INSURANCE FUTURES

Hybrid Realities

By Ian Kearns of The Oracle Partnership

FEBURARY 2020

Milliman

It is projected that a trillion devices will be connected to the internet world-wide by 2035, creating a huge and growing Internet of Things (IoT).[1] Among them: smart city, utilities and home technologies, industrial monitoring systems, connected health devices and cars, wearables, and white goods.

This mass deployment of connected devices and sensors will usher in what some have called a Mirrorworld. 'Every place and thing in the real world—every street, lamppost, building and room will have its full-size digital twin.'[2]

In this future, almost everything and everybody will become a source of data. Reality will rarely be experienced without an overlay of additional information relevant to location or circumstance. Alongside this historic shift, we are also witnessing continued growth in the use of virtual reality (VR) headsets and applications, with some suggesting there will be almost one hundred million headset sales a year by 2023.[3] Virtual replicas of the physical world are being built in order to better model and understand the dynamics of environments like homes and cities.[4] Entire virtual worlds are becoming locations for commerce, artistic expression, relationship building, education, and political argument.[5]

The combination of these changes foreshadow the emergence of a new hybrid-reality, in which the physical world, digital representations and extensions of it, and entirely virtual worlds will co-exist, with people moving from one environment to another frequently in daily life. One consequence will be unprecedented flows of real-time data on everything from the state of physical systems and traffic flows to the location and status of individual people. The implications for insurance will be profound.

A New Risk Management Era

When combined with predictive analytics the growing sources and flows of data will facilitate new approaches to the management of both systems and risks.

This is already happening. In the U.K., for example, the water companies are rolling out a networked approach to the management of water resources.[6] The sewage system and water network are increasingly being embedded with sensors that allow remote monitoring and early detection and repair of leaks. Elements of the water management system have also been automated.

In Jinan in China, the ride-sharing company Didi Chuxing and the local authorities are working together to develop a completely new approach to the management of traffic congestion.[7] Didi's fleet of drivers generate a continuous flow of real time locational data as they move around the city, allowing a detailed picture of traffic patterns to be built up. The city authorities have deployed sensors on traffic signals, taking Didi's data on real time traffic flows and synchronising traffic, easing congestion.

The same hybrid reality infrastructure of deployed sensors, real-time data flows and predictive analytics that allows these advances is also being used to manage very specific risks.

In a sign of what is to come AIG and NC4, a California based risk and incident management firm, are collaborating to build risk mapping solutions that provide real-time, site-specific incident detection at locations around the world. This allows notification of incidents to travelers, employees and others who may be in or heading in the vicinity of the incident. Some of these alerts relate to accidents, public disturbances or terrorist attacks and some to issues like public health scares.

AIG is also linking data on patterns of individual driver behavior to location, place history, and distance travelled to generate real-time, usage-based risk profiles of individual drivers. Safer drivers, travelling shorter distances in safer places can be offered lower usage-based insurance premiums. In Ireland, the company has also gone one step further and lobbied the government for legislation to make telematics facilitated usage-based insurance mandatory for drivers under 25, on the grounds that it stimulates safer driving and prevents accidents.

Elsewhere, in a context in which a worker dies somewhere in the world every 15 seconds due to a work-related accident or disease and 374 million non-fatal workplace accidents cost companies in the US alone $220bn a year, firms like IBM have been piloting the use of wearable technology to help keep employees safe.[8]

In one project with North Star Bluescope Steel, sensors have been embedded in safety helmets and protective vests to act as a real time early warning system for employees.[9] These are needed because workers are often operating in high temperature environments containing toxic gas, open flames and heavy machinery. Data on heart rate, body temperature, and skin response is correlated with external sensor data on ambient temperature and humidity in the workplace. North Star management then receives alerts when staff appear to be in danger or discomfort and can personalise safety guidelines for individual employees.

Augmented Reality (AR) and VR systems are also being used to gain a better understanding of risk and to manage it out or reduce it before problems occur. AR for example is being used to improve commercial aircraft safety by 3D scanning of the aircraft exterior to build a digital twin that makes it easier to identify problems that may not be visible to the naked eye. Sensors embedded in aircraft engines monitor engine performance and pick up early signs of stress, part fatigue or breakdown.

Virtual Reality models are being used to simulate major incidents in complex environments so that staff and the emergency services can better understand interdependencies between variables and plan more effectively in advance. In the US, the Federal Emergency Management Agency (FEMA) uses such a tool to allow community leaders to witness flood damage in a neighbourhood, experience the difficulties involved in carrying out an evacuation, and see the impacts of possible mitigation decisions.[10]

As discussed further in the essay in this series on crime, the new hybrid reality technology architecture makes widespread monitoring of public spaces and buildings possible in ways that can help detect and prevent crimes against both individuals and property. Sensors and cameras deployed in the home are being used to monitor and sometimes video unauthorised entry and to issue alerts. In Camden, New Jersey, gun-shot detection sensors have helped create a local sound map that led the police to realise a large number of shots were previously going undetected. Additional officers have been deployed to affected neighbourhoods as a preventive measure in response.[11]

New Vulnerabilities and Risks

Alongside these potential upsides, there are barriers to the full adoption of the emergent hybrid reality and its arrival will bring new threats, potential harms and risks.

Concerns over freedom, privacy and decisions by machines may destroy public trust in virtual monitoring systems. Claims of 'total surveillance' could become significant political flashpoints, placing constraints on the extent of their deployment, undermining their risk reduction potential. Already there are concerns that such surveillance technologies can facilitate the introduction of new mechanisms of social control, like social credit scoring systems that offer points and rewards for certain kinds of behavior while imposing costs and penalties for others. This system is being extensively trialed in China.[12]

The explosion in connected devices is also having an impact on sectors and manufacturers who never anticipated that they could become central to internet security concerns and have therefore done little to make their devices secure. Devices like baby monitors have already been hijacked to launch denial of service attacks on major websites. IoT deployments also often involve one layer of technology being placed on top of another and different generations of devices being connected together. These networks suffer legacy security weaknesses that are not always uncovered. Reliance on extended connectedness also means a growth in complex systems the intricacies and interdependencies of which are not always well understood.

As the scale of connected device deployment grows, the potential for human error to trigger unintended consequences grows with it too, as does the cyber-attack surface that could be exploited by state-sponsored or independent cyber-terrorists and criminals.

A recent survey of US security professionals working in the connected transport, manufacturing and health space found that IoT focused cyber-attacks were becoming widespread. Eighty per cent of respondents said they had experienced such an attack in the past twelve months and over half said their systems had suffered downtime. More than a third also reported data breaches as a result of attacks on IoT devices within their organisations. The potential legal and financial liabilities are mounting, suggesting a cost to businesses in the US alone of around $8.8 billion a year.[13]

For policy-makers, business leaders and insurers alike this is about far more than a new battleground in cyber-security. The potential risks and implications go much wider. As more and more systems become networked and automated, they will take over functions that are ever more central to the running of whole cities, societies and economies. This means that when an attack, disruption or unintended failure occurs the consequences will be cyber-physical and not only cyber in nature.

If and when autonomous cars and trucks rely on GPS technology for navigation and road transport signaling systems rely on other forms of connectivity, successful attacks will almost certainly cause physical chaos, accidents and deaths. When critical water infrastructure systems, partly monitored by networked sensors and managed by autonomous systems, are attacked and disrupted, the consequences could affect water supplies, heating and cooling systems and energy generation plants. They could also trigger a volatile human response, with riots, looting, and physical attacks by one group of people on another if disruption lasts for anything more than a very short period of time.[14]

In such incidents, there may also be spill-over effects from one networked system to another. Many IoT devices and sensors will be very widely deployed across multiple systems. Connections between water, energy, transport and industrial networks may mean an attack that targets a particular device will have effects on multiple networks across several geographies.

The increasing development and deployment of hybrid reality technologies may therefore reduce risks in some areas while creating new risks to companies, cities and society at large in others. The overall risk effect could be that there are fewer major incidents in total but when they do occur, they have higher or even massive impacts.

Implications for Insurance

There will be demand and opportunity to develop and adapt new insurance products and services in this environment. Processes such as claims will be speeded up and automated.

The connected device and sensor explosion also point to continued growth in the cyber insurance market. That said, there will be a need to innovate around cyber exclusion clauses, which may need to end as cyber becomes embedded in wider non-cyber specific policies.

Usage based systems will become more feasible, for example in motor insurance where use of telematics is a major development. There will also be opportunities to use policy content and pricing to change behavior in everything from health and life to motor insurance. Gamification will be easier in the hybrid reality world, with points being acquired for certain behavior patterns, like the amount of exercise taken, leading to rewards and/or reduced premiums for the insured.

Insurers should also be able to build IoT advisory services to help SME's cope with a confusing device and security landscape. They could also work with technology providers and cyber-security companies to offer approved device and product lists as a security improvement and risk prevention measure.

More strategically, insurers could partner with city governments and tech companies to build smart city platforms that drive down risks and costs across city relevant sectors, and 'export' that ability and know-how to others in return for fees. Smart city platforms could also generate revenues via API's made available to others who use access to data to generate new products and services.

While the opportunities are real however, insurers will also face major new challenges.

The complexity and interdependencies of the IoT will generate multiple layers of 'nested liability' that will be contested. Complex and expensive legal battles may follow when incidents occur.

It is also likely that major owners of data and the computing firepower to analyse it will emerge as players in the insurance landscape, since they will be control the data required to facilitate real-time risk assessment and management. Existing insurers that do not form partnerships with data owners, like city authorities and networked device providers will risk being shut out of the game.

There is currently also a gap in IoT risk modelling capabilities that the industry will need to address in order to be able to understand, underwrite and price risk. Doing this will require that different data-sets, owned by different stakeholders, both historic and real-time, be brought together to model the risks.

There will also be a need to blend risk assessments of physical assets with those of cyber-systems to gain a better understanding of the overall risk profile of cyber-physical systems.

Being able to imagine complex scenarios with wide-ranging consequences and to use counter-factual analysis and what if questions will be central to understanding the complexities and possible exposures. Getting at some of this will also mean developing close relationships with those being insured to get a sense of just how their systems are being configured, how they deploy sensors and other monitoring technologies, and the real risks and potential interdependencies that exist in relation to the IoT. VR simulation models might also offer useful tools to model and visualize the risks.

If it can achieve all this, the industry may be well-placed to answer perhaps the biggest strategic question facing it: does it want to work alongside regulators, governments and others to make the hybrid reality world a safe one for all, or is content to think in narrower terms about the risks only to the clients it insures or the assets it holds? The answer will have a major impact not only on the future of the industry but on society at large.

---

1 'One Trillion IoT devices will be produced by 2035' at: https://learn.arm.com/route-to-trillion-devices.html.

2 Kevin Kelly, 'Welcome to Mirrorworld', Wired, March 2019.

3 '2019: The Year Virtual Reality Gets Real' https://www.forbes.com/sites/solrogers/2019/06/21/2019-the-year-virtual-reality-gets-real/#4ed4d9bf6ba9.

4 See for example, a short video on Singapore Virtual City at: https://www.youtube.com/watch?v=Dix-8SNxlAo.

5 Read about virtual worlds Second Life and Sansar at: https://www.lindenlab.com/about.

6 https://www.waterbriefing.org/home/company-news/item/15953-thames-waterto-invest-%C2%A31-billion-to-build-a-digital-first-water-company.

7 How China's meshing ride-sharing data with smart traffic lights to ease traffic congestion, available at: https://venturebeat.com/2017/05/05/how-chinas-meshingride-sharing-data-with-smart-traffic-signals-to-ease-road-congestion/.

8 For more on the data on workplace deaths and non-fatal injuries see the International Labor Organisation at: http://www.ilo.org/global/topics/safety-andhealth-at-work/lang--en/index.htm.

9 North Star BlueScope Steel Taps IBM Watson and Wearable Devices to Monitor Activity of Workers in Extreme Environments, available at: https://www-03.ibm.com/press/us/en/pressrelease/49994.wss.

10 See https://www.fema.gov/immersed.

11 Ian Kearns, 'Crime and the Pros and Cons of the Internet of Things', The Police Foundation, 10th October, 2018, available at: http://www.police-foundation.org.uk/2018/10/crime-and-the-pros-and-cons-of-the-internet-of-things/.

12 It has been oversimplified and misrepresented in some western coverage but is happening, nonetheless. See 'How the West got China's Social Credit System Wrong', available at: https://www.ibtimes.com/internet-things-counting-cost-cyberattacks-2804695.

13 'Internet of Things: Counting the Cost of Cyber-Attacks', at https://www.ibtimes.com/internet-things-counting-cost-cyberattacks-2804695.

14 For a discussion of scenarios such as these, see 'Networked World: Risks and Opportunities in the Internet of Things', Lloyds and the Department of Science, Technology, Engineering and Public Policy at University College London, 2018.

About the author

Ian Kearns has 25 years' experience working in the public, private and NGO sectors, the last 13 of them in leadership positions. He is a former Acting Director of the Institute for Public Policy Research (IPPR), Britain's leading policy think tank, and launched the IPPR All Party Commission on National Security. In 2011, he co-founded the European Leadership Network (ELN), a political, military and diplomatic network of former Prime Ministers, Foreign and Defence Ministers, diplomats and senior military figures across greater Europe. Ian served as the organisation's first Director, establishing ELN as a well-respected feature of the policy landscape on foreign policy and security issues. He serves on the Executive Board of Directors. He has written for The Guardian, The Times, The Independent, Newsweek and The New Statesman and he has been a commentator on the BBC and international media. His recent book, 'Collapse: Europe After the European Union' was published by Biteback in April 2018.

More information on Insurance Futures and The Oracle Partnership can be found at:

oraclepartnership.com/insurance-futures

Milliman

Founded in 1947, we are an independent risk management, benefits and technology firm with offices in major cities around the globe. We serve the full spectrum of business, financial, government, union, education, and nonprofit organizations.

milliman.com