Since the first computer-managed elements entered service in a General Motors auto manufacturing plant in 1961, almost every service and manufacturing industry in the world has benefited from increased automation provided — to a greater or lesser degree — by robotics. And, as industries become more deeply interconnected as a result of the demands of globalization and ubiquitous connectivity, so the very nature of robots will also evolve. However, increased proliferation of robots will bring as many new or accentuated risks as benefits, heightening the need for control over our creations.

Today, there are many different types of robots in commercial and private use, with form factors varying considerably from the static to the fully mobile, from the microscopic to the truly huge and from the single function-specific design to the multi-function, modular types popularised by science fiction.

Risks and threats posed by robots will also vary considerably. This will have a profound impact on how many industries are regulated and insured.

**Industrial robots**
Industrial robots tend to be capable of limited movement and autonomy, programmed to carry out a series of repetitive tasks, often tied to a factory floor or theatre of operations. Service robots, which are increasingly used by the private sector for mundane household tasks, enjoy greater freedom of movement, albeit a freedom ultimately limited by programming or a human operator. Other than careless operation or accidental or wilful obstruction, robot-caused damage to property or injury to humans is exceptionally rare.

By 2050, tens of millions of robots will likely be in use worldwide. Growing demand for fully mobile units — or units incorporated into mobile environments, such as public and private transport means greater operational risks.

**Domestic robots**
Domestic robots have been available to buy off-the-shelf for more than a decade, and a few million robot vacuum cleaners and lawn movers are currently in service around the world. Such devices are beginning to move from luxury gadget or novelty status to affordable utility. Their small size and limited capacity to move around houses or offices unimpeded means that they are yet to become mass-market staples, but advances in programming and build quality will ensure that it happens over time.

The International Federation of Robotics (IFR) estimates that, by 2018, global sales of private-use service robots will increase to 35 million units, including 25 million domestic robots and 9 million “entertainment” robots. Over the 2015-18 period, total service robot sales will amount to almost $20 billion.

Relatively fewer industrial robot sales will be recorded over this timeframe, but their size and complexity means that this market will be worth in the region of $100 billion by 2018.
These values exclude after-sales support, upgrades and ancillary services, for which there will be highly specialised sub-markets.

**Out of the factories and into the home**
Health care, social services, hospitality, security and defence markets are most likely to take advantage of the robot revolution.

More advanced models will be adopted by the professional services market over the next 35 years, with the health care, social services, hospitality, security and defence markets most likely to take advantage of the robot revolution.

**Health care robotics**
In the health care sector, robots are beginning to be employed in physical therapy roles, helping people walk again after an injury or surgery, providing physical stimulation such as massages, or assisting the blind with movement around unfamiliar environments.

The outpatient care sector will also benefit from access to robots. Given the trend of an aging population, it may not be uncommon for the average household to have a robotic care assistant by 2050. Treatment and medication dispensing can be tracked and responded to remotely by human operatives while complex programming can help detect or diagnose changing health conditions.

**Entertainment robotics**
Entertainment robots are also expected to become more popular over time, with models ranging from simple interactive music and video-centric devices to more complex units capable of interpreting changing emotional behaviour to simulate companionship.

Besides augmenting or supplementing traditional children’s toys, such robots could also be used to help physically and mentally impaired youngsters: robots could be used to help autistic individuals learn how to better interact with their fellow humans, for example.

From there, it would not be too great a leap for companion robots to be created for adults. Unsurprisingly, the adult market is also beginning to invest in hardware and software that can take advantage of an increasingly digital-centric culture. Widespread distaste regarding interpersonal relationships with machines will mean that such scenarios will take longer to become commonplace, but will still likely be generally accepted by the end of the current century.

**Liability can be complex**
Programming and human intervention are seen as being key to the successful integration of robots into everyday life. However, human or operator error remains as high a risk in the robot environment as it already does in the analogue or manual environment. This poses considerable risks for the insurance industry, in particular, where identifying root liability in the event of an accident will be exceedingly complex.

Where operator error is clearly identifiable, existing insurance models will continue to be sufficient. However, where human interaction plays such a small or ill-defined part in a sequence of events, it will be very difficult to assign blame and decide which parties should make reparations. New models of degrees of liability are needed; these models will need to evolve in line with robot evolution.

Determining liability will be even more complex where an internet-connected robot must make a series of decisions based on available data.

Where operator error is clearly identifiable, existing insurance models will continue to be sufficient. However, where human interaction plays such a small or ill-defined part in a sequence of events, it will be very difficult to assign blame and decide which parties should make reparations. New models of degrees of liability are needed; these models will need to evolve in line with robot evolution.

Determining liability will be even more complex in a world of ubiquitous connectivity, where an internet-connected robot must make a series of decisions based on available data. Damaged or obscured sensors would yield inaccurate data from which a robot could make the first in an increasing number of wrong decisions, ultimately resulting in damage, injury or loss of life. This is a major concern for hospitals that are beginning to consider investing in computer-assisted surgical devices.

If a surgical robot goes awry due to a faulty sensor, does liability lie with the robot’s manufacturer, with the publisher of its software, with the hospital’s IT personnel, or with the duty operator/surgeon? Few of these issues are adequately addressed by hospitals’ existing insurance packages, and any legal proceedings brought against a hospital could set the robotics industry back by decades, impairing the value of those robots already in commercial use. Such a situation could see the medical industry launch its own counter-proceedings.
Accidents should be mitigated by careful programming, perhaps by using a variation of Asimov’s subtly flawed three laws of robotics (which, in essence, require a robot to prioritise a human’s wellbeing over and above its own and that of its surroundings, either through action or inaction).

What Asimov failed to take into account, considering the simpler times in which he conceived the three laws, was the potential for external malicious interference in a robot’s programming. Today, cybersecurity is a major concern for an internet ecosystem that largely hosts passive devices; in the context of a mobile autonomous robot world, cybersecurity represents a thin dividing line between safety and chaos.

**Robot insurrection unlikely**

The idea that a robot’s “brain” could be influenced to cause it to turn on humans or inflict damage on its surroundings is a well-worn science fiction notion. Fears that an internet-connected robot could be hacked and have its core programming subverted are deeply embedded in mankind’s collective consciousness. In reality, it would be very difficult for any individual or group to weaponize large numbers of robots as we know them today or as we expect them to be by 2050.

Today, a robot’s “brain” exists as much in the cloud as it does in the physical shell of the device itself. While the core operating system for a particular robot could be compromised in the cloud and redistributed back to the machines either individually or collectively, the machines ultimately rely on constant connection to their cloud-based core programs; cutting their access to the internet would therefore take down any rogue machines.

Altering the core programming for a particular model of robot would be very difficult to achieve, if the hacker were unfamiliar with the full coding. A minor alteration would disrupt thousands of core algorithms, and a compromised robot could be detected long before it could enact harmful instructions. This is not to say that the creation of an army of rogue robots could not ultimately be created by hackers; however, with many different types of robots on the market, all using different operating systems and programming, it would be difficult to compromise sufficient numbers in a reasonable amount of time.

That said, as a late-2015 cyberattack on a Ukrainian power station proved, a single brute-force compromised device has the potential to cause considerable damage, enough to justify the expenditure of a sustained hacking attack in the eyes of a rogue state, organisation or individual.

**Threat to human society?**

Some feel the most pervasive threat to human society comes from the increased efficiency and productivity of robots. As jobs in the manufacturing and service sectors are taken by robots, fewer humans will be able to find financially rewarding productive work, with manifold negative impacts on the global economic and social fabric.

**Will robots take the best jobs, leaving humans with the low-paid menial jobs that are not cost-efficient for robots to do?**

In an extreme scenario, with a large, unskilled workforce idle, it could be that robots would take the bulk of premium, skilled jobs, leaving humans to take up the low-paid menial jobs that are not cost-efficient for robots to do. Such a scenario has played out before in previous industrial revolutions and, since governments have yet to develop a coherent policy regarding the impact of robots and a highly automated society, it seems this is a cautionary tale whose lesson is yet to be learned.

As with any new technology and cultural shift, the most fundamental risks will only become apparent over time. Certainly, there will be difficulties in moving society toward a more robot-enhanced footing in the medium term while the technology proves its worth and as design flaws are discovered and overcome.

**Legal and insurance implications**

The legal and insurance sectors will be hard-pressed to keep pace with rapid change, and the risks are high that the requisite frameworks will be found to be wanting in many regards. We can expect an initial surge of resistance from workers’ unions, political opposition parties and small businesses as robotic workforces become more widely employed, followed by a period of acceptance. This is a good opportunity for the legal sector to fully define the parameters of the changing society.

Some cultures will likely feel more comfortable with the notion of robots than others. For example, recent research suggests Asian cultures seem more content to have humaniform robots than their counterparts in Europe and the Americas, where more functional non-humanoid designs are preferred. However, if industry becomes overly dependent on robots, the operational risks regarding the bigger issues of security, socio-economic wellbeing and the mental health of humans will magnify.

The question becomes, how soon will it be before the first cases of “robophobia” are recorded?
The observations, comments and suggestions we have made in this publication are advisory and are not intended nor should they be taken as legal advice. Please contact your own legal advisor for an analysis of your specific facts and circumstances.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW ) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 territories. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.