PaCCS - KTN POLICY BRIEFING

Innovation challenges in cybersecurity

KTN
the Knowledge Transfer Network

Partnership for Conflict, Crime & Security Research

Foreword

In November 2015, a select group - from academia, government, industry, and the investment sector - gathered to explore the barriers to innovation in cybersecurity, and means to overcome them. The group was chosen not only as authorities in their field but to provide a diversity of experience and opinion from different sectors. This policy briefing note captures the key findings and messages to emerge from these deliberations (run under the Chatham House Rule to encourage free and open expression of opinions). This note is our summary of proceedings, but we have checked with all the participants that the text reflects discussions held and points made.

The workshop took place soon after the Chancellor of the Exchequer announced a significant new National Cyber Plan (see Annex). He talked about "a painful asymmetry between attack and defence" which makes it easier and cheaper to attack a network than to defend it. The type and nature of threats are evolving fast, he said, and defending Britain means "we have to run simply to stand still." The volume of attacks is growing: GCHQ dealt with 100 national cybersecurity incidents a month in 2014; by the summer of 2015 this had doubled to 200 a month. But the attack surface is also expanding, with an increasingly connected world: by 2025, 100bn sensors will be networked, with 2m new connections made every hour.[1]

Our discussion was informed by a professional understanding of the problem as well as recognition that there are enormous opportunities to generate wealth and social value by delivering innovative cybersecurity solutions. Two dominant themes emerged from our workshop: how to take ownership of the problem; and how to maximise the opportunity for innovation and growth. In the following pages, we set out the workshop's analysis of each of these challenges (under the headings of "Market Literacy" and the "Innovation Pipeline"), together with our remedies for addressing them.

Although innovation is not, of course, exclusively about Small and Medium-Sized Enterprises (SMEs), they emerged as a focus of debate. We believe our recommendations could help to transform this sector: breaking innovation out of universities; giving start-ups the business and other support they need; and helping SMEs to secure kitemarks for their products and to get their first customers. All of which would bring knock-on benefits to our wider economy and society.

Our assessment is inevitably UK-centric, but we recognise that our findings are relevant to the rest of the world, not only in terms of the threat but also in terms of opportunities, market scale and partnerships. A successful national strategy will incorporate shaped international engagement.

The power of this Note derives from the combination of talent and expertise brought together to address Innovation Challenges in Cybersecurity. We hope that these authoritative recommendations will be given the attention they deserve.

Dr Tristram Riley-Smith, External Champion
Partnership for Conflict, Crime & Security Research

Dr Siraj Ahmed Shaikh, Cybersecurity Lead
Knowledge Transfer Network (KTN)

[1] Source: Huawei's Global Connectivity Index 2015 p 10.

Participants

Research

Dr David Aspinall	(University of Edinburgh)
Dr Jeremy Bryans	(Coventry University)
Dr Lee Gillam	(University of Surrey)
Prof John McCanny	(Queen's University Belfast)
Prof Steve Schneider	(University of Surrey)
Dr Jatinder Singh	(University of Cambridge)

Industry

Nick Coleman	(IBM)
Ruth Davis	(BT)
Stuart Laidlaw	(Cyberlytic)
Mike Loginov	(Ascot Barclay Cyber Security Group)
Dr Mike Short	(Telefonica)

Policy

Giles Cockerill	(Office of CSA for National Security)
Dr John Baird	(EPSRC)
Chris Ensor	(CESG)
Dr Paul Galwas	(Digital Catapult)
Matthew Gould	(UK OCSIA, Cabinet Office)
Robert Madelin	(European Commission)
Andrew Tyrer	(InnovateUK)

Investment

Steve Berry	(Waterbridge Capital)
Tom Ilube	(Crossword Cybersecurity)
Dr Mark Reilly	(IP Group)
Alex van Someren	(Amadeus Capital Partners)
David Leftley	(Bloc Ventures)
Auriol Stevens	(Restoration Partners)

Dr Greg Shannon (Assistant Director, Cybersecurity Strategy, OSTP White House) had hoped to join the discussions, but this was not possible. He did, however, feed in his Cybersecurity Research Challenges.

Disclaimer: the views expressed in this document may not necessarily reflect the views of all participants or organisations they represent.

The challenge of market literacy

Understanding the risk

- We do not know enough about the threat and our vulnerability to it; just as healthcare needs to understand disease, cybersecurity must understand attacks on our digital infrastructure/economy and our susceptibility to them.
- Communicating the risk is an additional challenge, since there is often insufficient information to allow sound management of risks; there is a common perception that the actual cost of cyber attacks is not so high that expensive countermeasures are justified.
- There is a lack of corporate ownership of the problem; causes vary from complacency to ignorance.
- Partly due to the above, it is not always clear where liability lies; dysfunctional economic mechanisms mean that sometimes those carrying responsibility for weak defences are not bearing the cost or suffering the consequences.

Determining effective cybersecurity

- There is an over-supply of technical solutions with few clear criteria to judge effectiveness and suitability; there are few kitemarks (or equivalent) denoting quality, or easy to follow recommendations, or trusted catalogues of solutions.
- There are few trusted cybersecurity professionals with the necessary mix of breadth and depth of sectoral expertise; it is difficult to distinguish noise and hype from authoritative advice.
- The human element is relatively little understood when it comes to responsible behaviour and insider threat; the problem of cybersecurity is essentially a fusion of technology, policy and behaviour, and crosses many disciplines.
- The various standards that do exist are disconnected, encouraging a "tick-box" approach to cybersecurity which has its limitations; a compliance-based approach risks "confusing the menu with the meal".

Plight of UK start-ups

- A lack of ambition constrains many start-ups from venturing abroad; is there good understanding of the global market opportunity?
- There is insufficient appetite from "patient", longer-term investors to support entrepreneurial aspirations to growth.
- An export-led approach will only come about with the right type of practical and logistical support to SMEs; their problems range from gauging and accessing the overseas markets to paying for the overseas trips which they need to make in order to begin exporting.
- Partly due to the above, SMEs are limited in their ability to secure investment, since the UK market is judged small and ill-defined; not encouraging for scale-ups to emerge.

Addressing the challenge of market literacy

Risk leadership

- Cybersecurity leadership, particularly from companies managing critical national infrastructure, needs the support of regulators and policy makers.
- The insurance industry (a major enabler) could be asked to play a strategic role in terms of addressing the problem, defining needs, clarifying standards, costs and liabilities, and driving an international approach.
- The National Cyber Centre (NCC) should establish a Cybersecurity Scientific Advisory Board, with responsibility for communicating threats and advising on solutions.
- Policy-makers should consider the need for an agency like the National Institute of Standards & Technology in the USA (http://www.nist.gov/), which works closely with commerce and industry.
- The creative arts can help make the invisible visible. Bodies such as PaCCS could sponsor a “Cy-Fi” Short Story Prize (or Short Film) designed to communicate the benefits of connectivity and data driven solutions and the hidden threat from cyber attacks and their consequences.
- The computer gaming industry could be invited to develop tools to help the public understand and counter cyber threats.

Towards better cybersecurity

- NCC should lead an effort to deliver better cybersecurity governance, supported by legislation if necessary.
- Set up a Cybersecurity Executive, following the model of the Health & Safety Executive. This is needed to impose an obligation on organisations to report attacks and breaches, and develop responses, including audits.
- Recognise excellence through kitemarks for quality cybersecurity products and services; Cyber Essentials and Academic Centres of Excellence in Cyber Security Research (ACE-CSRs) help, but more is needed to apply standards.
- Solutions catalogues and approved centres of excellence are both needed.
- Establish and promulgate mandated standards in hardware, software and services (through regulation and legislation).

Global ecosystem

- The Cyber Growth Partnership should develop a SME framework for exports.
- UK Trade & Investment (UKTI) should provide SMEs with more pragmatic guidance on operating overseas and gaining better market knowledge.
- UK Government agencies such as InnovateUK should encourage an ecosystem that enables global partnerships, for example working with the EU and NATO’s Security Investment Programme (NSIP) to identify shared needs such as those across Critical National Infrastructure and Law Enforcement; or the US National Strategy for Trusted Identities in Cyberspace (NSTIC), with its trials in he identity management space. The aim should be to benchmark “best in class” and to identify scaleable global solutions.

The challenge of the innovation pipeline

Skills gap

- The biggest constraint on national ambitions to deliver effective cybersecurity is the skills gap; the technical challenges associated with cybersecurity make this crucial.
- Lack of requisite talent is a problem in Chief Information Security Officers' operational teams and in start-up companies delivering solutions. This covers skills in Science, Technology, Engineering & Mathematical and in Social and Behavioural disciplines.
- Cybersecurity awareness is lacking at the board level; industry leadership can no longer afford to remain ignorant or disinterested.

Broken feedback loop

- The feedback loop between university, industry and government, the "triple helix" as Prof Henry Etzkowitz calls it, is broken; is there a "quadruple helix" that needs attention with investors added to the mix?
- Applied and interdisciplinary research into cybersecurity must be improved to trigger innovation; there is often a lack of clarity on research challenges over the next 3-5 years.
- Academic culture and incentives continue to work against multi-disciplinary research and the commercialisation of research insights; applied research and entrepreneurship is under-funded: PaCCS represents a rare example of how this can be done.
- Engagement between large engineering companies, investors and start-ups is difficult to get right, with cultural barriers often getting in the way; start-ups often struggle to get their messaging right when seeking funds, often being unrealistic and unfocused in their approach. Conversely large engineering companies are not geared to attract start-ups and can rarely act at a pace suitable to incubate outside innovation.

Working with HMG

- HMG procurement processes remain complex and incomprehensible; particularly for SMEs who find public sector procurement overheads high.
- Security "classification walls" introduce an added barrier, particularly in cybersecurity, making it difficult for suppliers to understand requirements. This, in turn, inhibits investment; commercial advantage is limited to a few companies (and investors) with high security clearance.

Addressing the challenge of the innovation pipeline

Narrowing the skills gap

- BIS and DCMS should commission a skills-capability-capacity audit for cybersecurity to gain a better understanding of the skills gap.
- We should welcome and promote new initiatives around higher and degree level apprenticeships, an Institute of Coding, cybersecurity MBAs, and engagement with schools;[2]
- Existing efforts across universities need to be encouraged around suitable industry sponsorship and postgraduate qualifications.
- Industry should facilitate and support 4-year university degrees with mandatory work-experience within the sector.
- Initiate low-cost, quick-wins to stimulate engagement with schools, which may include, for example, a cybersecurity computer game and a BBC 'Make it Digital' themed effort to develop cybersecurity modules.

[2] The UK Government, with strong industry support, is partnering with the British Computer Society and the Institution of Engineering & Technology to support and fund the Trustworthy Software Initiative. From 2015, a module on cybersecurity has been a mandatory component of all accredited UK software engineering degrees. And the first MBA in cybersecurity has been established at Coventry University), providing a platorm for executive awareness and education.

Fixing the feedback loop

- Stimulate and prioritise the research pipeline with a National Cyber Research Strategy to emphasise applied research with industry-linked routes to impact.
- Celebrate best practice in knowledge and technology transfer, using the model established by the Centre for Secure IT at Queen's University Belfast for the new innovation centres.
- Support the Dowling Review recommendation for a "one-stop shop" for business-university collaboration, e.g. through engagement with the National Centre for Universities and Business (NCUB).
- Support collaboration and secondments across all three sectors, adding entrepreneurial strands to ACE-CSRs, Research Institutes and CyberInvest.

Closer cooperation between industry and HMG

- SMEs need to be better educated about HMG and defence procurement, and EU and foreign markets, through existing mechanisms at DCMS, UKTI and the KTN.
- HMG's adoption (in February 2015) of the European Directive (2014) is a game-changer, introducing the Innovation Partnership Procedure. This must be publicised and HMG procurement teams should be urged to use it. New funding available through HMG's newly announced Defence and Cyber Innovation Fund needs to be better positioned with this regard.
- Coordinated efforts, possibly through NCC, are needed to break down the security "classification wall", getting more information into the open domain, alongside arranging security clearances for a wider community of researchers, industry professionals, investors and entrepreneurs.

Annex

Features of HMG's national cyber strategy relevant to the workshop[3]

- HMG is investing £1.9 billion over five years to protect Britain from cyber attack and to develop sovereign capabilities in cyberspace, almost doubling the previous provision;
- The capabilities of the National Cyber Crime Unit will be boosted and stronger defences will be installed for government (detecting attacks, finding where services are vulnerable and fixing them);
- A National Cyber Centre is to be established (under the Director of GCHQ), providing "a unified source of advice and support for the economy". It will:
  - make it easier for industry to get support from government, and for government and industry to share information on the cyber threat;
  - draw on secret world-class expertise (in GCHQ) while working with industry, academia and international partners to keep the UK protected against cyber attacks;
  - build important capabilities in the new Centre to handle incidents as they arise (ensuring a faster and more effective response to major attacks), including teams with sector-specific expertise (from banking to aviation) to advise companies, regulators, and HMG departments.
- An ambitious programme to develop cyber skills will be launched, finding young people with cyber talent,

  training them, and giving them a diversity of routes into cyber careers. To support this, HMG will:
  - run a £20 million competition for a new Institute of Coding to train the next generation in high-level digital and computer science skills;
  - build higher and degree level apprenticeships in key sectors, starting with the finance and energy sectors (creating a retraining programme for highly skilled workers who want to move into cyber);
  - roll out a major programme for talented 14 to 17 year olds, involving after-school sessions with expert mentors, challenging projects, and summer schools where those on the scheme can see where their cyber skills can take them.
- Create a commercial ecosystem in which cyber start-ups proliferate, get the investment and support they need, and are helped to win business around the world:
  - set up programmes to support the best cyber start-ups, providing training and mentoring for cyber entrepreneurs;
  - establish two cyber innovation centres - places where cyber start-ups can base themselves in their crucial early months, and which can become platforms for giving those start-ups the best possible support;
- Create a £165 million Defence and Cyber Innovation Fund, to support innovative public procurement (across both defence and cyber security).

[3] Taken from the Chancellor of Exchequer's speech given at GCHQ on 17 November 2015.

PaCCS and KTN

PaCCS (the Partnership for Conflict, Crime & Security Research) is an initiative of Research Councils UK. The Partnership aims to deliver high quality and cutting edge research to help improve our understanding of current and future global security challenges (currently focusing on the themes of Conflict, Cybersecurity and Transnational Organised Crime). It supports collaboration by bringing together researchers from across disciplines to work on innovative projects and creates opportunities for knowledge exchange between academia, government, industry and the not-for-profit sector.

KTN (the Knowledge Transfer Network) is the UK's innovation network. It brings together business, entrepreneurs, academics and funders to develop new products, processes and services. Established to foster better collaboration between science, creativity and business, the KTN has specialist teams covering all sectors of the economy – from defence and aerospace to the creative industries, the built environment to biotechnology and robotics. The KTN has helped thousands of businesses secure funding to drive innovation and support them through their business cycle to see that investment through to success.

PaCCS and KTN have a shared mission to enhance opportunities for engagement, understanding and knowledge exchange between academia and the wider community.