Disruptive Influences: Technology, politics and change in the financial sector

January 2016

Foreword

In recent months the public policy ether has been full of a miasma of e-buzz words: FinTech, cyber risk; automation; the sharing economy, the Internet of Things; e-payments, and big data to name but a few.

These and many other issues are captured in the phrase ‘digital disruption’.

Is this real step-change or another dot.com short-lived bubble which will fall back to a more normal cycle of development? The reality is this is a real change and it is already occurring albeit at an uneven pace across the range of financial services.

This report, the third in our collaborative series of risk reports with Cicero, focuses on the next wave of technological progress which is likely to have a fundamental impact on how the financial services world will interact with and impact on the wider consuming public.

In the words of Donald Rumsfeld, there are a number of ‘known knowns’ and ‘known unknowns’ here but possibly a few ‘unknown unknowns’ - the proverbial black swans that can provide a curve ball to any risk manager’s carefully calibrated risk assessments.

But equally important to the pace of technological change is the need to identify, analyse and understand the implications in terms their economic and societal impact. Big data, for example, raises a huge opportunity for many in financial services to do some innovative things but is it with the consent or even the awareness of consumers? Driverless cars threaten to rewrite how motor insurance is underwritten. And the Internet of Things can by-pass humans altogether - which raises interesting issues of privacy and public interest.

This report, ‘Disruptive Influences: Technology, politics and change in the financial sector’ looks at the new risks emerging from this new wave of digital change and what challenges this offers for public policy regulation and wider society. We hope you find it enjoyable and that provokes some fresh thinking.

David Thomson, Director of Policy & Public Affairs, Chartered Insurance Institute

Introduction

Are we on the verge of another industrial revolution? Cheap computing power and strides in machine learning make computers good enough to solve problems which only a few years ago could only be tackled by the human brain. This has the potential to turn the services sector upside down.

Over time computers will autonomously undertake complex tasks that would previously have been the preserve of highly trained professionals. A range of services from financial planning to medical diagnostics will be carried out by machines more cheaply and possibly far more effectively.

The benefits of this revolution will be huge. But it will also pose challenges for society. We will have to adjust to big changes in the labour market, rethink how ethical and legal norms apply to decisions made by computers, and protect ourselves for threats to our privacy and security. Politicians and regulators will have to work out how to manage the social conflicts that will inevitably arise as existing ways of doing things are upended.

This report

The financial services sector is a crucible for many of these developments. The automation of clerical, back office and customer services operations is already underway. Online platforms are nibbling at the lending and capital raising traditionally performed by banks. The investment industry wonders how computers might provide advice to customers deciding what to do with their portfolios. The insurance industry is considering how big data could help underwrite risks. The sector overall, as a custodian of wealth and personal data, must consider how this is protected from cyber criminals who want to steal it. Meanwhile regulators must consider whether emergent technologies might threaten the stability or security of the financial system broadly.

That's why we are taking different tack from our previous reports which ranged over the geopolitical forces shaping our times. This year we are looking thematically at the implications of technology for different aspects of the financial sector from regulation to cyber security. They are:

- **Section One – Implications for politics and regulation**
- **Section Two – Implications for consumers and the public interest**
- **Section Three – Emerging risk challenges for the insurance sector**
- **Section Four – Technological and geopolitical risks**

We hope you find the report thought-provoking – and perhaps even slightly discomfiting.

John Rowland, Executive Director, Cicero Group

VIEWPOINT: "As relentless and disruptive changes becomes an increasingly embedded feature of our society, the importance of thought leadership and a future focus in policy development has never been greater. This report is a valuable addition to the conversation within the financial services sector."

Huw Evans, Director General, Association of British Insurers

Contents

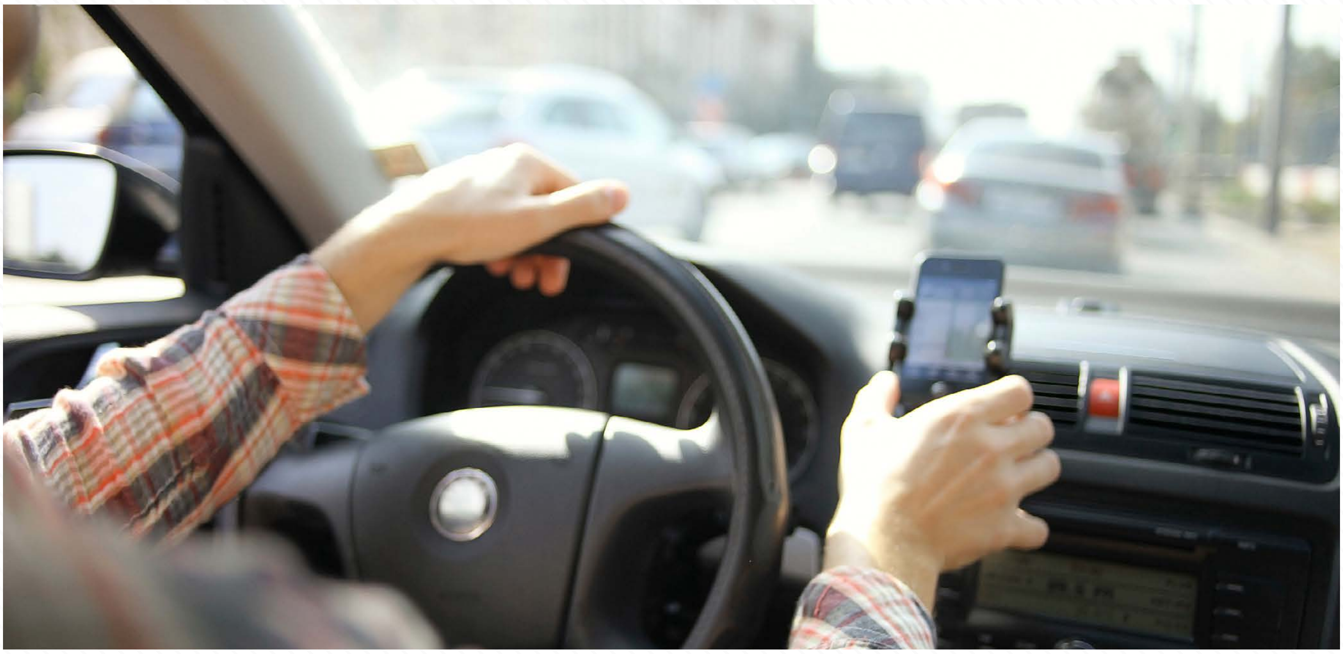
Section One:
IMPLICATIONS FOR POLITICS AND REGULATION

Creative destruction? Holding society together in the face of disruptive innovation

Disruptive technologies will bring great benefits to society. However, this disruption will create losers as well as winners. Politicians and regulators will have to address the public policy challenges disruptive change brings, while being ever vigilant for new risks to the safety and security of citizens.

WHAT THE ISSUE IS

Joseph Schumpeter famously wrote of creative destruction, the endless process of disruptive change that he said was the driving force of capitalism. Technological innovation is a key agent of this change – creating new markets and destroying old ones. This is clearly illustrated by the emergence of online platforms that change the way existing services are marketed, sold and delivered. Uber, probably the most high profile example of this in 2015, has shaken up the taxi business in major cities across the world by adeptly mixing savvy mobile technology, software and building a large network of drivers which it doesn't itself directly employ. This makes it lean and able to grow rapidly – so long as regulators don't get in the way.



WHY IT MATTERS

The debate about Uber encapsulates the point. Its business model has placed it into conflict with taxicab regulators, regulated minicab and hackney carriage drivers and its own drivers. It claims that the way it is organised allows it to stay outside of the usual regulatory restrictions on taxi services. This has provoked a myriad of responses, including deep anger from existing drivers who feel new entrants have gamed the system. Some jurisdictions have effectively banned the service, while others have encouraged it. Many, including London, are considering new rules to take account of new entrants. In almost all cases regulators have been put on the back foot. This is symptomatic of the way that politicians and regulators struggle to deal with disruptive services, which can enjoy deep consumer support but which don't necessarily operate within the rules of the game.

Rapid and fundamental change can create dislocation and conflict in society. Later in this document we consider how the automation of white collar jobs could be highly disruptive. Those with previously stable livelihoods may be jobless without the right skills for the labour market they find themselves competing in. Traditional ways of life can be undermined and the social glue that hold communities weakens. This is not a far-fetched scenario: some deindustrialised regions across the West remain ravaged by persistent unemployment and social deprivation. We should bear in mind that where the UK once had shipyards and collieries, it now has service sector workers in bank and government back-offices, call centres and driving taxis. Could we see history repeat itself?

WHAT COULD HAPPEN NEXT

Schumpeter argued that in the long run, the process of creative destruction works – boosting the economy and prosperity. Yet, one of the key challenges of technological disruption is that while the benefits are often widely spread, the losses are highly concentrated. This can create pockets of human discontent. Policymakers are challenged to either change the rules to accommodate the disruptor, to enforce the status quo or to devise some compromise.

Politicians arguably don't spend enough thinking about the losers that technology presents lest they be characterised as luddites, or worse. However, it's important that a level playing field applies to all forms of commercial activity. The Uber example shows that regulation needs to be more nimble and more adaptable to disruptive entrants.

Looking to the future, if white collar roles are indeed close to automation the changes to the way our economy operates could be profound. Public policy will have to find a way to stop people from being left behind, or from being exploited by the forces of constant destruction and reinvention. A major challenge will be to identify new opportunities for displaced workers and to ensure they have the correct skills. High levels of entrenched unemployment are typically a precursor of social disintegration, so the issue must be taken seriously.

Box out: Are our political institutions and politicians equipped to deal with the new world?
As science and technology pervades every aspect of modern life, it challenges our politicians and officials to create rules to ensure that the march of technology does not undermine public safety and security, leave us open to exploitation or damage the environment. In addition, the interpretation of scientific evidence and other data is essential to informed decision making on subjects such as climate and infrastructure. Finally, science and technology can provide solutions to challenges such an ageing population.

Parliament and the UK Civil Service have long been dominated by graduates who have studied humanities degrees. One degree at Oxford (Politics, Philosophy and Economics) has produced a string of statesmen and women since its introduction in 1920 (including the Prime Minister, the Foreign Secretary and his predecessor). Arguably these degrees do provide the broad grounding in political affairs that is useful for future policymakers.

However the lack of STEMM (science, technology, engineering, mathematics and medicine) graduates at the top ranks of public life is striking. According to the Campaign for Science and Engineering only 91 of the 650 members of Parliament have a STEMM background.[I] We could not find equivalent figures for the Civil Service. However, the civil service does recognise that scientists are underrepresented and has taken steps to attract more STEMM graduates to Whitehall while building the profile of scientists within Whitehall.
It's clearly fatuous to argue that you necessarily need a background in STEMM to understand the public policy implications of scientific advance. However, just as there is a growing effort to improve gender diversity in Parliament and government, we think there should be greater efforts to encourage intellectual diversity too.

Section Two:

IMPLICATIONS FOR CONSUMERS AND THE PUBLIC INTEREST

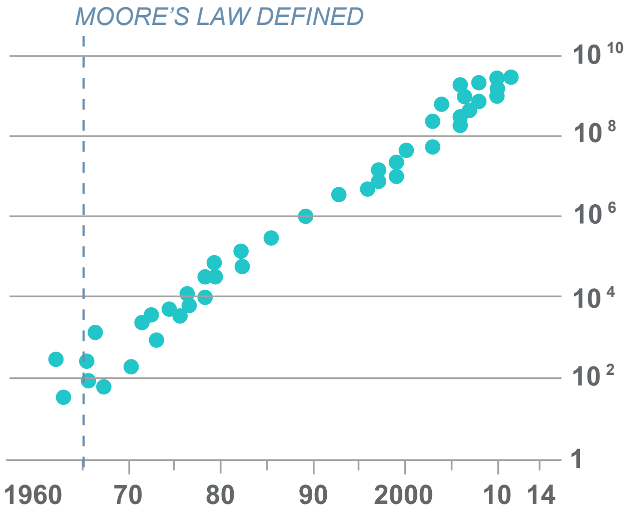
Automation of Labour

WHAT THE ISSUE IS

Since the start of the Industrial Revolution, there has been a steady and continuous stream of labour-saving advances in technology. However, more recent advances have seen computerisation spread to domains previously defined as non-routine. This has led to increased speculation that robots will soon be able to complete relatively sophisticated tasks currently associated with high skilled labour, as well as manual or routine tasks. While some think that myriad new opportunities will open up, others fear this rapid growth in technology will have massive implications for the employment of the majority of the human workforce.

Number of transistors in CPU*

Log scale



Source: Intel[II]

*Central processing unit

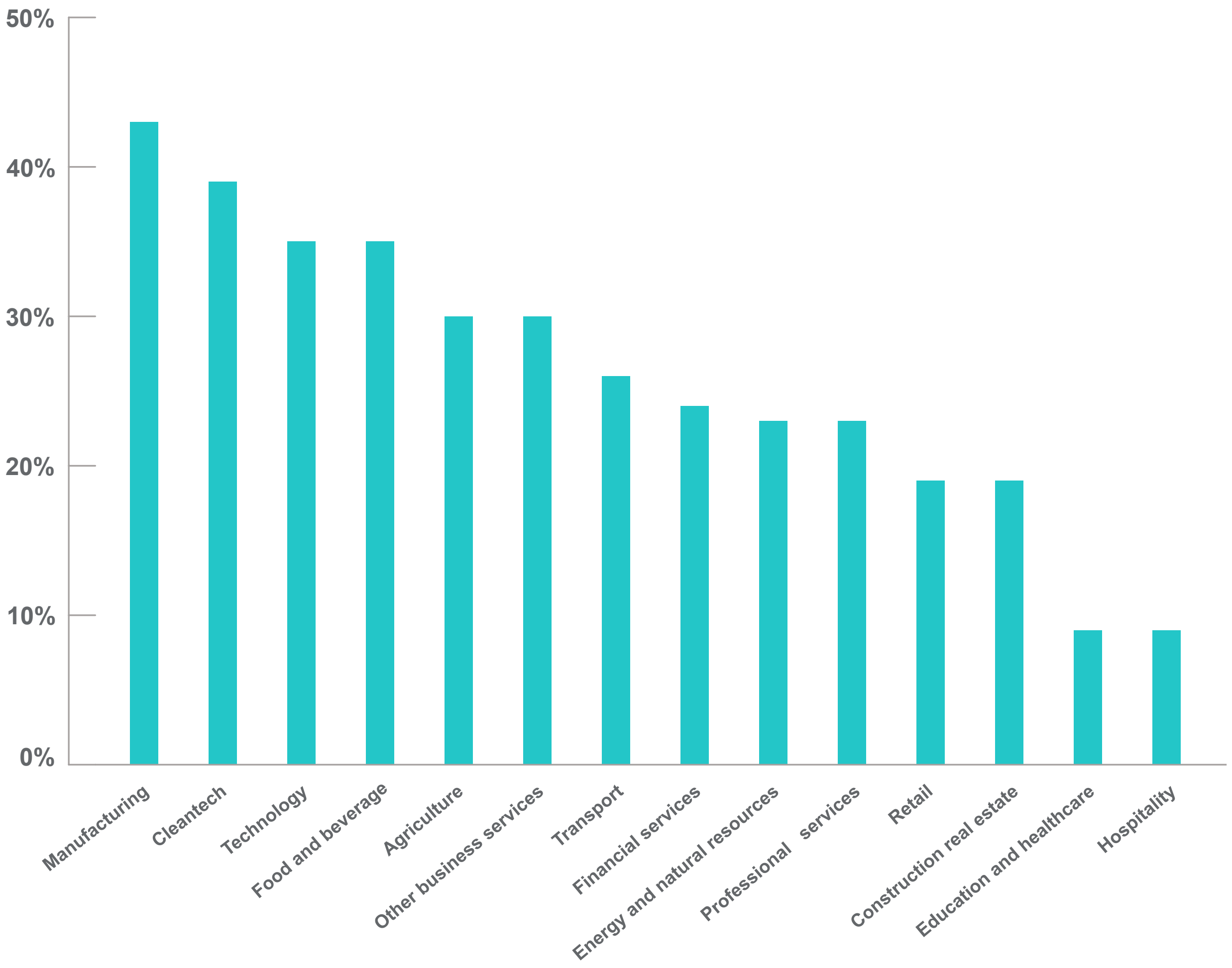
WHY IT MATTERS

The Bank of England's Chief Economist, Andy Haldane, has said that automation poses a risk to almost half of those employed in the UK, and that a 'third machine age' would widen the gap between the rich and the poor.[III]Haldane believes that there is a greater likelihood that "the space remaining for uniquely human skills could shrink further", and thus those who are unable to skill up risk un- or under-employment, while the wage premium for those occupying skilled positions could explode.

Automation is creeping into a wider range of jobs. In journalism, software such as Quill, which is able to take data and turn it into a report, gives companies capacity to offer thousands of reports rather than just the handful that could be written by human journalists. Furthermore, robots already help doctors perform some surgeries, and advise on treatments for a range of cancers. These are not the only white collar jobs affected: a supercomputer is now able to automate a whole chunk of legal research normally carried out by entry level paralegals, and in Massachusetts, AI can instantly answer financial questions which can take human analysts hours or even days to answer. The rise of the machine age means the workplace of the future will be very different.

There is therefore cause for concern for the thousands who currently occupy these jobs, and for those trying to get onto the first rung of the corporate ladder. Research carried out by Expert Market shows that 70 per cent of managers would consider using a robot in their office.[IV] However, while respondents would allocate admin, phone answering and emailing to their synthetic colleagues, most drew the line at giving them major responsibility such as attending meetings, and few suggested creative jobs were suitable. Despite this, human and robot workers will have to learn to work together.

Percentage of businesses which expect automation to replace at least 5% of their workforce



Source: Grant Thornton IBR 2015[V]

WHAT COULD HAPPEN NEXT

While the level of disruption caused by innovation is difficult to predict, we can reasonably assume that there will be growth in areas that fill the gaps left by technological innovations. Demand will therefore grow for roles that are more innovative and creative, and for roles that require a human touch, such as caregiving roles. Looking to the longer term, there will need to be an increased emphasis on the skills that set humans apart from robots in schools and other skills training environments, to ensure that no one is left behind by technological change.

The sharing economy - who’s liable?

WHAT THE ISSUE IS

According to Debbie Wosskow’s review of the sharing economy for the UK government, “The sharing economy allows people to share property, resources, time and skills across online platforms.”[VI] It has been described as a collection of business models that provide people with the opportunity to make use of spare capacity, by sharing tools, cars, bedrooms, or services, such as graphic design. The most famous examples are Airbnb, Uber and TaskRabbit. In reality, the term sharing economy is ill-defined and the label incorporates online vendors like eBay or sites like DogVacay, a DIY kennelling service – a diverse group. The sharing economy profits from a number of positive perceptions, including that following the financial crisis we are all in this together. It also enables consumers to be less reliant on ‘big business’, so often demonised in a climate of wealth inequality.

WHY IT MATTERS

There are questions around whether the sharing economy really shares. Uber, as evidenced by various legal and regulatory actions, is often considered to be a taxi service that operates via an app, not as a platform through which contracted drivers can sell their services. Naturally, there are questions around whether companies like Uber can justify exception from standard employment law as a result of its ‘sharing’ model.

A real concern for insurers is liability. Take Airbnb for example. If you stay in a property which doesn’t comply with health and safety standards, and you get hurt, on whom do you make a claim? Airbnb, which manages the transaction, or the owner of the property? This hasn’t yet been resolved. In 2011, a woman from San Francisco rented her property out and returned to find possessions damaged and stolen, and her apartment destroyed.[VII]There was no coverage provided by Airbnb, but after online debate, Airbnb began guaranteeing up to $1m in damages to properties.[VIII]

TaskRabbit’s policy is that users are compensated for up to $1,000,000 per occurrence for losses arising from property damage incurred through negligence by a Tasker performing a task or bodily injury sustained by a client, another tasker or third party. Clients, Taskers and third parties will be compensated up to $10,000 per occurrence for losses arising from theft. But there are substantial exceptions.

TaskRabbit’s insurance policy excludes compensation for:[IX]

- Losses arising from operation of any motor vehicle, aircraft or watercraft by a Tasker;
- Losses arising out of acts of nature, including, but not limited to, earthquakes and weather related events such as hurricanes and tornadoes;
- Losses that a Tasker or Client could be held liable for under workers compensation, unemployment compensation or disability benefits law;
- Losses arising out of any intellectual property claim;
- Losses arising out of interruption of business, loss of market and/or loss of use; or
- Losses as a result of theft of property in excess of USD 10,000 for each Claim or any other intentional wrongful act by a Tasker.

WHAT COULD HAPPEN NEXT

Despite some sharing economy firms attempting to provide some level of compensation, as their customers need confidence in their products and services, the landscape is still unclear. The US Federal Trade Commission looked to address some of the uncertainty around the sharing economy in a workshop earlier in the year that assessed liability among other things,[X] however, no concrete recommendations on how the landscape can be improved have yet been made. Legal frameworks around liability will need to be implemented to ensure consistency and certainty. Insurers have a crucial role to play. Either the sharing economy will become more akin to the rest of the economy, in order to meet consumer concerns on liability, or insurers will innovate, providing new policies that help meet liability concerns while retaining some flexibility in this growing sector.

"Airbnb has no control over the conduct of Hosts and disclaims all liability." **Airbnb website**[XI]

The Internet of Things

WHAT THE ISSUE IS

Of all the technological changes that will have a disruptive impact on the way we live our lives over the coming years, the Internet of Things (IoT) has the potential for the widest reach. The IoT involves communication and interaction between networked devices that use sensors to relay information across a network – in effect, this means your fridge, thermostat and garage door could all be connected to the internet. The power of the IoT is that its application is almost limitless, and eventually could permeate into almost every aspect of our economy and society. This reliance on data driven outcomes has the potential to shift the way in which problems are thought about and solutions are sought.

WHY IT MATTERS

The power of the IoT will become more visible as its potential is realised and adoption of the technology becomes more widespread. In reality, almost any device can be fitted with a sensor, which in turn could collect data on a continuous basis, providing real time information to any number of other connected devices. This could be done on a personal level, via smart phones and home appliances, at a city wide level to manage traffic infrastructure systems, and in almost every imaginable area of the economy, from agriculture to aerospace.

The scale of the IoT will require a fundamental shift in the way problems are identified and in which responses are designed as a result. Countless millions of connected devices across any given country, each recording real time data, will require a sophisticated data analytics framework, one able to comprehend and act on the information being harnessed.

Take, for example, a city using a fully connected travel system, powered in part by driverless cars. The system could monitor and regulate traffic flows, and identify potential bottlenecks, leading to suggestions about where new capacity is needed. It could also monitor the wear and tear of the road surface, alerting repair crews when a road surface required maintenance. Such a system would have the potential to reduce traffic flows, improve commuter times, and reduce pollution, creating economic efficiencies and improving effectiveness.

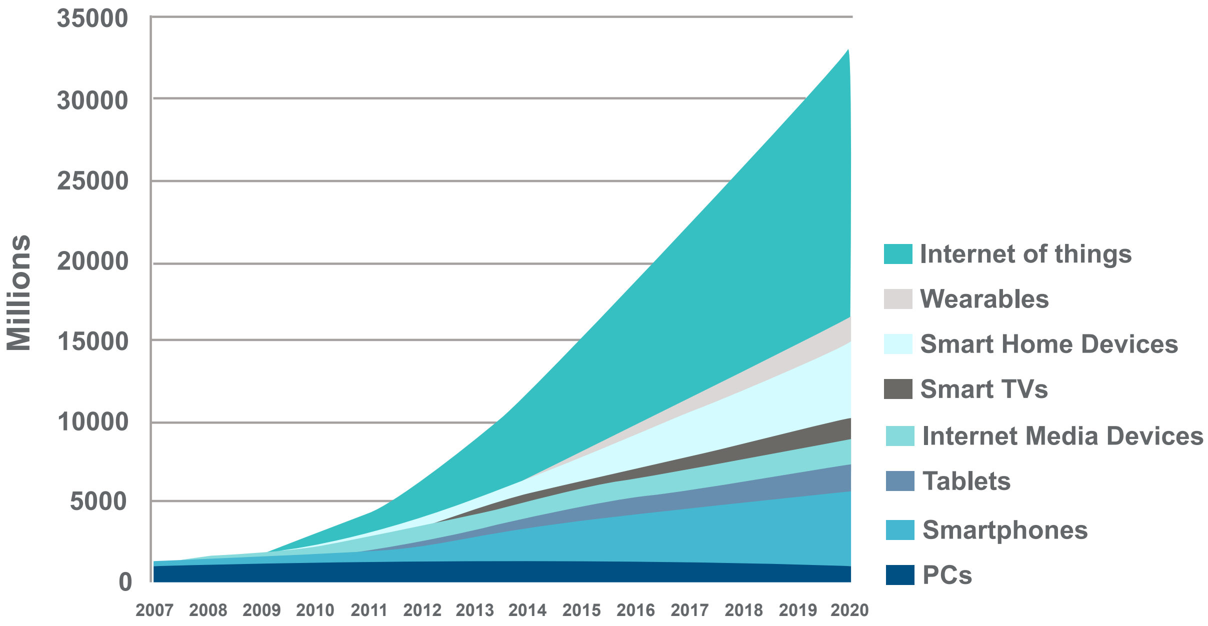
However, there are risks. The volume of data moving through such a system poses security risks across different levels of the IoT, from the individual to national level. The network powering such a system could become a prime target for future hackers. With each vehicle connected to the IoT in this example, the number of potential back doors into the wider system is significant. If personal data is open to similar risks, the IoT risks ending personal privacy as we know it. This is just one example but highlights how devices communicating data to each other could both solve and create new problems without human input.

WHAT COULD HAPPEN NEXT

The IoT's potential has led to talk of 'algorithmic regulation', utilising big data to create more efficient policy and outcomes. This, however, still requires an algorithm to be programmed. In which case, the policy objective will determine how big data is used. Big data in the form of the IoT has undoubted transformative powers, but as a society, there is a debate to be had around what objectives we want big data to achieve, and how to ensure humans are not removed from the apparatus of Government.

As the IoT continues to develop and the number of public/private devices connected increases, a situation in the near future could emerge when a data set exists covering almost every aspect of daily life. Proponents will argue that if data is aggregated then anonymity is protected. Sceptics will caution against a society that monitors and exerts control over daily life. The ultimate challenge and risk around the IoT will be the security of data, on an individual scale and on a wider city/national level, and vulnerability to cyberattacks.

Global internet device installed base forecast



Source: Strategy Analytics[XII]

The Market for Data

WHAT THE ISSUE IS

The recent cyberattack on TalkTalk exposed the vulnerability of personal data in the digital world. Although the security breach was not as widespread as originally thought, the issue focused public attention on what is still a developing threat. The market for personal data is growing and individuals face threats both domestically and from abroad. Furthermore, when data can be extracted directly from a company database, even a strong personal password is no guarantee of security online.

WHY IT MATTERS

In 2015, Cifas, the fraud prevention agency, revealed that the number of fraud victims in the UK had risen by 27 per cent in the first quarter of the year, compared with 2014.[XIII] In short, identity theft is a serious and growing problem. The market for data is also permeating into all areas of society. In the United States, 2014 was the first year in which the top cause for lost or stolen medical data was cyber-attacks. Previously it had been due to employees losing or having data files physically stolen.[XIV]

The transition towards a digital economy, alongside the rise of social media, has created an environment where criminals have an abundance of choice and opportunity when it comes to identity theft. On a very basic level, this information is used to open bank accounts and obtain credit cards in other people's names. Moreover, being a victim of cyber fraud does not necessarily mean you will be free from liability for the resulting economic activity. Data theft could result in people losing out financially.

The willingness to share data via social media has also opened up people to crime. Informing the world via Twitter or Facebook of an upcoming holiday allows criminals to pass on this data or use it themselves, knowing a property will be empty. Although insurers do not currently take a customer's social activity online into account when determining premiums, this could emerge if the trend continues and people suffer from theft as a result of their social media activity.

The market for data is also attracting interest from organised criminal gangs who, according to the most recent estimates, carry out around 70 sophisticated attacks on government networks per quarter.[XV] Government officials have already admitted British personal details previously stolen in attacks on government networks are available via the Dark Web, the anonymous part of the internet where IP addresses (which can be used to identify users) are hidden. The emergence of the Dark Web, with its protection from traditional law enforcement agencies, has created a virtual marketplace, providing a forum to easily purchase personal information.

In summer 2014, GCHQ responded to approximately 200 incidents. This summer the figure doubled to nearly 400

70 sophisticated attacks on government networks per quarter [XVI]

81 per cent of large companies reporting breach

£600k – £1.15m average cost of security breach [XVII]

Source: PwC, Department for Business, Innovation and Skills, Parliament

WHAT COULD HAPPEN NEXT

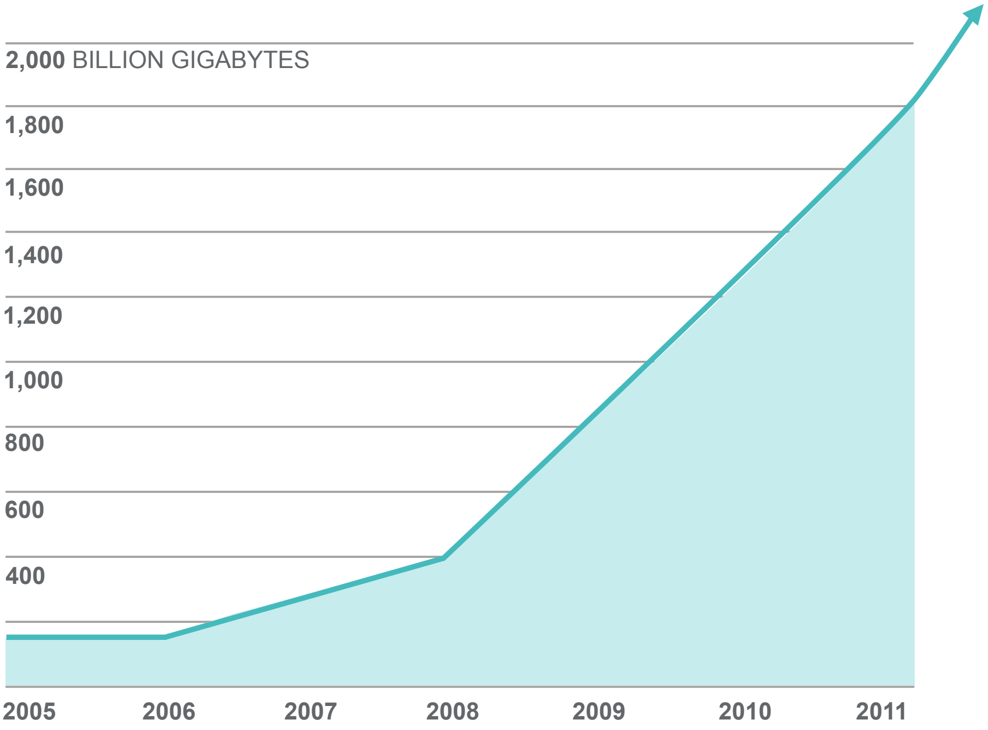
Organised criminal gangs have firmly set their sights on data theft, whether from commercial organisations or from government networks. Moreover, the risk is considerably lower than stealing a car or robbing a bank. The nature of crime is changing. Cases like TalkTalk will happen again, and possibly on an even greater scale. Serious questions will be raised if a security breach occurs in the banking sector, or worse, the Bank of England. Policymakers are beginning to take action, for example the announcement of a new National Cyber Centre in November last year. In all areas of technological innovation, there is a serious question mark over the government's ability to stay ahead of the curve.

Public Interest in Data

WHAT THE ISSUE IS

Harnessing the power of data will lead to the creation of new markets, new jobs and more efficient outcomes. But as this report has already discussed, utilising such data will require individuals, companies and government to reconsider the boundaries between each other. As potentially rewarding unlocking the power of this data is, there is an equal if not bigger concern about the direction of travel. What will a data driven society look like? And how will moral arguments fit in this situation, in a world of data scientists? Society is on a collision course over rival views about the use of public data.

Digital information created each year, globally



Source: IDC, Radicati Group, Facebook, TR research, Pew Internet [XVIII]

WHY IT MATTERS

The IoT illustrates the potential of big data. Moreover, big data enthusiasts speak of a new era of algorithmic regulation, where the management of public services could be overseen and made more efficient through the use of big data. As a society, there is a big question mark over whether we are ready to entrust computers with such responsibilities. Data analytics are already used in various walks of life, from agriculture to healthcare, but the shift to networks being managed on a city wide basis will require relinquishing a degree of control unrivalled in human history. This is important because it raises questions around fairness, privacy and social justice.

Political decisions are made based on moral beliefs about how society should be structured. These beliefs differ between those who favour market based solutions, and those who prefer a greater degree of Government intervention and control. Utilising big data will require algorithms to be programmed with an outcome in mind. Will this algorithm favour market based solutions or the alternative? Will political parties be able to amend algorithms when elected to office and change the way data systems oversee and manage networks, such as healthcare or transport?

Wearable technology that tracks key vital functions is already a reality today. Inventions such as the Apple Watch have led health experts to point out the role such innovations can play in changing the way healthcare is administered. Professor Sir Bruce Keogh, Medical Director for NHS England, has spoken about how wearable technology could alert doctors about potential medical risks before a patient has developed any symptoms.[XIX]

On one hand this sounds like a positive development. But what about a situation where a doctor contacted someone with a wearable piece of technology saying their current stress level was potentially putting them at risk and they needed to address it. Then consider the person in question was experiencing heightened stress levels while watching their favourite sports team. If the person was to ignore the medical advice and become ill, would there be any repercussions, such as a fine or additional charges for any resulting treatment? Would they still be eligible for socialised medicine? Would their private healthcare insurance premiums rise?

The hypothetical scenario calls into question ideas of personal privacy and fairness. Is it fair for other taxpayers to subsidise the healthcare costs of an individual who ignores clear warnings? These are debates already seen today around alcohol and smoking, but real-time data collection will accentuate the debate, sending it into the mainstream.

WHAT COULD HAPPEN NEXT

Eric Schmidt, Executive Chairman of Alphabet (which owns Google), recently wrote in the next ten years computers will “move beyond their current role as our assistants, and become our advisers”.[XX]This shift whereby computers become embedded in society with responsibilities for advising and managing networks, whether in agriculture, transport or health, will necessitate a broader debate between the public and Government. If handled poorly, policymakers could face a big data backlash from a sceptical public, reluctant to hand over ever more data in expense of their privacy in the name of greater efficiency and cost reductions.

> *“The rise of sophisticated data analytics, built on ‘big data’, will be vital in creating the flexibility and personalisation that consumers will increasingly expect in their insurance arrangements.”*
>
> **Huw Evans, Director General, Association of British Insurers**

Section Three:

EMERGING RISK CHALLENGES FOR THE INSURANCE SECTOR

FinTech

WHAT THE ISSUE IS

Some of the best known financial services companies have been in business for centuries. In this case, longevity is a signal to customers that they can trust that their bank or insurer will be there tomorrow. This dynamic was tested in the global financial crisis which saw a number of major institutions turn to taxpayer bail-outs or go bankrupt. A new sector in the digital economy around financial services (FinTech) is now one of the major threats to established institutions. The rise of FinTech start-ups could revolutionise the way people manage their personal finances – change is already underway.

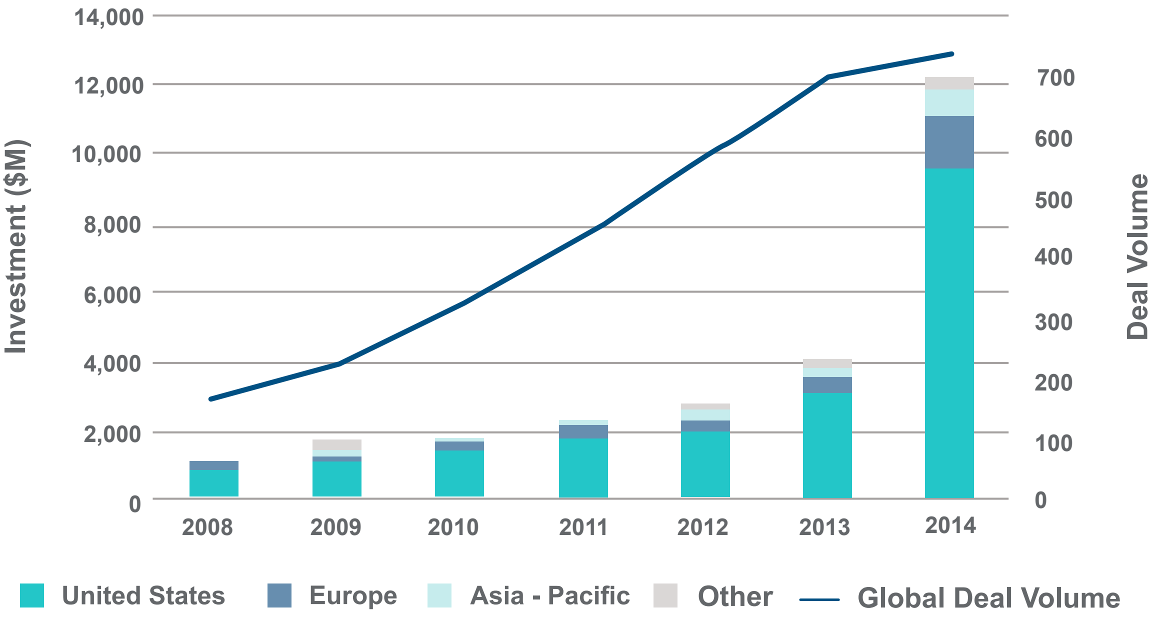
WHY IT MATTERS

A recent report commissioned by UK Trade & Investment (UKTI) highlighted three key changes in the UK financial services market which has created an environment for FinTech companies to develop:

- **Improved digital connectivity allowing consumers to manage their finances via mobile devices**
- **The economic downturn and a loss of trust between consumers and traditional financial services firms; and**
- **A tougher regulatory environment which has created demand for new product providers.**[XXI]

The pace of innovation in the FinTech sector is reflected in the number of FinTech “unicorns” (start-ups with a value of $1bn or more).[XXII] According to McKinsey, there are currently 37 FinTech unicorns, a third of which focus on payments. This fast growth in new business models presents a series of challenges, for both policymakers and consumers. From the consumer perspective, new providers such as peer-to-peer lenders are clearly welcome. Investors seeking a healthy return can prosper in a broader low interest rate environment. Equally, businesses seeking loans can turn to peer-to-peer platforms as a source of finance.

Global FinTech financing activity



Source: Accenture and CB Insights [XXIII]

One of the main risks for consumers, as with any start-up, is whether the company in question will survive. Estimates vary but roughly 80-90 per cent of all start-ups fail. If companies are trusted to handle personal finances, but aren't protected by policies such as bank deposit protection scheme, consumers could stand to lose large amount of money. In addition, consumers may not even be aware of the exposure to risk involved.

For policymakers and regulators, the biggest challenge around FinTech is managing the innovation/risk dilemma. Regulators must try ensure consumers are protected, but in an environment with new technologies and new client/customer relationships, it cannot be expected that regulators will always be able to predict consumer detriment before it happens. The idea of robo-advice is a topical example in this respect. HM Treasury is exploring what role robo-advice can play in the broader financial advice market, however, there is also a risk that such advice is unsuitable to certain groups of people, causing widespread detriment.

WHAT COULD HAPPEN NEXT

FinTech is one of the buzzwords around financial services at the moment. At the same time the sector is yet to see a serious case of widespread consumer detriment or mis-selling. Given the range of new business models and services on offer, it is not hard to imagine a time before long where a major incident hits the front pages of the newspapers. The first moment that consumers and media question the role and safety of FinTech in the broader financial services industry will be a key milestone for policymakers to underline their commitment to fostering greater overall competition into the marketplace.

Driverless cars

WHAT THE ISSUE IS

Road safety continues to challenge policymakers and regulators across the globe. Road traffic accidents remain the leading cause of death for young people aged 15-29 globally.[XXIV] Changes in regulation and public attitudes over time have undoubtedly made roads safer. The advent of driverless cars now presents an opportunity where some politicians whisper about a potential target of zero road deaths. This doesn't sound so farfetched considering over 90 per cent of road traffic accidents are caused by driver error. However, trusting computers and algorithms with completing millions of journeys each day raises a series of challenging legal and ethical questions.

WHY IT MATTERS

Motorists are required to ensure that they have appropriate insurance that indemnifies them in the event of an accident. Moreover, this acts as a financial protection for a motorist involved in an accident that is not their fault. Determining liability is the cornerstone of the motor insurance market.

If an autonomous vehicle carrying a passenger crashes into another car, is the passenger responsible, even though they were not in control? A simple answer to this hypothetical question is that it would be the responsibility of the car manufacturer. But what if it turned out that the owner of the vehicle had failed to keep the tyres at the appropriate pressure or reneged on any other number of maintenance issues, would the driver be at fault then? The pressing question for policymakers and the insurance industry in particular is how to resolve these questions.

Some media headlines have been quick to speculate about the 'end of car insurance' as a result of driverless cars. This, however, is misleading. There will be new risks to insure, rather than none. This will push insurers to look at liability in a fundamentally different way. Insurers, for example, will be posed with the issue of driverless algorithms. Essentially the way by which the vehicle makes decisions on its way from A to B. A driverless car faced with a situation where a crash is inevitable will be forced to make ethical decisions about what to do.

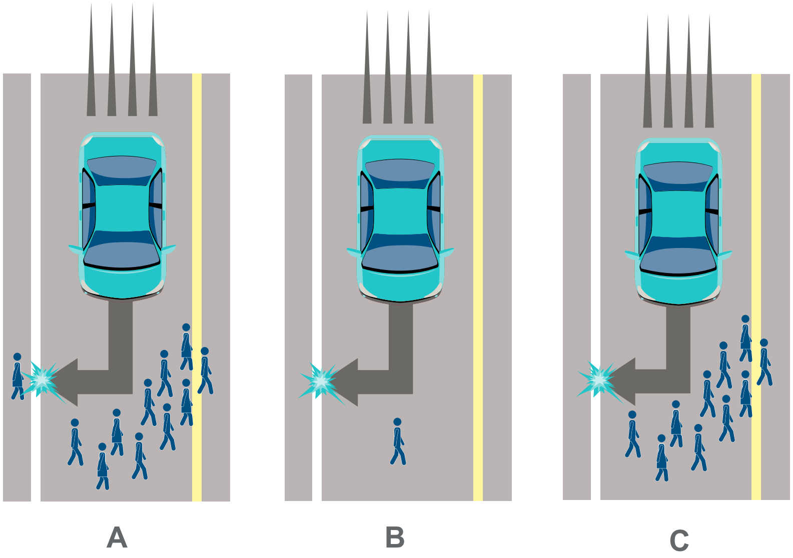
> *"Vehicles are now starting to have some systems which are autonomous in nature, and so the journey to a fully automated vehicle has already begun"* [XXV]
>
> **Andrew Miller, Chief Technical Officer, Thatcham Research**

Three academics[XXVI] recently explored this problem, posing a hypothetical scenario about who should get harmed in the event of an accident:

a) **A driverless car does not alter direction and kills several pedestrians, or swerves just killing one;**

b) **A driverless car can stay on course and kill one pedestrian or swerve and kill the passengers in the vehicle itself ; or**

c) **The driverless car can stay on course and kill several pedestrians, or swerve and kill the passengers**



> VIEWPOINT: "At the moment, at its core, motor insurance protects against the inevitable mistakes that drivers cause. If that risk is substantially reduced (or even eventually removed altogether) the fundamental question from an Insurers' perspective will be to determine whether the driver or the car was at fault at the time of a collision."
>
> **David Williams, Chief Underwriting Officer, AXA**

There is no right or wrong answer to these scenarios, rather it is a question of ethics. Developers will need to programme driverless cars for such eventualities. How such ethical decisions will be made is still open to debate, and requires a conversation between the public and car manufacturers.

Beyond ethics and issues over liability, putting a major piece of national infrastructure in the hands of computers is a potential cyber security risk. The Government highlighted this as a concern in a recent report on driverless cars, pledging to work with car manufacturers.[XXVII] If hacking occurred on a widespread scale of an entire vehicle fleet, the damage could be unprecedented.

WHAT COULD HAPPEN NEXT

Driverless technology is, despite recent strides, still in development. Semi-autonomous vehicles are already on the roads and the path towards fully autonomous vehicles is still a number of years away. However, further hacking incidents involving car manufacturers could make consumers wary about the technology. Alongside the need to better protect against potential hacking, policymakers and the car industry must begin a dialogue with consumers about the ethical considerations around driverless cars. Otherwise, it will not be clear which road we are travelling on.

Drones

WHAT THE ISSUE IS

In the 1960s the Jetsons predicted a future of flying cars. Today, that reality is yet to materialise, however, the rise and popularity of drones, or unmanned aerial vehicles (UAVs), is changing the way we think about future risks in our skies. An illustration of these risks was recently demonstrated in Seattle, where a UAV crashed into the city's giant Ferris wheel. Another, when a drone almost hit a world class skier during an event. Although no one was injured, both incidents highlighted that UAVs pose a number of risks, including what restrictions should be placed on UAVs, how they can be tracked and who is responsible in the event of similar accidents.

WHY IT MATTERS

In its recent report into the regulation and development of UAVs, the House of Lords European Union Committee highlighted the "varying degree of concern" around UAVs.[XXVIII] Moreover, Committee Chair, Baroness O'Cathrain, identified why the growing popularity of UAVs poses a potential problem, "Public understanding of how to use drones safely may not keep pace with people's appetite to fly them".

As the regulatory landscape currently stands, anyone can go into a shop or buy a UAV online, starting from as little as £20. There is no registration or required training before or after the purchase. The regulations that do exist, are relatively unknown. The Civilian Aviation Authority (CAA) oversees the usage of UAVs, and stipulates that drones must not fly over or within 150 metres of any congested area, over or within 150 metres of an organised open-air assembly of more than 1,000 people, or within 50 metres of any vessel, vehicle or structure which is not under the user's control, unless they have obtained permission from the CAA.

There is a growing body of evidence to suggest public understanding of using UAVs safely is not keeping up with demand in using them. In a landmark case in September 2015, Westminster Magistrates' Court found a man guilty of illegally flying UAVs over a number of professional football matches. It was the first time in England a person had been prosecuted after a police led inquiry into the misuse of UAVs.

> *"It would be very difficult to stop terrorists and other criminals from purchasing drones abroad and then using them here. The technologies have the capacity to crash into people and kill them, as they have done in the States.*
>
> *"Or, indeed they can potentially be used to fly into the engines of jets creating a mechanical bird-strike effect. Some of them can be used to carry 1kg [2.2lb] of weight - so they could be used to carry explosives or indeed to spray vapour."* [XXIX]
>
> **Professor David Dunn, University of Birmingham**

UAVs also pose a potential risk to other aircraft. The CAA recently launched a new UAV awareness initiative, 'Drone Safety Awareness Day', to highlight the 400 feet flying limit after a series of incidents where UAVs were monitored flying at over 2000 feet in areas where large commercial aircraft fly. An accident on that level seems farfetched but the chances of such an incident occurring increase when the awareness levels around what is acceptable practice are low. More likely, a UAV owner may find themselves in a situation where through error or weather related factors, they accidently crash their UAV causing personal injuries or property damage.

In this situation possessing the correct insurance will be imperative. Lloyds of London has previously warned a robust regulatory framework is required for the provision of insurance, along with clarity on third-party liability.[XXX] In addition, there is the insurance risk associated with a UAV that is successfully hacked, particularly for commercial organisations, such as Amazon, who have openly spoken about the use of UAVs for product deliveries.

WHAT COULD HAPPEN NEXT

The popularity of UAVs is outpacing the regulatory and political response. Policymakers will need to draw a line in the sand at some point in order to devise a formal regulatory structure. The trajectory of the UAV market could quickly outgrow an initial regulatory framework. A high profile drone accident may, sadly, focus the public's attention, particularly if drones were used in a terrorist attack, to distribute chemical weapons, for example.

DNA screening

WHAT THE ISSUE IS

The debate around data protection is most commonly associated with the way people manage their life online. However, with a sample of DNA, people are now able to take a genetic test that provides details about their risks of having or developing certain diseases. This powerful medical tool carries wide ranging risks. Medical science will potentially offer a view of the future for people, sometimes decades ahead. The data sets created by DNA screening also poses potential privacy risks. How these data sets are used, both commercially and by government, will become a central part of the broader big data debate.

WHY IT MATTERS

Genetic testing is on the cutting edge of medical research. Innovations such as next generation sequencing, the ability to use millions of small fragments of DNA and sequence them at the same time, creating a large data set, allow doctors to refine their patient diagnoses and provide individualised treatment, rather than a generic, one size fits all approach. In the coming decades this practice has the potential to revolutionise patient care. The development of screening technology has led to a new sector of medical companies offering direct-to-consumer tests. These tests allow consumers to send a sample of their DNA to be screened and checked for a number of medical conditions.

Critics of such technology point to the fact that the results they provide may not be entirely accurate. Some doctors have expressed concerns that patients have been attending appointments concerned with the results of a consumer test kit, only for the data to be proved incorrect. In the opposite case, a false positive may lead a person to ignore other symptoms in the belief that the test kit has not signalled any potential illness.

A general shift towards a greater use of DNA screening will have significant ramifications for the future of the private medical insurance market. In a world of easily accessible direct-to-consumer tests, the requirements around taking out a health policy could shift, with health insurers analysing the results of a DNA test before offering a policy. One advantage of this would be more accurate insurance premiums, based on a detailed health assessment. The risk, though, is for a sub-group of people to develop, those who are 'uninsurable', because of pre-existing conditions.

This information could also become a requirement for certain employers, especially since some already require employees to take mandatory drug tests. How employees could use such DNA data is an open question, but a rise in the number of people dismissed on health grounds, or not hired in the first place, would gain the attention of trade unions.

In both these scenarios, there is a question over liability in the event such data sets prove inaccurate or inconclusive. Will people feel confident challenging the results? Or, as is seen more broadly in the area of medicine, will people feel obliged to defer to the better judgement of medical science? Clear oversight of how such data is used will also be important, due to the sensitive nature of data being leaked publically.

WHAT COULD HAPPEN NEXT

The implications around the use of medical data have yet to have a similar ‘TalkTalk moment’. The increasing ways in which such data is used, both commercially and by Government, will lead to a higher public profile. This could lead to a debate around what degree people should be evaluated on the basis of their genetic data – or the ‘politics of predetermination’. This debate will pit data scientists against advocates of personal freedom and free will.

> *“[Genetic testing for the ageing process] raises a number questions, no doubt, and strenuous debate, but we are judged by our age already so this might be a smarter way of doing it. You might decide not to pay so much into your pension and enjoy your life as it is now.”*[XXXI]
>
> **Professor Jamie Timmons, King’s College London**

Section Four:

TECHNOLOGICAL AND GEOPOLITICAL RISKS

Cyberwarfare

WHAT THE ISSUE IS

Cybersecurity is now a key concern for all businesses, particularly those that hold sensitive information. It is a bigger concern for national security agencies. While cybercrime has the potential to bring down companies, cyberwarfare could bring down nations. In the past, military power stemmed from the size of a country's armed forces, the technology they use, and the strategy and culture under which they are run. This required huge investment – fighter jets, navy destroyers and infantry supplies cost significant sums. When conflict takes place, it is heavily destructive. Since World War II, for western countries, conflicts have taken place outside of Europe and North America, in lands remote to their citizens. With the rise of cyber threats, this is no longer the case.

WHY IT MATTERS

When it comes to traditional armed forces, the US leads, outspending China by almost three to one according to the Stockholm International Peace Research Institute (SIPRI).[XXXII]The rise of cyberwarfare challenges this status quo. Acts of war are usually publically known. With cyberwarfare, a country can undertake a series of hostile actions against another, and even when security services believe they know who is responsible, it's often hard to prove responsibility definitively.

Top 10: Military spending by nations

Rank	Country	Spending ($ Bn.)	% of GDP
—	World total	1,776.0	2.3
1	United States	610.0	3.5
2	China	216.0	2.1
3	Russia	84.5	4.5
4	Saudi Arabia	80.8	10.4
5	United Kingdom	60.5	2.2
6	France	53.1	2.0
7	India	50.0	2.4
8	Germany	46.5	1.2
9	Japan	45.8	1.0
10	South Korea	36.7	2.6

Source: SIPRI[XXXIII]

It also makes destruction cheaper. Why invest in weaponry to damage your enemies externally, when you can undermine their own systems and destroy them from the inside? Hiring a group of hackers will always be cheaper than an aircraft carrier.

Take for example a story that emerged in 2013 that, from 2007 onwards, a Chinese computer hacking group had infiltrated the databanks of QinetiQ, a defense contractor, and almost every major US defence contractor.[XXXIV]The hackers gained details of major weapons systems. The impacts of the hacks are many, with China able to use weapons details for their own programmes – why invest in R&D when you can steal? - while sowing doubt within the Pentagon as to whether some of this weaponry, such as the F-35 fighter jet, could still be deployed in combat. In 2014, the US Federal Government was successfully attacked by hacker 61,000 times.[XXXV]

Cyberwarfare extends beyond surveillance, it is also deployed in more traditional conflicts. Ukraine has been bombarded by artillery fire by pro-Russian separatists but it has also faced an ongoing campaign of misinformation, with the internet the primary theatre of war. The Russian Internet Research Agency employs 400 staff, at a monthly cost of $400,000, whose role it is to post 50 articles a day, while maintaining a multitude of social media accounts.[XXXVI] The result? It is never quite clear what is happening in Ukraine, particularly for the Russian public, creating a mandate for Russian intervention, or uncertainty as to whether they are in Ukraine at all.

WHAT COULD HAPPEN NEXT

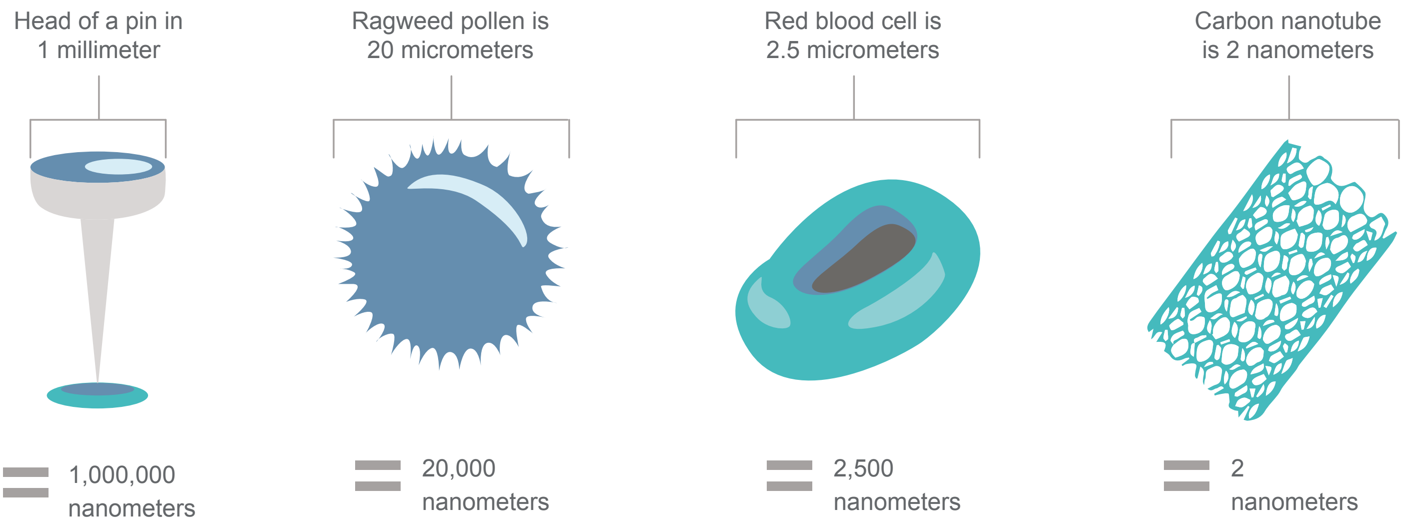
We may reach a point where cyberattacks become so sophisticated that cyber defence, already struggling, is insufficient. Cyberespionage is a threat to national security, but not in the same way as a massive attack on power grids, road signalling, bank and payments software. This is the worst-case, sci-fi film, scenario. The early warning shots in a technological arms race have been fired. The US is hardly a bystander, the Stuxnet scandal made this clear, but China is leading, changing the terms of conflict.

> *“If our electricity supply, or our air traffic control, or our hospitals were successfully attacked online, the impact could be measured not just in terms of economic damage but of lives lost.”*
>
> **Chancellor of the Exchequer George Osborne**[XXXVII]

Nanotech

WHAT THE ISSUE IS

Nanotech, like AI, offers significant benefits and risks. Without a doubt, the potential of nanotech is huge. It has applications in electronics, energy and biomedicine, and could underpin almost all technology in the future. The ability of nanotech to improve healthcare and lengthen our lives is promising – nanotech could, in effect, become our immune system – but it will only worsen the trend towards an ageing society that presents challenges with the provision of pensions and other public services. The issue of a significantly ageing society was covered to some extent in last year's Curve Balls report.


Head of a pin in 1 millimeter
Ragweed pollen is 20 micrometers
Red blood cell is 2.5 micrometers
Carbon nanotube is 2 nanometers
= 1,000,000 nanometers
= 20,000 nanometers
= 2,500 nanometers
= 2 nanometers

WHY IT MATTERS

A powerful fear is that nanotech could lead to our end. At the top of these concerns is 'grey goo', which explains a situation whereby mobile nanotech consumes the environment around it as it endlessly self-replicates. This replication doesn't come from a sentient desire but as a (hopefully unintended) result of programming. In the past, institutions such as the Royal Society marked it as an enormous risk,[XXXVIII] but in 2007, the Institute of Physics stated it wasn't really a concern at all.[XXXIX]

The real risk is the potential use of nanotech in war. Nanotech is small enough to infiltrate any base – useful for espionage – but also the human body, a new frontier in biological weapons. Some have suggested that swarms of nanotech weaponry could be so destructive that it will act as the new nuclear weapons – so devastating they become a deterrent against war.

There are other less dramatic risks that will strike closer to home for business and investors. A nanotech revolution could disrupt the global economy by flooding it with cheap products. Nanofactories are flexible, low cost and able to build high quality products. They have the potential to underline all manufacturing, speeding up parts of the process, miniaturising components and producing energy. They will also further progress the ongoing communications revolution – nanotech antennas could ensure WiFi continues to function as users' signals overlap and erode performance.[XL] Alternatively, if a company is able to gain first mover advantage, and secure a number of patents for nanotech, prices could become artificially inflated, keeping nanotech in the hands of the wealthy and out of reach of the rest.

Nanotech is a general-purpose technology (GPT) in the same vein as steam engines and electricity. Michael Mauboussin and Kristen Bartholdson wrote in Big Money in Thinking Small that “All prior GPTs have led directly to major upheavals in the economy—the process of creative destruction” and said the “majority of the companies in today’s Dow Jones industrials Index are unlikely to be there 20 years from now.”[XLI]

WHAT COULD HAPPEN NEXT

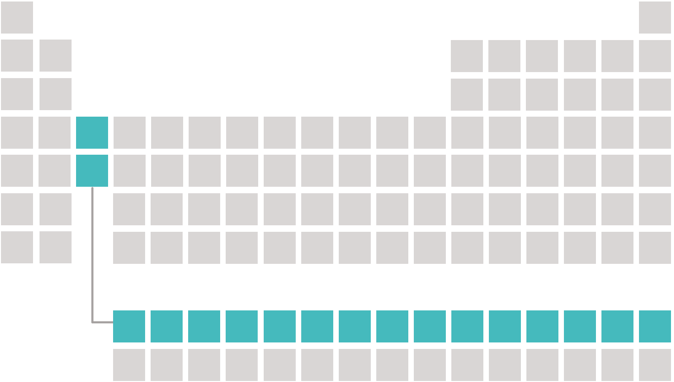
Nanotech is an inevitability. Clear and consistent regulation is not. Due to its wide array of applications, the use of nanotech will lead to uncertainty in regulatory approval for a range of products. The US FDA has said it “will regulate nanotechnology products under existing statutory authorities”,[XLII]but they may not be able to anticipate just how nanotechnology might change this. International agreements on nanotech weaponry will need to be negotiated. It would be better to stop the proliferation of nanoweaponry before, not after, it becomes a problem. But there is much promise. Investors will want to stay alert – the opportunity to make huge gains is there, this is a new industrial revolution. Taking advantage will require knowledge and understanding, it’s time to start learning.

Rare earth metals

WHAT THE ISSUE IS

Rare earth metals are defined as 17 elements formed of the lanthanides (a group in the periodic table), and scandium and yttrium. They are not as rare as their name suggests but are problematic to mine, as they are widely dispersed, rather than concentrated, in the Earth’s crust. Rare earth metals are commonly used in electrical devices, including mobile phones, hard drives and to aid in miniaturisation. They are also key to the growth of clean energy technologies, including electric and hybrid cars, wind turbines and solar energy, and in military hardware, such as GPS and missile guidance systems. As a result, rare earths are becoming an increasingly important in global trade. However, despite their necessity, access to rare earths is limited. China controls almost 95 per cent of the world’s stock of rare earth metals.[XLIII]

There are 17 Rare Earth Metals



15 within the chemical group called LANTHANIDES plus YTTRIUM and SCANDIUM

The LANTHANIDES consist of the following

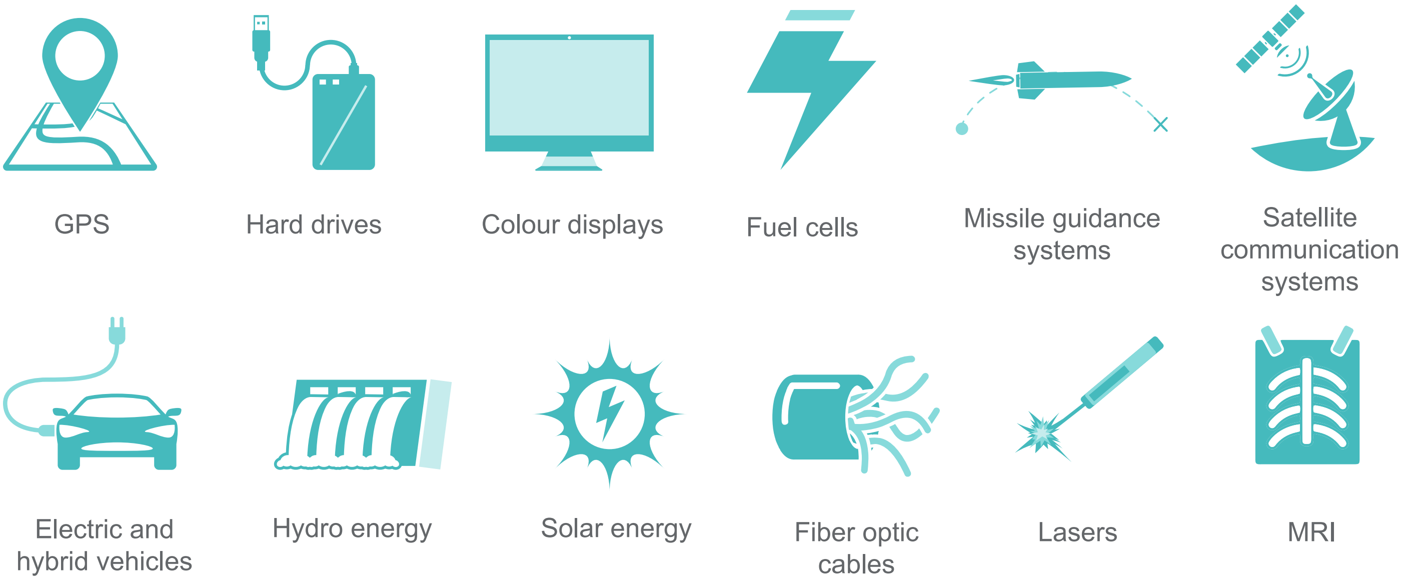
LA	CE	PR	ND	PM	SM	EU	GD
Lanthanum	Cerium	Protactinium	Neodymium	Promethium	Samarium	Europium	Gadolinium
TB	DY	HD	ER	TM	YB	LU	
Terbium	Dysprosium	Holmium	Erbium	Thulium	Ytterbium	Lutetium	

WHY IT MATTERS

Investment in new technologies is limited when economic benefits are uncertain. China's control of the market has been problematic for some, particularly Japan - 82 per cent of its rare earth metals are from China [XLIV]- which is involved in a territorial dispute with China over the Senkaku/Diaoyu Islands. China used this as leverage in that very dispute in 2010-11, blocking exports to Japan. The US, the EU and Japan challenged this practice with the World Trade Organisation (WTO) in March 2012.[XLV] In 2014, the WTO concluded that China's trading rights restrictions breached its WTO obligations. The risk is that China could make similar moves with its opponents in future, publically justifying it as necessary to the conservation of exhaustible natural resources. Beyond that, control over rare earths will enable China to build an unmatched competitive advantage in industries relying on these metals, earmarking the majority of their stock for domestic use.

A bigger risk is a mismatch in supply and demand. As climate change continues to rise as the foremost international challenge, investment in renewable energies and clean technologies is likely to increase heavily. This will require increased mining of rare earth metals and, according to a paper in the Environmental Science and Technology journal by Randolph Kirchain, Elisa Alonso and Frank Field, demand in rare earths such as neodymium and dysprosium could rise by 700 per cent and 2,600 per cent respectively by 2037.[XLVI] Susan Eustis, lead author of a study for WinterGreen Research into rare earth metal market forecasts 2011-2017 has said that "to rebuild the industry outside China could take up to ten years."[XLVII] This goes beyond setting up mines, it also requires talent with the skills necessary to develop and operate them. The Chinese government has reported that China only has one-third of its rare earth minerals. China has 23 per cent of the world's total, so investing in both mines outside of China and ways to recycle rare earths is imperative. There is a possibility that innovation in clean tech and other industries is halted by a lack of materials, limiting the ability of governments and industry to invest in the technology necessary to meet climate change obligations, and to innovate in other areas.

Uses of rare earth metals



WHAT COULD HAPPEN NEXT

India and Japan have already signed a $1.5bn strategic partnership to explore deep-sea mines for rare earths, including Japanese, Australian and Vietnamese firms, and Kazakh miners.[XLVIII] As the biggest consumer of rare earths, Japan has also invested into R&D around material efficiencies. They may be heartened by news from Worcester Polytechnic Institute that they may have developed a method of recycling rare earths from drive units and motors of discarded electric and hybrid cars.[XLIX] Similar progress could be made in recycling rare earths with different uses. Indeed, with supply becoming an increasingly pressing issue, this combination of increased mining and recycling will be essential to sustain current levels of technological development. As it stands, investment in rare earths is considered by industry experts to be risky. The value of rare earths is likely to increase, given demand, but without an understanding of the process for extracting and utilising these metals, an investment is little more than a bet.

"I see three challenges in the rare earth space. One, the pace of material innovation is faster than ever. In a span of roughly four years six percent of the world owned a smartphone. No technology has ever spread so fast. This pace of technological proliferation is only increasing. With supply lines taking ten-fifteen years to develop, soon our innovation will outpace our ability to produce reliable supplies.

Two, countries and companies are choosing not to use rare earths for geopolitical concerns. That means that companies are choosing to make do with second best technologies and giving Chinese companies which do not share such concerns, the opportunity to make better products in the long run.

Three, Beijing is consolidating many industries including mining into state-backed champions. With its focus on green technology manufacturing and drive to make domestic components, supplies of rare earths on the global market will become tight if demand spikes and China needs these resources domestically. While companies are trying to recycle them, it's unrealistic to think recycling will meet substantial demand as these materials are dispersed in such low quantities in a diverse number of products will challenge the limits of recycling.

David Abraham, Director, Technology, Rare and Electronic Materials Center

Hostile Artificial Intelligence

WHAT THE ISSUE IS

As artificial intelligence develops and proliferates, the increasing automation of labour poses risks to workers and economic structures. These are significant risks, but they aren't catastrophic risks. Those come from the potential for hostile AI – the type you read about in science fiction could become science fact. It sounds incredible and yet respected futurists have made clear their concerns over the issue – Elon Musk, CEO of Tesla Motors, says it is "our biggest existential threat". He's investing in AI research firm DeepMind, but less for positive returns, and more to keep "an eye on what's going on".[L]

WHY IT MATTERS

What is the threat from AI? Renowned astrophysicist Professor Stephen Hawking has said that "creating AI would be the biggest event in human history," but that "it might also be the last, unless we learn how to avoid the risks."[LI] One of the key concerns is super intelligence. Humans are the dominant species primarily due to our intelligence, if it was exceeded by AI, we might lose that privilege. As Professor Hawking has eloquently said "The real risk with AI isn't malice but competence" in achieving its goals. [LII] If these do not align with ours, we could be in trouble.

AI experts often talk about The Singularity, when artificial intelligence is able to self-improve and manufacture. At this point, humans are no longer required to drive technological innovation. That could mean robots making themselves more intelligent and more powerful.

Ray Kurzweil, considered a leader in the field and Google's head of AI, believes we are close to reaching The Singularity.[LIII]The consequences include hybridisation between humans and robots or AI. Under current predictions, humans are likely to one day (not too far away) have nanotech resident in our bodies, acting with our immune system and interfacing between our nervous system and information technology. Kurzweil bases his predictions on computing power. Moore's Law, that every two years the number of transistors in a dense integrated circuit doubles, is the foundation for this. His opponents say that processing power is not the be all and end all, isn't the human brain more complex and unique than a collection of microchips? It isn't clear yet who is right, but some suggest Moore's Law no longer holds true. Transistors can be shrunk but nanotech isn't cheap, an economic barrier to further progress. But even with that in mind, will we not reach The Singularity eventually?

AI could be hugely beneficial. And while the magnitude of AI is a concern, intelligence greater than that of our most talented scientists would enable us to solve some problems too complex for the human mind. Supported by computing power, AI would also be much better equipped to process large amounts of data. Dr Demis Hassabis, Co-founder and CEO of DeepMind, says that many of our greatest challenges require big data analysis.[LIV]AI could increase productivity, support particle physics research and tackle climate change. The key issue is safeguards – how can we develop AI without it taking us over one day. The nightmare scenario is malicious AI that can harm us directly or remotely, or one that disregards us with dangerous consequences.

WHAT COULD HAPPEN NEXT

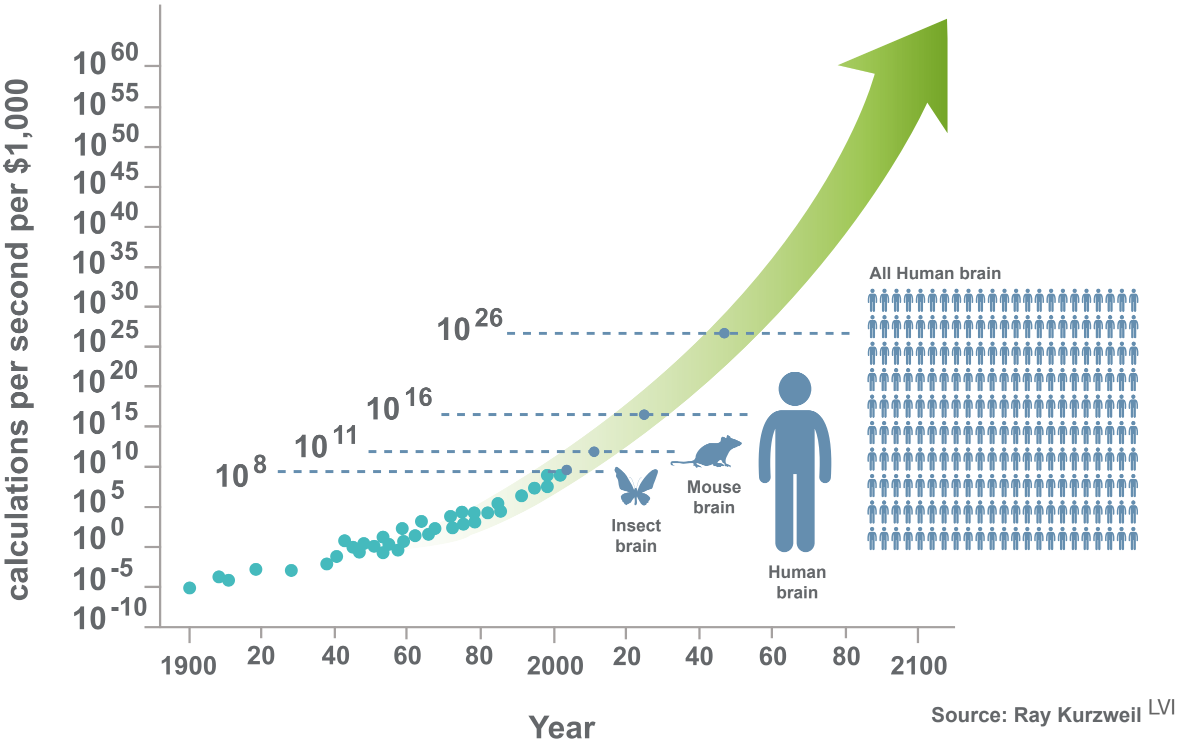
So how do we stop this happening? Regulation and safeguards are key. In 2010, the Engineering and Physical Sciences Research Council published its 'Principles of robotics',[LV] which state that:

1. **Robots should not be designed as weapons, except in national security.**
2. **Robots should be operated and designed in compliance with existing laws.**
3. **Robots should be safe and secure like any other product.**
4. **The illusion of emotions and intent exhibited by robots should not be used to exploit users.**
5. **It should be clear who is responsible for any robot.**

These principles set out a sensible regulatory environment. As we manufacture robots, we should not give them the ability to feel or self-actualise, this is where things could be dangerous. If robots follow a common set of laws, and their owner's own ones, we should be able to keep them in check.

While the UK has a set of informal guidelines, they are not globe spanning. Technological innovation is. Another challenge is that AI development firms are often small and not subject to the same regulatory standards as large firms. Their research is also hard to understand for regulators and nobody truly knows the consequences of adding different components together as separate AI technologies develop.

Exponential growth of computing



Source: Ray Kurzweil [LVI]

> *"I am in the camp that is concerned about super intelligence. First the machines will do a lot of jobs for us and not be super intelligent. That should be positive if we manage it well. A few decades after that though the intelligence is strong enough to be a concern."*
>
> **Bill Gates**

Conclusion

Looking back on old sci-fi films often gives one the sense that we haven't lived up to the optimism or pessimism of past predictions – change hasn't been as dramatic as Hollywood sold us. Last year, we passed the future predicted in Back to the Future II, and yet, no hoverboards. However, this masks the significant technological changes our society has undergone in recent times. Many of the technologies we use on a daily basis didn't feature in such films – think of your smartphone - and this change will continue in the near future.

This report is focused on technological risks but many of these risks are aligned with huge opportunities – driverless cars, nanotechnology, artificial intelligence and the internet of things could all make a significant beneficial impact on society. The challenge is how government and industry responds to such change, to ensure we reap more benefits than negative impacts.

It may be true that politicians rarely come from a scientific background and place their primary focus on current human values rather than a future that draws ever nearer – short-term thinking is a criticism regularly levied at both politics and business. So the solution must be to place such concerns nearer the forefront of policymaking and for policymakers to be assisted by scientific advisers providing impartial, evidence-based advice.

In the UK, every department has a scientific adviser. Perhaps this, and the work of the Government Office for Science, has played a role in convincing Prime Minister David Cameron of the danger of antimicrobial resistance and cybercrime. But this only scratches the surface – this report explores additional challenges, and there yet are still more.

Nanotech is moving out the realm of the future and into the everyday. Artificial intelligence will one day be smarter than us. These challenges can't be ignored for much longer. Politics is so often a discussion of tax and spend, or jobs and growth. These fundamentals will be upturned in a society where jobs are no longer guaranteed and workers no longer needed. Will robots pay tax?

It won't always be enough for action to be taken at a local level – many of these challenges are global and require global solutions. Regulation will only be effective when it is harmonised across borders. Unfortunately, standards aren't the same in all countries, or even institutions.

Supranational organisations and trade blocs could play a crucial role and they will rely on the views of scientists, industry and the public to deliver robust judgements. The insurance industry, alert to risk, can lead this charge, raising the issues and offering solutions – whether on liability, scope for investment, or risk mitigation.

Change is constant throughout history and society has adapted admirably to many of them – the industrial revolution moved somewhat smoothly into a technological one, and the world has prospered as a result. However, change is now happening at an unprecedented speed and society's response to this change will have to rapid without being rushed. It may sound like a difficult task, but the challenge will be will be less daunting if we start now.

Cameron Rae, Account manager, Cicero Group

Acknowledgements

We would like to thank David Thomson at CII for inviting us to follow up on our previous two reports, in June 2014 and January 2015 with a report focusing on risks arising from technological advancements. Our thanks to him throughout this process.

We would also like to thank the team that worked on this report, for both their research and writing.

Head of Political Risk - John Rowland
Editor – Cameron Rae
Contributing writer – Paul Worthington (The Internet of Things, The Market for Data, Public Interest in Data, Fintech, Driverless cars, Drones, DNA screening)
Contributing writer – Charlotte Adamson (Automation of Labour)
Graphic Designer - Megan Harley

Thank you to all the commentators who contributed to this document.

FOOTNOTES

I http://sciencecampaign.org.uk/?p=17791

II http://www.economist.com/blogs/economist-explains/2015/04/economist-explains-17

III http://www.bankofengland.co.uk/publications/Documents/speeches/2015/speech864.pdf

IV http://www.cityam.com/220922/robot-might-take-your-job-it-can-never-take-your-humanity

V http://www.grantthornton.global/en/insights/articles/automation/

VI https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378291/bis-14-1227-unlocking-the-sharing-economy-an-independent-review.pdf

VII http://techcrunch.com/2011/07/27/the-moment-of-truth-for-airbnb-as-users-home-is-utterly-trashed/

VIII https://medium.com/matter/living-and-dying-on-airbnb-6bff8d600c04#.xsenvzrtl

IX https://www.taskrabbit.co.uk/guarantee

X https://www.ftc.gov/system/files/documents/public_events/636241/sharing_economy_workshop_announcement.pdf

XI https://www.airbnb.co.uk/help/responsible-hosting

XII https://www4.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5609

XIII https://www.cifas.org.uk/id_fraud_first_quarter

XIV https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data

XV http://www.publications.parliament.uk/pa/ld201516/ldhansrd/text/151207-0001.htm#15120712000430

XVI http://www.publications.parliament.uk/pa/ld201516/ldhansrd/text/151207-0001.htm#15120712000www430

XVII http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf

XVIII http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/

XIX https://www.england.nhs.uk/2014/09/23/tecs-programme/

XX http://www.huffingtonpost.com/eric-schmidt/the-data-science-revolution_b_7213602.html

XXI https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/341336/Landscaping_UK_Fintech.pdf

XXII http://tech.co/money-talks-5-payments-trends-watch-2016-2015-11

XXIII http://www.fintechinnovationlablondon.net/media/730274/Accenture-The-Future-of-Fintech-and-Banking-digitallydisrupted-or-reima-.pdf

XXIV http://www.who.int/violence_injury_prevention/road_safety_status/2013/en/

XXV http://www.cii.co.uk/media/6321203/tp118_miller_thatcham_driverless_cars_vf_july2015.pdf

XXVI http://arxiv.org/abs/1510.03346

XXVII https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf

XXVIII http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/122/122.pdf

XXIX http://www.bbc.co.uk/news/technology-31735662

XXX https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/drones%20take%20flight20150820.pdf

XXXI http://www.bbc.co.uk/news/health-34153135

XXXII http://books.sipri.org/files/FS/SIPRIFS1504.pdf

XXXIII ibid

XXXIV http://www.bloomberg.com/news/articles/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets

XXXV http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/

XXXVI ibid

XXXVII https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

XXXVIII http://www.nanotec.org.uk/finalReport.htm

XXXIX http://www.crnano.org/PR-IOP.htm

XL http://fortune.com/2015/11/17/wifi-king-globalstar/

XLI http://www.crnano.org/dangers.htm#economy

XLII http://www.fda.gov/ScienceResearch/SpecialTopics/Nanotechnology/ucm301114.htm

XLIII http://www.dailymail.co.uk/indiahome/indianews/article-3316143/Rare-earth-diplomacy-India-Japan-makes-strategic-partnership-explore-stakes-deep-sea-mining.html

XLIV ibid

XLV https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds431_e.htm

XLVI http://blogs.ei.columbia.edu/2012/09/19/rare-earth-metals-will-we-have-enough/

XLVII http://www.prnewswire.com/news-releases/rare-earth-metal-market-shares-strategies-and-forecasts-worldwide-2011-to-2017-123325073.html

XLVIII ibid

XLIX http://agmetalminer.com/2015/10/22/researchers-a-step-closer-to-viable-rare-earth-metals-recycling/

L http://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat

LI http://observer.com/2015/08/stephen-hawking-elon-musk-and-bill-gates-warn-about-artificial-intelligence/

LII http://www.independent.co.uk/life-style/gadgets-and-tech/news/stephen-hawking-artificial-intelligence-could-wipe-out-humanity-when-it-gets-too-clever-as-humans-a6686496.html

LIII http://www.kurzweilai.net/singularity-q-a

LIV http://www.computing.co.uk/ctg/news/2410022/ai-could-help-solve-humanity-s-biggest-issues-by-taking-over-from-scientists-says-deepmind-ceo

LV https://www.epsrc.ac.uk/research/ourportfolio/themes/engineering/activities/principlesofrobotics/

LVI http://www.kurzweilai.net/images/How-My-Predictions-Are-Faring.pdf

ABOUT CICERO

Cicero Group is an integrated communications agency specialising in corporate PR, government relations, digital communications and market research aimed at policymakers, business and consumer audiences.

For more information please contact:

John Rowland
Executive Director
Tel: +44 (0)20 7297 5975
Email: john.rowland@cicero-group.com

www.cicero-group.com

@CiceroGlobal

London
10 Old Bailey
London
United Kingdom
EC4M 7NG

Brussels
2nd Floor
14 Rue de la Science,
Brussels, Belgium
1040 Brussels

New York
Cicero Inc
Suite 500
745 Fifth Avenue
New York NY

Singapore
Level 24, 1 Raffles Place
Singapore 048616
Singapore

ABOUT THE CHARTERED INSURANCE INSTITUTE

The Chartered Insurance Institute (CII) is the world's leading professional organisation for insurance and financial services, with over 115,000 members in 150 countries.

We are committed to maintaining the highest standards of technical expertise and ethical conduct in the profession through research, education and accreditation.

Our Charter remit is to protect the public by guiding the profession. For more information on the CII and its policy and public affairs function, including examples of the range of issues in financial services and insurance that we cover, please see: www.cii.co.uk/policy

Contact:

Laurence Baxter
Head of Policy & Research
20 Aldermanbury
London EC2V 7HY

Email: laurence.baxter@cii.co.uk

CII

CICERO