Scottish Science Advisory Council Report

scottish science advisory council

Cyber Resilience & Future Technology Developments

1. Executive Summary

Current attention in cyber security and resilience focuses on today's attack surfaces and breaches based around existing technology and infrastructure. But what about tomorrow? There is increasing awareness across government, industry and the public about the importance of living and working in a safe and secure environment to safeguard our futures. By looking ahead to emerging new technologies, can we predict what the challenges and threats are going to be so that we can mitigate future risks?

This horizon-scanning report looks ahead up to 2050 and considers likely key technological advances based on current research directions. From the context of cyber resilience and associated technologies, it sets out the Scottish Science Advisory Council's (SSAC) key conclusions in order to inform Scottish Government (SG) work on cyber resilience and associated technologies.

It is clear that future technologies and cyber resilience are inextricably linked and the cyber risks posed today and in the future will accelerate at a global level as we become more digitally connected through improved communications, tools, services and devices.

The SSAC organised a workshop involving leading academic stakeholders from Scotland's universities to discuss the future of cyber resilience in the context of current and emerging technologies. The workshop identified six thematic areas; Technology, Identity & Data, Socio-economics & People, Education, Innovation and Legal & Ethics, with each theme outlining benefits, risks, key points and considerations. A time-line for a technology framework was also captured:

2017 – 2020	2020 – 2025	2025 – 2050
5G communications	7G Space communications	Infrastructure, smart cities
Data ownership	Data - personal ownership	Global data sharing
3-D printing	Advanced manufacturing	Fully-robotic manufacturing
Education	On-line education	Virtual education
Citizen ID	Bio-technologies	Cyborg technology
Electronic health records	Genome health services	Longevity & increasing population
Blockchain	Smart contracts	Crypto banking
Internet of Things	Internet of AI	Internet of nano-things/everything
Quantum devices	Quantum communications	Quantum computing

Technology

In the medium and long term there is rapid technological progress being made. Large investments are already being made in several key areas, for example advanced manufacturing and quantum communications. It is felt that SG support is essential to ensure the success of these industries and this can be encouraged through:

- Setting up technology research and industry briefings.
- Carrying out cyber risk assessment studies for new technologies.
- Creating a database of organisations and supply chains that are cyber secure – i.e. audited and certified.
- Ensuring good technology support services – ensure that software and hardware from manufacturers is continuously maintained so that it does not become obsolete.
- Contributing to UK Government policies such as design for new technologies – CE/kite marking.

Identity & Data

As well as considering technology foresighting, the workshop raised broader issues such as social impacts, legal issues, ethics and education. In particular, the rights of an individual to privacy, protecting identity and personal information was considered fundamental and the recently introduced general data protection regulation (GDPR) was seen positively.

It was recognised, however, that there is a balance between the complexity of restricting access to personal data to ensure privacy, and the benefits provided by living in a digital society and organisations and companies needing access to such information – for example banks and NHS Scotland. The Identity & Data theme discussed this and suggested that the Scottish Government consider:

- Increasing public and business awareness of risks.
- Providing public information help lines.
- Encouraging multi-factor authentication.
- Improving police digital crime and fraud services.[1]

Socio Economics & People

One unexpected outcome the workshop identified was the risk of a growing socio-economic divide. The divide is being driven by those who are capable of using, or able to financially afford to use such technology and services, and those who cannot. We are become more digitally connected and reliant on digital services, e.g. on-line banking and shopping, contactless payments with credit cards, smart metering in homes and ticketless transport systems. This raises concerns that those not able to keep up would become increasingly vulnerable to cyber-attacks It highlights the need to increase the understanding of the ethical

[1] Cyber-crime in Scotland: A review of the evidence
https://beta.gov.scot/binaries/content/documents/govscot/publications/research-finding/2018/03/cyber-crime-scotland-review-evidence-research-findings/documents/00532990-pdf/00532990-pdf/govscot:document/

and social impacts that future digital technologies will bring, and invest in measures that can be taken to educate across the community. Actions for the Scottish Government to consider are:

- Conduct an analysis of the socio-economic divide in order to enable future potential challenges to be assessed and minimised.
- Conduct an analysis of current economic models with regards to cyber resilience and societal impacts and devise a plan to ensure beneficial outcomes.

Education

Scotland's ambitions cannot be attained without education. The Scottish Qualification Authority notes that "Scotland is world leading with the cohesive range of cybersecurity courses at school, college and university levels" and there is a real opportunity for Scotland to become globally recognised as a digitally well-educated country. The workshop identified:

- Marketing, communications and public relations is needed to promote Scotland's reputation.
- Embed education and training on new technologies into courses and curricula.
- There is a shortage in teaching expertise in cyber resilience and computing science.
- Provide broader cybersecurity engagement and education with the public to raise awareness, increase on-line safety and prevent social divide.
- Develop a 'driving licence' for cyber security as a way for businesses and individuals, including school pupils, to show that they are aware and trained.

Innovation

Being able to innovate in a safe, secure country with access to new research and technology creates enormous potential for benefits to society, wealth creation and economic growth across the wider economy such as; advanced manufacturing, financial services, transport systems, education, smart cities, medical services and utilities. This is recognised in the Scottish Government vision *Realising Scotland's Full Potential in a Digital World: A Digital Strategy for Scotland* [2] which states "*Industry believes that the number of people employed in digital technology roles across Scotland has the potential to rise to 150,000 over the next five years."* From a cyber security and resilience perspective Scotland appears to be well positioned to take advantage of a rapidly growing global market - valued at $137.85Bn in 2017 and expected to grow to $231.94Bn by 2022. [3]

Innovation in cybersecurity is essential for Scotland to remain competitive. The workshop suggested the following:

[2] A Digital Strategy for Scotland.
https://beta.gov.scot/publications/realising-scotlands-full-potential-digital-world-digital-strategy-scotland/documents/00515583.pdf

[3] Markets and Markets
https://www.marketsandmarkets.com/PressReleases/cyber-security.asp

- Invest in bringing expertise to Scotland to grow Cyber security research and talent at universities. Capacity building is essential by increasing sustainable critical mass for research and training programmes such as Centres for Doctoral Training.
- Professionally promote Scotland as a cyber innovative and secure nation and brand.
- Establish a national Cyber-resilience research network.
- Invest in cyber resilience incubator hub / innovation centre to increase collaborations amongst investors, academia, public sector and private sector.
- Fund speculative high risk, high growth disruptive innovation projects.
- To keep up-to-date with advances in this sector it is also suggested that regular technology, research and industry briefings are set up for the Scottish Government.
- This could be further reinforced through undertaking cyber resilience risk assessment studies for new technologies to ensure policies and risk mitigation can be implemented.

Legal & Ethics

One of the challenges is for legislation and industry standards to keep pace with technology. This raises a broad range of ethical issues for the cybersecurity industry to face. The workshop highlighted the importance of education, accelerating legislation and raising awareness and suggested the SG consider:

- Forming an ethics committee to address cyber security issues and act as an advisory body.
- Providing cybersecurity ethics workshops and raising awareness across education courses and communities.

2. Report Aims and Commission

The Cyber Resilience Unit in the Scottish Government (SG) commissioned the Scottish Science Advisory Council (SSAC) to deliver a report considering cyber resilience in the context of future technology developments. The specific aims were to help future-proof SG policies, and to consider potential new risks and likely advances.

The SG recognises that advances in technology are accelerating and that it is therefore of growing importance that public policy and services are not left behind due to obsolescence, or become more vulnerable to future attacks. It is also important that SG policies are agile enough to take advantage of opportunities that new technology may offer.

The SSAC was asked to consider a range of topics within this report including, but not limited to: data, devices, artificial intelligence, nanotechnology and augmented reality. Consideration of cyber-crime and its ability to use these advances were also part of the brief.

The SSAC provides independent advice, through its Chair, to the Chief Scientific Adviser (CSA) for Scotland and to Scottish Ministers, including the First Minister.

The aims of the SSAC are to support the Scottish Government to make effective use of science advice, knowledge and techniques when formulating and implementing policies, further enhancing Scotland's status as a science and innovation nation, and supporting Scotland's Economic Strategy's two mutually supportive goals of increasing competitiveness and tackling inequality. It carries this out by:

- Providing scientific advice to inform Scottish Government policy and priorities;
- Providing advice on developments in science and technology and implications for policy areas that are underpinned by or affected by science; and
- Developing advice based on a medium to long-term, horizon-scanning, strategic view to identify and harness future opportunities and mitigate future threats.

3. Background

Cyber resilience is defined as the ability to continue to use digital technologies despite adverse cyber events. It covers areas such as information security, business continuity, incident management and forward planning.

As part of cyber resilience, it is important for any organisation, including governments, to recognise advances in technologies and to recognise opportunities and risks that may arise.

Scotland has an enviable reputation for world class education, research and innovation with four universities in the world's top 200.[4] Areas of excellence for research and development across the computing sector include cyber security and resilience, cyber governance, digital forensics, ethical hacking, blockchain, cryptocurrencies, artificial intelligence and machine learning. Cyber resilience centres of expertise are now present across many universities. The University of Abertay was the first in the world to provide a degree course in Ethical Hacking and its MSc course has been recognised with NCSC certified accreditation.

Likewise Edinburgh Napier University has an NCSC certified Degree and MSc in Advanced Security and Digital Forensics and has created the Cyber Academy and Security Operation Centre for training (SOCLab). Glasgow Caledonian University also covers digital forensics and has a focus in secure networks. The University of Glasgow specialises in securing critical and national infrastructure and also has expertise in human computer interface (HCI) and quantum technologies. The University of Edinburgh is one of only 14 universities in the UK to have NCSC Academic Centre of Excellence in Cyber Security Research (ACE-CSR) status. Its expertise is broad, from robotics to AI and machine learning, bio-informatics, programming languages, Internet of Things and Blockchain - through the Block Chain Technology Lab.

Other areas include advanced manufacturing at the University of Strathclyde and 5G at the University of West of Scotland. Unsurprisingly, the University of Aberdeen and Robert Gordon University have resilience and technology expertise in the offshore oil and gas and the renewables industry. From a wider perspective, Dundee University works closely with Police Scotland, and is a founder of the Scottish Institute of Policing Research. The University of St Andrews has specialisms in cloud systems, but also expertise in International Security and Critical Security. This is synergistic with Stirling University which specialises in global security and diplomacy.

Of course, the areas of research and the capability of Scotland's universities are broad. Research pools such as the Scottish Informatics and Computer Science Alliance (SICSA) bring together research collaborations across universities through research themes - cybersecurity, cyberphysical systems, AI, data science, HCI, networks and systems - and deliver Scotland-wide programmes such as the SICSA Cyber Nexus. The Scottish Funding Council has established a number of Innovation Centres to support interactions between Scottish universities and businesses, working in collaboration with Scottish Enterprise and Highlands

[4] The Times Higher Education World University Rankings 2019.
https://www.timeshighereducation.com/student/best-universities/best-universities-scotland

and Islands Enterprise. Their focus on translational research is designed to recognise and address the disparity between HERD and BERD. [5] In Scotland compared to other countries. From a cyber resilience perspective these centres, for example, the Digital Health and Care Institute, the Data Lab and CENSIS, have a growing cyber resilience focus since it cuts across many of their activities.

All of this expertise and know-how places Scotland in a strong position to exploit research and future technologies and to become a world leader in cyber resilience, providing opportunities for Scotland to be a beacon of forward thinking and good practice.

[5] Higher Education Research & Development and Business Enterprise Research & Development performance. https://www.gov.scot/Topics/Statistics/Browse/Business/RD/KeyFacts

4. Scottish Government approach

The Scottish Government vision *Realising Scotland's Full Potential in a Digital World: A Digital Strategy for Scotland* [1] recognises the need to be a cyber resilient safe and secure nation. This is encompassed in their Cyber Resilience Strategy *Safe, Secure and Prosperous: A cyber resilience strategy for Scotland* published in November 2015 [6] which states - "*Cyber resilience is being able to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world.*"

The outcomes of the cyber resilience strategy are that by 2020 Scotland can be a world leader and:

- Our people are informed and prepared to make the most of digital technologies safely.
- Our businesses and organisations recognise the risks in the digital world and are well prepared to manage them.
- We have confidence in and trust our digital public services.
- We have a growing and renowned cyber resilience research community.
- We have a global reputation for being a secure place to live and learn, and to set up and invest in business.
- We have an innovative cyber security goods and services industry that can help meet global demand.

The Scottish Government aims to deliver these outcomes through action plans:

- Ensuring citizens have access to basic and specialist *learning and skills* [7] to help keep them safe and secure online.
- Working with partners in the *public, private and third sectors to enhance cyber resilience.* [8]
- Raising awareness of the importance of cyber resilience and how to achieve it, by providing easier access to authoritative *advice and support.*
- Taking advantage of the *economic opportunities* [9] resulting from greater cyber resilience.

To ensure that these outcomes and actions are supported, this report helps in the journey to understanding the importance of future risks and opportunities.

[6] Scottish Government. Safe, Secure and Prosperous: a cyber resilience strategy for Scotland. https://beta.gov.scot/policies/digital/cyber-resilience/

[7] Scottish Government. Cyber resilience Learning and Skills action plan. https://beta.gov.scot/policies/cyber-resilience/learning-and-skills/

[8] Scottish Government. Cyber resilience public, private and third sector action plans. https://beta.gov.scot/policies/cyber-resilience/public-private-third-sector-cyber-resilience/

[9] Scottish Government. Cyber resilience Economic Opportunity action plan. https://www.gov.scot/policies/cyber-resilience/economic-opportunity/

5. Context

Technology and cyber resilience are inextricably linked and the cyber risks posed today and in the future are changing at a global level. The World Economic Forum – *The Global Risks Report 2018* [10] highlights these dangers and risks to our infrastructure, services and way of life as the world becomes more interconnected, complex and automated. For example, the number of Internet of Things (IoT) devices was estimated at 8.4 Billion in 2017 and projected to reach 20.4 Billion by 2020 – far outstripping the human population of 7.6 Billion.

The vulnerability of IoT devices and their potential misuse was clearly demonstrated with the cyber-attack on company Dyn Inc, through a Distributed Denial of Service (Ddos) Mirai IoT botnet attack in October 2016.

> The DDoS Mirai botnet malware used over 100,000 IoT devices across the world – By exploited the device manufacturers default passwords and hardware settings, cameras, routers and baby monitors were compromised. The devices were then used to simultaneously increase internet traffic to their target Dyn – at over 1.2 Terrabytes / second. Unable to cope with these data speeds, the impact was to disrupt Dyn Domain Name Services (DNS) preventing their customers' services and websites operating. This disruption brought down web services across organisations as large as Amazon, Reddit, Netflix and Twitter. This was the largest attack of its kind in history.
>
> – Mirai was superseded a year later with Reaper, which further exploits IoT weaknesses.

Over the past two years ransomware attacks have also been highlighted. The Wannacry global ransomware attack in May 2017 was followed two months later by a variant, Petya.

> Wannacry hit the news in the UK in May 2017 with disruption to NHS systems. This was a random, try and hit everyone, global cyber ransomware attack using a cryptoworm (Wannacrypt) which could automatically install and duplicate itself once inside a system. When activated the malware encrypts the computer system data and displays messages demanding ransom - to be paid with bitcoin - before 'promising' to return the computer to the users control.
>
> WannaCry exploited computer systems that had not been updated with software 'patches'. Disruption to NHS systems showed the complexity in protecting large IT infrastructure. This 'wake up' event has shown how vulnerable IT systems can be and how seriously government, organisations and individuals must take cybersecurity protective measures.

[10] The World Economic Forum. The Global Risk Report.
https://www.weforum.org/reports/the-global-risks-report-2018

Looking to the future and the benefits technology can bring, the UK Government Office for Science published its own *Technology and Innovation Futures 2017* report. [11] The report recognised the potential to increase productivity and the efficiency of public services, if the UK and its government can create opportunities from increased interactions between technologies and data. This can be achieved by, for example, improved digital infrastructure by putting in place standards (i.e. for technological interoperability) and coordination of effort in government.

Recognising potential risks to future economic growth, the UK Government published the *National Cyber Security Strategy 2016 - 2021* [12] with the vision "*that the UK is secure and resilient to cyber threats, prosperous and confident in the digital world*". This is based around three themes: defend, deter and develop and is designed to ensure that the UK is able to defend against and respond to cyber-attacks, that it makes itself a hard target whilst taking the offensive when appropriate and that the UK has a strong and skilled cyber security industry.

Dixons Carphone Warehouse has been issued with one of the largest fines (£400,000) by the Information Commissioner's Office (ICO), after one of their computer systems was compromised as a result of a cyber-attack in 2015.
The company's failure to secure the system allowed unauthorised access to the personal data of over 3 million customers and 1,000 employees.

The compromised customer data included: names, addresses, phone numbers, dates of birth, marital status and, for more than 18,000 customers, historical payment card details.

Even with tighter processes in place in July 2017 Dixons Carphone has admitted another huge data breach involving 5.9 million payment cards and 1.2 million personal records. This is currently being investigated through NCSC and ICO.

Linked to this strategy the National Cyber Security Centre and National Crime Agency (NCSC and NCA) published *The cyber threat to UK business 2017/2018 Report*. [13] The report summarises current threats and also provides horizon scanning of future threats – again, predicting attacks on industrial connected devices and IoT technologies. The report also recognises the challenges and opportunities businesses face to mitigate risk through using technology, people and processes and the seriousness demonstrated with recent EU policy and legislation (GDPR and NIS), and the Financial Conduct Authority and ICO implementing financial penalties too.

[11] Government Office for Science Technology and Innovation Futures 2017.
https://www.gov.uk/government/publications/technology-and-innovation-futures-2017
[12] National Cyber Security Strategy 2016 – 2021.
https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
[13] NCSC and NCA published - The cyber threat to UK business 2017/2018 Report.
https://www.ncsc.gov.uk/cyberthreat

The cyber security industry is also watchful. FireEye's *Looking Ahead – Cyber Security in 2018* [14] considers a range of short-term predictions ranging from increases in ransomware (perhaps GDPR related), phishing and malvertising, the risks of putting critical data on the cloud, nation state attacks and infrastructure resilience.

Gartner too have published their *10 Strategic Technology Trends for 2018* [15] which includes looking ahead over the next five years. Artificial Intelligence (AI) is seen as the key enabler across industry by supporting digital technology, smart cities, autonomous vehicles, computer vision and speech. IoT including people, places and things will be more connected and will also present a greater risk. Interaction with technology will also increase through immersive and augmented reality. Digital businesses will be event centric – continually sensing and adapting to a changing world. Consequently, security and risk assessment of trust must continuously adapt too.

Trying to make predictions into the longer term, to 2050, is clearly more speculative. Areas such as quantum computing, biological computing technology, human sensor implants and perhaps even living off-planet seem to be in the realm of science fiction, but many of our technology developments are moving in this direction. Kaspersky Lab has created an interactive *Earth 2050* [16] where dreamers and innovators predict the global, technological and cyber threats over the next 30 years.

[14] FireEye. Looking ahead Cyber Security in 2018.
https://www.fireeye.com/blog/executive-perspective/2017/12/looking-ahead-cyber-security-in-2018.html
[15] Gartner *10 Strategic Technology Trends for 2018.*
https://www.gartner.com/doc/3811368?srcId=1-6595640781
[16] Kaspersky Lab Earth 2050.
https://2050.earth

6. SSAC Cyber Resilience and Future Technologies workshop

The SSAC organised a workshop involving key academic stakeholders (Annex A) to discuss cyber resilience in the context of future technologies. The aim was to consider the likely advances in this field up to 2050 and to provide considerations to the SG.

The plan for the workshop and aims and outcomes of the day were based on the project brief from the SG Cyber Resilience policy team.

Key questions considered were:

- how can SG policies be robust in a fast-changing world?
- what future risks might require new or updated SG policies?
- what are the opportunities?
    - for developing research excellence
    - for innovations & economic growth

Discussions were centred on a number of timeframes and themes and considered the following:

- Threats, risks, and vulnerabilities
- Opportunities & risk management
- Impact on individuals, families, business, public services, research

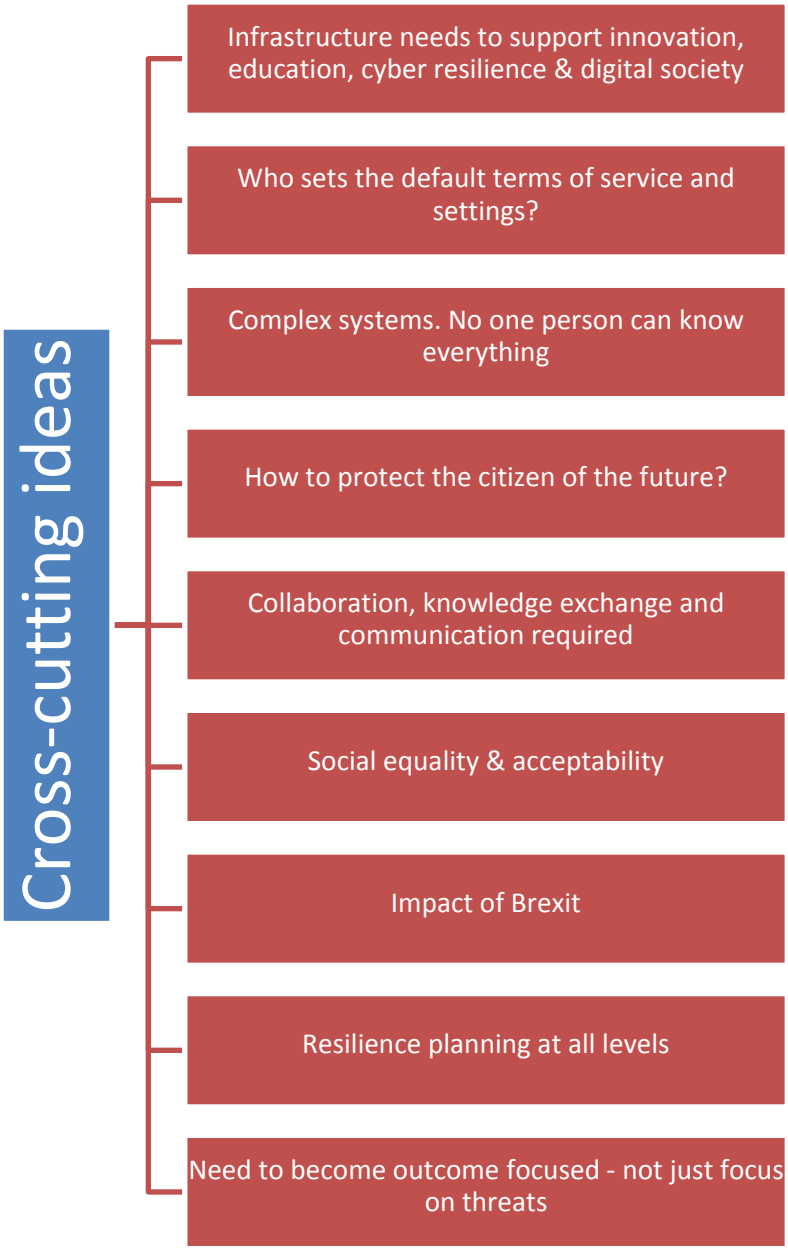
In addition, the social and economic aspects of cyber resilience were debated including trust and confidence, costs to the public, government and business, personal resilience and education.

7. Themes

Six key themes emerged from the workshop – the benefits, risks, key points and considerations for each are detailed below.

Although the themes can be considered separately, there was considerable overlap and cross-talk amongst them, which was reflected by the workshop discussions. The complexity of the feedback is captured in the workshop wordcloud.

There were also a series of cross-cutting ideas from the workshop that are applicable across the different themes and further indicate overlap.



7.1. Technology

Summary

Predicting new technologies can be challenging; however, there are a number of likely future technologies or current technologies that will advance and have significant impacts in the future. The technology areas most likely to have the greatest impact over both the short and long-term are:

- Artificial Intelligence
- Machine learning
- Nanotechnology
- Virtual reality
- Robots
- Internet of Things
- Autonomous vehicles
- Voice recognition and control
- Blockchain
- Medical
- Cloud computing
- Quantum computing

It is important to be aware of advances in both software and hardware and, critically, there is a cost in investment, time and effort required to keep up with these advances. In effect, this is the price individuals, organisations and businesses pay to benefit from living and operating in a digital world. The workshop also highlighted concerns of increasing obsolescence of technologies. We have seen cyber breaches in the past and managing legacy systems and maintaining current technology will continue to pose a substantial challenge for organisations, businesses and individuals.

Benefits

There are many potential benefits and opportunities arising from advances in technology, e.g. Internet of Things, robotics, digital services and 'smarter' homes and cities that will help improve our lives. Businesses too will benefit from improved communications, logistics and efficiencies. For example, digital 4.0 and advanced manufacturing will create new innovations in bespoke manufacturing allowing products to be made on demand to customer specifications.

The manufacture and availability of bespoke products using technology such as 3D printing will also develop significantly over the short and long-term and the diversity of products available will also grow.

Advances in technology through robotics and autonomous machines (including cars) will also develop rapidly and provide numerous benefits to individuals and to the public sector. The

application of artificial intelligence and machine learning to new technologies promises improved healthcare services in hospitals, at GPs and at the home.

These technologies are also benefitting from improved cybersecurity capability, for example 'smarter' data analytics, artificial intelligence, end-to-end point technology, multi-factor verification and authentication and improved chip level hardware for digital encryption.

Risks

The risks associated with introducing new technologies are well known. Finding early adopters and creating new business growth remains a challenge. However, the pace and scale of innovation is moving faster than ever. Those who do not have access or understanding could risk being left behind and not coping in the digital world.

There are some specific risks too. An increase in autonomous machines, robots and internet-enabled devices removes human intervention that is currently built in to 'manually' controlled systems. Unfortunately, more interconnectivity between devices and systems will offer opportunities for cyber-crime and unauthorised use of information. Companies producing both IoT and chip level devices will need to invest in ensuring these are proven to be secure.

Accelerating developments in technology also means increasing numbers of complicated, obsolete and unsupported legacy software and hardware systems that, again, present security issues. These advances will also lead to additional financial and time costs that will be required to maintain systems – placing an extra burden on people and businesses.

There are questions, too, about the physical resilience of technology and systems, for example their robustness to events such as extreme weather and their ability to remain secure under such conditions.

Key points

- Technology influences all aspects of our modern day lives.
- There is a need to ensure cyber security resilience is embedded in all sectors - technology and services: from corporate level down to the individual; e.g. driverless vehicles, healthcare (data and machine), financial transactions and contracts, manufacturing, smart homes, cities and rural environments.
- There is an increasing need for support and governance of autonomous technology.

Considerations for the SG

- Consider setting up technology research and industry briefings.
- Carry out risk assessment studies for new technologies.
- Offer support to the creation of policies to ensure secure by design for new technologies – CE/kite marking.
- Create a database of organisations that are cyber secure – i.e. audited and certified.
- Technology support services – ensure that software and hardware from manufacturers is continuously maintained so that it does not become obsolete.
- Enforce fines (via ICO) for patching not being implemented in a timely fashion.
- Encourage more stringent contractual agreements and / or smarter purchasing – e.g. leasing equipment, perhaps following the car leasing industry example to minimize obsolescence and keep abreast of the latest technology.

7.2. *Identity & Data*

Summary

Protecting identity and data integrity are critical and immediate issues that will remain important to our current and future cyber resilience.

Cybercrime relies on gleaning information about an organisation, a person's identity and associated data. The National Crime Agency (NCA) [17] highlighted the seriousness of cybercrime with on-line financial crime overtaking traditional crime in the UK in 2015. It is recognised that law enforcement and prevention across a digitally connected world is challenging. In response to the increased threat, the EU Cybersecurity Strategy has introduced GDPR and the NIS directive and the aligned UK / Scotland Strategies have invested in policy / action plans with investment in the NCSC and police services i.e. digital forensics increased.

There are legal processes in place through The Crown Prosecution Service (Legal guidance / on-line crime [18]) and The Crown Office and Procurator Fiscal Office. In addition the Information Commissioner's Office (ICO) is empowered to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

A number of questions around the issue of data arose in the workshop especially regarding individuals and organisations:

- What are an individual's rights?
- Who owns data? And does it depend on how it was generated?
- How long should data be held for and who manages it?
- Who can profit from data? Individuals and/or companies?
- Who has access to data? And what are they allowed to do with it?
- How are the various items of data linked?
- How is data validated? And who does this?
- What levels of data security are currently in place? And what levels should there be?
- Where is the balance between privacy and security?
- What happens to a person's data when their circumstances change, e.g. change bank accounts, jobs, divorce/separate or die?
- How and where is data stored? Does this impact ownership and use?
- How to deal with indirect data – i.e. data regarding the Internet of Things?

[17] NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016
http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016

[18] NCA The Crown Prosecution Service Legal Guidance, Cyber / online crime
https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

Benefits

There are many benefits to having access to the vast array of data and services available through digital technologies – to people, businesses and governments. Data can be used in positive ways, and often is to benefit the wider society. For example, the Scottish Government *Scotland's Digital Heath & Care Strategy* [19] recognises the advantages of digital technology and services that will be provided more effectively, i.e. universal health ID/card, digital prescriptions, access to patient and clinical databases, improved home care provision.

Risks

Alongside these benefits are clear risks – again, to people, businesses and governments. Data ownership and loss can have substantial negative outcomes. The validation and provenance of data and linking it correctly to its owner poses threats. For example, internet shopping to suit our needs is generally seen as beneficial and a convenience – although there are concerns about our shopping profiles being targeted by sales advertising. Buying on-line however creates risks in illegal access to private information and personal bank details. The risk of identity fraud is also increasing (over 174,000 cases reported in 2017) with easy access to personal information on social media (and the dark web) making us vulnerable. Social media has also highlighted how misuse can influence key events – Cambridge Analytica harvested personal information from over 50 million Facebook profiles to target US voters with biased political information.

Key points

- Protect individual and business rights to data and ownership of their data
- Protect key infrastructure around managing data and provenance
- Citizen ID – individual in control, not business or government

The SG should consider

- Increasing public and business awareness of risks
- Providing public information help lines
- Encouraging multi-factor authentication
- Improving police digital crime and fraud services.

[19] Scotland's Digital Heath & Care Strategy https://beta.gov.scot/binaries/content/documents/govscot/publications/publication/2018/04/scotlands-digital-health-care-strategy-enabling-connecting-empowering/documents/00534657-pdf/00534657-pdf/govscot:document/

7.3. Socioeconomics & People

Summary
Cyber resilience and future technologies have the potential to have a substantial impact on individuals and organisations at a variety of levels. This impact is likely to be both positive and negative. As with the other themes, it is important to consider short-term and long-term impacts to assess what can be done to maximise benefits whilst minimising risks.

One of the key points in this theme is the issue of socioeconomic division and the potential for it to become wider due to the release of sophisticated future technology. The inability for some of the population to adapt to change and develop the skills to use new technology will be a key issue. There are also issues regarding infrastructure for example: access to and speed of internet connections for people and businesses, and the ability to keep pace with advances in technology itself, including software and hardware.

A new type of economics is emerging where traditional banks and even national borders are increasingly less relevant. With the movement of vast sums of money online outside traditional routes, the role of taxes and funding of government will become challenging. The potential for a 'cashless' society is also an area of concern for the future as greater use of smart and digital payments grow in everyday life.

Benefits
The internet and associated technologies have brought a wide range of benefits to society in many different ways. It is important to ensure that future benefits, of which there are many, are shared across the socioeconomic spectrum to add value to people's lives and encourage businesses to thrive. The benefits of technology to deliver improved transportation services, better healthcare and medical services, access to global products, smarter homes and virtual worlds is exciting. Changes to lifestyles and work patterns are inevitable.

Risks
The great risk in this theme is of widening and deepening the already existing socio-economic divide – it is important that consideration is given to this issue. There are however many unknowns within this theme including how cyber resilience may affect education, quality of life, employment (both skilled and unskilled), and the provision of public services. The ability of people and businesses to keep up with technology, both in terms of the financial costs and having the skills required, is a high risk. The human element in the failure of technology will remain.

Key points

- Infrastructure and access is required to support individuals and businesses.
- Everyone will need to become more digitally aware and educated.
- Consumer support required to keep up with the pace of change and prevent or reduce obsolescence.
- Delivery of skilled people is required, with on the job learning, rather than degrees.

The SG should consider:

- Conducting an analysis of the socio-economic divide in order to enable future potential changes to be assessed and minimised.
- Conducting an analysis of current economic models with regards to cyber resilience and societal impacts and devise a plan to ensure beneficial outcomes.

7.4. Education

Summary

Education, in the form of improved and more positive two-way engagement with society in general, is widely recognised to be critical in building and maintaining cyber resilience. Education around all aspects of technology, including people, organisations, public services and infrastructure, should start from an early stage in a child's learning and be a continuous part of any curriculum.

It is equally important, however, that education is part of wider society and not just through formal learning. All individuals need to be aware of cyber resilience and technology as it becomes an increasing part of everyday living, especially with embedding of the Internet of Things and increase in digital services and perhaps even a cashless society.

Benefits

It is recognised that education, research and innovation, developing an entrepreneurial culture supported by government policy and access to financial investment will provide the ingredients to grow new products and services, create new markets, generate wealth and grow the economy. However, this will only succeed by having a better and more widely cyber-educated population and more cyber resilient nation. This will enable growth across a number of sectors and provide people and businesses with better security and increased opportunities. By starting young and embedding 'cyber' education across all ages a cyber-resilient mind set can be built to the benefit of society.

Risks

The risks are that, as with socioeconomics, a divided society is created with a vast gap between those people and businesses that understand and gain from technology and those who are left behind. Not only will this have substantial negative effects on the latter group, but society in general will be detrimentally affected with increased risks of cyber-attack and cyber-crime.

By falling behind with education, there is also the risk of losing Scottish talent and not attracting new skills and businesses to Scotland.

Key points

- Promote education and positive engagement with technology and cyber resilience across all people, businesses, organisations, etc.
- Improve access to education and help lines through councils and local communities.
- Engage all society and age groups appropriately – one size does not fit all.
- Better dissemination to the general public, breaking down the barrier between experts and everyone else.

The Scottish Government should consider:

- Helping to address identified gaps in teaching expertise in cyber resilience and computing science which needs addressing. The Scottish Qualification Authority notes that "Scotland is world leading with the cohesive range of courses at school, college and university levels".
- Supporting the real opportunity for Scotland to become globally recognised as a digitally well-educated country. This requires marketing, communications and public relations.
- How to embed education and training on new technologies into courses and curricula.
- How to support broader engagement and education with the public to address and prevent social divide.
- Developing a 'driving licence for cyber security' as a way for businesses and individuals, including school pupils, to show that they are aware and trained.

7.5. Innovation

Summary

In today's fast moving digital economy and with access to advances new and emerging technologies envisaged there will be opportunities through innovation to exploit these technologies to drive economic growth, create wealth and improve our lifestyles.

The areas of innovation will be wide-ranging i.e. from manufacturing and services (robotics), automated transportation (driverless cars) to socioeconomic impacts (public services, health, and education) and finance (mobile banking and retail).

However, as our world becomes more advanced, automated, digitally connected and complex, successful innovation is increasingly dependent on being cyber secure and resilient. Secure by design in hardware and software, along with cybersecurity risk assessment throughout the product lifecycle in business planning, product design and services are essential elements. Of course innovative testing and training environments are needed too, such as Edinburgh Napier University's Security Operation Centres (SoCLAB) to train students and companies to cope with phishing, ransomware, denial of service and data loss – including how to recover.

The cybersecurity industry itself is also advancing. Innovations in artificial intelligence are already being adopted in end-to-end point cyber forensics. Quantum communication devices have been developed and a satellite (*Micius*) link has used quantum key encryption – perhaps a first step towards a quantum internet.

To capitalise, the workshop recognised Scotland needs to invest in building technology alongside a sustainable cyber resilience research capability to provide a pipeline of skills and intellectual property. Investment in innovation will attract new business and corporates and speed the translation of the research needed to grow the ecosystem for Scotland to globally compete. The importance of the Scottish Government's role in supporting with policies and regulation is an essential part of this investment.

Today Scotland is focused on tackling current cyber security threats. Protecting critical national infrastructure and preventing the misuse of computers and mobile devices connected to the internet and social media remain the key challenges i.e. phishing attacks, ransomware and on-line invasion of privacy, identity theft, child pornography, stealing IP and valued data. The workshop recognised that technology solutions using multi-authentication, AI, machine learning and bio-metrics are maturing but need to be accelerated and implemented with closer cooperation with service providers to 'protect' users on networks and communication systems enforced. The SG can influence this policy as it will require continued cooperation at a national security level.

In the near future with Internet of Things devices, fibre roll-out, electronic patient records, citizen ID and 5G high speed communications expected, we will become more digitally connected and seamlessly digitally enabled at all times. To be secure and resilient it will be imperative that all devices are secure by design, have a traceable asset history and perhaps have Cyber CE / Kite marking for devices and products. The issues that have been identified

require support from the EU and the UK Department for Culture, Media and Sport[20] and the SG working with industry.

Also in the near-term, cyber resilience concerning the uncertainty associated with Brexit is a major issue. The workshop expressed concern about EU collaboration and funding for research and innovation, as well as the effects in attracting talent for academia and industry need. In the short term from a legal and enforcement security perspective, the EU GDPR and Network and Information Systems (NIS) Directive have been enacted into UK law to strengthen data protection, privacy laws and standardisation of networks and information systems. The UK has officially stated leaving the EU will not alter this. There are concerns, however, about UK law enforcement not having access to EU databases such as the Schengen Information System (SIS II) for real-time alerts and access to the European Criminal Records Information System (ECRIS).

The Scottish Government recognises the importance of innovation in the cybersecurity sector and its benefits to Scotland's economy and is investing £250,000 in cyber-resilience innovation challenges and £350,000 in developing a Cluster Management Organisation (CMO) to support cyber businesses. [21] The Scottish Innovations Centres, CENSIS and The Datalab are engaged and delivering collaborative academic and industry cybersecurity security projects, while the private sector and investment community are also active in the cybersecurity ecosystem.

Benefits

The importance of cybersecurity and resilience to Scotland and the UK is well recognised along with the benefits of living and working in a secure, safe and trusted environment. Cyber security and resilience is an enabler across all sectors creating and sustaining jobs, and allowing businesses to flourish.

> *"Scottish companies are at the heart of the digital revolution. Businesses that are cyber resilient stand to gain competitive advantage" Hugh Aitken, CBE former CEO, CBI Scotland.*

Risks

Scotland's economy and infrastructure is reliant on secure digital connectivity. Innovating and keeping up with technology is essential for businesses to remain globally competitive and deliver cost efficient services.

---

[20] Dept for Digital Culture Media and Sport, Secure by Design: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

[21] Delivering for Today, Investing for Tomorrow. The Government's Programme for Scotland 2018-2019 https://beta.gov.scot/binaries/content/documents/govscot/publications/publication/2018/09/delivering-today-investing-tomorrow-governments-programme-scotland-2018-19/documents/00539972-pdf/00539972-pdf/govscot:document/?inline=true

It is paramount that Scotland is able to provide skills and creative thinkers to drive innovation into industry – there is a risk that if there is not access to a pipeline of well educated 'cyber' trained graduates and researchers that innovation will stall.

The impact of disruptive innovation; for example a quantum computer being developed elsewhere, or an unstoppable cyber-attack on Scotland, are real concerns and must be considered as part of national security.

Key points

- Innovation in cybersecurity is essential for Scotland to remain competitive.
- Innovation requires creative thinkers – think tanks and collaborations required.
- Innovation Centres are key to encouraging industry / academic cyber projects.
- Create and grow cyber innovation hubs and clusters.
- Government, agencies, universities and businesses to promote Scotland as a champion of cyber resilience to attract expertise, investors and business to Scotland.

The Scottish Government should consider:

- Ways of supporting cyber security research and talent at universities through investment in bringing expertise to Scotland.
- Ways of supporting capacity building is essential by increasing sustainable critical mass for research and training programmes such as Centres for Doctoral Training.
- How to support the professional promotion of Scotland as a cyber innovative and secure nation and brand.
- Investing in cyber resilience incubator hub / innovation centre to increase collaborations amongst investors, academia, public sector and private sector.
- Ways of supporting speculative high risk, high growth disruptive innovation projects.

7.6. Legal & Ethics

Summary
The workshop raised a range of issues concerning legislation not keeping up with the pace of technology. Issues considered were: Legal ownership and safe havens for data – on remote servers, in data centres and particularly in the cloud (possibly located on multiple servers located in different countries),- who is legally responsible when systems are breached or fail – the service provider, or the organisation owning the data, or perhaps the manufacturer of the equipment providing the service? Concerns were also raised about cyber-attacks from individuals, organisations and nation states from abroad – how could our security services, police and legal systems deal with this? Unsurprisingly the two areas of greatest concern were keeping an individual's personal information private and secure, and protecting the country's national critical infrastructure.

Legislation is often perceived as a traditional instrument being used in a modern environment. It is true that it takes time to agree and implement new legislation and keeping abreast with rapidly evolving technology will remain challenging.

Governments are attempting to keep up. The realisation of these issues drove new EU legislation such as GDPR and the NIS directive, and these have been enacted into UK law through the Data Protection Act 2018, [22] Human Rights Act 1998 [23] and Computer Misuse Act 1990. [24] The USA also passed legislation – Clarifying Overseas Use of Data Act 2018 [25] which includes the 'Cloud Act' – addressing data access and privacy rights across cloud services from technology companies such as Google, Amazon and Apple.

The impact of these changes, and the implementation of them, is placing demand on resources and skills across governments, businesses, the legal sector and enforcement agencies. The additional uncertainty of Brexit is further adding to the complexity and speed in which organisations are making, perhaps delaying, decisions and actions.

On-line legal services are becoming more common place - digital and electronic signatures are now legally accepted to aid security and verification. Moreover, regulatory standards are in place in Europe and the UK through the electronic identification and trust services for electronic transactions (eIDAS) regulation. Smart contracts are developing and electronic identification will become the norm. It is expected that biometrics and smart authentication technologies will become part of everyday life.

[22] The Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf
[23] Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents
[24] Computer Misuse Act 1990
http://www.legislation.gov.uk/ukpga/1990/18/contents
[25] Clarifying Overseas use of Data Act (Cloud Act) 2018
https://www.hatch.senate.gov/public/_cache/files/6ba62ebd-52ca-4cf8-9bd0-818a953448f7/ALB18102%20(1).pdf

The use of smart digital contracts is likely to become widespread and embedded within society. These are automatic computerised agreements that are flexible and self-executing with the terms of the agreement between buyer and seller being directly written into lines of code. For example with Blockchain technology there is no third party needed in the transaction. Imagine a contract deployed by using code *./peer chaincode deploy –n exo1 c'{"Function":"init", "Args": ["{\"version\":\"1.0\"}"]}'*
There are a range of issues these contracts would raise and legal expertise will need to understand how the contractual terms are 'translated' and executed in code.

Ethics for cybersecurity, and understanding the legal impacts arising from new technologies were highlighted as significant areas requiring expertise. Addressing ethical issues is of course not new, but the speed of introduction of new technology, the sophistication of digital connectivity and dealing with unprecedented volumes of data is creating fresh challenges – morally and legally. For example, tracking the geographical location of individuals could be ethically wrong and an invasion of privacy, or on the other hand an essential service in emergencies.

Another example is 'Super Apps', – mobile device apps that combines several apps or functionalities into a single app may be the way forward as industry moves in the future. SuperApp WeChat is already successful in China and there is debate about the pros and cons on having many services e.g. Facebook, Skype, Google, WhatsApp rolled into one application. Interestingly, current legislation does not appear to be equipped for these integrated services.

Benefits

Smart contracts, online verification, active control of data, standardised terms of agreement and other similar innovations will greatly benefit all areas of society. The potential to support and protect individuals, organisations and businesses through smart governance and legislation has the potential to improve Scotland's cyber resilience, and help to make it a world leader in the field. It is envisaged that 'blockchain' contract transactions will become the norm. The integration of citizens, data and public services would also be mutually beneficial.

Risks

There are risks that governments and legislation cannot keep pace with technology making legal enforcement difficult. Having legal expertise familiar with new areas such as GDPR and blockchain is essential, but will need staff resourcing and training in place. There is also a risk that having strict legal standards and growing government oversight may lead to a reduction in opportunities for innovation.

Key points

- Ethics plays a critical role in moving forward safely with new technologies
- Legislation, and enacting that legislation, must keep abreast with technology, government, and business needs.

The SG should consider:

- Forming an ethics committee to address cyber security issues and act as an advisory body.
- Providing cybersecurity ethics workshops and raising awareness across education courses and communities.

8. Considerations & Actions

Considerations for each theme have been captured throughout the report. The following considerations review the context of key issues that may arise in the future as technology develops:

i. Research and Innovation

By 2020, the Scottish Government, working in partnership with the Scottish Funding Council, Scottish Enterprise and Highlands and Island Enterprise, need to establish a national Cyber-resilience research network. The network will connect key academic groups, established and emerging companies and end-users of new digital services. Innovation Centres such as the DataLab and CENSIS, will strengthen the network to support economic opportunities for Scotland's national strengths in innovation and cyber-resilience. To compete globally, investment will be required to build on Scottish strengths in academic research to create the innovations and skills needed for future business growth, and will also prime the future roll-out of new, secure digital products and services across private and public business sectors. Speculative investments in disruptive technology through grand challenges should be encouraged. Moreover, it is proposed that other key Scottish research centres working in a range of areas e.g. robotics and AI and healthcare are integrated into security and resilience activities. The research network should connect with existing cybersecurity technology hubs operating across key sectors such as advanced manufacturing, finance, transport, infrastructure and utilities. Where feasible, increased economic impact can be achieved through integration into City Deal initiatives.

ii. Education and Outreach

By 2025 the technology will be digitally encompassing all elements of our lives, smart homes, AI driven machines, autonomous electric transportation and 7G communications connecting Internet of Things devices across the globe to thrive in this digital world, Scotland's citizens need to become amongst the most cyber-aware of any nation. On-line social media campaigns and targeted advertising will be required to direct the public to a range of on-line information. These are to be aimed at ensuring Scottish citizens are not only aware of key personal cyber-security issues, but have a growing awareness and are able to use new technologies such as Blockchain and the Internet of Things which government will begin to use to deliver secure and enhanced public services. Pilot projects to roll-out secure on-line voting using Blockchain will be delivered through local elections for a number of council wards, backed-up by leafleting campaigns. Other measures suggested are to include continuous cyber-security education through schools, colleges, universities, at work and in the home. Aimed at raising awareness of personal cyber-security and cyber-resilience, these measures will ensure that existing inequality is not further widened through those who are able to access and use digital services, and those who are not.

iii. Public Services

Looking to 2030, having safe, secure and resilient public services in Scotland is recognised as essential to underpin many of the key services affecting our day to day lives. One of the predicted cybersecurity requirements across these services will be the need for the Scottish Government to support, provide guidance and perhaps legislation to ensure the supply chain is secure. It is envisaged that smart contracts will be widespread resulting in streamlining of government procurement, reducing overhead costs on transactions and delivering greater security. This growth in public sector innovation will extend to the use of blockchain [26] including government asset registers, on-line voting and overhauling historic databases such as land registers. The acceptability of these innovations will be aided by prior public engagement programmes through government led education initiatives. Moreover, as public sector innovation grows, start-up companies will be encouraged to locate in Scotland due to the ready market for new digital products and services. Along with growing strengths in research and innovation, this virtuous circle can lead to Scotland becoming an international beacon for the entirely new digital technologies of the future.

iv. Disruptive Technologies

By 2050 there will be significant changes through entirely new technologies impacting all areas of our lives. Some technologies will be highly disruptive – for example quantum computers will transform cybersecurity encryption. Not having ready access to such technology would disadvantage Scotland, and would lead to missed opportunities in preparing Scotland for the future. To mitigate these risks the Scottish Government will need to continue to invest in research and innovation, invest in foresighting programmes and invest in skills and education.

[26] Blockchain in Public Sector Transforming government services through exponential technologies https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-blockchain-noexp.pdf

9. Workshop Key Messages

- Make Scotland a ‘cyber-aware’ nation.
- Build and maintain infrastructure to protect and support cyber resilience.
- Engage society appropriately and with two-way communication.
- Use positive messages to promote the beneficial aspects of cyber resilience.
- Ensure the cyber security and protection of society.
- Protect rights to data ownership and use.
- Educate everyone - of all ages, and start early.
- Adopt a ’cyber security by design‘ culture and mind-set.
- Continue investment - funding and support for innovation.
- Provide governance and legislation where necessary.
- Provide leadership to build trust and support across society.
- Ensure that Scotland has the opportunity to lead on cyber resilience and be recognised globally (e.g. innovation centres, communications).
- Encourage collaboration through a national and international cyber-resilience research network – academic, government, business, legal, and law enforcement.

10. Summary & Conclusions

The workshop demonstrated that current and near-term technologies and risks, whilst complex, are well understood. This was substantiated by the detailed information and views expressed. However, concerns remain regarding the potential effects of cyber-attacks and risks affecting our daily lives. On an individual level, the nuisance of phishing, issues of privacy, data ownership, and of keeping us all safe and secure were considered critically important. But there was also an awareness of the potential for divisions in society between those with education, skills and access to technology and those who do not. This raised a range of ethical questions and it was felt that 'cyber security ethics' would be one of the key issues needing to be addressed.

Linked to this, new legislation such as GDPR and the NIS directive is being introduced; however, the rapid pace of technology development and associated risks raise concerns that their implementation and enforcement will continue to lag.

The increase in cyber-attacks on businesses, government, public services and national infrastructure pose challenges. These are being addressed by a broad range of current initiatives at local, national and global levels. In the future, the use of new technology will provide more robust solutions, but may also provide greater scope for cyber risk and opportunities for exploitation. The progression to more complex interconnected devices, networks and systems, and a digital economy built around information and data with highly automated software leads to a world of artificial intelligence and deep learning where machines make decisions. In this future digital world, risk, ownership, legal implications, policing and governance will require cooperation at an international level between businesses and governments.

Predicting future technology development is a challenge; however, there are a number of issues that are unchanging regardless of software and hardware implementations. People and businesses need support and infrastructure to make use of and have access to technology. Where possible or necessary this may require the backing of legislation, which will have to be flexible to keep up with the pace of change.

The issue of data is a pressing concern with the scale and challenges associated with ownership growing with future technological change. International boundaries limit policing and the reach of legislative powers, but there is progress through international cooperation and initiatives such as GDPR and the Cloud Act.

To remain competitive in the digital world, and to ensure a secure and prosperous society, cyber resilience must be embedded across society, businesses and the public sector. Achieving this will ensure that Scotland is a future-focused country that is open for growth, investment and innovation.

Annex A – Workshop attendees

The Cyber resilience workshop met in November 2017 and worked together to feed into this report. There were representatives from:

- Abertay University
- Edinburgh Napier University
- Glasgow Caledonian University
- Heriot Watt University
- Robert Gordon University
- Scotland IS
- Scottish Informatics and Computer Science Alliance
- The Royal Society of Edinburgh
- University of Aberdeen
- University of Dundee
- University of Glasgow
- University of the Highlands and Islands
- University of St Andrews
- University of Stirling
- University of Strathclyde
- University of the West of Scotland

Produced for Scottish Science Advisory Council in June 2019 by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA

scottishscience@gov.scot