, The Washington Times, April 13, 2006: *https://www.washingtontimes.com/news/2006/apr/13/20060413-105217-7645r/* (accessed August 2022).

71 *Luddites*, The National Archives UK, n.d.: *https://webarchive.nationalarchives.gov.uk/ukgwa/20210803115630/https://www.nationalarchives.gov.uk/education/politics/g3/* (accessed August 2020).

72 Marc Prensky, *Digital Natives, Digital Immigrants Part 1,* On the Horizon, MCB University Press, Vol. 9 No. 5, October 2001.

73 Ibid.

74 *UCLA study finds that searching the Internet increases brain function*, UCLA Health, October 14, 2008: *https://www.uclahealth.org/news/ucla-study-finds-that-searching-the-internet-increases-brain-function* (accessed August 2022).

75 Rhonda M. Layer, *The Millennial Student: A Strategy for Improved Wellness*, University of Minnesota, December 2012.

76 Kathy Bloomgarden, *Gen Z and the end of work as we know it*, World Economic Forum, May 19, 2022: *https://www.weforum.org/agenda/2022/05/gen-z-don-t-want-to-work-for-you-here-s-how-to-change-their-mind/* (accessed August 2022).

77 Naomi Nix, *Gen Z Workers to Triple by 2030, Snap-Commissioned Report Says*, Bloomberg, March 10, 2021: *https://www.bloomberg.com/news/articles/2021-03-10/gen-z-workers-to-triple-by-2030-snap-commissioned-report-says#xj4y7vzkg* (accessed August 2022).

78 Rick Levine, Doc Searls, David Weinberger, and Christopher Locke, *The Cluetrain Manifesto*, Basic Books (Hachette Book Group), January 2001.

79 Julian Jang-Jaccard and Surya Nepal, *A survey of emerging threats in cybersecurity*, Journal of Computer and System Sciences, Volume 80, Issue 5, August 2014: *https://www.sciencedirect.com/science/article/pii/S0022000014000178#!* (accessed August 2020).

80 *2022 BrightCloud Threat Report*, March 2022: *https://www.carbonite.com/cp/mm/2022-brightcloud-threat-report* (accessed August 2022).

Chapter 6

81 PrivSec Report, *Human error remains the main cause of data breaches*, GRC World Forums, January 19, 2021: *https://gdpr.report/news/2019/06/20/human-error-remains-the-cause-of-data-breaches/* (accessed August 2022).

82 *organization (n.)*, Online Etymology Dictionary: *https://www.etymonline.com/word/organization* (accessed August 2020).

83 *The Roman Imperial Legion*, UNRV Roman History: *https://www.unrv.com/military/legion.php* (accessed August 2022).

84 Gary P. Pisano, *You Need an Innovation Strategy*, Harvard Business Review, June 2015 Issue: *https://hbr.org/2015/06/you-need-an-innovation-strategy* (accessed August 2020).

85 Brendan Saur, *Car Show Classic: 1958 Edsel Corsair – Failure Is A Five-Letter World*, Curbside Classic, August 5, 2015: *https://www.curbsideclassic.com/curbside-classics-american/car-show-classic-1958-edsel-corsair-failure-is-a-five-letter-world/* (accessed August 2022).

Chapter 7

86 Carole Cadwallad, *Digital prophet Kevin Kelly: I've learned a lot from Spielberg*, The Guardian, June 12, 2016: *https://www.theguardian.com/books/2016/jun/12/kevin-kelly-interview-the-inevitable-book-song-ai-future* (accessed August 2020).

87 Alex Shee, *The AI Element: A podcast about how AI is transforming industries*, Medium, July 24, 2018: *https://medium.com/element-ai/the-ai-element-a-podcast-about-how-ai-is-transforming-industries-4857c286066* (accessed August 2022).

88 Daniel Goleman, Christina Congleton, Ellen Langer, Annie McKee, and Adam Waytz, *HBR Emotional Intelligence Series*, Harvard Business Review, May 9, 2017.

89 Daniel Goleman, Annie McKee, and Adam Waytz, *Empathy*, HBR Emotional Intelligence Series, Harvard Business Review, May 9, 2017.

90 Graeme Burton, *"Garbage in, garbage out" - a bad model for data collection...*, Computing, November 14, 2014: *https://www.computing.co.uk/analysis/2381673/-garbage-in-garbage-out-a-bad-model-for-data-collection* (accessed August 2020).

91 Daniel Goleman, Christina Congleton, Ellen Langer, Annie McKee, and Adam Waytz, *HBR Emotional Intelligence Series*, Harvard Business Review, May 9, 2017.

92 *From fighter pilot to robotics pioneer: An interview with Missy Cummings*, McKinsey Global Institute, September 22, 2021: *https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/from-fighter-pilot-to-robotics-pioneer-an-interview-with-missy-cummings* (accessed September 2022).

93 Emily Sullivan and Laurel Wamsley, *Google Employees Walk Out To Protest Company's Treatment Of Women*, NPR, November 1, 2018: *https://www.npr.org/2018/11/01/662851489/google-employees-plan-global-walkout-to-protest-companys-treatment-of-women* (accessed August 2020).

94 Azeem Azhar, *AI, Accountability and Power: My conversation with Meredith Whittaker*, Exponential View, December 27, 2019: *https://www.exponentialview.co/p/-ai-accountability-and-power* (accessed September 2022).

95 Michael McKenna, *Three notable examples of AI bias*, AI Business, October 14, 2019: *https://aibusiness.com/document.asp?doc_id=761095* (accessed August 2022).

96 Jake Silberg and James Manyika, *Notes from the AI frontier: Tackling bias in AI (and in humans),* McKinsey Global Institute, June 2019: *https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/tackling%20bias%20in%20artificial%20intelligence%20and%20in%20humans/mgi-tackling-bias-in-ai-june-2019.pdf* (accessed September 2022).

97 Daniel Cossins, *Discriminating algorithms: 5 times AI showed prejudice*, New Scientist, April 12, 2018: *https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/* (accessed August 2022).

98 Kashmir Hill, *Wrongfully Accused by an Algorithm*, New York Times, June 24, 2020: *https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html* (accessed August 2020).

99 Ibid.

100 Derek Major, *Black Unemployment Rate More Than Doubles To 16.7% in April*, Black Enterprise, May 8, 2020: *https://www.blackenterprise.com/black-unemployment-rate-more-than-doubles-to-16-7-in-april/* (accessed August 2022).

101 *The Color of Coronavirus: COVID-19 Deaths by Race and Ethnicity in the US (March 5, 2021)*, APM Research Lab, March 5, 2021: *https://www.apmresearchlab.org/covid/deaths-by-race-03-05-21* (accessed August 2020).

102 *Criminal Justice Fact Sheet*, NAACP, 2020: *https://www.naacp.org/criminal-justice-fact-sheet/* (accessed August 2020).

[103] *Fatal Force* (police shootings database), The Washington Post, (updated regularly): *https://www.washingtonpost.com/graphics/investigations/police-shootings-database/* (accessed August 2020).

[104] Benjamin Wilson, Judy Hoffman, and Jamie Morgenstern, *Predictive Inequity in Object Detection*, Cornell University, February 21, 2019: *https://arxiv.org/pdf/1902.11097.pdf* (accessed August 2020).

[105] Shana Lynch, *Andrew Ng: Why AI Is the New Electricity*, Stanford Graduate School of Business, March 11, 2017: *https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity* (accessed August 2022).

[106] Amit Pandey and Suchma Mirshra, *Understanding IT Change Management Challenges at a Financial Firm*, Proceedings of the Information Systems Educators Conference, Robert Morris University, Pennsylvania, 2014.

Chapter 8

[107] *rehearse (v.)*, Online Etymology Dictionary: *https://www.etymonline.com/word/rehearse* (accessed August 2020).

[108] *UCLA's Augmented Reality Sandbox*, YouTube: *https://www.youtube.com/watch?v=CE1B7tdGCw0* (accessed August 2022).

Chapter 9

[109] Richard Florida, *How to Rebuild After the Retail Apocalypse,* The Atlantic, December 23, 2017: *https://www.theatlantic.com/business/archive/2017/12/retail-apocalypse-malls-rebuild/549056/* (accessed September 2022).

[110] Derek Thompson, *What in the World Is Causing the Retail Meltdown of 2017?*, The Atlantic, April 10, 2017: *https://www.theatlantic.com/business/archive/2017/04/retail-meltdown-of-2017/522384/* (accessed August 2020).

[111] *Amazon.com Announces First Quarter Results*, amazon.com, April 30, 2020: *https://press.aboutamazon.com/news-releases/news-release-details/amazoncom-announces-first-quarter-results* (accessed August 2020).

[112] Forbes Insight Team, *The Reality Of Digital Disruption - How To Stay Ahead*, Forbes, July 17, 2018: *https://www.forbes.com/sites/insights-treasuredata/2018/07/17/the-reality-of-digital-disruption-how-to-stay-ahead/#61d6c36143c1* (accessed August 2022).

[113] Lisa McQuerrey, *What Percentage of Customers Does a Business Lose Each Year?*, Small Business, n.d.: *https://smallbusiness.chron.com/percentage-customers-business-lose-year-79271.html* (accessed August 2020).

[114] James G. Barnes, *Secrets of Customer Relationship Management*, McGraw-Hill, October 1, 2000.

[115] Patrick Hull, *Don't Get Lazy About Your Client Relationships*, Forbes, December 6, 2013: *https://www.forbes.com/sites/patrickhull/2013/12/06/tools-for-entrepreneurs-to-retain-clients/#3936de324432* (accessed August 2020).

[116] Blake Morgan, *50 Stats That Prove The Value Of Customer Experience*, Forbes, September 24, 2019: *https://www.forbes.com/sites/blakemorgan/2019/09/24/50-stats-that-prove-the-value-of-customer-experience/#2ac6d7404ef2* (accessed August 2020).

[117] Ken Dooley, *The No. 1 reason why customers stay or leave*, Customer Experience Insight, June 10, 2013: *https://www.customerexperienceinsight.com/the-no-1-reason-why-customers-stay-or-leave/* (accessed August 2020).

[118] Scott Magids, Alan Zorfas, and Daniel Leemon, *The New Science of Customer Emotions*, Harvard Business Review, November 2015: *https://hbr.org/2015/11/the-new-science-of-customer-emotions* (accessed August 2022).

[119] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, January 15, 2019.

[120] Scott Keller and Mary Meaney, *Attracting and retaining the right talent*, McKinsey & Company, November 24, 2017: *https://www.mckinsey.com/business-functions/organization/our-insights/attracting-and-retaining-the-right-talent* (accessed August 2020).

[121] Ed Michaels, Helen Handfield-Jones, and Beth Axelrod, *War for Talent (Excerpt)*, Harvard Business School Working Knowledge, October 29, 2001: *https://hbswk.hbs.edu/archive/war-for-talent* (accessed August 2020).

[122] Nelson D. Schwartz, *In Hiring, A Friend in Need is A Prospect Indeed*, New York Times, Jan 27, 2013: *https://www.nytimes.com/2013/01/28/business/employers-increasingly-rely-on-internal-referrals-in-hiring.html* (accessed August 2020).

[123] Joseph V. Micallef, *The First Attack: Pearl Harbor, February 7, 1932*, Military.com, 2020: *https://www.military.com/navy/pearl-harbor-first-attack.html* (accessed August 2020).

[124] *Iron Curtain*, Britannica: *https://www.britannica.com/event/Iron-Curtain* (accessed August 2020).

[125] Helen Regan and Joshua Berlinger, *Protests break out in Hong Kong as first arrest made under new security law*, CNN, July 1, 2020: *https://www.cnn.com/2020/07/01/china/hong-kong-national-security-law-july-1-intl-hnk/index.html* (accessed August 2020).

[126] Kevin Davies, *Blinking Red: 25 Missed Pandemic Warning Signs*, Genetic Engineering and Biotechnology News, April 17, 2020: *https://www.genengnews.com/a-lists/blinking-red-25-missed-pandemic-warning-signs/* (accessed August 2020).

[127] Ibid.

Chapter 10

[128] Dwight D. Eisenhower, *Quotes: Remarks at the National Defense Executive Reserve Conference, 11/14/57*, Dwight D. Eisenhower Presidential Library, Museum & Boyhood Home, updated January 19, 2022: *https://www.eisenhowerlibrary.gov/eisenhowers/quotes* (accessed September 2022).

[129] Neil Gaiman and Terry Pratchett, *Good Omens*, William Morrow, 2006 (p. 176).

THE AUTHORS

Mark J. Barrenechea joined OpenText as President and Chief Executive Officer in January 2012, and also serves as a member of the Board. In January 2016, Mark took on the role of Chief Technology Officer. In September 2017, he was appointed Vice Chair, in addition to remaining the Chief Executive Officer and Chief Technology Officer. As CEO of Canada's largest software company, Mark oversees the strategic direction of the organization and upholds the company's position at the forefront of the industry. Under his direction, the Company has grown both organically and through strategic acquisitions into a $3.5 billion technology company.

Mark J. Barrenechea
VICE CHAIR, CEO AND CTO
OPEN TEXT CORPORATION

Major-General (Ret.) David Fraser, OMM was the commander of the Multinational Brigade for Regional Command South in Afghanistan's southern provinces in 2006. One of the most decorated generals in Canadian Armed Forces history, Fraser was the commander of Operation Medusa in Afghanistan, the largest combat engagement of Canadian Armed Forces in more than fifty years. General Fraser was the Commandant of the Canadian Forces Staff College. After retirement, he has served as an executive with three different corporations, among them Blue Goose Pure Foods, and has experience leading in both the battlefield and the boardroom. David is the recipient of the Order of Military Merit.

David Fraser
CORPORATE GOVERNANCE & NOMINATION COMMITTEE MEMBER
OPEN TEXT CORPORATION

One of Canada's leading experts on innovation and digital technologies, Tom Jenkins is the Chair of OpenText Corporation, the largest software and cloud company in Canadian history and one of the most successful internet companies in the world. Tom has served or continues to serve on the boards of OpenText Corporation, Manulife Financial, Thomson Reuters, TransAlta Corporation, BMC Corporation, and Slater Steel. He also served as the Chair of the National Research Council of Canada. He received his commission as an officer in the Canadian Armed Forces and as the Honorary Colonel of an infantry regiment and a fighter squadron in the Canadian Armed Forces. He was the 10th Chancellor of the University of Waterloo, and he was inducted as a Companion into the Canadian Business Hall of Fame. Tom is a recipient of the Federal Republic of German Order of Merit (Knight's Cross), and he is an Officer of the Order of Canada.

Tom Jenkins
CHAIR
OPEN TEXT CORPORATION

ALSO BY

Mark J. Barrenechea

The Quarantine Chronicles

The Intelligent and Connected Enterprise

Digital Manufacturing

The Golden Age of Innovation

On Digital

E-business or Out of Business: Oracle's Roadmap for Profiting in the New Economy

Software Rules: How the Next Generation of Enterprise Applications Will Increase Strategic Effectiveness

with Tom Jenkins

Digital: Disrupt or Die

Enterprise Information Management: The Next Generation of Enterprise Software

Digital Financial Services: The Greatest Revolution Since Minted Money

E-government or Out of Government

David Fraser

with Brian Hanington

Operation Medusa: The Furious Battle That Saved Afghanistan from the Taliban

Tom Jenkins

Behind the Firewall: Big Data and the Hidden Web

Enterprise Content Management: What You Need to Know

Managing Content in the Cloud: Enterprise Content Management 2.0

with David Johnston

Ingenious

Innovation Nation

with Kevin Lee

Shoeboxes: Rediscovering Canada's Irish Roots

with Mark J. Barrenechea

Digital: Disrupt or Die

Enterprise Information Management: The Next Generation of Enterprise Software

Digital Financial Services: The Greatest Revolution Since Minted Money

E-government or Out of Government

with Bill Forquer and Peter Jelinski

Enterprise Content Management Solutions: What You Need to Know

with Walter Köhler and John Shackleton

Enterprise Content Management Methods: What You Need to Know

with Michael Hood

The Valiant Skies: 100 Years of the RCAF

Technology is driving civilization's transformation from analog to digital. Achievements in time, speed, scale, and domain are changing everything about the way we live. Information is relayed not in minutes or seconds, but in nanoseconds. The development of new products and services—from idea to product to global distribution—has never been faster, easier, or cheaper. And key decisions and analyses once made by humans, are now the domain of intelligent machines.

The Anticipant Organization is a survival manual for those who are tasked with leading their organizations along the path from analog to digital. It's about how to survive when you're moving at a pace and operating on a scale never seen before, and how to thrive in the new hybrid world of human-machine management.

This is now every leader's most pressing challenge.

Leaders who follow the strategies for becoming anticipant will be ready for whatever lies ahead. They will discover gaps and identify potential catastrophes in advance. They will know how to respond when a crisis hits. And they will transform their organizations to thrive in a world of constant disruption.

There is always another headwind coming. Get ready.

Authors Mark J. Barrenechea, Major-General (Ret.) David Fraser, and Tom Jenkins are pioneering strategists in the boardroom and the battlefield. Mark is OpenText's CEO and CTO, and a recognized business innovator who has transformed software companies into global leaders in information management. David is one of the most decorated generals in Canadian Armed Forces history and commander of Operation Medusa in Afghanistan. Tom is Chair of the World Wide Web Foundation, Officer of the Order of Canada, and Chair of OpenText's board.