CORSHAM
INSTITUTE

Cyber and resilience

Digital's role in regaining resilience

A consultation in partnership with the Corsham Institute Thought Leadership Programme 2016

Report April 2016

WINDSOR CASTLE
COLLEGE OF ST GEORGE

This report was produced following a consultation at St George's House, as part of a programme of events in the Corsham Institute 2016 Thought Leadership Programme.

The report should be viewed in conjunction with reports from the series.

The consultations in the 2016 programme were:

- Digital health: Digital's role in health and care – March 2016
- Cyber and resilience: Digital's role in regaining resilience – April 2016
- Digital living: Getting the most out of digital society – May 2016
- Trust and ethics: Building a more informed digital society – June 2016

This programme hosted at St George's House was developed in partnership by Corsham Institute and RAND Europe.

St George's House is a place where people of influence and responsibility in every area of society can come together to explore and communicate their views and analysis of contemporary issues. The aim is to effect change for the better in society by nurturing wisdom through dialogue.

Corsham Institute (Ci) was formed in 2013 to explore the opportunities and benefits of the digital society, both social and economic, with particular focus on shaping a future where individuals can realise their potential in a highly connected world.

RAND Europe is a not-for-profit research institute whose mission is to help improve policy and decisionmaking through research and analysis. Lying on the spectrum between that of universities and consultancies, RAND Europe's work combines academic rigour with a professional, impact-oriented approach.

The report should be cited as: Corsham Institute (2016). Cyber and resilience: Digital's role in regaining resilience. Windsor: St George's House.

Published October 2016.

Key Findings

Context

Society's reliance on technology systems and processes makes it increasingly more vulnerable to the threat of cyber-attacks. Plenty of attention has been paid to the question of how to react to system-disrupting cyber-attacks as and when they occur. Far less attention, however, has been paid to the question of how to build resilience, which would mean that cyber-attacks are not able to disrupt systems to the same extent or that the systems are designed and constructed to be self healing. This is seen by many as one of the biggest challenges in the modern digital age. The topic, building a digital resilience to new and existing cyber-threats, formed the basis of the discussion during the second session of the 2016 Thought Leadership programme.

Key discussion points

What is resilience in the digital age?

Discussion about the definition of resilience in the digital age focused on three key areas:

- The adaptability of technology systems to manage cyber-threats, while accepting that attacks will occur.
- Being alert to new cyber-threats, no matter how shocking and surprising they may be.
- The ability to continue to make significant technological developments and progress in spite of any cyber-threats.

How can we build resilience?

There is broad agreement that the internet is structured to be resilient. Its interconnected and redundant nature means that a cyber-attack will not affect the whole system, so individuals can continue to use it, albeit in a reduced capacity. The discussion explored the vision for digital resilience, which in some ways matches the very nature of the internet: adaptable and agile to new and existing cyber-threats. As part of this future vision, the group sees each stakeholder, such as government, non-government organisations, industry and civil society, having defined roles, rights and responsibilities to help build a digital resilience.

What are the barriers to realising this new vision?

The main barrier highlighted in discussions is a lack of understanding and research around creating resilience in the modern digital age. As a result, there are insufficient skills to develop resilient infrastructure and manage the threat of cyber-attacks. The high pace of technological change and lack of societal investment are considerations to achieving effective digital resilience.

Next steps

Increased awareness of digital resilience is needed at a political and societal level, as is a clear narrative about why it is important. This is an issue that transcends nation states and needs to be addressed at a supranational and global level. Individuals and institutions can help to build a digital resilience by being told in clear and practical terms what is expected of them when they are online and what they can do to be safe. This engagement can occur through a range of methods, such as in-house training for employees, outreach education for elderly or isolated groups of people, and tailored in-school provision for pupils. Overall there is a need for strong leadership from national governments, if a vision for digital resilience is to be realised. More research is also needed on how to build digital resilience; research has traditionally been focused on being reactive to cyber-threats, with minimal studies on how society can become proactive and resilient.

Introduction

The Corsham Institute (Ci) Thought Leadership programme, which was designed and delivered in conjunction with RAND Europe, was established to explore the opportunities and challenges that digital technologies are creating within society. The programme seeks to bring together senior leaders from across academia, industry, government and non-government sectors in order to enable the emergence – through a combination of robust debate, knowledge sharing and personal reflection – of new thinking and ideas on how everyone in society can benefit from the use advantages that digital technologies can offer.

This report represents the main findings from the consultative event on cyber and security that was held on 14 and 15 April 2016 at St George's House. The overarching question which was initially proposed for this consultation was:

'How can society build stronger resilience in a less certain but more digitally enabled world?'

Participants noted that the term cyber security is well understood, both as a concept and in more practical terms within society, since there is a wide range of products and services available to help organisations and individuals to manage such risk, but that the concept of 'cyber resilience' was not well understood or even discussed. While our initial group discussions centred on cyber security as a defining digital imperative, the common understanding quickly shifted to the benefits of good digital behaviour and the critical role that this plays in underpinning a resilient society in a digital world. In this respect, it was felt by participants that the overarching question for this consultation needed to be refined to better reflect this imperative. The following revised overarching question was therefore proposed and agreed on for our discussions:

'How can we create a more resilient digital society and realise its benefits?'

Throughout this consultative event, therefore, the focus on seeking new ways of describing what it means to be resilient in a digital world – and to find a clear and easy-to-understand imperative as to why resilience is needed in society – was seen an invaluable. If we are to create a sense of priority that places resilience at the centre of a new, digitally focused, society, developing such a narrative will require society to move beyond the narrow silos and myopic viewpoint that seem to exist today. This will require new behaviours from everyone and a new clearly articulated vision or framework all can understand. We need a new 'digital covenant'.

Building greater resilience in a more digitally enabled world is seen by many as being one of the greatest challenges facing modern society. We live in a more digitally connected and yet, some would say, more uncertain and less secure world. Digital technologies are disrupting traditional methods of interaction, and citizens need to feel confident in their use of digital technologies if the goals of economic growth and social progress are to be achieved. The 'rules of the game' are being redefined as we interact differently, becoming increasingly dependent on digital technologies for everyday aspects of our lives.

If we are to gain the most from a digitally enhanced way of life, society needs to adapt so that it is better prepared to address possible disruptive events and new threats. In effect, we need to find a new approach, which allows us to balance the convenience of living in a more digitally enabled age against the risks that are emerging as a result of a dependency on such technologies for managing more and more of our lives.

This report aims to capture the main ideas and views put forward during the consultation, with the understanding that not everybody involved in the discussions will necessarily have endorsed all of the proposals and viewpoints reported. The report has been structured to reflect the main findings and conclusions, under the following headings:

1. Background and context
2. A new vision for cyber resilience
3. Making cyber resilience a reality
4. Barriers to developing cyber resilience
5. Societal preparedness for cyber resilience
6. Conclusions and next steps

As with all St George’s House consultations, this report has been prepared under the ‘Chatham House Rule’. Any phrases that are italicised and in double quotation marks are direct, but unattributed, quotes from the discussions during the event.

It should be noted that while cyber resilience is a global, trans-national issue for society, the need to consider practical experience has meant that much of our discussion during this event focused on a UK-centric perspective.

Ci and RAND Europe would both like to extend their warm thanks to the participants who introduced each of our sessions, and to all participants for stimulating and contributing to the high level of discussion that took place. A list of all participants is provided at the end of this report.

1. Background and context

Societies across the globe are more connected than ever before, and they are conducting more of their business online. We heard how data should be positioned as *"the new oil"* in economic resource terms – an essential commodity that societies need and use to maintain economic output and growth. At the same time, governments around the world are using digital delivery for ever more public services and transactions, as we move away from face-to-face and paper-based processes to meet efficiency and cost saving targets. As consumers, consumer-creators and users of public services, we have all put enormous amounts of personal data online; as one participant noted, *"As a society, we've decided to digitise everything".* Much of this activity has occurred without any consideration for the privacy or security implications of such actions.

The increased use of digital technology in day-to-day life has created huge opportunities for people to interact, for businesses to innovate, and for governments to deliver more efficient and tailored public services. However, it also means that society has become more reliant on technology systems and processes for the delivery of many day-to-day services and products – digital systems that are potentially vulnerable to failure or even attack. To give one recent example of that vulnerability, in 2015, a cyber crime company announced its discovery of the 'Carbanak'[1] computer-hacking process, which, it was estimated, had resulted in up to $1bn having been stolen from banks and private customers. As some participants noted, perhaps even more worrying was the potential loss of personal data that accompanied the financial theft.

The issue of cyber security, however, is not new. We heard that, as far back as 1989, the LOpht hacker collective (their name is believed to be a play on the loft apartment they shared together) warned the US Congress that government regulators, computer manufacturers and software developers were grossly underestimating the risks posed by under-protected online networks. At a time when the entire world was moving enthusiastically towards an online world, LOpht warned that nobody really knew how to create secure systems or stable platforms for managing the entire data bank and keeping it from falling into the wrong hands. As one participant noted: *"Their [LOpht's] message was 'Don't build an economy on an unstable platform'. But we went ahead anyway and did!"*

[1] Virus News. 2015. 'The Great Bank Robbery: Carbanak Cybergang steals $1bn from 100 Financial Institutions Worldwide.' Kapersky Lab. As of 7 October 2016: http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide

As *The Washington Post* stated in a 2015 article,[2] the LOpht group were listened to politely at the time, but no action was taken. *"What happened instead was a tragedy of missed opportunity, and 17 years later the world is still paying the price in rampant insecurity".*

While insecurity in the digital world is simply a manifestation of risk and a fact of modern life, some participants felt that we do not actually live in a less secure world but, rather, in a more uncertain one, where being the subject of a cyber-attack or breach is just 'part of life'. The overriding priority for our society should therefore be to better understand how to manage such risk and to prevent these uncertainties from contributing to other socio-political uncertainty. We need to reframe our thinking about control and accept that cyber events will take place and that we need to have the ways and means to put in place rapid and resilient responses to them.

Interestingly, the term 'resilience' is not widely recognised or understood across society. It can mean different things to different people and is a very context-specific concept. For instance, the resilience needed within a medical context might be very different to the resilience needed to be able to continue to communicate using social media. As a group, we agreed that there is no consistent understanding of what 'resilience' means within society; however, for the purposes of this consultation, we considered the following definitions:

- The ability to recover or 'bounce back' from setbacks, both large and small
- The ability to adapt to change
- The adaptability of systems, groups, and, ultimately, individuals to shock, and the ability to continue to make progress in the face of adversity
- Where appropriate and without becoming the nation's "cyber life support system", the ability of government to identify, assess and respond to a potentially disruptive situation in order to prevent it from becoming a crisis

Assessing the level of risk

In considering the level of risk faced within society today and the need for a new, more resilient approach to digital, it is perhaps worth considering what level of risk is actually faced. Participants expressed different views on the level of digital security risk faced by UK society today.

[2] Timberg, Craig. 2015. 'A Disaster Foretold — and Ignored: LOpht's Warnings about the Internet Drew Notice but little Action.' *The Washington Post*, June 22. As of 7 October 2016: http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/

Some argued that we face a significant and growing level of risk due to a number of factors, including: a growing reliance on digital systems and processes; a growth in the number and range of malicious actors and cyber-attack vectors; individuals as well as nation states looking to capitalise on opportunities to disrupt and destabilise organisations for their own ends; the difficulty of accurately determining a cyber-attack's attribution (although capability in this field has increased significantly in recent years); and the growing ability of nation states to conduct espionage through digital means.

Other participants felt differently, stating that the level of risk is arguable decreasing, or at least being held steady, as a result of the *"greater interconnectivity of networks"* that allows security and regulatory organisations to pool resources and share information; populations that are becoming increasingly 'net savvy', including 'digital natives', who have grown up online; and the increasingly proactive roles played by national governments in launching well-funded cyber security strategies. All are helping to stabilise the system and reduce the ability of malefactors to launch cyber security attacks. Others went further, saying that it could be argued that, *"because we have such digital connectivity that in fact we have far greater resilience than existed before."* By its very nature, interconnectivity provides the ability to manage cyber security issues more effectively by maintaining continuity of services and by creating a more resilient approach to managing networks.

Another common theme which emerged throughout our discussions, was the low level of personal risk faced by the perpetrators of cyber security attacks. As one participant noted, *"If you compare the risk of robbing a bank in the conventional 'heist' sense to that when conducting a 'cyber-attack', then the former involves significant risks to the criminal at every stage of planning and execution: getting hold of a weapon; modern closed-circuit television [CCTV] and security measures; the difficulty of escape, and so on. Whereas attempting to hack into a bank from 'sitting at your desk two countries away' entails a much lower level of personal risk."*

Finally, it is perhaps worth noting that there was agreement throughout our deliberations on the need to strike a balance between discussing the risks faced as a result of cyber security and resilience issues, on the one hand, and the benefits that digital technologies can deliver, on the other. Yes, we need to be clear and honest about the level and type of risks which exist in a more digitally enabled world; however, as one participant noted, *"the debate cannot be dominated by fear, as this will paralyse some into inaction, turn others off digital completely (particularly older people), and be seen by others as simply scare mongering".* If we are to maintain and build confidence as we become more digitally connected, there is a need to find a new narrative which balances these arguments and which helps to create a clearer, more motivational narrative about the need to take cyber resilience seriously.

2. A new vision for cyber resilience

Building on the need to consider a new narrative for cyber resilience which is able to deliver clearer and more consistent messaging about cyber resilience, participants felt strongly that there is a need to define a new vision of what is meant by resilience in a more digital society.

First, it was felt that the new vision needs to have a global perspective and that it needs to be developed and owned in partnership among government, industry, academia and civil society, rather than being something which is imposed by governments. It is important to recognise that *"this is a systemic problem, an ecosystem problem, where we all need to recognise new paradigms"*. We heard how no one actor should be considered solely responsible for creating and delivering a new vision for cyber resilience across society and, more importantly that, while *"governments like to regulate",* government regulation may not be the best solution for such a complex and inter-connected issue.

While a new vision is needed to protect our society, there is also a need for "*fundamental change"* and a need to *"map globally"* the changes required. This is essential given how interconnected we are in digital terms. And if data is the "*new oil"* within the global economy, then we need to consider how to protect this critical resource. This led to the idea that data could be defined as part of our critical national infrastructure (CNI) and afforded the same level of protection. At the same time, we need to consider equality of protection, ensuring that those who are most vulnerable to online threats have access to the same level of support, regardless of their societal status so that everyone is given the ability to transact with confidence in a more digitally connected world.

There is a concern that, without a new, shared vision for cyber resilience, different parts of society and the economy may be reduced to living in what one participant described as a *"Darwinian state"*. In this scenario, only individuals and organisations that have access to the resources and abilities to respond to threats will be able to protect themselves and prosper. This creates a false sense of security, whereby large portions of society are likely to remain at risk unless we support them to become more aware of the risks and how to manage them. The interconnectivity of modern society means that *"the weakest link makes the whole system weaker"* and exposes everyone else to the same risks, regardless of the actions of the few. So unless we all change our behaviours and become more security conscious as a society, we will continue to remain at risk and less able to respond resiliently.

An equally clear message from participants concerned the need for flexibility and a co-designed approach to the new vision, rather than adopting an inflexible, top-down approach. As one participant summarised: *"we are living in the industrial age in terms of processes and policies – an age built along the straight lines of big, inflexible plans".* Society may be saturated by constantly evolving technology, but our regulatory systems and policymaking processes have not kept up. In effect, we have been caught flat-footed, and *"our thinking is still from pre-cyber days".* By contrast, there was enthusiasm for a vision that is flexible, adaptable and alert to new developments and intelligence.

A more evolutionary approach is needed, where *"to fail, learn, and adapt"* is seen as a success rather than a negative outcome. These principles have to form the core components for a new vision for cyber resilience and its associated narrative. While recognising that this consultation is just the start of that process, we have considered what should be included in such a new vision.

Core components of a new vision for cyber resilience

There was general consensus on what aspects should be contained within the core of a new vision for a more cyber-resilient society. Components that the participants came up with were:

(i) **Systemic**. The new vision needs to go beyond specific silos and sectors, beyond individual agents acting in isolation within their own specialisms, and recognise that the digital world is more of an ecosystem of interconnected actors; it has no single leader. There will be a need for the new vision to forge cross-boundary ways of working to deliver change across entire systems rather than to individual areas of society.

(ii) **Adaptable and agile**. The new vision needs to be adaptable, recognising the need to shift and evolve in response to emerging threats and technologies as well as the opportunities which may emerge to promote and embed resilience across society. Malicious actors can strike with alarming speed and hide their tracks by moving across different networks and platforms. It will be crucial that the new vision for cyber resilience be both dynamic and nimble in its delivery and evolution. This, in turn, will require greater cooperation and communication between all actors within the digital ecosystem if such information sharing and agility is to be achieved.

(iii) **Trust.** The new vision needs trust for its effective delivery. A high level of trust is needed between actors within the digital ecosystem if information and threats, as well as failures, are to be shared and society is to learn and adapt quickly to threats as they emerge. Furthermore, trust will lie at the very heart of effective resilience because it will be the glue that binds collective adaptability and response in times of attack.

(iv) **Learning.** The new vision needs to demonstrate a strong commitment to learning, not only from each other's digital experience, but also from emerging technologies and from the understanding of new and emergent threats. The ability to share such learning with confidence among actors within the ecosystem will require a high level of trust (see Trust, above).

(v) **Realistic.** The new vision needs to recognise the limits of any interconnected system, as such systems can never guarantee total security. There will always be risk, there will always be threats, and there will always be accidents and human-induced errors. The new vision needs to explain that *"we'll never be fully secure or totally in control",* but that we can manage the risks to an acceptable level.

(vi) **A human approach**. The new vision is about generating change among people, not within systems and processes. Participants felt it will be important to take a people-based, human approach to implementation. The vision should be inspired by the infinite adaptability of people to adapt and change as the context evolves. *"The vision needs to be human – humans are the most resilient things".*

(vii) **Defined rights and responsibilities.** The new vision is about building on the conclusion that cyber resilience is everybody's responsibility and that we all, therefore, have a stake in making the new vision a success. Participants felt there is a need to define the rights and responsibilities of everyone in relation to implementation. Because we cannot, as a society, opt to abandon our personal responsibilities and treat cyber security as something to be *"delivered"* by government to passive citizens, we all need to become more active in our digital citizenship, by taking our responsibilities to each other and to ourselves more seriously in the digital world.

Linked to the previous point about roles and responsibilities is the need to recognise and define the different roles that are required by government, industry, academia and civil society in implementing the overall vision. The role of government, for example, might be to establish a transparent and flexible legislative framework while providing a form of facilitative leadership, while the role of academia would be to pioneer world-class research into cyber resilience and provide a stream of highly skilled innovators.

(viii) **Good communication.** The new vision needs effective communication to wider society in order to be understood and accepted. As mentioned previously, any communication should be designed without overreliance on the language of fear or threat. There is a need for clear, consistent messages about what organisations and individuals can do to protect themselves and how everyone can have a positive cyber experience. Equally, the vision must not be communicated in dry, technical jargon, but in easily comprehensible language, accessible to a wide range of stakeholders. *"Language will be crucial. Let's talk in human, about 'community', not in tech speak, like 'network'".*

3. Making cyber resilience a reality

While we can define the core components of a new vision for cyber resilience, participants expressed concern that, unless the new vision gains buy-in and support from the various actors and agents who form the so-called ecosystem that is dependant on digital technologies, little traction will be achieved in terms of implementing change. The case needs to be made in terms of the beneficial impact of being more cyber resilient, so that a strong level of buy-in to the new vision and its implementation is created. For this to happen, it will be important to understand who currently has a 'stake' in creating a more cyber-resilient society.

Some organisations and agencies are already invested in developing and implementing a new vision for cyber resilience. Trans-national institutions, such as the World Bank and the International Monetary Fund, have an interest in global cyber security and also have access to significant resources. The Organization for Security and Co-operation in Europe and the Organisation for Economic Co-operation and Development have also adopted a proactive role, and the learning from their work is likely to be highly relevant to the development of any vision following this consultation. At the same time, providers of critical national infrastructure around the world take the need for cyber resilience seriously, because they are mandated to ensure continuity of such critical national infrastructure (CNI). But, as mentioned earlier, where does digital (and more importantly data) sit in terms of being considered part of the new CNI within society?

From a UK perspective, we heard how responsibility within the government for cyber security sits across a number of different departments, including the Home Office, the Cabinet Office, the Ministry of Defence and associated intelligence, and crime prevention and defence agencies. All have a remit and a mandate to consider the national security implications of cyber security and to help develop the country's cyber resilience capacity. To date, there has been limited central coordination of such activities. However, with the recently announced National Cyber Security Centre (NCSC),[3] it is likely that there will be much more central coordination of such activities across the different UK departments and agencies and a clearer message from the UK Government about how the country aims to facilitate cyber security and resilience.

Outside government, key participants of the cyber industry, such as 'cloud' providers, major software developers and managed service providers, all have an essential stake in promoting cyber security and, to some extent, cyber resilience. Some of the participants felt that there is an inherent tension for commercial providers between, on the one hand, the need to sell bespoke security solutions, which to date have focused on specific cyber security solutions, and, on the other hand, generating resilience more generally across society.

[3] HM Government. 2016. *Prospectus Introducing the National Cyber Security Centre*. As of 11 October 2016: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/525410/ncsc_prospectus_final_version_1_0.pdf

The focus for the new vision needs to be on generating greater awareness of cyber resilience across society, and this will not necessarily sit well alongside the commercial objectives of such providers. Notwithstanding this issue, it is important to recognise that many of the commercial providers of digital services are high-profile brands, whose services and products are used by individuals and institutions across the world, and they all have a desire to ensure that their customers remain safe and resilient when using digital services. As such, they represent an important and potentially effective communications mechanism for creating better awareness of the need for cyber resilience among the wider population.

Our discussions also identified a range of other agencies that, to date, have not been fully engaged or consulted with regards to cyber resilience. Some of these agencies may have an important role to play in shaping and implementing the future vision for cyber resilience. Local Authorities, for example, have generally not developed a clear or prominent presence in relation to cyber security, despite being responsible for the wider resilience of their neighbourhoods.

In a wider context, civil society as a whole may take an interest in online security issues when there are high-profile cases of, for example, data breaches, but most people generally do not have a good understanding of or interest in cyber resilience; this lack of interest needs to be addressed as part of implementing the new vision. As one participant noted: *“At a personal level, it is concerning how weak the cyber concern is”* among individuals.

Creating greater interest and engagement

Given the fragmented and mixed levels of engagement that were revealed through our discussions, it was agreed that a critical issue for this consultation should be to consider how we can create greater interest and engagement across society with regards to cyber resilience. To date, the narrative from government has focused on the opportunities which digital can provide to the UK economy and on the need for cyber security, rather than on the need for greater resilience. A key recommendation, therefore, which was raised throughout our discussions, is the need to stress the benefits of developing more cyber resilience within society, rather than simply focusing on the threats and risks that are faced.

Because commercial interests will ultimately drive businesses to invest resources in generating better cyber security and resilience, the private sector must be engaged on the basis of operational and brand risk. Problems associated with data management and protection, both key elements of cyber resilience, can have significant impact on the commercial reputation and brand value of any business, and digital aspects of business continuity are taking a higher priority for many organisations. At the same time, we heard that data integrity is an increasingly important issue for many businesses, and that the ability to protect clients as well as their own operational data is crucial to many commercial operations.

How to protect operationally sensitive data is a key issue for many businesses, including, for example, in the extractive industries, where protecting data about extraction sites is core to the business’s survival. As one participant observed, *“Losing commercially sensitive data is catastrophic*”.

The capacity for engaging government was considered by many as more difficult due to *"poor coordination in government"* as highlighted by one participant. This only reinforces the challenge of establishing an agenda across all parts of government, some of which have different policies, priorities and stakeholders. Moving forwards, national leadership is required at a ministerial level for cyber security, so that a clear mandate to coordinate action across all departments can be created. Such leadership might help to deliver more *'joined up'* activity, which, together with the newly established NCSC and soon-to-be-published National Cyber Security Strategy (NCSS)[4] and revised UK Digital Strategy,[5] should help to galvanise a more coordinated and linked approach across government and, in turn, help to generate stronger levels of trust in digital and cyber resilience.

We also noted that there is scope to learn from the experience of other nations as they are also responding to the challenge of cyber resilience. We heard several suggestions through this consultation for how greater knowledge sharing might be undertaken, but we noted that experience in other countries is rarely replicable in different parts of the world. What is interesting, however, is experience and knowledge, which can be adapted, rather than directly adopted, in such a way that it advances thinking and practice in the UK.

UK academia currently lacks research capacity in cyber resilience. Research is taking place on cyber security at 13 Centres of Excellence[6] across the country, but this research is not considering the issue of cyber resilience within society. There is an opportunity for the UK to lead the research agenda in this area by setting out the requirements and by considering what partnerships are required to fund and deliver research that specifically looks at resilience, rather than security, in a digitally enabled world.

In civil society, the key driver for people to engage with the resilience agenda is a simple desire to have uninterrupted access to the Internet (for pleasure and convenience) and to do so safely, in the knowledge that their data and identity are secure and private. We heard several suggestions that government should play a more proactive role in raising awareness of the need for basic security precautions among all segments of the population. This is different from cyber resilience, where many citizens already expect government, businesses and civic society (i.e. the digital ecosystem) to have a clear strategy and plan to provide resilient responses to any threats faced.

[4] At publication the strategy was still unpublished, however, the annual report was available: The UK Cyber Security Strategy 2011-2016 Annual Report (2016) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

[5] Current UK digital strategy (2015) can be found at: https://www.gov.uk/government/news/uk-digital-strategy-the-next-frontier-in-our-digital-revolution

[6] Academic centres of excellence (2016) can be found at: https://www.cesg.gov.uk/articles/academic-centres-excellence-cyber-security-research

So while citizens have a clear expectation that they should have continuity of access to the Internet and digital technologies, they do not consider the development of a more cyber-resilient society as something that is important to them.

Working across boundaries

Although different incentives will engage different stakeholders in developing and implementing the vision, ultimately, progress will depend on creating a collaborative approach that crosses sectoral and national boundaries. We need a systemic approach rather than a silo-based one, and we therefore need to think beyond traditional sectoral delineations to forge new models of dynamic collaboration.

The benefits of such an approach are multiple. It allows us to draw on knowledge from across the ecosystem, and to catalyse and create new solutions by drawing on different experience and strengths as well as combining different approaches and ideas that already exist.

Adopting such a self-organising approach would also mean that delivery of the vision is not reliant on a government-approved or -administered system. The state would still have an important role to play, but not as a dominant partner in the process. As one participant put it, *“government can be bureaucratic, slow moving, tick box-y”*, and what is needed is a more agile approach, capable of responding to emerging threats and of healing itself when security exposures and faults have been discovered.

4. Barriers to developing cyber resilience

Before we consider how prepared society is to embrace a new vision for cyber resilience, it is perhaps important for us to reflect on some of the barriers which might exist to developing and implementing such a vision.

A primary challenge identified in our discussions was the **relative lack of understanding and research** around cyber resilience. The concept of personal and societal resilience has become an increasingly important feature of public policy, but across the UK as a whole there is only an emergent awareness and understanding of the need for cyber resilience. *"This is a new science. There's little historical data or experience."* So in academic terms, this means that there has been little research undertaken to date and that *"the research base is extremely weak; there's not much solid evidence out there".* This lack of robust evidence is an issue in policy terms, and it needs to be addressed urgently.

Even as we learn more, however, there is the additional barrier of the **pace of technological change**. The speed at which technologies are evolving, in ways that can both promote and undermine resilience, means that knowledge and experience can quickly become redundant. One participant used the famous quote *"known unknowns and unknown unknowns"*, often used by intelligence services and based on the Johari Window[7] model, to capture how little is known about the implications of rapid technological change and the emergent opportunities and threats which are created as a result. As another participant noted: *"Systems develop and die so quickly, they can't develop a culture of resilience".*

In the face of such change, some suggested there is *"industrial inertia"* in the sectors concerned with promoting digital security. As mentioned earlier, the digital security sector is able to exploit the current situation, where individuals and organisations are sufficiently confused and frightened to pay for commercial solutions, giving the digital security sector little or no interest in developing more resilient, *"self-organising and self-healing systems"*. As one participant noted: *"The cyber industry is part of the problem. The status quo works for them because some of them miss-sell and over-promise".*

The **'positioning' of cyber resilience** is likely to be a challenge for everyone who has a role in developing and implementing the new vision. The agenda is seen as both highly specialist and 'techy', even though it impacts on almost every part of daily life. It is, therefore, difficult to identify who should take responsibility for developing cyber resilience. Within many businesses, responsibility typically sits within the IT department, while accountability sits with the Chief Financial Officer, with the result that there is a clear mismatch at board/Chief Executive Officer level. This also translates into a particular challenge for academic partners, as cyber security can – and in some cases does – fit in to the remit of many different

[7] Luft, J. & H. Ingham. 1955. 'The Johari window, a graphic model of interpersonal awareness.' In *Proceedings of the Western Training Laboratory in Group Development*. Los Angeles: University of California, Los Angeles.

departments. As a result, responsibility for cyber security is everywhere and nowhere, a point well summarised by one participant, who noted that *"Cyber issues have no natural hub, so there is no ownership of the issues".*

Many participants highlighted the **skills gap** that currently exists, which stems in part from the locational challenge described above. The UK is not producing sufficient numbers of skilled graduates with both the technological understanding and the broader capabilities (creativity being frequently cited) to support the development and promotion of cyber resilience. Further adding to this problem is that many businesses continue to focus on IT security measures in response to specific known threats, as opposed to investing in a creating greater levels of resilience.

And, finally, as a society, we are not clear how much **personal responsibility** individuals should be expected to take when they conduct digital transactions. Shortly before this consultation event, Sir Bernard Hogan-Howe, Chief Commissioner, Metropolitan Police, argued that customers who have poor online security arrangements should not be refunded if their bank accounts are compromised.[8] By abnegating their own responsibilities with regard to personal security, Sir Bernard argued, such people should also abdicate their right to recompense. Automatically refunding customers with poor security simply 'rewards the public for being lax about internet security'. While this comment created some controversy, it does underline the current ambiguity about what level of personal responsibility is acceptable and should be expected of anyone completing digital transactions. It also underlines the need for a debate about what level of personal responsibility is acceptable.

[8] Peachey, Kevin. 2016. 'Sir Bernard Hogan-Howe Online Fraud Refund Claim Provokes Anger.' BBC News. As of 7 October 2016: http://www.bbc.co.uk/news/business-35890028

5. Societal preparedness for cyber resilience

If the new vision for cyber resilience is to be implemented, there is a need to consider how prepared we are in the UK to embrace such a change in behaviour. As one participant highlighted, *"the threat posed by being non-resilient is not well understood by the population. Until it is, all our efforts are likely to be in vain".* Throughout the consultation, we heard that creating the awareness and the changes in behaviour that are needed is likely to be achieved most effectively through collaboration between different actors within the digital ecosystem, rather than through a 'top-down', government-driven approach.

A useful analogy was drawn to the change behaviour generated around the use of seat belts in cars, where, today, most drivers wear a seat belt as a matter of course and without thinking about the need to put one on. Those who do not are breaking the law and, perhaps just as importantly, are subject to social shaming. *"Initially, people wore a seat belt because it was the law. Then it becomes part of the culture – though that takes time, and it doesn't capture everyone."* The key challenge for cyber resilience is how to get to the same point, where, individually and collectively as a society, we are prepared to embrace the need for greater cyber resilience.

To create the behaviour change required for a more cyber-resilient we considered the current situation from the perspective of the four key stakeholder groups represented at the consultation, namely, citizens, business, government and civic society. A summary of the key insights generated on each group is provided below.

Citizens

Having previously concluded that citizens feel that they have a very limited active role to play in helping to create a more cyber-resilient society, we noted that this group has certain expectations. These include the very clear expectations that network access should always be available and that they should have the ability to communicate and transact securely, safe in the knowledge that personal data will be protected from malicious actors. Notwithstanding these expectations, there is a noticeable lack of interest in cyber resilience, suggesting the need for further research to determine what attitudes are held by citizens around cyber resilience, and how this varies across society and the different generations.

At the same time, we identified the need to consider what behaviours are needed from citizens if we are to create a more resilient digital society. As society becomes more digitally enabled, there is a need to consider what 'good citizenship' means in a more digitally connected world.

Business

Participants felt that it is important to reflect on the primary role of a business, which is to meet the needs of the customers and generate a return for investors. Both these outcomes are linked to corporate reputation, and there are clear resilience risks which need to be considered if businesses are to avoid commercial risks from digital security breaches and business continuity problems. We concluded, however, that many businesses seem ill-prepared to tackle the cyber risks and challenges they most likely faced. As one participant noted: *"How many of these things are discussed at board meetings? Do they even understand the risks?"*

There was broad agreement, however, that business should not be expected or required to lead the societal change that is required to make society more cyber resilient. While business has a role to play in encouraging other stakeholders (most notably customers) to change their behaviour, it cannot be held responsible for leading a wider societal change.

One opportunity for business might be to gain competitive advantage from the change that is needed. There are potential reputation and brand benefits from positioning a business as a good 'corporate citizen', and these opportunities need to be better exploited by companies. This might also help to raise awareness of the issue among key customer groups, using a corporate social responsibility approach to support both societal and commercial benefits.

Government

Many participants felt that it is government's role to provide leadership and to drive the development of stronger levels of reassurance and, more importantly, trust that are required, by ensuring we have the appropriate structures and process in place for cyber resilience as a society. Others, however, felt that the UK government has lost the authority to provide the level of leadership that is required and that, following the introduction of devolution (at both the central and the local level), responsibility for leadership is now more devolved from the centre, and that this requires a new model of knowledge sharing and leadership to be created.

There was consensus that government does have an important role to play in creating trust around digital resilience. There are already good examples of government institutions providing such reassurance in other aspects of the digital world, for example, publishing travel advice (Foreign and Commonwealth Office), health advice (Department of Health) and weather advice (BBC). A key challenge, however, is the need to agree who is responsible for setting the policy and strategy. Currently responsibility is too fragmented; responsibility is devolved to different departments, with no one single leader setting the direction and strategy. As mentioned earlier, the creation of the National Cyber Security Centre and the soon-to-be-published UK Digital Strategy may help to rectify this issue.

Many participants felt that, although government has a responsibility for establishing the structures and framework, it should not be government's role to create the content, nor to be responsible for communicating the advice and guidance that is needed. This is where the power of the ecosystem could be utilised to greater effect, ensuring that the most relevant channel is used for communication to each target group.

Academia

Academia has two significant roles to play: first, to produce strong and robust evidence with regards to the risks faced and to help create the business case that change is worth undertaking in terms of cost and benefit, and, second, to educate society about those risks and how to become a 'good digital citizen'. The latter role will likely require changes to the curriculum and must consider cost-effective delivery mechanisms for the skills development required.

At present, academia is undertaking limited research into cyber resilience, focusing more on cyber security. There is a need to consider where resilience as a subject area should sit within the academic establishment. When raising awareness among the population, there is a need to consider the development of new training modules and mechanisms which are capable of delivering risk awareness and cyber resilience training to different sections of the population.

The greatest opportunity to deliver the academia benefits will come via greater academia–industry collaboration driven by real-world issues, both current and anticipated. The legacy, stovepipe approach is not working. A good example of this opportunity is the current corporate venturing for cyber in Israel and the USA, which continues to rise and deliver measurable benefits for those respective societies.

Importance of trust

Achieving the kind of collaborative, connected working that is required to implement this approach will require one crucial element: trust. It is trust that will enable people to work together, to share information they might otherwise withhold and to accommodate the needs of others.

We identified four elements that will be crucial to building the trust required to enable society to embrace a new vision for cyber resilience:

- **Transparency**. All actors across the interconnected ecosystem of the digital world need to be clear about what decisions are being taken, by whom, and to what end, so that any decisions can be openly debated and challenged. There is also a need for greater transparency about the level and nature of risk, so that we can identify and agree on priorities and build confidence across society. A calm, fact-based and accessible dialogue is needed, involving a balanced discussion – one which does not play down risks for fear of upsetting people, and at the same time doesn't shock people as a means of encouraging behaviour change from a perceived state of complacency.

- **Rights and responsibilities**. Nothing is more effective for building trust than individuals and organisations respecting each other and living up to their responsibilities and commitments to one another, meaning that rights are respected and responsibilities are remembered.

- **Collaboration and engagement**. It will be important to undertake changes with people. Imposing change on people creates a dynamic in which individuals are treated as passive recipients of services, and this can lead to suspicion and disengagement.

- **Prioritisation**. It will be important that all actors have a clear sense of agreed upon current priorities for building cyber resilience. Recognising that we cannot prioritise everything, and in the spirit of transparency described above, we need to be clear about the priorities for change across the ecosystem.

If we can generate a consistently high level of trust, we can create what one participant described as a *"civic narrative around cyber resilience"*, and this will help to create a stronger, more consistent understanding about the vision and changes that are being implemented.

6. Conclusions and next steps

Reflecting on the discussions throughout this consultation, we identified eight high-level conclusions, together with subsequent recommendations and practical actions, which should be considered if we are to embed cyber resilience as a stronger feature of digital society within the UK. First, we outline the general conclusions which were agreed upon:

(i) **Strengthen the political imperative.** There is a need to raise cyber resilience up the political agenda at both the national and the local level. This will require all partners to actively promote why cyber resilience is important. This will also include challenging and supporting government and political parties at all levels to take the issue more seriously.

(ii) **Establish civic dialogue.** It was felt that, in parallel to the political engagement, there is an opportunity for engagement with wider society and for creating a civic dialogue about the importance of cyber resilience and about how small changes in individual daily behaviour can make a difference. Any dialogue should involve all parts of society and be focused on educating organisations and individuals about the importance of cyber resilience, while 'crowd sourcing' ideas for implementing the vision.

(iii) **Shape a new role for government**. Throughout our discussions, it was felt that government has not yet found a clear role in relation to the cyber-resilience agenda. Some argued that government has lost the authority to lead this agenda, but the broader conclusion was that government can, and should, play a facilitative leadership role. *"The government needs to understand the appropriate leadership model".* This means we need to create an environment in which different partners can lead on different issues. Some partners may act as thought leaders; others may provide leadership on technical and practical questions. As one participant put it, we do not need a state plan but, rather, *"an environment where things will grow"* in an evolutionary fashion.

(iv) **Identify what works**. A suitable task for government would be to lead a discussion about what works and what does not work or works less well in the realm of cyber resilience. The current research base is limited. This makes it all the more important to identify relevant intelligence and highlight the gaps in our knowledge, so that further targeted research can be undertaken. One participant reflected that we need to *"increase the evidence base to help demonstrate the importance of issues, inform planning, convey messages, and test theories".*

(v) **Craft a new charter of cyber rights and responsibilities.** There is a need for a new charter of rights and responsibilities to set out in clear and practical terms what individuals and institutions can expect, and what is expected of them, in terms of online behaviour to promote cyber resilience. This will provide a much firmer basis for generating trust and will provide a framework for the growth of further digital collaboration.

(vi) **Invest in education, skills and training**. There is a need to invest in a wide-reaching programme of education, skills and training around cyber resilience. It was felt that civic dialogue alone will not sufficiently raise awareness of cyber resilience. The approach to educating society needs to be multi-layered and look to engage different groups through a range of methods, such as in-house training for employees, outreach education for older and/or isolated households and tailored in-school provision for pupils.

(vii) **Capitalise on the devolution agenda**. Throughout our discussions, we focused on the UK as a whole, but we also heard a consistent message about the importance of translating national strategies into actions that can be implemented locally and regionally using local governance structures. Much is happening at a local level, but this needs to be better understood and shared. As one participant explained, *"We need to turn the cyber national plan into a regional plan, and come up with a resilience plan for it."*

(viii) **Think globally**. We felt that, at the same time as we focus on the regional and local devolution agenda within the UK, we need to look outward to the rest of the world. Cyber resilience is a global issue, and a great deal could be learned and shared about cyber resilience through supra-national bodies, nation states, academic institutions, companies and others interested stakeholders. There is, however, a need to create the infrastructure for such sharing to take place in a trusted and confidential manner.

Recommendations and practical actions

Progressing from the conclusions described above, we make the following recommendations for moving forward:

(i) We need to work with governments to create a new national network for cyber resilience. Such a network would bring together all interested parties and act as the convenor and facilitator of the political and civic dialogue that, we concluded, is needed to increase awareness of cyber resilience. A key initial output from this forum would be the development and publication of a new charter of cyber rights and responsibilities. Government should be requested to provide the resources needed to establish this independent network, with participants at this consultation being asked to help create the terms of reference and identify potential membership.

(ii) Central government needs to be encouraged to identify and appoint a minister with responsibility for cyber resilience and a policy lead to coordinate cyber resilience activities across government. A key barrier to creating a higher-profile cyber resilience agenda across government is the confusion about where responsibility for cyber resilience should sit, so the creation of such an appointment would help to create better leadership across government.

(iii) Further dialogue is needed with central government on how to translate the National Cyber Strategy into regional strategies for different parts of the UK. The devolution agenda presents a timely opportunity to achieve this. The appropriate level of devolution would need to be agreed on by the relevant partners, including the Department for Communities and Local Government (DCLG), the Cabinet Office and the devolved administrations, where relevant. The strategies should operate within overall national principles but should set out the specific issues, threats, infrastructure strengths and needs, and priority actions for the specific region. To inform this process, we recommend that DCLG lead a roundtable event designed to generate and review ideas for devolution and local collaboration around cyber resilience and, more specifically, to review the CyberNorth model from the perspectives of scope, stakeholder involvement and work streams currently being undertaken.

(iv) Government should consider the establishment of regional cyber resilience partnerships (using a similar approach to the Local Enterprise Partnership network) that will be responsible for local cyber resilience infrastructure. These partnerships would bring together universities, the police and industry to ensure that resilience infrastructure is planned for and provided. The emerging CyberNorth initiative provides a model of how this might work.

(v) There is a need to establish a new cyber resilience observatory that is capable of gathering intelligence about what works well and what does not work or works less well. This should be managed by an independent organisation with a standing remit to monitor academic, theoretical and practical developments for new evidence. It should monitor UK and international developments and should not simply focus on good or best practice but, rather, on the wider range of intelligence and learning, including failed initiatives and unsuccessful outcomes.

(vi) Knowledge and experience gathered from the observatory discussed above should be used to inform a national programme of education, skills and training that can be used to educate the population about cyber resilience, including the rights and responsibilities that are set out in the new charter of cyber rights and responsibilities. There is a need to create a behaviour change strategy in relation to cyber resilience. Linking to the development of the new charter of digital rights and responsibilities, we need to consider how to create fundamental shifts in behaviour across society.

(vii) There is a need to consider how we maintain an international dialogue with interested parties (and potential partners in research and commercial ventures) in terms of cyber resilience. There is a need to review what international initiatives and networks already exist to determine how existing infrastructure can be leveraged to support ongoing dialogue and sharing of knowledge and experience.

Next steps

This consultation was one of four topics covered in the Corsham Institute 2016 Thought Leadership Programme investigating the opportunities and challenges created by digital technologies in society.

The other topics were:

- Digital health: Digital’s role in health and care
- Digital living: Getting the most out of digital society
- Trust and ethics: Building a more informed digital society

A key findings report[9] highlighting the overarching themes to emerge from across this year’s programme, as well as the key findings from each of the four consultative events, is now available for download on the Corsham Institute website.

Ci and RAND Europe look forward to building on the findings from the 2016 Thought Leadership programme with a series of further Thought Leadership consultative events to be held during 2017 that will focus on:

- Education
- Open science
- Currency
- Civic engagement

[9] Corsham Institute and RAND Europe. 2016. Thought Leadership 2016 Programme: Key Findings. RR-1771-CI Santa Monica, Calif.: RAND Corporation.

Participants

First Name	Surname	Position and organisation
Claire	Alexander	Chief Operating Officer, Corsham Institute
Gregory	Austin	Professor, Australian Centre for Cyber Security, University of New South Wales
Richard	Bach	Assistant Director, Cyber Security, UK Government
Matthew	Blades	Chief Insecurity Officer, XQ Digital Resilience Ltd
William	Barker	Deputy Technology Leader (Strategy, Resilience & Futures), Department for Communities and Local Government
Andrew	Beckett	Managing Director, Cyber EMEA Region, Kroll Associates
Kamall	Bob	Programme Manager (Local Cyber Resilience), Department for Communities and Local Government
David	Carroll	Chief Executive, XQ Digital Resilience Limited
Christopher	Crowther	Head of Information Security, Regency IT Consulting
Philip	Dawson	Chief Executive, Assured Digital Group
Matthew	Ettelaie	Manager, Cyber Defence Services, KPMG LLP
Tarquin	Folliss	Director, Sequitur Ltd
Sarah	Grand-Clement	Research Assistant, RAND Europe
Alasdair	Greig	Director, Northstar Ventures
Alexandra	Hall	Research Leader, RAND Europe
John	Houghton	Principal Consultant, Shared Intelligence
David	Hudson	Consultant, Diospyros Ltd
Kevin	Jones	Professor and Executive Dean, Faculty of Science and Engineering, Plymouth University
Andrew	Jones	Service Owner – Industry Schemes, Communications-Electronics Security Group

First Name	Surname	Position and organisation
Anthony	Klein	Managing Director, Airbus Defence and Space CyberSecurity Consulting
Richard	Knowlton	Executive Director (Europe), Internet Security Alliance
Catriona	Manville	Senior Analyst, RAND Europe
Sarah-Emily	Mutch	Engagement Director, Smart Societies Institute
Brian	Parry	Director of Strategy and Thought Leadership, Corsham Institute
Neil	Robinson	Policy Officer, NATO
Jeremy	Sanders	Director and Founder, Corsham Institute
Siraj	Shaikh	Reader in Cyber Security, Coventry University
Erik	Silfversten	Analyst, RAND Europe
Daniel	Sprague	Technical Director, Smart Societies Institute
Nicky	Stewart	Commercial Director, UKCloud Ltd
Jeffrey	Thomas	Founder and Director, Corsham Institute
Timothy	Watts	Director, Levels Consulting
Scott	Wilkie	Senior Advisor, CSIRO/Data 61
Elisabetta	Zaccaria	Founder and CEO, Cyber Y Ltd

Thought Leadership 2016 programme delivered by:

Corsham Institute

http://corshaminstitute.org

Corsham Institute (Ci) is a not-for-profit organisation whose mission is to accelerate an inclusive digital society that is citizen centric and trusted. We do this by creating a physical and intellectual space to convene, connect, educate and innovate across sectors.

Ci was formed in 2013 to explore the opportunities and benefits of digital society, both social and economic, with particular focus on shaping a future where individuals can realise their potential in a highly connected world.

Our four key areas of work are promoting digital skills and education, driving research and thought leadership, powering enterprise and realising digital communities.

Our values are to work openly and collaboratively and to make a sustainable contribution to the economy for both national and commonwealth public good. We do this by imagineering, co-developing and sponsoring services for citizens and government where trust, ethics and informed consent come first.

RAND Europe

http://www.randeurope.org

RAND Europe is a not-for-profit organisation, whose mission is to help improve policy and decision-making through research and analysis.

Part of The RAND Corporation, we were founded in 1992 to provide quality impartial research and rigorous fact-based analysis, and to serve the policy needs of EU institutions, governments, charities, foundations, universities and the private sector. Our work lies between that of universities and consultancies, combining academic rigour with a professional, impact-oriented approach. In other words, we operate as a research-focused business, using a professional services model within the context of a public good mission.

We combine deep subject knowledge across many policy areas – including health, science, innovation, defence and security, transport, infrastructure, criminal justice, education, employment and social policy – with proven methodological expertise in evaluation, impact measurement and choice modelling.

St George's House

http://www.stgeorgeshouse.org

St George's House was founded in 1966 by HRH The Duke of Edinburgh and the then Dean of Windsor, Robin Woods, as a place where people of influence and responsibility can gather to grapple with significant issues facing contemporary society.

The House offers a safe physical and intellectual space, rooted in history but focused firmly on the future. The emphasis throughout our carefully-crafted consultations is on dialogue and discussion to encourage creative thinking, informed debate and sustained engagement. This is a place where participants can make a real contribution to society, where personal enrichment and social progress are mutually compatible, and where Wisdom is nurtured.