A report on how digital resilience can be advanced alongside developments in Artificial Intelligence, Quantum Technology and Cloud Computing

May 2022

DIGITAL RESILIENCE

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

RESILIENCE FIRST
SURVIVE & THRIVE

In collaboration with accenture Cranfield University

CONTENTS

FOREWORD

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Professor Brian Collins

Emeritus Professor, Dept of Civil, Environmental & Geomatic Engineering, Faculty of Engineering Science, UCL. He served as Chief Scientific Advisor to two UK Government departments (DfT and BIS) with responsibility for overseeing science, engineering, and technological policy and evidence activities. He was Professor of Information Systems at Cranfield University, and Chief Scientist and Director of Technology at GCHQ between 1987 and 1991.

Resilience has become an essential part of commercial and social life, made more visible as a result of the extreme events triggered by climate change, economic growth and by population density in our cities. Increasingly our world is dependent upon the exploitation of good data not only to provide effective services that are both economic and efficient but also to provide us with the capability to adapt to changing circumstances very quickly. The combination of artificial intelligence (AI), quantum technology and cloud computing are significant not only individually but more importantly as a collective set of technologies and derived services that support these social and economic necessities for the future of humankind and our environment on the planet.

This paper addresses the essence of these technologies and services and discusses the issues of their integration as well as the properties of the individual services and technologies in such a way as to illustrate how important it is that our populations are better educated and capable in the exploitation of these technologies to help ensure that society becomes more resilient in the face of more extreme events and unexpected circumstances.

AI and machine learning (ML) have been in gestation for decades so what is it that has caused them to become more available to us now than before? First, it is a realisation of Moore's Law in providing sufficient computer power that their potential can be envisaged although, as this paper points out, the full potential will only be realised when it is combined with much more powerful computing metaphors than has been available up to now. Secondly, they have become available because of the openness of data sources at scale which allows their training to become more robust and the context in which they can be used enlarged. Crucial to their efficacy is that the data on which they are trained and which they then exploit have provenance and integrity which are verifiable. Whilst this is outside the scope of this paper, these parameters are critically important to the delivery of resilience.

Quantum computing, and the exploitation of quantum technology, has a more recent history although understanding quantum phenomena has been around for decades and the development of quantum computing of several different types has only recently become mature enough for its exploitation to be predictable. However, it is probably a bigger game changer in a number of ways than other subjects discussed in this paper, partly because of its impact on security and partly because of its impact on the speed by which computing results can be delivered. Both of these factors are many orders of magnitude different from what we currently enjoy. The integration of quantum sensors into our infrastructure and service delivery world is also likely to provide us with much better data sets than we currently have. Together with the other two components discussed in this paper, we should have a data-rich, data-driven world which is capable of providing more resilience and more predictability in support of the major services that we expect to be available to us, primarily in energy, health, transport and finance.

Cloud computing is an extension of models of outsourced IT which again have been in existence for some time. It is the scale, range and reach of IT capability through the lower cost of servers and networks that helps enable cloud computing to become a game changer in the way in which digital services are provided. Whilst digital as a service is not a new concept, what needs to be borne in mind is that managing cloud computing implies understanding of legal and social contracts, of how to express requirements, and how to manage the relationship between a cloud service provider, public or private, in a way which is dynamically reconfigurable as contexts change. Otherwise, they do not provide resilience and become a brittle factor in the architecture of digital business and society.

This paper provides indicative indications of where some of the solutions to these issues are but it also signposts where much more work is needed both in research and education in order to provide the solutions that will be required for a resilient digital world to be developed.

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

EXECUTIVE SUMMARY

Top

Contents

Foreword

Executive Summary

Introduction

Part 1: Artificial Intelligence

Part 2: Quantum Technology

Part 3: Cloud Computing

Part 4: Conclusions

Acknowledgements

Already underway, the 4th Industrial Revolution is characterised by a fusion of technologies that blur the lines between the physical, digital and biological spheres. Compared to previous industrial revolutions, the latest one is moving at an exponential pace. Moreover, it is both advancing and disrupting almost every industry in every country. The breadth and depth of these changes herald the transformation of entire systems of production, management, and governance. The key questions are how resilient the new technologies can be and how can they affect the resilience of organisations.

While the core concept of **Artificial Intelligence (AI)**, namely the ability of machines to learn and exhibit human-level intelligence, remains unchanged, the astounding growth of AI innovations and applications has achieved success across a wide spectrum of different sectors and has exhibited great potential for further impact. The developments are particularly significant in finance, healthcare, entertainment and the automotive industry.

Ways to improve the identification of AI features that give rise to new resilience challenges, as well as detect potential cascading risks, are important aspects, as are the security challenges in the data pipelines that supply AI engines, the nature of adversarial attacks on AI, and the wider issues of system integration and trust. The ways in which AI can be used to identify risks and better understand the role played by different system attributes in enhancing resilience will become crucial.

Although high-performance computing is much more available and affordable than ever before, the overall cost and environment impacts are considerable. This means that some parts of AI technology will remain unaffordable to small businesses and developing countries as they usually cannot afford the construction of large-scale data centres. Also, their computation limit is likely to be insufficient for some AI applications.

Quantum Technology can take us a step closer towards providing more accurate predictions and allow us to plan and become resilient. The power of quantum brings immense potential to multiple facets of enterprise resilience, making it easier for businesses to prevent, prepare for, and learn about possible disruptions, and then respond and recover quickly when they occur. As the technology matures and the full power of quantum computing is realised, companies that take advantage now can be the first to achieve new levels of resilience.

Quantum computing can enhance simulations and create a more complete picture of possible outcomes. It can also help understand and modify supply chains. It can help enable manufacturers to create necessary buffers pertaining to inventory, time, capacity and develop standardised processes that are easier to replicate across employees and facilities. In cyber security, it can help with threat detection and network intrusion.

A quantum computer of sufficient size could be able to break standard encryption, prompting a re-evaluation of this threat and the first steps to understand and mitigate the risks. At the same time, technologies powered by quantum sensors show promise to enhance earthquake detections, volcanic eruption predictions and see underground, even detect the SARS-CoV-2 virus that causes Covid-19. Enterprise resilience stands to benefit in many ways from quantum technology.

With the speed provided by **Cloud Computing**, enterprises can shift away from operations that focus on keeping the lights on, thereby freeing up their budgets and their teams' time to rethink fundamentally how the business operates, and how it creates value. This is the ultimate objective of a cloud journey – to create a platform for innovation, for resilience and for future business reinvention.

The two most cited factors that stand in the way of satisfaction with cloud services are: first, concerns relating to security and risk compliance; and, second, the complexity of business and organisational change. In respect of both, leveraging a qualified third party to manage cloud services has proven to be the key decision that has led to increased satisfaction in usage in respect of cost savings, speed to market, business enablement and improved service levels.

As organisations continue to rely upon cloud computing for their business needs, they should ensure that their strategies are designed to consider resilience. The use of cloud computing comes with significant responsibilities for managing and configuring IT assets and resources, protecting customer data, managing applications, servers and operating systems, maintaining and securing access to data and resources and protecting and encrypting client-side data. If managed and configured appropriately, cloud computing can provide an improved resilience and risk profile as compared to the traditional data-centre model.

The challenges and opportunities presented by three technologies described here are enormous. There is the potential to raise global income levels and improve the quality of life for many around the world. Technology will make it possible to produce new products and services that increase the efficiency and resilience of many organisations. On the other hand, technology can insert societal inequalities (between the haves and have nots), reduce resilience (by making us ever more dependent on those technologies), and question our ability to control progress (within fragile social structures). The 4th Industrial Revolution will need managing carefully and we need to balance the upsides with the downsides.

INTRODUCTION

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Heather Adams

Managing Director, UKI Risk Strategy and Consulting Lead at Accenture

For organisations in all industries and geographies, digital technologies are increasingly pervasive and embedded across their operations, activities and interactions. It is a trend that has been accentuated and accelerated by the effects of the Covid-19 pandemic.

The result? Today, powerful advanced technologies like AI, quantum technology and cloud computing are helping firms worldwide to become faster, more agile and more cost-effective. But are we getting stronger too? While these new technologies offer unprecedented insight and processing power, in turn opening new vistas of business opportunity, they can also create profound risks to the resilience of organisations.

At root, resilience is about having both the agility and adaptability needed to pre-empt and recover from disruption. Resilience is not new: questions about resilience in the cloud, for example, have been voiced by industry for many years, and now being increasingly focused on by regulators.

Alongside such widely recognised resilience considerations, new risks are now emerging with the advent of the leading technologies and the interplay between them. One example is the untold outcomes and unpredictable societal impacts that could result from combining quantum's immense computing power with AI's rapidly evolving self-learning capabilities.

However, more positively, today's advanced technologies create promises of enhanced resilience, not just perils. They can be the basis for developing smarter, more powerful, real-time solutions to the resilience challenges that organisations face in areas like maintaining the security of online communications and the interaction points along their supply chains.

> *…today's advanced technologies create promises of enhanced resilience, not just perils. They can be the basis for developing smarter, more powerful, real-time solutions to the resilience challenges that organisations face in areas like maintaining the security of online communications and the interaction points along their supply chains.*

By way of example, take the cloud. Today, Cloud Service Providers (CSPs) offer a wide range of control features to help their business customers better protect their data and assets through more effective management of resilience. Examples include Identity and Access Management (IAAM) capabilities that define who can access cloud resources, and expert guidance for companies on what good looks like in terms of 'well-architected design', such as creating fault-tolerant processes that eliminate single points of failure.

Quantum technology too has a huge potential to help improve resilience through capabilities ranging from the ability of quantum sensors to detect earthquakes to the power to manage the increasing and multi-layered complexities in today's supply chains. Each of three primary forms of quantum technology – computing, communications, and sensing – offers opportunities to improve various aspects of resilience for individuals, businesses and governments.

> *...businesses should apply a Resilience First lens to their adoption and implementation of the technologies, anchored in broader business considerations such as strategy, operating model, and regulatory trends.*

In this regard, a particularly important role that quantum communications can play is in enabling 'active resilience'. This leverages quantum's ability to help strengthen cyber-security resilience against various threat actors and – through quantum-key distribution – to help provide a more secure way to encrypt and share data compared to current techniques.

Aside from the possibilities presented by individual technologies, it is when they are used in combination that they can really promise to move the dial on resilience.

For instance, quantum-enabled active resilience can be further enhanced by orchestrating quantum technologies with AI-powered machine learning via the cloud, creating a powerful combinatorial effect that unlocks even greater capabilities. When these methods are used for cyber-security threat detection, quantum versions of common machine learning (ML) models have proved able to detect Distributed Denial of Service (DDOS) attacks with over 95% accuracy.[1] When quantum methods are combined with classical ML to produce a hybrid quantum-classical neural network, the accuracy of detection can rise to nearly 100%. The implications of such statistics for the future resilience of organisations are both profound and encouraging.

With this, I am delighted to share this report that reviews the landscape of resilience considerations and implications associated with the most front-of-mind technologies for business leaders.

To balance the resilience promises and perils of cutting-edge technologies the approach is not to play wait and see, nor to be naïve about the challenges. Instead, businesses should apply a Resilience First lens to their adoption and implementation of the technologies, anchored in broader business considerations such as strategy, operating model, and regulatory trends. No matter how advanced a technology may be, it remains an enabling tool rather than an end in itself – and it should be viewed and used as such.

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Reference:

[1] https://www.researchgate.net/publication/349828355_Quantum_machine_learning_for_intrusion_detection_of_distributed_denial_of_service_attacks_A_comparative_overview

PART 1:
ARTIFICIAL INTELLIGENCE

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Professor Weisi Guo

Head of Human Machine Intelligence Group, Director of the Smart Living Grand Challenge and
Expert Contributor to The Resilience Grand Challenge at Cranfield University.
Course Director of the Applied AI MSc at Cranfield.

Introduction

AI, and specifically deep-learning algorithms, is being ubiquitously integrated into society, infrastructures and organisational processes. Deep learning can not only create new challenges in resilience as new attack vectors appear but it can also contribute to improving our understanding of resilience.

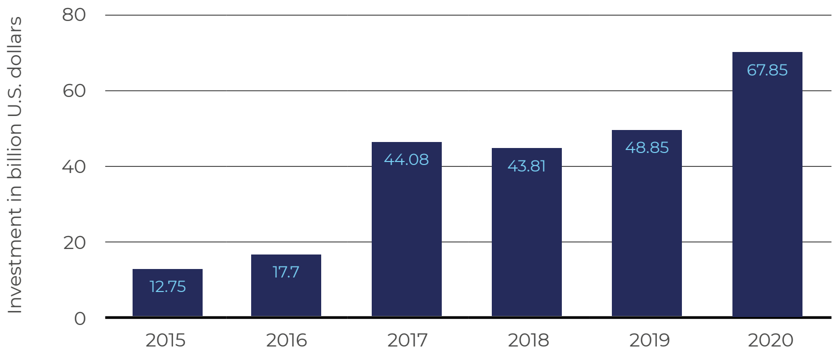
Since its birth in the Dartmouth Workshop in 1956, the concept of AI has appeared in generations of technological advances, from reasoning machines that prove mathematical theorems, to expert systems that react according to a large set of strict rules, to deep neural networks that outperform humans in various tasks.

The core concept of AI, namely the ability of machines to learn and exhibit human-level intelligence, remains unchanged. However, the past decade had witnessed the astounding growth of AI innovations and applications. To date, AI generally refers to a combination of technologies that is capable of acquiring adaptive predictive power through some degree of learning from data and task information.

State of the AI revolution

The past decade has witnessed the astounding advancement of the current wave of AI tide. Ignited by affordable high-performance computing and big data, and fuelled by corporate venture capital, as well as a prosperous open-source community, AI applications have achieved remarkable success in a wide spectrum of different sectors and have exhibited great potential for further impact. *(See Figure 1.)*

Global total corporate artificial intelligence (AI) investment from 2015 to 2020 (in billon U.S. dollars)



Sources

Stanford University; S&P Capital IQ; CrunchBase; NetBase Quid

© Statista 2021

Additional Information

Worldwide; S&P Capital IQ; CrunchBase; Netbase Quid; 2015 to 2020

Figure 1. Global total corporate AI investments US$, 2015-2020.

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Finance

Well supported by large volumes of numbers and data, AI technologies are most welcome in the financial sector. Areas such as fraud detection and wealth management have particularly benefited from the application of AI: AI fraud detectors are highly regarded and widely deployed. State-of-the-art AI fraud detectors can capture patterns from users' transactional history and can decrease fraud rate to less than a quarter of the industry's average.

In risk management, financial institutions have been deploying AI solutions as aid to the decision-making processes in assessing risk associated to their loan portfolios, based on the behaviours and demographic displayed by their customers.

For wealth management, the employment of robo-advisors, which continuously learn from customer information and preference to provide highly personalised advice, has been increasing. Some institutes have formed strategic relationships with service providers. Other global institutions have chosen to build proprietary AI engines or invest in third-party developers. Other areas in the finance sector such as insurance and banking are also gradually adopting AI technologies to automate service processes and aid decision making.

Healthcare

The introduction of AI to healthcare is gradually changing the landscape of business. AI technology has been extending the capabilities of surgical assistant robots, like the 'da Vinci' system by Intuitive Surgical[1] which was merely for supporting minimally invasive heart-bypass surgery, can now act as both an assistant in multiple laparoscopic procedures as well as being a data platform of surgical process studies. AI systems have also shown potential to assist and accelerate drug discovery and engineering. Apart from the traditional core of therapy and treatment, high-precision AI models help enable healthcare to shift towards health digital resilience in terms of prevention and early diagnosis through risk prediction and medical imaging, helping avoid complications and helping cure patients who could hardly be helped in later stage of their disease.

Entertainment

AI technologies have been known to the entertainment industry for a long time as both a source of ideas for fiction and a tool for content creativity and productivity. AI-powered recommendation engines have drastically improved the performance for precise, personalised recommendations for content and advertisement, playing a major role in the uprising of big names such as Netflix, TikTok and YouTube. AI-based algorithms for image, video and audio processing have also been an essential component of multi-media production software like the Adobe Creativity Suite, and such significance is now being emphasised even more. In addition to these applications, a new trend of introducing AI to music composition and movie making is growing, where preliminary success has been seen in the auto-trailer generation.

> *…AI-powered recommendation engines have drastically improved the performance for precise, personalised recommendations for content and advertisement, playing a major role in the uprising of big names such as Netflix, TikTok and YouTube.*

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Automotive

Since the first industrial robot installed on a General Motors assembly line in 1961, the automotive sector has been a pioneer in AI technology, especially in robotics. Over the past decade, advanced driver-assistance systems, or autonomous driving systems, have become widely available, further escalating the importance of AI in the sector. On one hand, new passenger cars are commonly equipped with L2+ automation systems which help enable core functionalities such as Adaptive Cruise Control and Lane Centring Control. On the other hand, commercial vehicle manufacturers tend to skip the lower levels of machine autonomy and directly pursue L4 autonomous driving capabilities for robo-taxis, trucks and some specialised vehicles: multiple successful experiments and trial services have been carried out and achieved initial successes. With more and more data accumulated from road tests to support development, autonomous vehicles are expected to perform better and have a larger impact in the near future.

Alongside the successes, the following limits to current AI technology have also been revealed, leaving some other sectors nearly barren to AI applications.

Data

The development of an AI application ideally requires large amounts of data of good quality. In actual scenarios, available data are rare to meet both requirements, hence the result of AI models with sub-optimal performance. Apart from sectors lacking quality data, the long-tail effect also haunts those which have obtained preliminary success. Current popular AI models are mostly variants of statistical ML that inevitably retain a degree of ambiguous decisions and actions in rare or unseen scenarios, potentially causing major damage in some applications.

Computation power and energy

Although high-performance computing is much more available and affordable than ever before, the overall cost and environment impacts are considerable. This means that some parts of AI technology remain unfriendly to small businesses and most developing countries as they usually cannot afford the construction of large-scale data centres. Also, their edge on computational power is insufficient for some AI applications. For example, training Google's BERT-Large[2] nature language processing model takes 64 of its Tensor Processing Unit (TPU) chips for four days, while the final version of AlphaGo[3] requires 48 Central Processing Units (CPUs) and eight Graphics Processing Units (GPUs) for searching strategies for the boardgame 'Go'. Both consume large amounts of energy and leave an overly large carbon footprint for the task, not to mention those larger commercial AI models with orders of magnitudes larger volumes of data and mega-data centres across the world.

Domain knowledge

AI technology by itself is merely an enabler. Successful applications to date mostly occurred in sectors that are familiar with computer assistance. AI practitioners lack certain knowledge to harvest the AI advantage to the traditional workflow without collaboration with domain experts, while domain experts struggle to identify opportunities of improvement and resources to prepare for the development of AI applications. Such sectors include various traditional industry such as farming, fishery and mineral mining.

Top

Contents

Foreword

Executive Summary

Introduction

Part 1: Artificial Intelligence

Part 2: Quantum Technology

Part 3: Cloud Computing

Part 4: Conclusions

Acknowledgements

▲

▼

Leveraging AI

The vast majority of complex ecosystems consist of a network of individual components. Often, these span the socio-technical realms. Sophistication and co-operation arise from co-operation of the networked components and their resilience, frequently sensitive to cascading effects.

Traditional analysis of complex systems can help understand organisational, socio-technical, infrastructural, and supply networks. State-of-the-art approaches consider both the role played by local functional elements (e.g. data pipeline, human-decision makers, memory buffers, power generators), and macro-scale topological elements (e.g. graphical properties of the whole ecosystem). Here, AI can be used to identify areas of weakness or fragility in networked systems which are often hard to quantify using classical learning techniques.

In this context, businesses have tried to leverage AI to chief financial officers who have deployed it to improve cash flow whilst securing and existing financing sources. Powered by data across all core corporate functions and lines of business, AI has allowed for an agile, data-driven response. AI has mitigated risks associated with large-scale disasters or disruptions (e.g. Covid-19) and improved resilience in global cash visibility and funding, optimised working capital, and client vendor enablement.

In the healthcare sector, we have seen the development of AI models to support business seeking to understand the impact of large-scale disasters on the supply chain.

The application of AI-driven scenario modelling provides businesses with the capability to develop what-if scenarios, the likelihood of events to be occurring, the development of alternative options and solutions to support health-system logistics, and the route needed to connect products to consumers.

Health System Inventory Allocation

In this use case, an AI model plays the role of an optimisation tool to help health systems to better organise their resources, people and medicines in the face of large-scale disasters. Similar to other AI applications, this approach strictly relies upon on the availability of up-to-date data that include distribution of medical personnel and infrastructure in the territory, predictions on the evolution of the disaster as available from statistical models, real-time news feeds and an inventory of medical resources distributed in the territory.

All data sources have been integrated into a single health database that was used to develop the AI models that supported what-if scenario analysis. These models enabled the healthcare provider with simulation capabilities to help companies taking the right decisions to smooth the Covid-19 impact in their supply chains, reducing the disruption in the provision of healthcare by optimising medical personnel scheduling and product routing to consumers. The central health authority was also able to monitor the situation by accessing a dashboard that was reporting the evolution of the pandemic by a health centre, county or city in near real time.

Health System Logistic Support

Risks associated with supply-chain disruptions can also be mitigated with an AI-based tool to support the health system with inventory capabilities to better allocate medical products across the country.

Up-to-date feeds of data about medical inventory, purchase orders, as well as predictions on the evolution of the disaster as available from statistical models and real-time news feeds, were ingested and pre-processed in a set of features that were used during the modelling. In this case, AI was used to build a simulation engine that, using inventory-level information and spread of the disaster, was able to estimate likely medical products demand and allocation. As the engine was producing the results of its scenario evaluation, the health authority was able to mitigate vulnerabilities generated by the natural disaster and support optimal allocation of medical supplies according to the demand in the territory.

Resilience of AI and data science

The current acceleration of AI and data science at scale is sustained by the successful applications of these methodologies to support humankind in the decision making process. However, AI deployments rely on methodologies and processes which may not always have a high level of resilience as listed below:

Observation Data

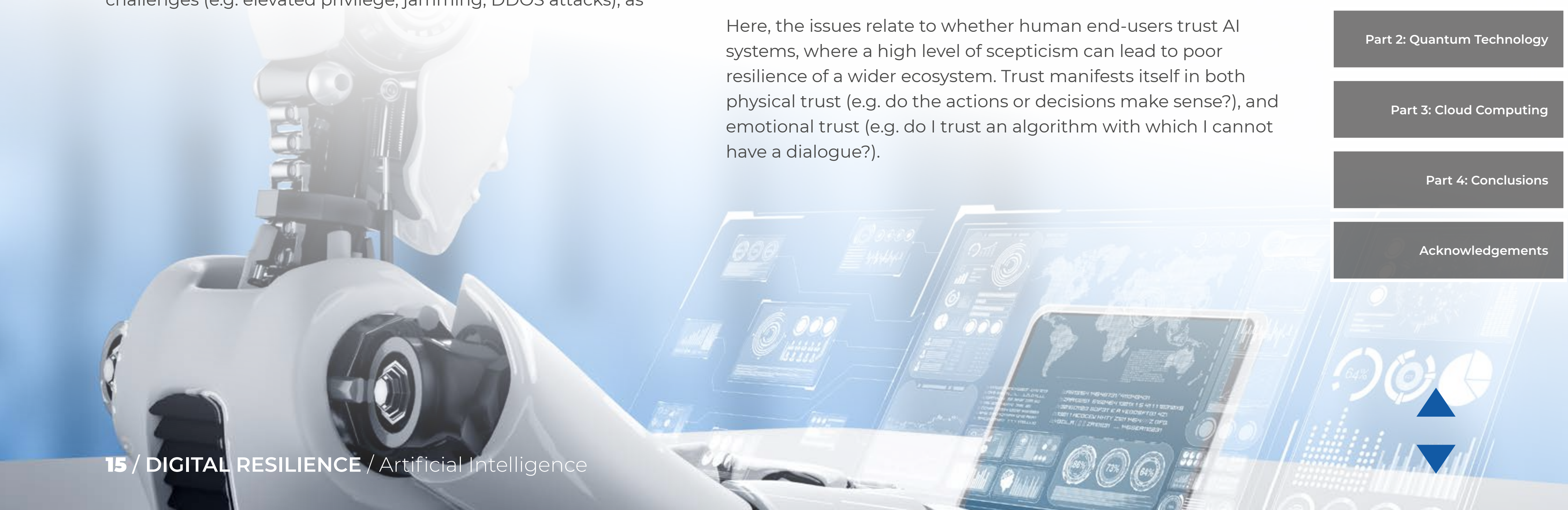
The data chain or pipeline that supplies the AI engine can be compromised in a number of ways. Both traditional cyber-security challenges (e.g. elevated privilege, jamming, DDOS attacks), as well as newer forms of attack (e.g. poison data, malicious gaming of system) can cause the downstream AI engines to create undesirable behaviour. In safety critical (e.g. autonomous driving) and time-sensitive applications (e.g. financial trading, remote surgery), this can lead to serious issues that can negatively affect the overall resilience of the applications.

Adversarial AI

Related to the data chain are the new vulnerabilities that AI algorithms (especially deep algorithms) can be malicious or have poisoned data. Here, the key difference is that whilst traditional Bayesian, physics-informed, and feature-based algorithms are transparent, and the vulnerabilities well understood, deep algorithms interpret data at the hyper-dimensions and the vulnerabilities are often opaque. Exploiting those by a more sophisticated attacker or through trial and error by end-users can lead to undesirable or unintended consequences.

Trustworthiness

Here, the issues relate to whether human end-users trust AI systems, where a high level of scepticism can lead to poor resilience of a wider ecosystem. Trust manifests itself in both physical trust (e.g. do the actions or decisions make sense?), and emotional trust (e.g. do I trust an algorithm with which I cannot have a dialogue?).



Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Adoption of AI

Strengths

As organisations consider the increased adoption of AI, its strengths include:

- The increased use of automated reasoning which can be desirable given the highly complex, increasingly uncertain and emerging scenarios with which firms will increasingly be confronted.
- The removal of human bias, such as 'anchoring' (i.e. the tendency to be overly influenced by the first piece of information that we hear), 'confirmation' or searching for information that confirms our preconceptions, 'pattern-matching' or sorting and identifying information based on prior experience – all of which can contribute to errors in judgement and cause disruptive events or affect an organisation's resilience.
- The integration of large volumes of data for time-sensitive analysis necessary to anticipate and prepare for complex risks and threats across a variety of time horizons, for example when considering global supply chains.

Weaknesses

In contrast, the adoption of AI might confer weaknesses including:

- The inability to integrate successfully domain expertise necessary for contextualised analysis, produced by people who notice and react to threats and respond effectively to unfamiliar or challenging situations.
- The attraction and retention of AI expertise which is hard for many sectors that have typically restricted or lower than normal AI market salary scales.

Resilience of AI

The resilience of AI arises from secure data chains to feed reliable and secure data to ML algorithms, robust algorithms that can cope with missing data, adversarial data, and the trustworthiness of that data.

One must also consider the resilience that emerges from systems of systems, a thorough understanding of interconnected issues, including the adaptive capacity in organisations and critical infrastructure soon to include AI, which should be actively managed.

Use of AI to improve resilience

Organisations often attempt to make their programmes as 'bulletproof' as possible, hoping that incidents will mostly disappear when a rigorous programme is in place. If something does go wrong, the hope is that having a comprehensive plan based on best practice management standards will help convince regulators and the public that their actions were reasonable and responsible. The improvements made in enhancing resilience over the years has been laudable. Most of the time, the existing system works. Every day, normal business processes cope with the myriad of minor disruptions and issues. More significant incidents are usually covered by the organisation's business continuity plan. Resilience is assured by plans, procedures and compliance and focuses on recovering the organisation's assets in a crisis: AI has a role to play in such an approach identifying fragility and weakness in the system. However, complex and more severe events are forcing organisations to be agile and fluid in their approach to respond and adapt effectively to unfamiliar or challenging situations. Many leaders now realise that relying on a reactive strategy is not enough on its own to meet the potential scale and pace of change imposed by sudden shocks and future challenges. Organisational resilience requires more than a reliance on procedures to recover assets – what if they can't be recovered within reasonable timeframes, or at all?

Organisational resilience is not purely defensive in orientation. It is also progressive, building the capacity for agility, adaptation, learning and regeneration to help ensure that organisations are able to deal with more complex and severe events and be fit for the future[4]. The challenge of adaptation is exacerbated by today's uncertain, complex, highly demanding and rapidly changing context in which organisations operate. Recent crises have raised serious questions about how rapidly organisations can adapt to changing threats, disturbances and perturbations e.g. a pandemic or climate change. AI-driven scenario modelling provides organisations with significantly increased ability to apply adaptive innovation to resilience challenges, potentially applying a progressive mindset and approach to challenges in a way not previously possible.

We need to find ways to get company boards, governments and society in general to invest in resilience, including the expert adoption of AI – even when it can be difficult to build an economic argument for doing so.

References:

[1] https://www.intuitive.com/en-gb

[2] https://www.marketingaiinstitute.com/blog/bert-google

[3] https://www.techtarget.com/whatis/definition/AlphaGo

[4] Denyer, D., 2017. Organizational Resilience. UK: BSI and Cranfield University.

Recommended Reading:

Schwartz R., Dodge J., Smith N. O., Etzioni O. Green AI. CoRR, abs/1907.10597, 2019. http://arxiv.org/abs/1907.10597.

Silver D., Huang A., Maddison C. J., GuezA., Sifre L., Van Den Driessche G., Schrittwieser J., Antonoglou I., Panneershelvam V., Lanctot M., Dieleman S., Grewe D., Nham J., Kalchbrenner N., Sutskever I., Lillicrap T., Leach M., Kavukcuoglu K., Graepel T., and Hassabis D. Mastering the game of Go with deep neural networks and tree search. Nature 2016 529:7587, 529:484–489, 1 2016. ISSN 1476-4687. doi:10.1038/nature16961. https://www.nature.com/articles/nature16961 .

Szegedyv C., Zaremba W., Sutskever I., Bruna J., Erhan D., Goodfellow I., and Fergus R. Intriguing properties of neural networks, 2014.

Carlini N., Wagner D. Audio adversarial examples: Targeted attacks on speech-to-text. In 2018 IEEE Security and Privacy Workshops (SPW), pp1–7, 2018. doi:10.1109/SPW.2018.00009.

Alzantot M., Sharma Y., Elgohary A., Ho B-J., Srivastava M., and Chang K-W. Generating natural language adversarial examples, 2018.

Carlini N., Wagner D. Towards evaluating the robustness of neural networks. In 2017 IEEE Symposium on Security and Privacy (SP), pp39–57, 2017. doi:10.1109/SP.2017.49.

Na T., Ko J H., Mukhopadhyay S. Cascade adversarial machine learning regularized with a unified embedding, 2018.

Tramèr F., Kurakin A., Papernot N., Goodfellow I., Boneh D., and McDaniel P. Ensemble adversarial training: Attacks and defenses, 2020.

Meng D. and Chen H. Magnet: A two-pronged defense against adversarial examples. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, pp135–147, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450349468. doi:10.1145/3133956.3134057. https://doi.org/10.1145/3133956.3134057 .

Buckman J., Roy A., Raffel C., Goodfellow I. Thermometer encoding: One hot way to resist adversarial examples. International Conference on Learning Representations, 2018. https://openreview. net/forum?id=S18Su--CW.

Top

Contents

Foreword

Executive Summary

Introduction

Part 1: Artificial Intelligence

Part 2: Quantum Technology

Part 3: Cloud Computing

Part 4: Conclusions

Acknowledgements

PART 2:
QUANTUM TECHNOLOGY

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Carl Dukatz

Global Lead of the Quantum Computing Program at Accenture

Introduction

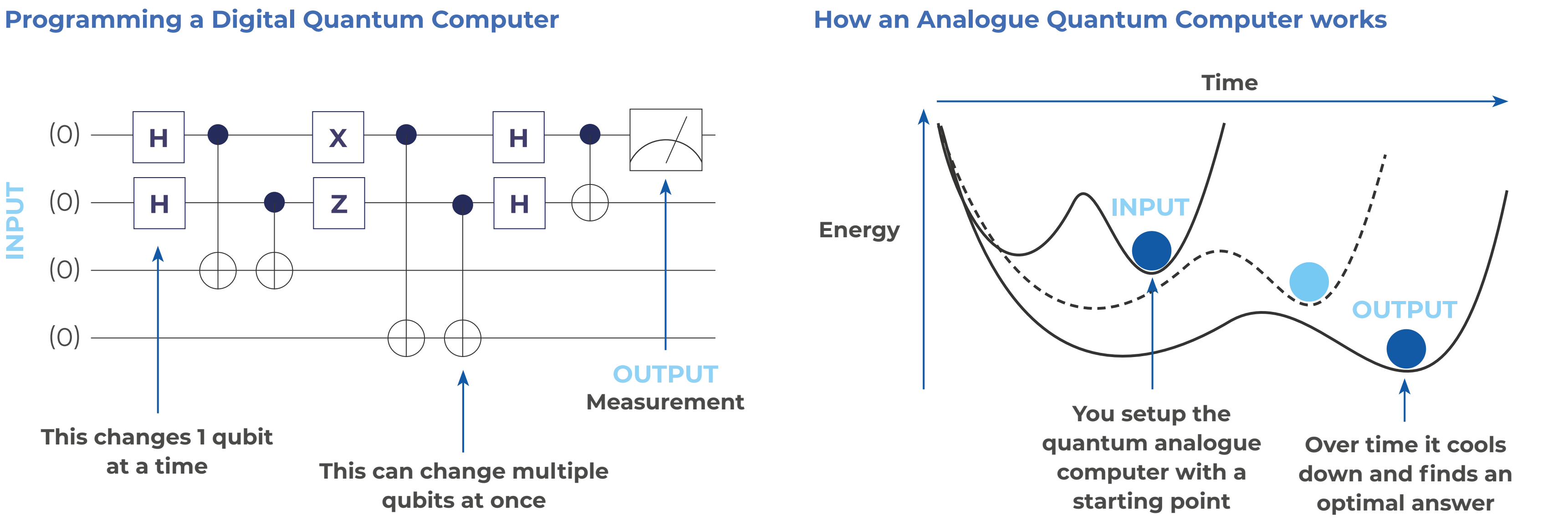
The concept of a quantum computer was first proposed by David Deutsch in the 1970s. In the following decades, much theoretical and experimental work has been done to progress from idea to an existing reality. It is now understood that quantum technology is a paradigm shift for the world of computing. All computers (which we will call 'classical computers') were based on binary code, made up of bits that are only ever 0 or 1. In contrast, quantum computers have qubits which can be both 0 and 1 at the same time. Qubits are comprised of subatomic particles and their strange behaviour is made possible by quantum-mechanical effects. At the microscopic level, the physical laws that govern interaction with everyday objects do not apply. Particles can be in more than one place at a time (known as 'superposition'), pass information across distances (known as 'entanglement') and effectively teleport across barriers ('tunneling').

Computations can be executed by controlling the properties of the qubits according to a specific set of instructions and then measuring their final states as output. Because the qubits can be in multiple states at once, more advanced operations than can be realised on classical computers can be applied. Problems that were once thought intractable can be solved.

Two high-level approaches have been identified for leveraging quantum-mechanical phenomena to run computations: analog and digital. *(See Figure 2.)* In analogue-quantum computing, information is processed continuously. Analogue-quantum simulation is a well-known application in which a fully controllable analogue-quantum computer is used to simulate efficiently the complex evolution of a targeted quantum system. Adiabatic- and quantum-annealing computers belong to this category. In digital-quantum computing, information is processed by a quantum algorithm which is a discrete sequence of logical quantum gates. Many existing quantum algorithms hold advantage in algorithmic complexity over their classical counterparts. Information in digital-quantum computers can be protected by quantum error-correcting codes; this lays a promising future for a fault-tolerant quantum computer.

Quantum technology is not only limited to computing. Sensors and information channels built on quantum-mechanical systems have also emerged in recent years. Quantum sensors and communications share the same physics (superposition, entanglement and tunneling) as quantum computers. However, their uses are very different. Quantum sensors offer enhanced ways to observe and measure physical properties such as gravity and light. Quantum communication methods are known to be more secure than classical encryption. Together with quantum computing, these new technologies can have the potential to transform businesses by creating solutions for problems that were previously thought insolvable.

A challenge in implementing this novel technology is the massive workforce skills' gap. Bringing a workforce up to speed on quantum technology may involve a combination of hiring



Programming a Digital Quantum Computer

INPUT
(0)
(0)
(0)
(0)
H
H
X
Z
H
H
OUTPUT
Measurement
This changes 1 qubit at a time
This can change multiple qubits at once

How an Analogue Quantum Computer works

Time
Energy
INPUT
OUTPUT
You setup the quantum analogue computer with a starting point
Over time it cools down and finds an optimal answer

Figure 2. In digital quantum computing (left), the programmer can specify the input (initial configuration of qubits) and the specific set of operations to be applied to the qubits, including how and when the qubits are measured to get the output. In analogue-quantum computing (right), only the input can be chosen, and the entire system of qubits evolves over time to settle in its lowest energy state.

quantum experts and upskilling internal employees. Finding experts is difficult because quantum skills are very specific. Quantum computers are built by highly-skilled scientists with years of training in experimental physics and engineering. But these are not the only people involved with industry quantum computing. Data scientists and software developers are also necessary to implement quantum-powered solutions, and hiring those who have experience in physics and chemistry can be key to bridging the gap between quantum hardware and software. Upskilling current workers is also becoming more feasible as quantum technology matures. Software kits continue to abstract the physics from quantum programming, making them accessible to traditional developers. Now some quantum computers are made available to be programmed remotely, and these are accompanied by extensive training guides on how to use them.

Today, quantum computers are approaching 100 qubits and experiments on them. They are no longer limited to the academic world as more and more businesses ready themselves to begin folding in quantum to their technology stack. In a survey of more than 415 large organisations, 69% said they already have some in-house quantum computing programmes, with an additional 21% that plan to create one within a few years.[1]

The power of quantum can bring immense potential to multiple facets of enterprise resilience. Businesses will have enhanced ability to detect and prevent disruptions. Quicker response and

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

recovery is possible when events occur. As the technology matures and the full power of quantum computing is realised, companies that take advantage now can be the first to achieve new levels of resilience.

Computing

During the learning, preventive and adaptive phases of resilience programmes, businesses could use quantum computers to predict the most likely or costly disruptions as well as play out scenarios and conduct testing on how to recover. Resilience at scale means understanding the trajectory or predicting the future of complex systems. These systems can so easily be knocked off course: a company that finds itself on the brink of disaster may have unknowingly sealed its fate years prior with a seemingly innocuous decision. For example, imprecise demand predictions at the start of the Covid-19 outbreak in Southeast Asia at the beginning of 2020 had a year's long domino effect that plunged supply-chain operations into complete chaos and led to global shortages for all types of goods by the end of 2021.[2]

These types of disruptions, and the need for reliable systems to mitigate them, will not end with the pandemic. Climate change has the potential to wreak havoc on all kinds of seemingly stable systems and is a likely cause of the Texas storm in February 2021 that killed hundreds and left millions without power for days.[3] When extreme low temperatures hit, state-wide energy demand outstripped supply and the result was a cascade of system failures for which even the most extreme winter planning scenarios could not account.[4]

Systems as complex as weather patterns are highly volatile and can be completely upended by small changes in minor variables. Therefore, the technology that underpins applications built to simulate these systems and predict what may happen is critical to enterprise resilience. Quantum computing can enhance these simulations and create a more complete picture of possible outcomes. For example, the quantum computing company Rigetti demonstrated that weather prediction which used synthetic data generated by a quantum computer can meet classical benchmarks, and even exceed them when a quantum layer is added into the simulation model.[5] Furthermore, for more general types of forecasting techniques, quantum computers can speed up some of the most computationally time-consuming processes, enabling more complex models to be simulated.[6] In all, quantum technology can offer companies a window into the future that is impossible with classical computers, readying them for possible disruptions.

...Systems as complex as weather patterns are highly volatile and can be completely upended by small changes in minor variables. Therefore, the technology that underpins applications built to simulate these systems and predict what may happen is critical to enterprise resilience.

Today, supply-chain resilience is about not only handling disruptions but also embracing increasing complexities due to evolving market trends and consumer behaviour. This means a sudden rise of unanticipated competition and a focus on hyper-personalisation i.e. the use of data to deliver more personal and tailored products, services and information. Active resilience can help enterprises: in the case of supply-chain management, it can help diversify their manufacturing network and ecosystem partnerships. This, in turn, can mitigate a concentration risk from a few suppliers, distributors or even countries, and thereby can help eliminate the power to disrupt operations easily. It can enable

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

manufacturers to create necessary buffers pertaining to inventory, time, capacity and develop standardised, repeatable processes that are easier to replicate across employees and facilities.

The most resilient and agile supply chains are built using state-of-the-art technologies that help enterprises to identify the most critical processes, evaluate vulnerabilities related to them and prepare to mitigate quickly the risks and capitalise on the opportunities while delivering valued business services. Resilience, when integrated with efficiency, can help achieve the ultimate lean operation.

Active resilience can be further enhanced through quantum-powered machine learning (ML) to detect anomalies. At a basic level, ML is the process of a computer understanding and reproducing specific distributions of data. Quantum mechanics inherently creates unique and unnatural data patterns that are incredibly difficult to reproduce classically. Since quantum computers can produce these patterns, they may also be able to recognise them and thus take on ML tasks that classical computers cannot. Indeed, many ML algorithms based on quantum computing routines can solve problems faster than their classical counterparts.[7]

When used for cyber-security threat detection, these methods prove powerful. For example, quantum versions of common ML models were able to detect successfully distributed denial of service (DDOS) attacks with over 95% accuracy.[8] While results like these are impressive, many think that even better techniques may come from a mix of quantum and classical ML. When quantum methods were combined with classical ones to produce a hybrid quantum-classical neural network, the accuracy of detection of DDOS attacks rose to nearly 100%.[8] This is important for resilience because modern web applications are complex, and it can be very expensive in terms of computer resources to produce even just a single page for a user. Classifying and predicting which traffic is associated with the attack before servicing the request can mean the difference between keeping a system responding to legitimate traffic or being knocked offline.

In another study concerning network intrusion detection (used to detect malicious activity in networks), a hybrid quantum-classical support vector machine reached nearly identical accuracy to its purely classical counterpart (92% v 93% respectively).[9] As quantum computers scale past the few dozen qubits they have today, they are expected to overtake quickly their classical counterparts for problems such as the ones identified here. Businesses that start on their quantum journey now can take advantage and become more resilient in the future.

Although robust techniques exist for preventing and planning for cyber and physical disruption, it is inevitable that unexpected incidents will occur, and a swift response will be necessary to keep critical operations intact. In such scenarios, a course of action must be chosen and resources dispatched appropriately. Yet, identifying the optimal strategy in the face of disaster is never easy and can be close to impossible for certain types of disruptions. Returning to the global supply-chain issues brought about by Covid-19, anyone who has studied supply chains will know that optimising them is a costly and time-consuming challenge. For example, a simple network of a handful of trucks needing to make a couple dozen stops results in many trillions of possible routes which would take more than a thousand years to sift through to identify the most efficient.[10] When expanded to supply chains that span the globe, one can see how time consuming it would be to find an alternative plan after disruption. For these types of optimisations, because of the near impossibility of finding the exact best solution, planning applications often search instead for options that meet some pre-defined threshold of 'good enough'.

Quantum technology offers two main ways to tackle optimisation that may provide better solutions faster: adiabatic quantum computing (also known as 'quantum annealing') and variational quantum algorithms. Adiabatic quantum computers evolve a quantum system to its lowest energy state. If the system can be modeled to represent a minimum optimisation problem, then the lowest energy state would also be the solution. Quantum annealers are computers made only to perform adiabatic quantum computing tasks and so they are much easier to scale compared to universal quantum computers. Today, there are quantum annealers with thousands of qubits available for businesses to use remotely.

Variational quantum algorithms combine digital quantum and classical computers to create hybrid workflows to solve optimisation problems. Quantum computers are used to sample efficiently a parameterised objective function, working in tandem with a classical machine that checks and iterates the parameters until an answer appears. The hybrid nature of these algorithms allows them to be demonstrated on non-fault tolerant quantum computers and provide value in the near term.

These optimisation techniques can be used to solve problems across the entire supply chain. *(See Figure 3.)* During upstream operations, raw material must be sourced and transported to production sites. Freight trains are a common way to transport the raw materials, but ensuring efficient operations of today's complex railway systems is no small feat. Companies such as AlphaRail use quantum-inspired techniques to build software to help enhance operational decision making for railways.[11] These solutions can offer the ability to do dynamic scheduling based on demand and just-in-time staffing of crews, drastically increasing a railway's ability to adapt when disruptions such as staff shortages occur.

The complexity of a global supply chain

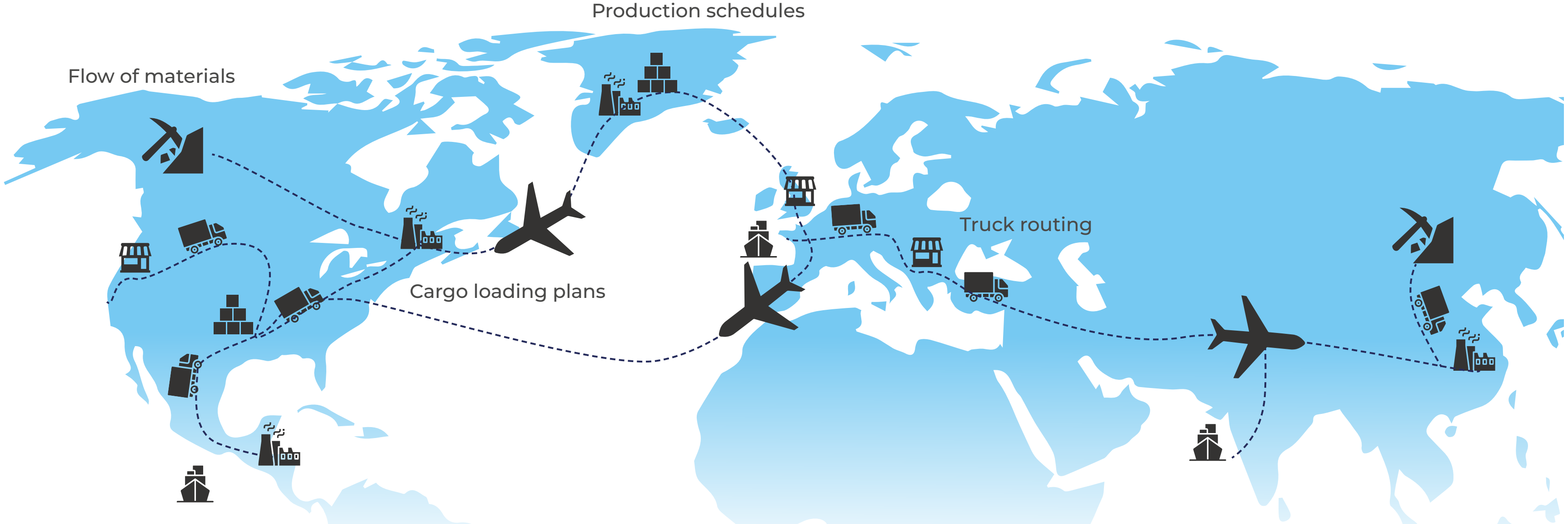


Figure 3. Many stages of global supply chains face complex optimisation problems whose solutions could be improved with quantum computing. Current optimisation methods do not scale well, forcing companies to rely on 'good enough' solutions to large problems. Even small increases in efficiency from finding better answers to these optimisation problems can result in major cost savings.

Once raw materials reach manufacturers, the resources and machines necessary to complete the production of goods are scheduled to perform operations in a way that minimises time between an order being placed and completed.[12] For large manufacturers seeking to minimise costs across an entire production line, these production plans can become very complex. Even advanced production planning systems usually have built-in assumptions to make the problem small enough to optimise, and if these assumptions are wrong then the absolute best answer might be missed, meaning loss of efficiency. Recent research has shown that methods based on quantum optimisation techniques can analyse the same production plan problem and evaluate it in less time.[13] Faster results may mean that larger systems can be optimised, thus leading to truly optimal production plans.

In the last steps of the supply chain, the goods are distributed to end customers. Over a third (35%) of world trade value is transported by air, and the efficient packing of cargo in the lower decks of aircrafts is a more difficult problem than it might seem.[14] Critical safety conditions around weight and distribution must be maintained while simultaneously maximising value and profitability. Airbus is in collaboration with quantum scientists and research organisations to leverage quantum computing to optimise the aircraft loading problem and early results are very promising.[15]

A variety of other downstream supply-chain problems can be tackled with quantum optimisation methods as well. In recent years, applications powered by quantum computers have been launched that involve quickly rerouting trucks, creating shift schedules for drivers, and planning delivery routes based on the pickup and delivery of packages. From upstream to downstream operations, quantum computing serves to redefine what problems are possible to solve. This can provide the speed and accuracy necessary for efficient decision making after disruptions occur, helping businesses to continue critical operations with limited downtime.

Communications

The Covid era has led many organisations to undergo digital transformations (e.g. launch and promote digital banking channels), adopt ‘digital only’ strategies (e.g. market and sell products on e-commerce platforms) and switch to virtual corporate environments (e.g. using Zoom meetings) to keep up with the global industry trends and evolving client requirements. Many organisations acknowledge the high level of dependence that their core business processes have on digital technology. However, they are at a stage where, in the event of a process failure or disruption, switching to alternate non-technology independent processes is no longer a possibility.

A secure, robust and operationally resilient communications capability is important to provide uninterrupted core business services and thereby help avoid operational, financial and reputational losses to the firm. Insecure communications channels present major risks to individuals, businesses and governments. Amazingly, quantum computing presents what might be the greatest threat against current information security, while quantum technology also offers a possible solution to the threat.

Digital data is often secured using encryption which scrambles it until it reaches the intended audience who hold the key to descramble (decrypt) it. One of the commonest forms of encryption, RSA, is built from a 2048-bit subprime (product of two primes) number. The two factors of this large number make up the decryption key, and if they are found – that is, if the subprime number is factored – then decryption of the data is possible. Classical computers would take billions of years to factor a typical RSA key but a quantum algorithm discovered in 1995 by Dr Peter Shor could theoretically do it in a matter of hours (or minutes, depending on the source). To run Shor’s algorithm, an error-corrected quantum computer with thousands, if not millions, of qubits is needed, however such a system is several years away from current quantum technology.[16]

However, once a fault-tolerant quantum computer of sufficient size is available, all data encrypted with RSA methods can be compromised. The implications of this cannot be understated because RSA is the basis for almost all communications today. If an adversary collects encrypted information today, they could decrypt that information with a quantum computer in the future, prompting everyone to evaluate this threat today and begin taking steps to understand and mitigate the risks. *(See Figure 4.)*. Governments are taking action now, for example, the United States issued a Presidential mandate for agencies to implement quantum safe cryptography by July 18th, 2022.[17]

Other types of quantum technology can offer sound mitigations to this threat. One of the hallmarks of quantum mechanics is that a quantum system cannot be observed or measured without noticeably and irreversibly modifying the system. Taken in the context of communication, this means that an eavesdropper attempting to intercept information could not do so without changing the information and alerting the sender and receiver to their presence. Built on this idea is Quantum Key Distribution (QKD) which has emerged as a virtually impenetrable method to communicate the secret keys used to encrypt and decrypt data.

Last year, Chinese scientists built the first integrated quantum communication network with 700 optical fibres across 4,600 kilometres.[18] The network was secured with QKD and serves banks, government websites and power grids. There are efforts to build quantum communications networks underway all around the globe, as well as extending to outer space with satellite communications. In theory, they can be impenetrable communication channels that are highly valuable when quantum computers are built large enough to run Shor's algorithm and break encryption. Although other algorithms may be identified as being safe from quantum attacks, quantum-key distribution could prove to be the most secure of all because it is built with a system that is naturally immune to observation.

If an eavesdropper intercepts the data and the public-key then the data could be decrypted with Shor's algorithm.
Here are three examples of eavesdropping techniques:

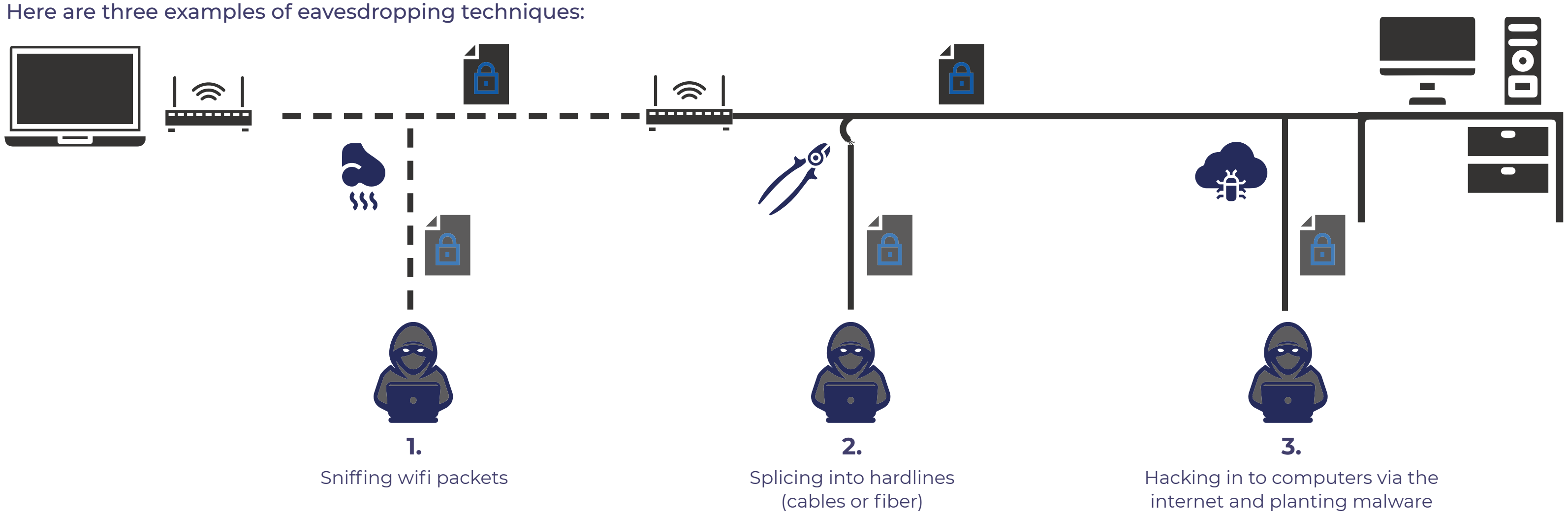

1.
Sniffing wifi packets
2.
Splicing into hardlines (cables or fiber)
3.
Hacking in to computers via the internet and planting malware

Figure 4. Attackers can carry out Store Now, Decrypt Later attacks. Once quantum hardware scales are large enough to be able to run Shor's algorithm, they can unscramble highly sensitive that they have intercepted in transit.

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Sensing

Ascertaining an inappropriate physical location for a new business venture can result in a costly mistake. Recently in India, a whole complex was sited in a vulnerable location and was ruined before completion.[18] For the manufacturing or energy industries choosing a location with a constant supply of raw materials to attain continuous production operations is of the utmost importance. A negative downstream impact could be avoided on the end user while preventing costs associated with business disruptions. With detailed, accurate and real-time knowledge of the physical location, steep costs can be alleviated and the correct decisions to attain business resilience can be taken.

Quantum sensors differ from quantum computing and communication in one major characteristic. The physical systems that make up qubits are very fragile and susceptible to the disturbances from electromagnetic waves, invisible to humans, but constantly around us. Thus, critical to these quantum technologies is insulating the qubits from all external noise. In contrast, quantum sensors are built specifically to be hyper-attuned to specific types of external noise. They can detect with extremely high precision certain natural forces such as gravitational fields and light and sound waves.[19] *(See Figure 5.).* Technologies powered by quantum sensors show promise to enhance earthquake detections, volcanic eruption predictions and see underground.[20]

Perhaps most exciting is recent work that shows the potential of quantum sensors based on nano-diamonds to detect the coronavirus that causes Covid-19. The researchers describe techniques that could deliver test results with higher accuracy than the gold standard PCR tests, which take hours to analyse, in just a few minutes. And even if the real-world results fall short of what the mathematical models predict, it is still likely that there can still be a significant advantage over current PCR testing.[21]

Quantum phenomena is not just revolutionary to computers but can also enhance many types of current sensors. It is important that companies ready themselves to take advantage of this step change in technology so they can become more resilient against the natural world.

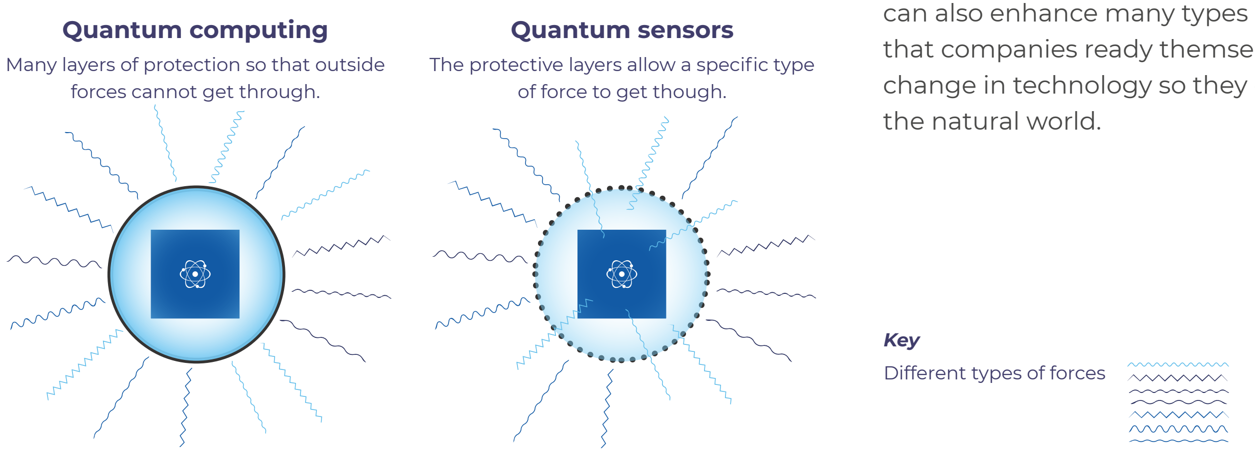

Quantum computing
Many layers of protection so that outside forces cannot get through.
Quantum sensors
The protective layers allow a specific type of force to get though.
Key
Different types of forces

Figure 5. For quantum computing (left), qubits need many layers of protection because of their extreme sensitivity to outside noise. Qubit operations can be rendered useless if they are not completely isolated from outside forces such as light, noise and gravity. In contrast, quantum sensors (right) are built to harness this extreme sensitivity by allowing the qubit to come in contact with only a specific type of noise that is of interest to observe: for instance, a nearby minor seismic wave that could indicate an earthquake.

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Quantum and the cloud

Governments and industry need begin gaining experience using quantum today. Fortunately, preparation can be done by accessing quantum computers remotely through the cloud. This means submitting jobs and circuits via Application Programming Interfaces (APIs). Already major cloud providers are integrating quantum hardware into their offerings. AWS has launched Braket, a fully managed quantum-computing service that allows developers to build circuits, test algorithms on simulators and access various quantum computers remotely.[22] Microsoft offers Azure Quantum which also allows for connection to quantum hardware as well as use of various quantum-inspired algorithms and a comprehensive software developmental kit.[23]

These cloud platforms lower the barrier of entry for businesses interested in quantum computing. A company that would have otherwise needed specific agreements with quantum providers and pay hefty sums for long-term contracts to use quantum devices, can now pay for just what they need. Such allows for democratisation of quantum across businesses. Thus, companies looking to use quantum can leverage synergies with cloud capabilities to unlock quantum advantage and supremacy for themselves.

Quantum and AI

In recent years, AI has transformed many aspects of business as well as our everyday lives. However, there remain many barriers to scaling certain AI systems. Adding quantum computing techniques into existing workflows may help unlock even more value.

Neural networks are one of the most popular examples of AI, displaying impressive abilities to learn and reproduce patterns of data for image recognition and highly accurate predictions. Unsurprisingly, neural networks are incredibly complex to build. The amount of data needed to train them effectively increases exponentially with the number of variables in the model, leading to scalability issues and underfitting of the model. Quantum computers may be able to relieve some of this data burden by producing representative synthetic data when there is a shortage of real data. As mentioned above, weather prediction models were found to be just as accurate using synthetic data generated by a quantum computer.

Data is not the only barrier to scaling ML models. The most advanced AI models are expensive to train and require more GPUs to run than is accessible to most developers. One of the most highly discussed ML models is GPT-3 from OpenAI. GPT-3 was the largest language model ever built at the time of its release.[24] However, training the full model is nearly impossible. One calculation by Lambda Labs estimated that it would cost millions of dollars and hundreds of GPU years to train GPT-3 fully.[25] This is an extreme case, since many advanced models are built to be able to take on new tasks without requiring extensive retraining. However, as ML evolves, the high costs and computational overhead will need to be addressed.

Integrating quantum computers into AI workflows may be one answer. For example, the HONE engine developed by SavantX and Fenix Marine Services combines AI and quantum annealing to optimise port operations. Since its initial deployment in 2020 at the Port of Los Angeles, 'it has doubled cargo handling equipment productivity and produced more predictable cargo flows', according to SavantX.[26] This is one of the first hybrid quantum-classical commercial applications: the need for more scalable AI solutions may mean more will follow.

Enhancing resilience

Quantum technology has massive potential to level up enterprise resilience, both by itself and working in tandem with other emerging technologies like AI and the cloud. Broadly, quantum technology consists of computers, sensors and information communication methods that leverage quantum-physics phenomena known as superposition, entanglement and tunneling to perform operations that are impossible with classical technology. Quantum computers show promise in tackling optimisation and simulation problems, as well as enhancing ML techniques.

Enterprise resilience stands to benefit in many ways from quantum technology. Active resilience can be improved by the ability to simulate chaotic systems and make more precise predictions about what may occur. The near constant disruptions to normal business operations over the last few years from climate-change-induced disasters and the Covid-19 pandemic prove the need for a better understanding of these complex problems. Quantum computing shows promise in offering us a clearer window into the future.

When disruptions do occur, and companies must react and respond to maintain critical operations, quantum optimisation can find a reasonable plan of action for many different scenarios. Problems such as rerouting trucks or figuring out the best way to schedule shifts during staff shortages cannot be solved precisely on classical computers in a reasonable amount of time. However, these same problems have been proven to be able to be formulated to run on quantum computers, and as the hardware matures, it is possible that the performance could exceed that of classical methods.

Other quantum technology can also protect against disruptions. Quantum sensing has the potential to improve how we understand and interpret the world around us. We can better detect earthquakes, predict volcanic eruptions, and test for diseases, including Covid-19. Quantum communication methods may be the most urgent of the quantum technologies since quantum computers may threaten popular encryption methods when they are built big enough to run Shor's algorithm. RSA encryption will need to be replaced with a method that is safe from quantum attacks, and quantum-key distribution may be the most secure way ever found to transfer data.

References:

[1] https://www.youtube.com/watch?v=fk4r8yTJtPo

[2] https://www.nytimes.com/2021/10/22/business/shortages-supply-chain.html

[3] https://dshs.texas.gov/news/updates/SMOC_FebWinterStorm_MortalitySurvReport_12-30-21.pdf, https://www.sciencedirect.com/science/article/pii/S2214629621001997?via%3Dihub, https://www.eurekalert.org/news-releases/926889

[4] https://www.sciencedirect.com/science/article/pii/S2214629621001997?via%3Dihub

[5] https://www.hpcwire.com/off-the-wire/rigetti-enhances-predictive-weather-modeling-with-quantum-machine-learning/

[6] https://www.researchgate.net/publication/333679417_Quantum_algorithm_for_logistic_regression

[7] https://arxiv.org/pdf/1611.09347.pdf

[8] https://www.researchgate.net/publication/349828355_Quantum_machine_learning_for_intrusion_detection_of_distributed_denial_of_service_attacks_A_comparative_overview

[9] https://www.gsd.inesc-id.pt/~mpc/pubs/Quantum_NIDS_final.pdf

[10] https://www.sciencedirect.com/topics/earth-and-planetary-sciences/traveling-salesman-problem

[11] https://www.alpharail.com/

[12] Lutkevich, B. (2020, November). Production Planning. Tech Target. https://searcherp.techtarget.com/definition/production-planning

[13] Denkena, B., Schinkel, F., Pirnay, J., Wilmsmeier, S. (2021). Quantum algorithms for process parallel flexible job shop scheduling. CIRP Journal of Manufacturing Science and Technology, 33, 100–114. doi:10.1016/j.cirpj.2021.03.006

[14] Brandt, F. (2017). The Air Cargo Load Planning Problem. 10.5445/IR/1000075507.

[15] Airbus. (2019). Airbus Quantum Computing Challenge: Aircraft Loading Optimisation. https://www.airbus.com/sites/g/files/jlcbta136/files/2021-10/Airbus-Quantum-Computing-Challenge-PS5.pdf

[16] https://ieeexplore.ieee.org/document/365700

[17] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

[18] https://phys.org/news/2021-01-world-quantum-network.html

[19] https://onlinelibrary.wiley.com/doi/full/10.1002/qute.202100049

[20] https://hellofuture.orange.com/en/quantum-sensors-are-beginning-to-leave-the-laboratories

[21] https://www.laboratoryequipment.com/582191-Sensor-Based-on-Quantum-Physics-Could-Detect-SARS-CoV-2-Virus/

[22] https://aws.amazon.com/braket/

[23] https://azure.microsoft.com/en-us/services/quantum/#features

[24] https://bdtechtalks.com/2020/09/21/gpt-3-economy-business-model/

[25] https://lambdalabs.com/blog/demystifying-gpt-3/

[26] https://www.prnewswire.com/news-releases/quantum-computing-application-sees-real-world-success-at-pier-300-at-the-port-of-los-angeles-301455106.html

Top

Contents

Foreword

Executive Summary

Introduction

Part 1: Artificial Intelligence

Part 2: Quantum Technology

Part 3: Cloud Computing

Part 4: Conclusions

Acknowledgements

PART 3:
CLOUD COMPUTING

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

Hamish Wynn

Managing Director at Accenture and Leader within Digital Risk, Operational Resilience and Cloud Transformation

The journey to digital and the associated cloud transformations are not new and while some organisations have already begun the ride others are just starting. With the speed provided by the cloud, and by working with CSPs, enterprises can shift away from operations aimed at keeping the lights on, freeing up their budgets and their teams' time to rethink fundamentally how the business operates, and how it creates value. This is the ultimate objective of a cloud journey – to create a platform for innovation, agility and future business reinvention.

Management teams are seeking to understand better both the extent to which the benefits of cloud computing can be fully realised and the factors that need to be overcome in order for these benefits to be maximised. According to Accenture's survey to 200 senior IT executives in companies with revenues above $1 billion, across seven countries in 10 industries, two-thirds of companies using it fail to obtain expected benefits despite the immense potential of the cloud.[1]

The two most cited factors that stand in the way of satisfaction with cloud services are: first, concerns relating to security and risk compliance; and, second, the complexity of business and organisational change. In respect of both concerns, leveraging a qualified third party to manage services has proven to be the key decision that has led to increased satisfaction in cloud usage in respect of cost savings, speed to market, business enablement and improved service levels.

The starting position is that without the cloud the customer is 100% responsible for resilience which can be a scary place to be.

Cloud resilience can offer a huge potential as it increases agility along with reducing risk and cost. This notwithstanding, resilience capabilities should be planned for, and implemented during, the journey. Otherwise, the transformation to the cloud may result in enterprise-wide risk increase.

> *...Cloud resilience can offer a huge potential as it increases agility along with reducing risk and cost. This notwithstanding, resilience capabilities should be planned for, and implemented during, the journey. Otherwise, the transformation to the cloud may result in enterprise-wide risk increase.*

Management of resilience is centred on strategic planning activities designed to recover from the effects of a hazardous situations such that restoration and preservation of basic risk-management structures and functions can be maintained. To understand this better and how it can be addressed, let us first review some of the cloud concepts.

Cloud computing is a model in which organisations access a shared pool of configurable computing resources such as servers, networks, storage, development tools or applications. The cloud is not a one-size-fits-all solution; organisations can choose from different types of cloud computing and different types of cloud services. When planning for the cloud journey, organisations choose whether they will go on a public cloud, private cloud or hybrid cloud.

The public cloud is defined as computing services offered by third-party providers over the public Internet, making them available to anyone who wants to use or purchase them.[2] Connecting to a public cloud means using an Internet connection to access computing resources hosted on data centres managed by a third-party CSP rather than owning and maintaining these resources on premise. A shared public cloud has many organisations (or tenants) sharing the same infrastructure.

The cloud model can also be implemented on servers owned and maintained by the organisation and accessed by Internet through a private internal network. This model is a private cloud. Private clouds facilitate the control over data and security, and may ease the need to meet specific regulatory and compliance requirements in certain industries e.g. HIPPA for healthcare, GDPR, GxP for Pharma, etc.

A hybrid cloud approach is a combination of public and private cloud and can include the use of some on-premises infrastructure as well.

In addition, companies may adopt a range of cloud services to support their business requirements from basic utilisation of cloud-based applications (software as a service or SaaS), application development functionality (platform as a service or PaaS) and full IT data centre functionality within the cloud (infrastructure as a service or IaaS).

Enhancing resilience

Public cloud data-centre architecture is world leading (in power, cooling, etc) and built-in clustered pairs (availability zones), with the principle that customers deploy to a zone, not a specific data centre. The cloud provider duplicates or extends all workloads across multiple data centres, availability zones or even regions to provide inherent resilience. Many cloud services are platform based; they contain orchestration to help ensure the health of the platform to monitor continually and fix issues in real time – this applies to anything serverless or platform as a service but also some infrastructure components like Kubernetes and Terraform which are managed on a declarative loop.

> *...Cloud services are also elastic and can be seamlessly scaled for demand – this removes issues around headroom or over-demand that leads to failure.*

Unlike private clouds, public clouds can save from the expensive costs of having to purchase, manage and maintain on-premises hardware and application infrastructure. They allow organisations to pay only per usage for the CPU cycles, storage or bandwidth they consume. Cloud services are also elastic and can be seamlessly scaled for demand – this removes issues around headroom or over-demand that leads to failure.

Public clouds also bring benefits of increased speed and agility as they can be deployed faster than on-premises and with an easily scalable platform. Cloud native deployment patterns are diversified away from big-bang upgrades to help increase resilience after deployment in case of error. One key thing that you get out of the

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

box is leading edge monitoring and observability. This alerts you to problems before the damage hits or reduces the time to learn something is failing. Again, this can be done on-premises but lots of hard work to maintain anything good: in most organisations it is a clear pain point.

Although having a more resilient organisation is expected to be one of the main benefits that organisations can have from utilisation of cloud resources, many have not fully leveraged the tools and resources that CSPs offer, or they have not established the strategic and governance foundation for leveraging these benefits.

The Organisation for Economic Co-operation and Development defines resilience as the ability to absorb and recover from shocks, whilst positively adapting and transforming in the face of long-term stresses, change and uncertainty. Yet, most organisations do not realise that operational resilience in the cloud has to be strategically planned and intentionally implemented. In other words, moving to the cloud may not automatically result in an increased resilience.

> *...Yet, most organisations do not realise that operational resilience in the cloud has to be strategically planned and intentionally implemented. In other words, moving to the cloud may not automatically result in an increased resilience.*

As operations and applications are moved to cloud environments, organisations should have a clear understanding of the interdependencies among their applications and services, develop and implement capabilities to enhance their resilience (i.e. architecture their applications to take advantage of the cloud resilience properties) keeping in mind the need for alignment with the business's critical level of operations, along with an efficient disaster recovery testing.[3]

CSPs offer a range of services that are designed to help enable organisations to prepare for, and respond to, adverse events that can cause a disruption to business operations. Within the cloud computing shared responsibility model, the underlying infrastructure for these services is supported by CSPs while the configuration and utilisation of cloud resources are the responsibility of the customers.

Along with the organisation, based on the cloud service model used, the CSP is also held responsible for building resilience for all management and maintenance of the system. The shared responsibility model distinguishes between the customers' responsibilities for managing resources when using the cloud resources and the CSP's responsibility for managing the underlying infrastructure of the cloud. The customer is responsible for customer data, platform, applications and identity and access management, operating system, network and firewall configuration, client-side data, encryption controls over client data, servers, systems, and networking traffic. The CSP is responsible for software within the virtual machines, computation, storage database and networking, hardware and global infrastructure including regions, availability zones and edge locations.[4] The organisation is responsible for ensuring that business operations are resilient such that controls are in place to prevent and be responsive to events that can disrupt business operations.

Governance controls should be in place to help ensure that the organisation is managing its risk in a consistent and strategic manner. Management should set out a clear IT governance cloud strategy with defined parameters for consistent guidelines and tool sets for configuration within the cloud resilience IT risk management e.g. Disaster Recovery (DR) solutions and procedures. These parameters should also apply to any third parties contracted to support the cloud deployment efforts. Furthermore, care should be taken to define cloud resources and assets in accordance with specific organisational principles with clear accountabilities and tagging procedures for billing and pricing. Monitoring and audit metrics should be in place to measure key risk and performance indicators and a structured governance model should be in place at specific layers of the organisation to ensure that consistent processes exist for the evaluation of thresholds and the escalation of commentary regarding breaches and emerging risks.

IT assets should be configured to ensure that data can be generated for monitoring and auditing purposes. Without a clear IT risk strategy for strategically addressing these cloud protocols, resilience can be difficult to quantify and manage.[4] CSPs offer a variety of preventative and detective control features that help customers protect their data and assets through the management of resilience. The functionality and resilience of these features are independently reviewed by the American Institute of Certified Public Accountants' System and Organisation Controls (SOC) oversight reporting process.[5] For example, IAAM is used to define access to cloud resources in accordance to defined roles and responsibilities set out in organisational service catalogues. Multi-factor authentication offers a layer of security at the individual user level, while monitoring controls are used to aggregate data across IT assets for the purpose of identifying capacity levels and thresholds and to identify and respond to external threats such as DDOS threats or data breaches. Audit controls allow for detective methods to enable traceability in identifying which users performed which actions on cloud resources and what API activity occurred. These audit logs, supplied by the CSP, can be retained for compliance purposes.

Compliance with regulations is a standard of sound IT risk and because companies use client data in their cloud resources, they must be aware of internal and external threats associated with data breaches. Further, companies should understand the regulatory landscape in which cloud computing exists, particularly in respect to the specific articles of legislation that have been enacted to protect customer data within the cloud. These frameworks require digital service providers (including CSPs) to take appropriate measures to protect customer data. Examples of such frameworks include: the EU's General Data Protection Regulation (GDPR)[6] which subjects organisations to tight controls over the collection and use of personal data; the US CLOUD Act (H.R.4943) which clarifies that US federal law-enforcement agencies can request data stored by US internet service providers (including CSPs) and their foreign subsidiaries regardless of whether the data is stored in the US or abroad; the UK Network and Information System (NIS) Regulations (2016) which requires that digital service providers, including CSPs, to take appropriate security measures to prevent security breaches and other events that have the potential to compromise their stored data or services.[7]

> *Compliance with regulations is a standard of sound resilience risk and because companies use client data in their cloud resources, they must be aware of internal and external threats associated with data breaches.*

Companies are also expected to take ownership for the responsibilities of their cloud resources and data within the cloud. To accomplish this, the CSPs have provided guidance on what good looks like in terms of 'well-architected design' in the customer's realm of responsibility within the cloud. These principles set out best practices to help ensure that user access is granted based on the principle of least privilege access provisions, that functionality performed is automated where possible and that fault tolerant processes are in place to eliminate single points of failure. Examples include automated recovery from anticipated failures through pre-scripted autoscaling (to augment cloud computing and storage resources) and load balancing to redirect traffic to the replacement resources. Furthermore, testing of recovery procedures should be a standard operational process step to help ensure that such automation can occur at the moment of failure.[4]

Fully automated disaster recovery testing should be performed to help ensure that failover occurs seamlessly without disruption to business operations. DR testing can be performed based on either a multiple-availability zone model or based on a multiple regional model.

Importance of testing

In the move to cloud migration, DR testing is a must even when the underlying cloud infrastructure is designed to provide redundancy through continuous monitoring, clustering, load balancing, detecting failure and automated failover to a redundant secondary (DR) sub-system or component when the primary fails: all of this happens at the infrastructure layer. The underlying infrastructure resilience is usually covered by the CSP but each application that is migrating to the cloud is responsible of redesigning, remediating and architecting the application to be resilient to failures.

Application resilience testing is important to realise fully the value promise of cloud. Post-migration performance issues often persistently affect applications, particularly when on-premises applications are migrated to the cloud without appropriate remediation and testing. This is one of the main factors contributing to the failure of organisations experience in obtaining the expected benefits.[8]

A patterns approach provides the ability to prove if the cloud DR strategy is reasonable and fit for purpose from a technological standpoint and ensures all applications can be subsequently tested in the cloud as dictated by the annual DR schedule. Applications should be representative of the full environment. Defined logical groupings can be used to help ensure accurate representation through migration by creating a subset of applications that will be used to prove out each landing zone as it becomes available. DR for each tier and or applications by each major database platform and replication approach can be demonstrated through a single occurrence of defined test cases. The defined test cases are based on a subset of representative applications to validate the DR capabilities, not to perform DR validation for each application.

The achievement of these objectives can enable the business, application and technology teams to assess properly the dependencies and recovery requirements of business processes and match them to the applications and technology which support them. It can also allow validation of the modernised and migrated applications to meet established standards in preparation for business-as-usual DR exercises.

The future of cloud

As regulators continue to focus on the management of resilience and risk in cloud computing, organisations should have plans in place for three facets of resilience.

First, organisations should continue to manage their resilience through appropriate deployment of their cloud resources. Infrastructure and applications should be configured based on a defined technology strategy that is linked to strategic business outcomes. Cloud computing risks should form part of the enterprise-wide risk assessment and these risks and associated controls should be included within the control framework. Appropriately skilled individuals should be in the right roles to help ensure that the organisation's use of cloud computing can evolve and advance in a compliant manner within the context of the growth agenda and the control framework. Ongoing testing should be performed to test the viability of the technical components within a single availability zone as well as the viability of multi-regional availability zone strategies.[9]

> *Cloud computing risks should form part of the enterprise-wide risk assessment and these risks and associated controls should be included within the control framework.*

Second, organisations should understand that resilience and risk management means being able to sustain operations if their CSP or sub-contractors are unable to perform as expected.[10] The European Banking Authority reported in its 2017 guidance recommendations that organisations need to be prepared to articulate the materiality of their CSP's outsourced business operations and have processes in place to inform their supervisory regulators of these outsourcing agreements.[11] Furthermore, organisations should have exit plans to transition cloud computing to new vendors when needed. To this end, contracts with CSPs should allow for on-site audits to measure defined performance thresholds and governance should be in place to evaluate the key performance metrics.[12]

Third, organisations should keep abreast of the regulators' interest in concentrating risk relating to dependencies on specific CSPs and the potential for systemic, economic implications in the event of failures by the CSP to maintain and operate their cloud-computing infrastructure.[13] Although such systemic risks are deemed theoretical at present and the regulators have not specified expectations to utilise multi-cloud solutions, organisations should be considering multi-cloud solutions as a potential solution for their ongoing resilience needs and for their exit strategies.[14] In considering their options for resilience and risk solutions, organisations should know that regulators, policy makers and CSPs are working to support organisations to manage their cloud-computing resilience.

With these three areas of focus in mind, organisations should develop risk management strategies to maximise the benefits from cloud-computing solutions by helping ensure that their IT assets and cloud resources are correctly configured and designed and that the teams supporting these solutions are skilled and trained to adapt to changes. Organisations should also have a strong governance framework in place to measure and track the health of their IT assets to help ensure that the cloud functionality is operating as intended. Processes should be in place to conduct ongoing impact assessments and to identify control weaknesses. Any issues should be self-identified and tracked to completion with appropriate governance oversight. Further, organisations should maintain continued engagement and awareness in respect of legislative and regulatory trends. Preparations should be made to incorporate key proposals into multi-year change programmes.

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements
▲
▼

Modernisation is the key to reducing technical debt and ramping up organisational speed and agility in the cloud. Yet, full-scale modernisation will not be right for every application, every circumstance or even every company. There may be good business reasons for focusing initially on rehosting as a means to get to the cloud quickly, but even if you choose to defer modernisation for now, it could be on your agenda for the future. Ultimately, if you want to benefit from the full value of the cloud, you should be working towards cloud-native applications, infrastructure and data. A carefully considered modernisation programme is how you get there.

> *...organisations should develop risk management strategies to maximise the benefits from cloud-computing solutions by helping ensure that their IT assets and cloud resources are correctly configured and designed and that the teams supporting these solutions are skilled and trained to adapt to changes.*

The way forward

The cloud migration journey is more complex than most companies anticipate. To achieve greater innovation and efficiency, organisations should ensure that they have strategic IT cloud priorities that are designed for growth and sustainability. Organisations should be thinking about three facets of resilience and risk. First, organisations are required to have controls in place to help ensure that their IT assets and cloud resources are deployed optimally, and that staff are trained and skilled to perform configurations, testing and ongoing maintenance. Second, organisations are required to have clear exit strategies in place based on defined performance thresholds and they should be prepared to transition their cloud computing under certain defined circumstances. Finally, organisations should maintain continued awareness of regulatory trends particularly in respect to the regulators' interest in concentrating risk and the systemic risks that CSPs pose if they were to be unable to perform as expected.

The cloud marketplace offers proven configurations with high level of community activity i.e. it can use off-the-shelf images for a virtual machine, or an entire application setup like SAP, that can de-risk the possibility of misconfiguration and/or baking in of high-risk items. Most services are offered with multiple levels of quality – you can pay to get something really powerful, safe, etc. It would be impractical to build this on-premises due to lack of scale and excessive engineering required.

We talked about the importance of DR testing during migration to the cloud to safeguard resilience but there are also multiple best practice resilience DR architectures that can be established, and can be setup very quickly. Each organisation should need to assess its recoverability requirements and it may not even be the same for each organisation.

There are four key offerings available each of which has its own pros and cons:

- **Back-up and restore** – cheap but takes a bit longer, leverage cloud durability.
- **Pilot/Cold** – second, safe location has live data but idle services. In case of a disaster, the services are turned back on – still quite cheap.
- **Warm** – second, safe location has live data and service always on but deployed at minimum scale. In case of a disaster, the services are scaled up – bit more cost, but faster.
- **Hot** – second, safe location has live data and services at full scale – zero downtime, but most expensive.

What if after all the preparation and risk management there is an outage anyway? Public-cloud providers will offer service-level agreements for uptime, durability and latency of each service, and offer financial liability terms when they are not met. Having a key understanding of your application and infrastructure requirements, coupled with effective contract management, can allow for optimal setup and help permit an organisation to be as resilient as possible in its utilisation of the cloud.

References:

[1] https://www.accenture.com/_acnmedia/PDF-103/Accenture-Cloud-Well-Underway.pdf#zoom=50

[2] cloud Computing Terms | Microsoft Azure https://azure.microsoft.com/en-us/overview/cloud-computing-dictionary/

[3] Supervision Tip 2018-04, Identifying Risks Associated with Outsourcing in a Public cloud Environment (ffiec.gov) https://www.ffiec.gov/press/PDF/FFIEC_Cloud_Computing_Statement.pdf

[4] AWS Certified cloud Practitioner Exam Training [New] 2022 | Udemy

[5] SOC Compliance - Amazon Web Services (AWS) https://aws.amazon.com/compliance/soc-faqs/

[6] How to comply with both the GDPR and the CLOUD Act (iapp.org) https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/

[7] POST-PN-0629.pdf (parliament.uk) https://researchbriefings.files.parliament.uk/documents/POST-PN-0629/POST-PN-0629.pdf

[8] cloud outcomes: Expectation vs. Reality (accenture.com) https://www.accenture.com/us-en/blogs/cloud-computing/kishore-durg-cloud-migration-strategy

[9] Board of Directors Handbook cloud Risk Governance FINAL (google.com) https://services.google.com/fh/files/misc/gcat_board_cloud_risk_governance_full.pdf

[10] AFME_cloudComputing2021_05.pdf https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME_CloudComputing2021_05.pdf

[11] Recommendations on outsourcing to cloud service providers | European Banking Authority (europa.eu) https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers

[12] 10 questions to help boards safely maximize cloud opportunities | Google cloud Blog https://cloud.google.com/blog/products/identity-security/10-questions-to-help-boards-safely-maximize-cloud-opportunities?utm_campaign=601ceea1702a26000184455a&utm_content=61e06c4fd61c4f00012a0bd2&utm_medium=smarpshare&utm_source=linkedin

[13] Concentration_Risk_Perspectives_092020.pdf (microsoft.com) https://azure.microsoft.com/mediahandler/files/resourcefiles/concentration-risk-perspectives-from-microsoft-/Concentration_Risk_Perspectives_092020.pdf

[14] AFME_cloudComputing2021_05.pdf https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME_CloudComputing2021_05.pdf

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

PART 4:
CONCLUSIONS

Top

Contents

Foreword

Executive Summary

Introduction

Part 1: Artificial Intelligence

Part 2: Quantum Technology

Part 3: Cloud Computing

Part 4: Conclusions

Acknowledgements

Robert Hall

Director of Strategy at Resilience First, and Editor of this report

According to Klaus Schwab, the founder and Executive Chairman of the World Economic Forum, ‘We stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before. We do not yet know just how it will unfold, but one thing is clear: the response to it must be integrated and comprehensive, involving all stakeholders of the global polity, from the public and private sectors to academia and civil society.’[1]

The challenges and opportunities are significant. There is the great potential to raise global income levels and improve the quality of life for many around the world. Technology will make it possible to produce new products and services that can help increase the efficiency and resilience of our organisations and societies. On the other hand, technology can insert societal inequalities (between the haves and have nots), help reduce resilience (by making us ever more dependent on those technologies), and question our ability to control progress (within established social structures).

The revolution will need managing carefully and we need to balance the upsides with the downsides. This paper has revealed many of the elements and impacts that should to be considered by business in three particular areas if we are to manage expectations and demands. The modern cliché that information is the ‘new oil’ may be irritating and a problematic analogy but the technologies explored here that allow us to share and process information will undoubtedly be the crucial sources of power in the future.

Applied AI developments have been claimed by Sundar Pichai, Google’s CEO, to be ‘more profound than fire, electricity or the internet’.[2] Already, AI has acted as the main driver of other emerging technologies like big data, robotics and the Internet of Things, and it will continue to act as a technological innovator for the foreseeable future. In terms of resilience, AI can help to identify areas of weakness or fragility in networked systems which are often hard to quantify using classical techniques.

...Applied AI developments have been claimed by Sundar Pichai, Google’s CEO, to be ‘more profound than fire, electricity or the internet’.

This makes it uniquely qualified, for instance, in helping to understanding the cascading impacts of major disruptions. This will be important for both the public and private sectors. However, if AI technology is to have more universal application for businesses, then the scale of data handling and storage, as well as computational power and energy usage, will become determining factors. Businesses and employees alike need to be prepared for what is likely to widespread change as AI is adopted, as well as the ethical, skills and regulatory challenges that come with it.[3]

Quantum technology is set to help significantly improve the reliability, speed, accuracy and security of many products and services. It can enable new medical diagnostics and pharmaceutical techniques, dramatically help improve the precision of navigation above and below water, reveal potential earthquakes, and more. It is also an opportunity and a threat for cyber security. Typical encryption will need to be replaced with a method that is safe from quantum attacks but quantum-key distribution may be the most secure way ever found to transfer data thereby enhancing resilience.

> *...Alone, quantum computing promises enhancements to enterprise resilience but when combined with AI via the cloud, these synergies could vastly change the landscape.*

All this signals a real commercial opportunity for business but it will require users to understand the technology and become active in the next few years. According to a report by McKinsey, 'prescient business leaders in almost every industry should develop some kind of quantum strategy now.'[4]

When quantum computers are combined with the cloud and AI, even more resilience can be unlocked. The cloud is a key technology to quantum computing because of how infeasible on-premises quantum computers can be for most businesses. Most of the quantum programming will take place remotely, with much of it on the cloud which means that cloud capabilities can be key for companies looking to leverage quantum. Alone, quantum computing promises enhancements to enterprise resilience but when combined with AI via the cloud, these synergies could vastly change the landscape.

Cloud resilience alone can offer enormous potential as a way to cut costs, help increase agility and help reduce risk. Yet, failure to plan for and implement resilience can result in an unintentional increase in overall enterprise risk. With the speed provided by the cloud, enterprises can free up their budgets and their teams' time to rethink fundamentally how the business operates, and how it creates value. This is the ultimate objective of a cloud journey – to create a platform for innovation, for agility and for future business reinvention. The cloud provider can help duplicate or extend all workloads across multiple data centres, availability zones, or even regions, to provide inherent resilience.

As Klaus Schwab concludes, 'as a complement to the best parts of human nature – creativity, empathy, stewardship, [technology] – can also lift humanity into a new collective and moral consciousness based on a shared sense of destiny. It is incumbent on us all to make sure the latter prevails.'

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

References:

[1] https://www.marketwatch.com/story/artificial-intelligence-is-more-profound-than-fire-electricity-or-the-internet-says-google-boss-11626202566#:~:text=Alphabet%20CEO%20Sundar%20Pichai&text=This%20feature%20is%20powered%20by%20text%2Dto%2Dspeech%20technology.&text=%E2%80%9CI%20view%20it%20as%20a,with%20much%20more%20intelligent%20systems.

[2] https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[3] The impact of AI on business and society. Financial Times, 16 October 2020. https://www.ft.com/content/e082b01d-fbd6-4ea5-a0d2-05bc5ad7176c

[4] A game plan for quantum computing, McKinsey, February 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing

ACKNOWLEDGEMENTS

Resilience First would like to thank both Accenture and Cranfield University for their significant contributions to this paper. It is the respective authors who have given their valuable time and expertise to help make this report a meaningful contribution to the subject.

In addition, Resilience First would like to thank in particular Claire Aldworth, Risk Consulting Senior Manager at Accenture, and Mike Sutliff, Project Director – Grand Challenge Resilience at Cranfield, who have done much to marshal resources in their respective organisations in parallel to their content contributions.

This belies the contributory effort that those from those organisations have made to this paper. From Accenture, this includes:
Francesco Vivarelli, Data Scientist Principal Director; Lorena Ruiz Monroy, Technology Consulting Senior Principal;
Shreyas Ramesh, Technology Innovation Strategy Senior Manager; Bernard Leddy, Risk Consulting Manager;
Apoorva Jain, Consulting Manager; and Julianna Harwood, Technology Innovation Strategy Consultant.

Finally, thanks go to Helen Dale from HD Designs who has produced a document layout of merit.

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements

accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 674,000 people deliver on the promise of tech-nology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities.

Visit us at www.accenture.com

Disclaimer: This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.

Top
Contents
Foreword
Executive Summary
Introduction
Part 1: Artificial Intelligence
Part 2: Quantum Technology
Part 3: Cloud Computing
Part 4: Conclusions
Acknowledgements
▲
▼

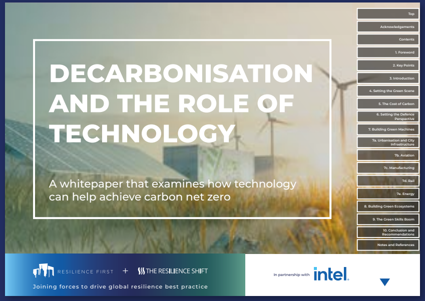
OTHER PUBLICATIONS BY RESILIENCE FIRST

EMOTIONAL RESILIENCE

Lessons from the real world:
A practical guide after crises and major incidents

RESILIENCE FIRST

In partnership with KRTS INTERNATIONAL LTD.


DECARBONISATION AND THE ROLE OF TECHNOLOGY

A whitepaper that examines how technology can help achieve carbon net zero

RESILIENCE FIRST + THE RESILIENCE SHIFT

Joining forces to drive global resilience best practice

In partnership with intel.

RESILIENCE IN THE ROUND

OPERATIONAL RESILIENCE

A GUIDE FOR NON-EXECUTIVE DIRECTORS

RESILIENCE FIRST + THE RESILIENCE SHIFT

Joining forces to drive global resilience best practice

POOL Re

RE-EMERGENCE GUIDE

BUILDING SMALL BUSINESS RESILIENCE

RESILIENCE FIRST + THE RESILIENCE SHIFT

Joining forces to drive global resilience best practice

In partnership with Russell Cooke FACEBOOK

RESILIENCE FIRST

SURVIVE & THRIVE

RESILIENCE AND FLEXIBLE WORKING

WHAT HAPPENS NOW?

Part 2: the hybrid office

A guide for employers and employees

Thank you to our partner

March 2021

Russell Cooke

RESILIENCE FIRST

SURVIVE & THRIVE

TRANSITIONING FROM RISK TO RESILIENCE

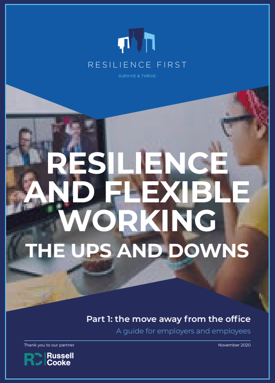
A WHITEPAPER IN PARTNERSHIP WITH

FUSION RISK MANAGEMENT

Edited by

Robert Hall
Resilience First, London

January 2021


RESILIENCE FIRST

SURVIVE & THRIVE

RESILIENCE AND FLEXIBLE WORKING

THE UPS AND DOWNS

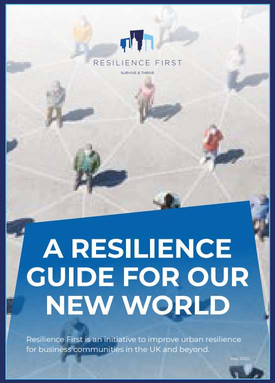
Part 1: the move away from the office

A guide for employers and employees

Thank you to our partner

November 2020

Russell Cooke

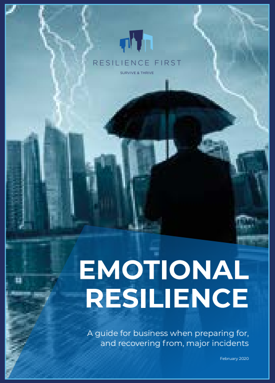

RESILIENCE FIRST

SURVIVE & THRIVE

A RESILIENCE GUIDE FOR OUR NEW WORLD

Resilience First is an initiative to improve urban resilience for business communities in the UK and beyond.

May 2020

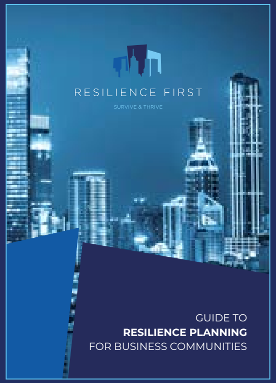

RESILIENCE FIRST

SURVIVE & THRIVE

EMOTIONAL RESILIENCE

A guide for business when preparing for, and recovering from, major incidents

February 2020


RESILIENCE FIRST

SURVIVE & THRIVE

GUIDE TO
RESILIENCE PLANNING
FOR BUSINESS COMMUNITIES

Top

Contents

Foreword

Executive Summary

Introduction

Part 1: Artificial Intelligence

Part 2: Quantum Technology

Part 3: Cloud Computing

Part 4: Conclusions

Acknowledgements

RESILIENCE FIRST

SURVIVE & THRIVE

www.resiliencefirst.org

@Resiliencefirst

www.linkedin.com/company/resilience-first/