This document is a record of the outcomes of a workshop held by EPSRC on 22 September 2014. The workshop discussions were brought together in a report by Professor Chris Hankin (a member of the Strategic Advisory Group of the RCUK Partnership for Conflict, Crime and Security Research) at EPSRC's request.

The initial report has been accepted by EPSRC. As such, this document's contents are now the responsibility of EPSRC. Any questions or comments should be directed to alex.hulkes@epsrc.ac.uk.

Human Dimensions of Cyber Security

When thinking about cyber security, it is easy to focus on the technical issues such as malware detection and intrusion detection and prevention systems. It is salutary to observe that many recent, major cyber security breaches have started with a failure in the human interaction with technology – increasingly because of sophisticated social engineering by the attacker. The human dimension of cyber security is therefore an essential area for further study.

The UK has internationally leading groups in this area. Representatives of this community have worked together to identify priority areas for investigation within Human Dimensions of Cyber Security.

The rest of this document is organized into 5 sections which reflect the results of these deliberations:

1. Design, build and measure

The central issue is how we can design security into products from inception, considering and pre-empting possible criminal attacks in advance. However, much unexpected or unplanned use of technology is not only non-criminal; it is also highly valuable. Constraining the use of a product thus prohibits innovation. The beginning of a solution to this tension is to understand the achievement of security as a process, rather than a one-off check-box.

There is much to be said in favour of co-design of technology: combining reflective practitioners with input from users both in the design of products and in the selection of research. A better understanding of how to achieve security practices that are endorsed from their conception by active citizens as end-users would significantly improve the resilience of our systems.

How do we measure security? There would be both theoretical and practical benefit in further work on security impact assessments. Theoretically, there is a case to be made for the view that we know security when we see it, and thus the best way to embark upon a conceptualisation of security is to develop better tools for its measurement. Practically, security impact assessments are a clear and deliverable instrument that academic researchers are well-placed to design.

What is security?

There is a common, over-narrow understanding of security. This extends only to the direct integrity of one's person and possessions: whether, for example, one's mobile phone's encryption would withstand a brute force attack. Discussion encouraged a broader perspective on the concept. The working understanding used was that where things that should not occur can occur, we are less secure. A secure system is one that does not permit improper outcomes. A yet broader definition carries the notion of 'human security'. This includes people's wellbeing and prosperity. Doubt was expressed about this conception: by incorporating welfare, it threatens the idea that there are conflicts between security and with other values. The theoretical research on a framework that answers the question 'what is security?' would supply us with a concept that both extends to the broader, systematic context, but does not extend so far that intuitive tensions between security and other values become meaningless.

The broadness of the concept of security, so that it extends beyond a mere technological idea and into a human context, emphasises the need for interdisciplinary work throughout the field. Study of security includes study of people's behaviours, of their manipulability, and of ecosystems of ideas, norms, and practices.

How do we measure security? There would be both theoretical and practical benefit in further work on security impact assessments. Theoretically, there is a case to be made for the view that we know security when we see it, and thus the best way to embark upon a conceptualisation of security is to develop better tools for its measurement. Practically, security impact assessments are a clear and deliverable instrument that academic researchers are well-placed to design.

The functioning of markets is of particular interest in understanding the dynamics of security. Do markets render us inherently insecure through the creation or stimulation of needs and wants, and is security threatened where reasoning that is appropriate to commerce enters the political realm? Or is there an economics of security, a way of reaching an efficient degree of free public space, constrained by limits that aim at its protection? A research question in this connection is whether we can have an idea of rankings of security that is independent of the sphere that is supposed to be rendered secure.

Security design

The central issue is how we can design security into products from inception, considering and pre-empting possible criminal attacks in advance. However, much unexpected or unplanned use of technology is not only non-criminal; it is also highly valuable. Constraining the use of a product thus prohibits innovation. The beginning of a solution to this tension is to understand the achievement of security as a process, rather than a one-off check-box. The nature of attacks is unpredictable, and so resilience-testing should be understood not as a single test, but as a form of institutional architecture. The Heartbleed attack is an illustration of how our present structures fail to meet this challenge.

There is much to be said in favour of co-design of technology: combining reflective practitioners with input from users both in the design of products and in the selection of research. A better understanding how to achieve security practices that are endorsed from their conception by active citizens as end-users would significantly improve the resilience of our systems. Thus, one model for design is the open source movement; another is the direct

funding of proprietary systems. With limited resources, there is a choice for policy-makers regarding the extent to which they facilitate each of these models. Some authors refer to the problem of 'security in the wild', noting, for instance, how PGP has not become widely adopted[1]. The route for research here is to understand how we can 'domesticate' security by extending the ambit of the conception of research and design projects.

This informs, furthermore, our view of the design of laws. Statutes consistently lag behind technology. For instance, identity misuse is not directly covered in law, and illegal drugs may be tweaked so that they are similar but no longer fall under the laws that ban them. There is therefore need for investigation into how we can consistently put decision-making with regard to security issues in the hands of citizens.

[1] Dourish, P., Grinter, R., Delgado de la Flor, J., and Joseph, M. 2004. **Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem.** *Personal and Ubiquitous Computing*, 8(6), 391-401.

2. A theory of everyone

A key problem emerges when designers design for themselves and their colleagues, not for the end users. A designer's perception might be: "if it works for me, then it works for everyone; if I put in the effort as a designer then that's the work that is important or significant". An analogy is the world of fashion: high fashion is about designing imaginative clothes that look good on models, not on the average person.

Major research questions to address in this area include collecting more demographic, ethnographical and experimental evidence about users' behaviour and perceptions – with respect to cyber-security measures, and related issues – including the opportunity costs of time and "work arounds" associated with real-world online behaviour.

An underlying theme was users' rationality and the extent of behavioural bias (issues covered by other groups), but a broad consensus formed by this group was that human users are not stupid. They are capable of making sensible decisions if enabled to do so; but their rationality is bounded by constraints on information and cognitive processing. In designing for real-world users, designers need to respect users and focus on understanding how they make decisions about protecting themselves (or not) from privacy and security violations.

The designer-user interface: empathetic design

A key problem emerges when designers design for themselves and their colleagues, not for the end users. A designer's perception might be: "if it works for me, then it works for everyone; if I put in the effort as a designer then that's the work that is important or significant". An analogy is the world of fashion: high fashion is about designing imaginative clothes that look good on models, not on the average person. Similarly, in privacy and security design, the focus is on the intellectual challenge and/or the attitudes of colleagues – designers are rewarded for clever, complicated designs that will appeal to their peers, and these are not necessarily the designs that ordinary people will use well. Partly the problem is a misalignment of goals and incentives: the designer is seen to be the main actor in the process; in some sense the hero of the story. This connects with the public imagination – high profile online innovators are glorified, partly because what they do seems mysterious, almost magical, to the user. This distorts the process. The designer's experience/perspective is indispensable, but designers do need to understand end-users too. There may also be over-confidence in the designers that their design should rule versus what the user

needs or desires: this is what the user *should* want and need, rather than what the user *does* want and need. A key challenge is how to encourage designers to engage more effectively with end users; drawing on an empathetic "theory of mind" approach, encouraging designers to empathise with the end-users, most of who have limited technical knowledge. Designers also need to recognise the emotional dimensions of decision-making, particularly the fact that users' emotional responses in online versus offline contexts will differ significantly.

Diversity, fairness and wellbeing

Diversity amongst user groups is another important factor to incorporate into security designs. Designers need to embed to recognise that people are not the same; people relate to machines in different ways, and their online behaviour has profound implications, good and bad, for their wellbeing. A "middle-aged" perspective often dominates cyber-security innovation, and this may unwittingly exacerbate exclusion and vulnerabilities amongst particular groups. Demographic change is an important issue to consider in design: the barriers to adoption may be rigid amongst the oldest age groups; the youngest users' fluency in the online world is both an advantage and a challenge – if younger users under-estimate their vulnerabilities. More work is needed in understanding these trends. We (viz. Ladan Cockshut) have personal experience of an exercise in which participants were asked to map their own engagement with social networks onto a map of the online games they play. The results were very different, even within a given demographic group—the lesson being that one approach will not necessarily serve even the same 'profile' or 'demographic' group. More evidence is needed about these trends.

One key challenge lies in understanding the diversity of obligations and expectations with respect to cyber security – should people expect businesses and/or government to protect them from violations? Does the ordinary user have obligations in terms of making sure that they protect themselves, e.g. via anti-virus updates and basic security measures. We should make digital society fair for people who don't choose how they live in it. Digital society writes the code and decides how it works, and everyone else has to live by his or her rules. More evidence is needed about how people have reacted to this. In addition, issues of fairness and equity are crucial, especially as many users have not chosen to live and operate in a digital world – e.g. online banking is ubiquitous now, but it is not clear that everyone embraces it. Issues of fairness link to participation – to promote fairness we need to ensure that users have opportunities to participate in a dialogue about ethics

and rights. Political scientists can contribute to these debates in unraveling the power dynamics between creators/designers and users – and in analysing if and how users' needs are marginalised. For example, 'terms and conditions' are inconsistent with notions of fairness and participation because so few people have the time or expertise to read and understand privacy policies, and website terms and conditions. For example, McDonald and Cranor (2008) estimated that the average US user would have to spend 201 hours reading privacy policies properly – at an opportunity cost of US$781 billion a year[2]. More research is needed to see if this result is robust and to explore similar potential economic impacts for the UK and other economies.

Key research questions to address in this area including collecting more demographic, ethnographical and experimental evidence about users' behaviour and perceptions – with respect to cyber-security measures, and related issues – including the opportunity costs of time and "work arounds" associated with real-world online behaviour.

Risk, uncertainty and irreversibility

The interplays between risk, privacy and security can be tricky to unravel. There is some insularity in the way we view risk in security research. People's risks attitudes vary across different groups and, as behavioural economics shows, will vary even for a given person dependent on the context. This is a key question in the privacy and security design. We need more evidence about risk perceptions, how they vary across contexts, and how people respond in the real world to risks in different situations. One problem is that there are many potential commentators. Who knows what risk are, who identifies the risks? Vendors have an interest in marketing their own products – they have vested interests in these discussions. So do we keep the vendors out of the discussion?

Another research question is how to understand how risk and uncertainty affect online decision-making. In economics, this distinction is made between situations governed by quantifiable laws, or easily replicable and so can be expressed in terms of frequency distributions. To illustrate the first: e.g. rolling dice and betting on a double six is a situation of quantifiable risk; it's not possible to know what will happen, but it is possible to get an objective quantifiable measure of probability. Uncertainty is about what's unknown. For issues relating to privacy and security, the

[2] McDonald AM and Cranor LF (2008). The Cost of Reading Privacy Policies, *I/S: A Journal of Law and Policy for the Information Society* 2008 Privacy Year in Review issue http://www.is-journal.org/. Downloaded from http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

problem is unquantifiable uncertainty; there are so many possibilities and drivers, the situations are so complex that it is impossible to quantify the chances of different outcomes. For example, a business investing in an innovative new security design that has never been marketed before – it is impossible in this situation to quantify the likelihood of success, as there is no prior information on which to base an estimate of success. A businessperson is still able to imagine a numerical estimate of likely profits for example, but these numbers will be spurious, often without objective basis. More research is needed in understanding the difference between uncertainty and risk in scenarios relating to security design. We also need more work on understanding how vulnerabilities and threats feed into the problem of uncertainty.

Another question is how the various stakeholders (users, designers and vendors) can come together to properly understand the implications of complexity and uncertainty for online privacy and security. Given perceptions of risk and making security, which doesn't inhibit people's actions. Ironically, whilst data security issues are strongly emphasized for online financial transactions, in the financial world there is at least some reversibility. One crucial distinguisher is irreversibility: once security has been breached, it is impossible to go back to a secure situation. This is an important question to address in assessing the risks of being online. If your passwords are compromised, how bad is that? Often, banking and financial sites are most securely protected. There are risks in online shopping and banking but by and large if you incur a financial loss you can be refunded with relatively small implications. This is because, in economic terms, all money is "fungible" – one £20 note is the same as every other £20 note – and each can be used in the same way in a wide range of situations. Money can be recovered, insurance policies can be devised to compensate people who are victims of financial fraud; money can be earned again. Personal data is very different, and issues of privacy and security are therefore potentially much more profound and important. If your naked photographs are circulated and this causes distress, nobody can undo that – the outcome is irreversible. If a security breach causes a death, that can't be undone either. People may react differently if they understand not just how much it's worth but to what extent it's irreversible. Google's recent concessions - deleting past histories of personal information from Google searches - reflects an attempt to respond to a problem of irreversibility. Ultimately, the best cure is prevention, but people are often much more careless with their personal information than with their financial information. More research is needed to explore how and why people form their mental models of different online decisions, and how they can be enabled to develop a better understanding of

their online interactions.

Key challenges

In addition to some of the challenges identified above, the following challenges were identified at the conclusion of the sessions.

How to get people to buy-in

Getting human beings to "buy-in" to security is a challenge, and participatory measures could be employed to encourage user security, but more evidence is needed about design issues, business process issues, and the interplay between incentives and human behaviour. There is no common understanding of measuring success, and we need to understand in more detail how different users respond to security issues.

Empathetic security design

A key challenge is respecting all cyber-security stakeholders: users, designers, and system administrators. We also need to understand real world behaviours, taking into account diversity both in user populations, and security risks/perceptions. Research is needed in developing empathetic approaches to cyber-security education, design, and new business processes. This is necessarily a multi-disciplinary research agenda, requiring engagement with the business sector too. Research and business communities together need to make an effort to understand end users and practitioners. If this can be achieved then both users and designers can develop effective mental models of privacy and security. Related issues include understanding relationships between risk, uncertainty and irreversibility - in particular on issues of reversible versus irreversible harm?

Understanding diversity and impacts on well-being

Understanding diversity, motivation, well-being and perceptions in risk, studying in different groups and users, etc. is a key challenged. More evidence is needed about demographic and other influences on online behaviour and/or perceptions of risk and uncertainty.

3. Risk, trust and response

Users cannot distinguish between serious risk and consequence if all risks are presented as equally important. It is important that the user recognises their role in ensuring security in business and society and that as they make risk decisions they carry responsibility. People try to minimise the complexity of their decision-making when they have to make a decision. Less information can be better than more; having simple and strong rules can be easier than more permissive and complex rules.

In addition to developing a knowledge base to understand the factors that influence human behaviour, an understanding of methods to eliminate the bad advice that is so pervasive is also needed.

With regard to risk and uncertainty, one of the first issues discussed was whether there were commonly understood definitions for risk and uncertainty. Risk can mean different things to different people and is context dependent. To fully explore risk and uncertainty requires understanding of the particular context. It was discussed that a micro-analysis of behaviour in situ, how individuals respond to risk and trust decisions, might be useful. However, it was noted that assessing an individual's understanding of risk may be difficult since they may react out of the ordinary when they become the focus of a study. It was felt that the reactions of individuals would vary depending on their level of experience. Inexperienced people have been found to be sensitive to expert advice whereas experienced people ignored warnings. Understanding the micro behaviours of groups was required so that unintended consequences didn't arise. It was felt that a longitudinal study should be considered to provide understanding around who people look to for advice, how does that factor into the decisions they make.

The group discussed the work of Gigenrenzer[3] and that was a theme that recurred throughout the first session. In particular, risk from a psychological perspective and how risk varies over time they experience.

The group discussed relationship formation cyberspace and considered issues such as when developing trust at rapid speed whether it affects risk appetite. This ties in closely with

[3] Gigerenzer, G. (2015). *Simply rational: Decision making in the real world.* New York: Oxford University Press.

ethnosecurity and the individual in the context of the relationships they have.

A key issue identified was that users cannot distinguish between serious risk and consequence if all risks are presented as equally important. As such the communication of the risks is vital. This will empower users to make security decisions. It is important that the user recognises their role in ensuring security in business and society and that as they make risk decisions they carry responsibility. It was recognised that people try to minimise the complexity of their decision-making when they have to make a decision. Less information can be better than more; having simple and strong rules can be easier than more permissive and complex rules.

It was thought that in addition to develop a knowledge base to understand the factors that influence human behaviour, an understanding of methods to eliminate the bad advice that is so pervasive was also needed. Simple, pragmatic advice was required and needs to be led by the Government.

During the second session the group considered the research challenges. The importance of empirically-based research concerning what is actually happening on the ground in a micro fashion, was identified early in the session. Knowledge of how people engage with the Internet would be needed to ensure the success of a research programme.

It was noted that the challenges should consider the role of the human in cyber security. It was felt that there were too many disparate pockets of work currently. We need to think of the human as an active collaborator in the process. This requires many disciplines coming together. The group discussed that it is not only the user who may be attacked that is human – but so too is the attacker. More work was needed regarding understanding of the motivations of these attackers. Understanding the role of these people would require knowledge and expertise from a number of disciplines.

It was felt that current work isn't as extensive or collaborative as required. If the community is serious about interdisciplinarity it needs to consider how the research would be conducted. New thoughts are required – the standard approach used for projects would not be appropriate. Rather there was a need for much more stakeholder buy-in through a network that would allow ideas to be shared and a community of practice to be constructed.

The issue of micro and macro understanding pervaded the discussions. Understanding of the complexities was needed and information should be shared up from the micro to the macro and back down again. A challenge is to relate the micro to the macro - exploiting micro-level outputs to form theory. There is also a need for horizontal communications – across different problem areas – to drive forward understanding of the issues. There may be more information if we can get sectors of industry to trust each other and share information, experiences and understanding across their sector and then hopefully also sharing with other sectors.

The group considered whether there could be a Unified Theory of Security.
Currently there exists no unified theory, and that can hamper progress. Engineers have different understanding and opinions around security to those of social scientists. Talking a common language would enable coherence in the solutions and understanding of the subject. It was felt there was a need to understand system-wide security in context. Security fits within a context there are different actors, different technologies at play, a full context wide understanding is lacking. We are attempting to protect information when we don't understand the utility of that information to different attackers –a system-wide understanding would help in this regard.

The session concluded that the three key challenges around the subject would be:

- Multi-disciplinary micro analysis of user behaviour and perceptions
- Exploiting a micro-analytic understanding – a new theory
- Understanding system-wide security and context

4. Understanding people

How much are individuals able and willing to invest in return for cybersecurity. Ability rests in part on cognitive capacity to meet the requests for multiple usernames, complex passwords, unique PINs etc., across multiple systems or devices in use. In contrast, willingness may depend on more subjective assessments, including judgements of trust and transparency between provider and user, or between one user and another. A novel approach is to consider cybersecurity as a pseudo-social trust-contract. Three challenging areas are:

- Public Understanding of Risks, Likelihoods and Consequences: The research challenge outlined here demands the exploration of individuals' assumptions, decision making and resultant behaviour. Key to this may be a move to greater transparency and accountability over data collection, storage, onward use, and risk of breach so that individuals have a better appreciation of risk and likelihood.
- Proportionality – or 'How Much is Too Much?': Key to this challenge is the need to understand (i) the value of what is being secured by the provider, and (ii) the value of what is being requested of the individual. A full understanding of these issues will support the development of cybersecurity systems that earn implicit if not explicit social acceptability.
- Trust, Transparency and Accountability in Cyber Security contexts: The research challenge outlined here calls for a twofold approach involving the identification of trust markers and models, and the development of reparation pathways.

Whilst these three challenges undoubtedly overlap, they also have in common the ethical issues of informed consent (knowing what you are disclosing and for what purpose), information creep (use of information given for one purpose to satisfy another purpose), and data ownership (whose data are they anyway). As a consequence, it is recognised that issues of security overlap with issues of privacy.

Cybersecurity is understood to depend vitally on two components – the design of systems to deliver effective cybersecurity; and the capacity of individuals to comply rather than bypass those systems. Whilst the sector may cite human failure as the major risk to cybersecurity, it is clear that individuals must be at the centre of the design process to begin with so that systems are clear, robust and acceptable without being intrusive. This calls for a better awareness of individuals' capacities and boundaries within cybersecurity.

At the heart of this issue is the question of how much individuals are able and willing to invest in return for cybersecurity. Ability rests in part on cognitive capacity to meet the requests for multiple usernames, complex passwords, unique PINs etc., across multiple systems or devices in use. It also rests on cognitive understanding, and this raises issues of plain English legal reform, appreciation of risks, and appreciation of likelihood of those risks. In contrast, willingness may depend on more subjective assessments, including judgements of trust and transparency between provider and user, or between one user and another. It may also depend on individual's values and boundaries around social acceptability, and key to this may be the demonstration (or otherwise) of a fair request for a fair return. A novel approach is to consider cybersecurity as a pseudo-social trust-contract. This brings with it not only a rich body of theoretical research on issues of relationship formation and maintenance, but also the opportunity to capture the nuanced differences that exist between users and contexts rather than continue a blanket approach to cybersecurity. As a consequence, three challenges are articulated:

Public Understanding of Risks, Likelihoods and Consequences

We make security choices all the time without necessarily having a full appreciation of the risks. For example, how likely is it that our computer is part of a bot net, that our bank details are being stolen as we type them in, or that our data from two quite transparent sources may be mashed together for a third unintended purpose? Amidst the dialogue on the privacy paradox, it is understood that the very nature of the online environment can encourage otherwise risk-averse individuals to make risky decisions for the sake of instant gratification through social media, gaming or online purchases. Part of their rationale may be a false impression of risks or of the likelihood of those risks, together with an 'it will never happen to me' attitude. Consequently, the core of this research challenge is a fundamental enquiry into the public understanding of cybersecurity in terms of risks, likelihoods and consequences.

The research challenge outlined here demands the exploration of individuals' assumptions, decision making and resultant behaviour. Only with a full understanding of this may the cybersecurity sector respond by providing information of relevance in shaping or nudging behaviour. Key to this may be a move to greater transparency and accountability over data collection, storage, onward use, and risk of breach so that individuals have a better appreciation of risk and likelihood. This will support the cognitive judgements that sit behind their 'ability' to invest in cybersecurity.

Proportionality – or 'How Much is Too Much?'

How did we get to a situation in which children are now asked to provide fingerprints in the school dinner queue, and face recognition software now makes it possible to identify and tag individuals in photographs on social media sites? Both may reflect 'technology taken too far' with the result that high value information is used to authenticate access to low value goods, services, information or entertainment. As a consequence, there is a call for proportionality within security and cybersecurity sectors.

Key to this challenge is the need to understand (i) the value of what is being secured by the provider, and (ii) the value of what is being requested of the individual. A socially acceptable system may depend on these two elements being balanced. Of course, this is a far from trivial issue as the value of information may change across time and context. For instance, a particular identifier may increase in value as technologies emerge to enable its use in new and more precise contexts. Similarly, the value of what is being secured may be perceived differently by users and providers, making the issue of proportionality very complex.

Nevertheless, the research challenge outlined here suggests a need for much greater understanding of the cost/benefit balance so that cybersecurity as a practice becomes trustworthy through inherent fairness. This challenge recognises the need to expect and respect diversity across individuals and groups. Indeed a plethora of research questions exists if we are to understand differences in risk perception, levels of habituation to risk in the short term, and shifts in perceptions of risk over a longer term or life course. A full understanding of these issues will support the development of cybersecurity systems that earn implicit if not explicit social acceptability and, in the wake of the UK Identity Card project, this must remain a priority. This will support the subjective judgements sitting behind an individual's 'willingness' to invest in cybersecurity.

Trust, Transparency and Accountability in CyberSecurity contexts

If the user is not the 'enemy' in the cybersecurity arena, who is? Reflecting back on the development of a trust relationship, a key cybersecurity problem is that we cannot tell friend from foe. Indeed, con artists, hackers, government and big business may all be perceived as 'the enemy' so any simple model of trust is inadequate.

The research challenge outlined here calls for a twofold approach involving the identification of trust markers and models, and the development of reparation pathways. The identification of trust markers is a complex task given that the online world 'never forgets'. Amidst current and future technologies underlying Smart Cities, the mediators of trust are fundamental so that we can understand, build, and repair trust in online relationships. Similarly,

the development of routes for reparation are clear in financial sectors, or in legal sectors, but currently the same cannot be said for the cybersecurity sector. Thus, there is currently no answer to the question of who a person should turn to in the event of a breach.

This is a timely challenge amidst the current discussion of Trusted Identity Providers. With their introduction, the potential exists to explore different models of governance to build local trust networks that can mediate global business. In an arena where smart censors are ubiquitous (the so-called 'Internet of Things'), the capacity to collect, transfer, and breach identity and security makes the trust relationship central, and requires that designers and lawyers work hand in hand with social scientists to understand the landscape of mutual trust and reparation. This will support the subjective judgements sitting behind an individual's 'willingness' to invest in cybersecurity.

Overarching Issues

Whilst these three challenges undoubtedly overlap, they also have in common the ethical issues of informed consent (knowing what you are disclosing and for what purpose), information creep (use of information given for one purpose to satisfy another purpose), and data ownership (whose data are they anyway). As a consequence, it is recognised that issues of security overlap with issues of privacy. Nevertheless, the research challenges outlined here hold security as the primary focus.

5. Evolution of Cybercrime

The priorities here follow the "4 Ps" of the CONTEST programme as they apply to cybercrime:

- Cybercrime **Prevention** – Do we need to rethink approaches?: New technological developments that are anticipated to mainstream from 2020 will enable people to network laterally across networks, make their communications untraceable and facilitate transactions via crypto currency (e.g. bitcoin). Thus circumventing many traditional forms of regulation and potentially disrupting investigative approaches. Mis-information can result in social and moral panics. How can the culture of fear around cybercrime be reduced and the public be informed so that demands for security match what police can deliver?
- **Pursuing** CyberCriminals – How does cyber-criminality and its regulation evolve?: Where do the ideas for crime emerge from; by what mechanisms do they develop from ideas into practice? Linked to this is a third question over how do cultures of cyber criminality evolve? To what extent, for example, are cybercrimes simply another fashion that will go out of fashion?
- **Protecting** Computing Systems and Infrastructure - How do we balance security with freedoms to avoid developing an over-protective state?
- **Prepare** to respond to new types of cybercrime - How do we know when new types of cyber-victimisation are emerging?: The problem is that victims do not always feel the helplessness, outrage, or alienation that is felt with offline crime. They may not sometimes be aware that they have been a victim. How then you do reduce repeat victimisation in such cases?

Our working group covered a lot of ground in discussion, but inadvertently addressed the 4P's that exist in the National Security Strategy which collectively increase the level of (in this case) cybersecurity. These are to 'prevent' it, 'pursue' cyber-criminals, 'protect' systems and 'prepare' to respond to new forms of cybercrime. Underlying the responses is the interdisciplinary issue of understanding the relationship between science and social science - the technical and the human factors. There is also the important need to distinguish between the threat/risk agenda of the security and the harm agenda of crime, though where networked technologies are concerned; both are different aspects of the cybersecurity debate.

1. Cybercrime Prevention – Do we need to rethink approaches to <u>Cybercrime Prevention?</u>

We discussed a range of issues relating to cybercrime prevention which led to the following questions that need to be answered with quality empirical research.

a) Do we need to rethink approaches to cybercrime prevention in light of recent technological and political developments to provide a higher levels cybersecurity? New technological developments that are anticipated to mainstream from 2020 will enable people to network laterally across networks, make their communications untraceable and facilitate transactions via crypto currency (e.g. bitcoin). Thus circumventing many traditional forms of regulation and potentially disrupting investigative approaches.

b) How do users consume preventative computer security? Why do particular user groups adopt or reject different computer security techniques and products. What information informs their choices? The cybersecurity industry is dominated by a few clear players who have a vested interest in insecurity. Are the messages that are being given to the general user communities practical, or are they driven by economic interest? What, for example, are the benefits of the many free security products that are currently available? Also, would it be in the general public interest for operating system manufacturers to provide security updates for illegally downloaded OS?

c) Who is responsible for cybercrime prevention? With regard to i) individuals ii) companies iii) government iv) agencies, each of which play different roles in cybercrime prevention? Of particular concern is whether or not the various preventative messages are coherent and part of a broader preventative strategy. Alternatively, are they fragmented by self-interest?

d) How do the various public agencies deal with the interaction between people and the software they use? This links to b) & c). Do they all work to the same end goal?

e) How do you prevent the circulation and perpetuation of mis-information including folk wisdoms, internet mythology taboos? Mis-information that can result in social and moral panics. How can the culture of fear around cybercrime be reduced and the public be informed so that demands for security match what police can deliver?

f) How do you reduce fears of insecurity so that users feel less inhibited? Following on from this, what do the different stakeholder groups consider to be appropriate levels of cybersecurity? The above and also previous questions can be answered through an Ethnographic study of computer use and security consumptions.

2. Pursuing CyberCriminals – How does cyber-criminality and its regulation evolve?

a) How does cyber criminality evolve i) where do the ideas for crime emerge from ii) by what mechanisms do they develop from ideas into practice? Linked to this is a third question iii) over how do cultures of cyber criminality evolve? To what extent, for example, are cybercrimes simply another fashion that will go out of fashion? Do folks simply follow others or are they politically or socially 'cause' driven. To what extent are 'traditional' motivations present, e.g. financial gain etc., revenge, kudos?
b) How do you improve the pursuit of cybercriminals? Is this a problem for the police and improving police effectiveness or is it a question of developing a more joined up approach towards cybersecurity? How do policing methods evolve?
c) How do you prevent recidivism amongst cybercriminal? What evidence is there that it is, in fact, a problem? Do sentences for cybercrimes vary across jurisdictions? There is a need to identify comparisons across jurisdictions? How do you deal with the problem of multi-jurisdictionality, where a crime could be prosecuted in more than one jurisdiction?
d) What evidence is there that current sentencing structures deter offenders from reoffending? Are there alternatives to imprisonment (where they could become recruited by organised crime groups), for example, forms of re-education, training, therapy (in some cases).

3. Protecting Computing Systems and Infrastructure - How do we balance security with freedoms to avoid developing an over-protective state?
a) As national Security concerns rise about cybercrimes and responses develop, are we witnessing the effective 'criminalisation' of civil space as a by-product through increased and intrusive surveillance online and offline? Are we witnessing a loss of civil liberties as the result of this process?
b) How does the politics of the risk agenda match interfere with the capabilities to protect computing systems? (links with 1 e)).
c) What are the comparative impacts of cybercrime across jurisdictions? Are all jurisdictions impacted by cybercrime in the same way? The globalising qualities of cybercrime suggest a transcendence of geography, but is the geography of cybercrime manifested in some other way, for example, language?
d) How legitimate are proactive actions against future cybercrimes? To what extent are they legal?

4. Prepare to respond to new types of cybercrime - How do we know when new types of cyber-victimisation are emerging?
a) How can the UK Cybercrime intelligence model be improved to develop a more strategic and quicker approach to emerging cybercrimes?

b) How does vulnerability towards victimisation evolve with technological developments? Is this because of technological ignorance of risks, or is it because of criminal ingenuity, or a combination of both? This raises questions of levels of public awareness and learning about risks. Why, for example are users deceived? What are the dynamics of social engineering? How do users become risk aware and risk averse?
c) How can repeat victimisation be reduced? The problem is that victims do not always feel the helplessness, outrage, or alienation that is felt with offline crime. They may not sometimes be aware that they have been a victim. How then you do reduce repeat victimisation in such cases?