Viewpoints on artificial intelligence and quantum computing

Context

Gareth Byatt recently liaised with three fellow Risk professionals to discuss how modern technology is impacting the management of risk.

Our panel:
Neil Allan, MD Systemic Consult and partner at RiskIQ,
Gareth Byatt – Principal Consultant, Risk Insight Consulting and an Ambassador for the Institute of Risk Management,
Chris Corless – Enterprise risk and audit leader
Hans Læssøe – Principal Consultant, AKTUS

Our discussion

How do you see AI impacting risk management? Are there also risk opportunities around AI?

Chris:
For me I see quite a bit of upside when it comes to AI (and machine learning) in risk management, especially when it comes to operational risks. For quite some time the approach to risks which have very large impacts has been to ensure they are managed by closely monitoring the effectiveness of the controls over time, and to do our best to detect and communicate potential issues so they can be fixed before a significant event occurs.
A challenge to avoiding significant events is that, for many industries, they are wedded to the idea of detecting these faults through various forms of audits.
I think AI will be instrumental in helping us to identify data sets and triggers that will help to automate this control effectiveness monitoring. In many cases the what needs to be monitored is intuitive, but the challenge comes down to volume of risk/controls to analyse all the time and the dynamic relationships between risks and controls in a complex environment.

As for the risks associated with AI technology - that's a bit tougher to see. While AI will likely be able to help us solve some of the greatest problems facing humanity (perhaps climate change, for example), there could well be unintended consequences if we create a new sentient being with greater cognitive capability than all of humanity combined. Life on earth has been dominated by carbon-based lifeforms - will the creation of AI begin a transition towards silicon-based life forms and what will that mean for the future of the species of the planet... I don't think I have a deep enough understanding of the technology to provide a solid answer.

Hans:
AI will surely have a profound impact on risk management – and everything else we do – in a number of ways, for example:

- Risk data will be much more precise and faster to obtain – and enable decision makers to make more precise decisions faster than they could do so before. However, whilst AI will help to reduce the level of uncertainty, it may be potentially matched by the increase in uncertainty driven by the increased speed of change, competition and globalisation. All in all, I see a sustained level of "hardship", just at a higher level. You can compare it to playing an instrument well. A violin is inherently difficult to play, so the level of added "tricks" and playing speed is at a level which matches the capabilities of the musician. A piano is somewhat easier (you cannot hit a false note), and hence the added tricks and playing speed is higher as an equally capable musician will be able to do more than he could on the violin.
- One area where I agree with Chris and expect the most and "first seen value" is in early warning monitoring (nowadays known as the more fancy-termed "predictive analytics") and risk detection – which will be vastly enhanced. This resonates with the point that Chris has made.
- For many types of risks, I also see automated mitigating response systems being applied – as they have been for decades in, for example, nuclear power plants, where a "scram" (emergency shutdown) leads to IT systems taking over controlling the power plant to make a safe handling at a time, when people may panic. This may include currency risks handled by auto-trading, traffic risks handled by self-driving vehicles, etc. The list of possible applications here is very long.

Neil:
A key aspect to how we evolve to use AI is that we must always bear in mind that we need to maintain a focus on the good fundamentals of risk management. New technologies will advance in society and business in various ways, and AI is certainly doing that. Whilst this progresses, we need to make sure that, as Risk practitioners, we continue to use good decision-making techniques and approaches with our businesses and teams that we know work well. AI will help us to gather data and to interpret data at many levels. So we need to ensure that we are getting meaningful insights from AI and that we can triangulated these findings by alternative verification and experience. A key challenge is governance of the AI process and how to communicate the insights to senior teams. We need to avoid another black-box mentality where only a few people actually understand how the process works and how it relates to other aspects of the business.

Gareth:
I wonder how many people appreciate how long AI has been talked about. The roots of AI date back to the 1950's, when it was introduced as a sub-division of computer science. It's come a long way since then.
Three particular points come to my mind on the subject of AI and what it means for risk management:

1. **How we create AI, to then put it to use**
   We need to create AI to assist us with the points that Chris, Hans and Neil make in a way that does not "build in the biases of its creators". The field of cognitive bias has been understood for a long time, and I think that this needs to be applied to the way that AI is created.
2. **How we use AI to make risk-informed decisions**
   As Chris and Hans have pointed out, there are many examples of how AI is already helping organisations improve their operations, and "do more with less". I agree that AI is a valuable tool to spot anomalies and inconsistencies, and perhaps formative trends. I believe that these human-centric mechanisms of audits and checks and "sense-making" of data will continue to be important, whilst using AI as an aide in industries that will benefit from real-time monitoring of controls and control effectiveness.
   We need to make sure that we have good governance in place for what AI is being used for, how often it is being checked and the like. This ranges from keeping abreast of, and anticipating, regulations that may be adopted for the use of AI to the impact that AI has on how the organisation actually operates.
3. **How the Risk team uses AI to "free is up" our focus on important matters**
   As Risk professionals, we are here to help people to navigate uncertainty. A lot of us spend a lot of time reviewing registers and consolidating data.
   One of the things to come out of a recent RIMS conference, for example, which was covered by StrategicRISK, was Google's use of chatbots to lighten the workload of its risk management team, for routine tasks like certification and low-level insurance claims. Put another way, AI and associated technologies can hopefully move us more and more towards being able to analyse data for decision-making.
   Hopefully, with the help of AI we can minimise the time we spend on administrative tasks and maximise our time with people, holding reviews and helping to facilitate good risk-informed decisions, and ensuring people are empowered to speak up about concerns and risks.

What impact do you expect quantum computing will have on the risk landscape?

Chris:
I have a limited understanding of quantum computing, but what I understand is that the speed of computing becomes radically quicker which means that data sets that once took hours, weeks or months to model and understand can be handled much, much faster which then allows us to move more quickly and use much broader data sets in the computations and analysis. This should make the results of this analysis more closely approach reality which should improve decisions made from them.

Hans:
To me, quantum computing means faster/better computers that can solve complex problems and scenarios. We have seen faster computers that can solve more complex situations for more than half a century. Quantum computing may be a bigger step – but then again, it will not be implemented "overnight". To me, it's technology and how it impacts risk practitioners, time will tell.

Further, I do not believe in 100% model-based decision making. 40 years ago, the mantra was “linear programming”, where constraints and performances were modelled, and the technical optimum was found. Some believed it would be “the new way of reaching any decision”. People simply do not make decisions like this, which was well documented by Richard Thaler’s Nobel prize winning work.

Neil:
Quantum computing is a fascinating area, which can boggle the mind when you delve into it in detail!
The way the technology works, with qubits and having “multiple states” active at the same time, is highly complex. Whilst it’s not yet all-pervasive, quantum computing will have an increasingly large impact on society in the coming years. Certainly Quantum Mechanics is all around us, as a proven technology in mobile phones, MR scanners and nuclear power plants. Quantum computing will have undoubtedly have many positives but, as always, there are risks to consider. For people dealing with risk, there are the “upsides”, and the potentially harmful risks of this processing power being used to create problems or negative impacts of some sort.

Gareth:
I agree with Neil that quantum computing is a fascinating area, one that I believe in time may become an increasingly important area of focus for those of us who work in risk management.
The technologies being used to develop these super-fast silicon-based computers will likely have major ramifications for our ability to handle massive amounts of data. This should help us with risk-informed decision-making, and therefore it should help us to take risk better and, per the point that Chris makes, help us to understand and prepare for uncertainty in a complex world.

What little I know about quantum computing, I know it is complex and, like Hans, I understand that putting it into business applications is not something that will happen overnight.

As Chris says, for risk management in various sectors, quantum computing should aide our ability to use data to look at modelling scenarios of how risks could turn into events. With superfast computers at our disposal, it could become practical to run scenarios with lots of “moving parts” to simulate a complex eco-system.
Will quantum computing also change the technology tools that we use in risk management, such as for running quantitative analysis? In at least some cases, yes. Also, will more and more data “live” in the cloud, with quantum computers being used to power instant analysis of complex situations?

For example, consider a sector that is often at the forefront of using new technology to assist with risk management: finance. Many people in the finance sector believe that quantum computing will help them to solve complex challenges, such as improving financial risk assessments, optimising portfolio risk and dealing with fraud detection.

Consider financial risk assessments first. They can be complex to run. Quantum computing could improve how they work. Second, portfolio risk often involves thousands of financial assets with a myriad of interconnected dependencies and risks – quantum computing could greatly assist with scenarios to decide the best portfolio structure. Third, to combat fraud, quantum computing could help finance firms to spot fraud indicators more quickly, to reduce the risk of fraud occurring.

As with all new technologies, there are potential risks, including specific elements of Cyber risk.

One thing I'd like to finish on is to return to Neil's point in your first question about AI, which is that we need to maintain a focus on the core activities that risk management can help people with to navigate an uncertain world. Quantum computing will I think help us in many ways, but it isn't the answer to everything in risk management.

If quantum computing could defeat all modern encryption, what does this mean for cyber security, and current cyber threats such as data theft and breach?

Gareth:
I'll take a stab at this!
We all know of data theft and Cyber hacks that continue to take place. Quantum computing may change the game on this, and from what I understand, experts are racing to ensure cyber security keeps in step with increased computing power.

I read an article in Wired last year which talked about the increasing cyber security risk that quantum computing brings. This article highlighted that quantum computers will have a significant impact on IT security protocols which protect global financial markets, businesses and governments around the world.

With quantum computing predicted to be mainstream by the late 2020's, the world is less than a decade away from quantum computers being able to render many of today's most sophisticated encryption systems more or less useless. Some people are talking about a "Y2Q" risk, meaning "Years to Quantum".

A particular element of this risk is how quantum computing could allow hacking into public key cryptography. Public key cryptography currently provides the foundation of trust required to protect pretty much all of our online data and digital transactions. New encryption techniques will be required, and new standards will have to be developed. Data security requirements and regulations will continue to evolve as a result (including for new technologies such as blockchain).

For businesses, is this is a Board level matter for discussion? Risk Managers should be working with IT teams and digitisation teams in their business to consider the impact that quantum computing will have on IT security. They may benefit from liaising with experts in the field to understand what is happening. Such experts are in IT firms as well as small incubators in academia and elsewhere (the University of New South Wales, for example, has created a quantum computing business).

Risk Managers could consider conducting scenarios in their businesses to understand what the impacts could be – which is good practice to be resilient against today's Cyber risks, as well.
On top of all this, there still needs to be a focus on the basics of tackling Cyber risk – including 'the human factor" of being vigilant, and not being tricked into providing data to thieves.

Chris:
Of course, the speed of quantum computer will also make our traditional approaches to encryption and security pretty much useless. That said like most times in history when our defences are breached humanity will build a bigger wall. I believe Google is already working on quantum encryption to combat the challenge of quantum computing on our current security backbone and I am sure they are not alone. (anyone who is selling cloud services has a deep vested interest in this, especially in light of increased data protection regulation)

AI will likely play a larger role in the cyber security space as well. At the moment my understanding is that a lot of the cyber defences are quite static, similar to the walls of traditional physical castles, but with AI and quantum computing the ability to monitor for breaches and have cyber defences that can morph and even multiply when threats are detected become more of a reality. Sort of like the dynamic shields of the Starship Enterprise, I can imagine a world where cyber security is largely controlled by AI with little human interaction.

Hans:
It may very well become true that quantum computing can defeat all modern encryption – but it may also be the mother of unbreakable encryption. The technology will move the level of risks and risk management to another level, but not essentially "change things" and the way we operate

The increased use of biometrics may be a bigger game changer in terms of data security – and then again – most (by far) data breaches are made possible through human stupidity, ignorance or carelessness – which is not changed. Just look at how Facebook and Google (and many others, I am sure) collect data – including data they have no right to collect – including covert listening through the microphones of your PC and cell-phone.

Neil:
I think the guys have pretty much covered my views on quantum computing.
As Gareth suggests, let's focus on ensuring we keep matters practical, whilst being aware of the security threat that exists.