Rustat Conference Report

Cyber Security - An Assessment of the Threats to National, Economic and Individual Security

Rustat Conferences, Jesus College, Cambridge   Thursday, 3 February, 2011

Jesus College
Cambridge

Contents

Rustat Conferences
www.rustat.org

FOREWORD TO RUSTAT CONFERENCE REPORT
By Dr Rex Hughes
Visiting Fellow for Cyber Security
Wolfson College, Cambridge

As this Rustat Conference has chronicled, securing cyberspace has become one of the great security challenges of the early 21st century. In the UK alone, the Cabinet Office estimates that cyber crime costs the UK economy no less than £27 billion annually.[1] According to their estimates the majority of this cost results from intellectual property damage to business.

This year alone we have already learned of numerous widely publicised examples of how cyber crime has adversely impacted large scale multinational business operations. The Lulz Sec exfiltration attack on Sony's Play Station Network forced the Tokyo based electronics giant to shut down one of its most lucrative consumer services. Even the economic future of cloud computing became more uncertain when Seattle based Amazon.com's S3 service was shut down by covert tactics from hacker group Anonymous. And in the public sector numerous foreign ministries are still assessing the damage from the unprecedented leaking of classified diplomatic cables via Julian Assange's infamous 'WikiLeaks' website.

As several Rustat Conference participants have noted, mitigating these risks will take a concerted effort by a diverse set of public and private partners. Whereas cyber security solutions have traditionally been developed and managed almost exclusively by the IT community, the growing criminality and proliferation of hazardous 'rogue code' calls for greater engagement by experts beyond the engineering community. Diverse non-technical experts such as risk managers, economists, criminologists, psychologists, law enforcement and military personnel, are increasingly called upon by institutional leadership to help broaden the scope and reach of cyber defences.

Developing a comprehensive approach to national cyber security challenges is increasingly seen as the way forward by senior British Officials. As articulated by UK Armed Forces Minister Nick Harvey in July of this year,

---

[1] *The Cost of Cybercrime:* A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, February 2011

"Information technology systems underpin the functioning of government, finance and business, so we need to be smart about what we protect, ensuring we include all the systems upon which components of our critical national infrastructure rely," "But I don't believe we yet have a full picture of what all the threats and defence capabilities are, and therefore the first step should be to improve information sharing across as many sectors of the UK economy as possible so that a combined response can be made, National security cannot be guaranteed without international action, but there is a lot of work to be done in developing a common understanding of the threats and how best to defend against them," [2]

Fortunately, as this Rustat Conference has shown, the University of Cambridge and its Silicon Fen partners are well positioned internationally to contribute innovative ideas and solutions to this growing security/economic dilemma. At the University, a number of important innovations are on the horizon, including more secure routing protocols and quantum cryptology. And in keeping with the spirit of the 'Cambridge Phenomenon', in time a number of these innovations will be transformed into new products, services, and perhaps if lucky even the next ARM corp.

In order to build upon the rich exchange of ideas and perspectives from this Rustat Cyber Security meeting, a conference will be convened in London on 29 September 2011 (in association with the Rustat Conferences) – named the Cyber Security Forum 2011 . Now that we have taken an inventory of issues, this second meeting will begin to explore a range of options for new programs, policies, and partnerships. In time we hope several of these projects will attract national and international support for the advancement of UK global leadership in cyber security.

We are grateful for your support and participation in the first Rustat Cyber Security Conference, and we look forward to welcoming you as well as new partners at the London conference in September. In the meantime, we look forward to your ideas for business collaboration or joint research.

Dr Rex Hughes
Visiting Fellow for Cyber Security
Wolfson College, Cambridge
July 2011

---

[2] Remarks by Nick Harvey to National Security 2011 – July 5th London

Introduction

The revolution brought about by computer technology and the Internet has delivered huge benefits and opportunities to society, but it also poses a threat as it may expose us – government, organisations and individuals – to digital attack. How real is this and how clear and present this danger? On 3 February 2011 the Rustat Conference on Cyber Security was attended by approximately 50 high-level delegates drawn from government, academia, media and industry. They came together to provide an informed judgment on the extent and nature of this threat to governments, commerce, national infrastructure and individuals and to question what the object of cyber security should be.

This report is a synthesis of the speakers' prepared remarks and the ensuing discussion, held under auspices of the Chatham House Rule.

Towards a Cyber Lexicon

'Cyberspace' is a term understood in different ways by different people. It was first conceived in the 1982 short story *Burning Chrome* by William Gibson, and developed in his novel *Neuromancer* written in the Orwellian year of 1984. Gibson had observed children playing early video games in arcades and noticed the way in which they seemed to conceptualise a world behind the screen. In his novels he developed this observation to describe a virtual environment in which data from interconnected computers is abstracted into a graphical representation that operators can navigate and access. As of early 2011, 'cyberspace' has become journalistic and academic shorthand for the physical infrastructure of the Internet, as well as the metaphorical environment in which websites 'exist'. A clear majority of the conference participants identified this rather vague label as unhelpful when considering the range of challenges relating to information security and the protection of both public and private computer networks, as well as individual computers. In particular, one participant cautioned that a conceptual over-reliance on the virtual aspect of 'cyberspace' could lead to a failure to assign locality to threat scenarios, and thus to complicate needlessly the legal dimension. Using the example of an Internet-enabled car, which was further referenced on several occasions by other conference delegates, it was noted that for all the manipulation of computers possible in the virtual world, "car brakes still fail in three dimensions".

Additionally, another participant observed that although the word 'cyberspace' was inappropriate shorthand for the TCP/IP protocol that governs the Internet and could and should be discarded by the policy community, the term 'cyber warfare' was probably here to stay.

This led to a discussion of the difference between 'cyber warfare' and 'cyber security'. It was agreed that far from being a navel-gazing exercise, this was in fact a crucial point as it went to the heart of deciding how governments conceptualise, plan for and resource their cyber strategies. One conference delegate observed the need for a new lexicon to describe this subject, citing the

general lack of technical expertise and understanding amongst the political class. Another highlighted the relevance to military doctrine, which relies upon agreed definitions. A third participant posited that the lack of understanding currently demonstrated by politicians and non-specialist senior officials was in large part driven by the lack of definitional clarity and served to exacerbate bureaucratic rivalry and jurisdictional competition between the military and security and intelligence agencies.

It was agreed that the military play and will continue to play a key role in cyber security. It was however suggested in discussion that the delineation between military tasking and that of the security and intelligence agencies needed clarity. This came back to the earlier point about what precisely constitutes a cyber attack. In addition to their status as stand-alone threats, it was agreed that cumulative acts of cyber espionage and cyber crime retain the potential to be construed as a military attack. Thwarting attacks on military networks and communication systems were agreed to be the responsibility of the military themselves, although there was no consensus over attacks on major military contractors or privately owned defence research establishments.

Discussion turned to the question of media representations of 'cyber-geddon' in which an attack or series of attacks by a hostile state entity represented a doomsday scenario equivalent in destructive terms to defeat in a conventional war. It was agreed that this represented an extremely unlikely scenario, as the scale of such an attack would inevitably reveal the identity of the attacker and thus leave them vulnerable to retaliation by the allies of the injured state. Furthermore, hostile states harbouring ambitions on such a scale were deemed unlikely to rely solely on cyber attacks and to discount other methods of coercion. Cyber crime and espionage were agreed to be the main threats in the current era.

The State's Role

The cyber environment has few bars to entry for states that are unable to compete with established powers in a conventional military sense. One participant noted that to some extent this levels the playing field in competition between nations, in part as a vector for intelligence collection, which can in turn lower the cost of military defence. However, another participant noted that not only hostile states act in this way, and that organisations which display some state-like characteristics such as Hamas, Hezbollah and Al Qaeda also make use of the cyber environment for these purposes. A third participant reminded the group that liberal democratic nations also possess legitimate intelligence collection needs and that would-be cyber regulators need to leave room for intelligence collection when considering implementation of new legislation both at the national and international level. Additionally, cyber defences would need to take account of individuals acting in a malign fashion from the inside of organisations belonging to democratic nation.

The Internet was originally designed to be a survivable military Command and Control (C2) system. It was only when academic research institutes were added to the network and the US government deregulated the protocols to allow an open design to be embraced that the rapid growth of commercial connections took off. Its success as a platform for and driver of prosperity was therefore very much an unintended consequence and several participants observed that governments must weigh their desire for computer network security against the economic opportunity afforded their citizens by a largely unregulated Internet. Further discussion highlighted that in democratic societies such as the UK, a number of institutions run courses that actually teach people how to hack into computer networks, even if this is not their raison d'etre.

It was noted that the public sector continues to run a lot of its own systems and is also in the process of expanding its online presence both to drive out bureaucratic inefficiencies and to provide a better level of service to its citizens. This greater online presence thus represents a greater level of interest to criminal groups and hostile governments. Furthermore, the neat boundaries separating spheres of the public sector, private sector and the citizen were observed to have blurred, if not disappeared altogether and that therefore the entire national 'ecosystem' must be protected in a holistic fashion.

Nonetheless, the vast majority of the networks that constitute the area of interest for governmental cyber defenders belong to the private sector. Another participant posited that in macroeconomic terms it is the role of government to correct perceived market failures. The same individual observed that the four main generally accepted causes of market failure and cases necessitating government intervention are present in the cyber domain, namely:

1.   **The provision of public goods**
    - *Including legal frameworks and instruments of state power*

2.   **The correction of information asymmetry**
    - *Under-reporting of criminal attacks by the private sector for PR reasons leads to misunderstanding of the risks being run*
    - *Information exchanges between the government and the private sector in a trusted environment to protect commercial sensitivities*

3.   **The counteraction of market power**
    - *Regulation can impact commercial competitiveness*
    - *It is unrealistic to expect companies to be responsible for defending against acts of foreign state espionage*

4.   **The reduction of negative externalities**
    - *Striking a balance between short term commercial gain and long term detrimental effects to the economy as a whole*

Human Factors

It was an oft-repeated point during the conference proceedings that technical solutions are only one aspect of cyber security and that processes and practices governing human-machine interaction were equally if not more important. As one participant put it, "You can't legislate against a stupid or malicious user". Line management of individuals with network and system access is therefore crucial, as demonstrated by the WikiLeaks case where one low-ranking individual with malicious intent had access to a huge portion of US military and diplomatic cable traffic on the US SIPRNET classified network. One participant noted that SIPRNET was created in response to post-9/11 accusations that US security and intelligence agencies did not share enough information but that it was a combination of poor personnel management and network management that led to the disclosure of the sensitive information, rather than the technical integrity of the system itself. The same participant further noted that the use of digital rights management technology, which controls which users on a network can see and do what from where, would have mitigated the SIPRNET disclosures, although probably not eliminated them completely.

When considering the dynamics of human behaviour relating to the use and protection of computer systems, two significant cultures need to be brought together, namely computer scientists and engineers. It was noted that the former tend to be more concerned with 'winning the space race' and developing leading edge technological capabilities, whereas the latter develop and build systems, whether physical or virtual. It was further observed that these two closely related disciplines were nonetheless distinctive working cultures that had developed over decades. Some participants questioned just how long it may take to develop a true, universal cyber-security culture and highlighted the inherent challenges.

It was regarded as crucial that organisations develop a culture whereby security was a "day one consideration" and built in as the system is developed. Several participants observed that retrofitted security measures nearly always required a large capital investment that many organisation were unwilling to commit to, leading to the abandonment of the security upgrade altogether. One participant suggested that over 30% of the cyber attacks in 2010 could have been prevented if both private and public sector organisations had applied the latest security patches to their operating systems. It was further noted that these patches are provided free of charge by the manufacturers and are very easily installed. Another participant took the point further by suggesting that the government subsidise private citizens for the cost of having their personal computers scanned and cleaned by a high-street computer vendor. He suggested an analogy with the public health system, in which infections rates of 3-5% of a given disease amongst the general public was viewed as unacceptable and requiring of major governmental intervention. Why not apply a similar philosophy to the diagnosis and treatment of infected and vulnerable computers? Another participant noted that anti-competition laws had actually forced at least one major software provider from including free anti-virus software with their other products, and that a way round this might be to provide a government sponsored anti-virus package to the citizenry.

When considering how ordinary users might become increasingly vulnerable to the proliferation of Internet-enabled devices, significant concern was voiced by one participant regarding the concept of the 'Internet of Things'. This refers to the addition of an Internet connection to everyday electrical items such as cars, fridges and toasters. The participant noted the rationale ascribed to the ability to remotely control the functions of devices through the Internet, but questioned the overall utility of such an approach and recommended that users consider the full range of associated risks implications, including the Internet-enabled car cited earlier, whose safety and braking systems could conceivably be interfered with through an Internet-enabled remote computer. Another participant noted that despite the risks, commercial companies are wont to disregard certain security measures in order to meet strict deadlines.

Additionally, the use of smart electricity meters was highlighted and it was questioned why the world's billions of Internet users would have an interest in the national grid. The discussion emphasised the point that the utility of smart devices was not being questioned by the group, merely the need to connect them to the Internet. With 80% of UK households expected to be in possession of smart meters by 2018, the question of whether the government was clear about the benefits to users, let alone the risks, was raised. It was suggested that the installation programme seemed to represent a case of 'technology for technology's sake'. Another participant observed the phenomenon of 'Internet time' whereby the rapid pace of technological change inhibits the adoption of well thought through policies and adoption practices, citing the fact that social networking site Twitter did not exist five years ago but already has 200million users.

The question of identity was raised again but this time in the sense of individual privacy. It was noted by one participant that online shopping websites do not care who a person is as long as the credit card details match up, whereas governments want individuals' online identities to be the same as they were the day before, and for users to be real people who can therefore be coerced. This was identified by another participant as a question of differential privacy, where the shopping website only requires information to be disclosed for the purposes of that particular transaction, whereas the governmental approach tends more towards digital certification or fingerprints and iris scans. It was noted with some irony by a different participant that in the commercial aspects of cyberspace, governments are not special, but just another customer.

A different participant observed that anonymity cannot happen in isolation and that it necessitates hiding in a crowd. The proliferation of anonymity software should furthermore not be regarded with trepidation, as most people want it for good reason most of the time. Its proliferation means that it will become more prevalent whether we want it to or not, and that we should therefore take advantage of the beneficial effects, for example by encouraging democratic protests in repressive countries.

Nevertheless, a different participant affirmed that as a security official, the first people he would investigate were the ones who wished to remain anonymous.

Legislation and International Regulation

Discussion turned to the fact that in cyberspace, borders and distance have no meaning as they do in the physical world. One participant noted that since the end of the Cold War, the Signals Intelligence (SIGINT) community has talked of 'shaping the environment' that came to be known as cyberspace, with different major powers responding in different ways. In Russia and China for example, the environment has most certainly been shaped by the intelligence agencies. On the other hand, the UK's Regulation of Investigatory Power Act (RIPA) has provided a clear and accountable legal footing for intelligence agencies when their work necessitates exploitation of the cyber realm. By contrast, the US approach embraces executive fiat for similar operations. It was suggested that far-reaching international regulation on cyber operations would be fiendishly complex to enact and enforce, and that as a result a Highway Code might prove an easier and more satisfactory approach to squeezing organised criminals out of the cyber environment. Yet another participant noted that criminals congregate where the law is weakest, and that the UK faces particular challenges in negotiating with the states where the criminals are located. Despite the difficulties associated with ensuring that the criminals were not masking their true physical location through the use of a false online presence, several participants remained confident that the UK and allied nations were capable of prosecuting cyber criminals effectively.

On the other hand, some participants underscored the fact that not all countries share the same perspective on what exactly constitutes criminality, and that the difference in government policy between active support for nefarious cyber activity to plausible deniability was a very thin one. One participant raised the analogy of non-spying agreements between states, which he suggested should be taken with a pinch of salt.

Another cautioned that whilst governments were right to be cautious about the Internet as a source of cyber attacks, they should not neglect private networks, most of which share the same routers as the Internet even if they do not use Internet Protocol (IP). He reiterated that although common infrastructure has its problems, the technology to secure the networks does exist, but that cost and human error are likely to be barriers to its widespread adoption.

When discussing the need for inter-governmental collaboration, a number of participants cautioned that if international arms control treaties were to be used as a model, that governments should be careful what they wished for. Key to the success of the arms control treaties of the Cold War were trust and verification, two things that are particularly difficult in the cyber domain. Some participants lamented that the Council of Europe's Convention on Cyber Crime had not received as much support as they might have wished, whilst others preferred the developing 'corpus of norms' approach. In the military sphere it was noted that the existing Laws of Armed Conflict and the Geneva Conventions were widely supported tenets of international law and that there was no reason that these should not be applied to the cyber domain. In the opinion of one participant, this posed challenges in determining how to discriminate in cyberspace and what level of disruption should be viewed as excessive.

Private Sector Concerns

Several participants representing large multinational providers of network technology, services or software raised the challenges associated with operating in the majority of the world's nations where conflicts of interest inevitably arise. Sometimes legislation from different jurisdictions can be contradictory, such as between the US Patriot Act and the EU Data Protection Directive. In other cases the supply of information that can help one state customer improve their cyber resilience can also be used by that state as an offensive capability against the systems of another nation. It was suggested that the STUXNET virus that attacked Iranian nuclear facilities in 2010 was created in part through the use of privileged information provided to a government by a major corporation. The difficulties of balancing the desire to be a helpful supplier to valued individual customers and the desire to run a global business was reiterated, and the participants were united in their belief that as governments begin to develop doctrines to facilitate international cyber security efforts, they must keep industry involved from the very beginning. The duties of responsibility on the part of industry was also reiterated, both hardware and software providers, especially as the latter were unlikely to develop 100% secure code in the near future. The concept of a layered defence was mentioned, built on partnerships that include academia as well as governments and industry. However, one participant cautioned that true information assurance was a result of behaviour, not technology.

It was agreed that while government-industry information exchanges represent a good step in the right direction, more must be done. In particular concerns were raised that the current model was not scaleable given the centrality of personal trust and understanding. One participant in particular identified the need to expand and build on the Public-Private Partnership model. Another participant reminded the group that governments must recognise that companies would always be reluctant to share data with other companies present, even in a trusted environment. The whole group agreed that continuing to find new ways to build trust between public and private sector organisations was essential, and that crime prevention was perhaps the easiest area of common interest on which to build. Some participants made the point that Small and Medium Enterprises (SMEs) were often repositories of considerable expertise and thus should be involved alongside the more established 'big beasts'. Several participants cautioned that current trends in the UK were moving towards a compliance-based relationship rather than one based on co-operation, and strongly suggested that the government should reign in this troubling development.

Olivier Grouille - Rusat Conference Rapporteur

University of Cambridge

Definitions discussed at the conference

Cyber War – conflicts between states or states and hostile organisations are unlikely to ever take place entirely in the cyber domain. For one thing, an adversary is likely to employ as many different forms of attack, both physical and virtual, against the victim state. However, militaries should expect and prepare countermeasures against cyber attacks on their IT, communications and command and control systems as a feature of modern conflict, just as they would prepare for attacks from the air, land or sea.

Cyber crime – hostile entities are just as likely to attack private sector networks and systems as those belonging to the government departments and agencies. The motivations may include theft of personal data, economic and industrial espionage and 'nuisance' denial of service operations. Governments must however decide whether a series of small-scale attacks against their citizens and commercial enterprises cumulatively constitute an 'attack', and if so, what the threshold is, as opposed to a single large-scale attack.

Statistics - the following were cited during the meeting to demonstrate the scale of the challenge facing this webmail provider

➤ 1.3 billion Hotmail accounts

➤ 360 million active users sending 3 billion messages a day

➤ 1.5 billion photos sent every month

➤ 150 petabytes of data and growing by an extra 2 every month

_____

Note:
This conference was held subject to the Chatham House Rule. This report was written on a thematic approach rather than following chronologically the course of the sessions and related discussions.

Rustat Conferences,   Jesus College, Cambridge, CB5 8BL
Email: info@rustat.org   **Tel:** +44 1223 328 316   **Web:**   www.rustat.org

Rustat Conferences

Cyber Security - An Assessment of the Threats to National, Economic and Individual Security

Jesus College, Cambridge - Thursday, 3 February, 2011

Jesus College
Cambridge

Conference Timetable

Conference Registration	08.45-09.45

Prioress's Room, Cloister Court – refreshments served. Between 09.30-09.45 proceed to Upper Hall – venue for the conference

Conference - Upper Hall, Jesus College	09.50

Welcome

Professor Robert Mair CBE FREng FRS - *Master, Jesus College, Cambridge and Chair, Rustat Conferences*

Session 1	09.55-11.00

Introduction and Overview

Chair - Dr Rex Hughes - *Visiting Fellow, Cyber Security, Wolfson College, Cambridge*

Cyber Capabilities for Intelligence, National Security and Foreign Policy Objectives

Sir Richard Dearlove KCMG OBE - *Master, Pembroke College, Cambridge and former Chief, Secret Intelligence Service*

A History of Internet Security Failures – Cultural Mismatch between Old and New Technologies

Professor Jon Crowcroft - *Marconi Professor of Communication Systems, Computer Laboratory, University of Cambridge*

Break - tea and coffee	11.00-11.15

Session 2	11.15-12.15

The Government Perspective

Dr Steve Marsh - *Deputy Director, Office of Cyber Security*
Robert Hayes - *Senior Fellow, Microsoft Institute for Advanced Technology in Governments, Microsoft Research*
Chair - Dr Tristram Riley-Smith - *Centre for Protection of National Infrastructure*

Lunch - The Master's Lodge	12.15-13.30

Session 3	13.30-14.30

Cyber Risks and Preparedness in the Private Sector

Jon Moynihan OBE - *Executive Chairman, PA Consulting Group*
Dr Ian Brown - *Oxford Internet Institute, University of Oxford*
Chair - Lord Macdonald of Tradeston CBE PC - *Senior Adviser, Macquarie Infrastructure and Real Assets*

Session 4	14.30-15.30

Governing Cyberspace - Law, International Cooperation and Cyber Crime

Dr Richard Clayton – *Computer Security Group, Computer Lab, University of Cambridge*
Charlie McMurdie - *Detective Superintendent, Head of Economic and Cyber Crime, Police Central e-Crime Unit*
Chair - Tim Dowse - *Director, Intelligence and National Security, Foreign and Commonwealth Office*

Break - tea and coffee	15.30-15.45

Session 5	15.45-16.45

The Threat to Individuals and Freedom Online

Dr Steven J. Murdoch - *Computer Security Group, Computer Laboratory, University of Cambridge*
Paul Collacott – *Deputy Director Cyber Policy, GCHQ*
Chair - John Naughton - *Professor of the Public Understanding of Science, OU, and Fellow, Wolfson College, Cambridge*
Response and Final Comments - Dr Rex Hughes - *Visiting Fellow, Cyber Security, Wolfson College, Cambridge*
Closing Words – Professor Robert Mair – *Master, Jesus College and Chair, Rustat Conferences*

Conference Close	16.50

The conference (and written report) will observe the Chatham House Rule.

Rustat Conferences
Jesus College
Cambridge

The Rustat Conferences are an initiative of Jesus College, Cambridge, and are chaired by Professor Robert Mair CBE FREng FRS, Master of Jesus College. The Rustat Conferences provide an opportunity for decision-makers from the frontlines of politics, the civil service, business, the professions, the media, science and education to exchange views on the vital issues of the day with leading academics. They were founded in 2009 - the themes of the first three Rustat Conferences were *The Economic Crisis*, *The Future of Democracy* and *Infrastructure and the Future of Society* - see *www.rustat.org* for more information..

Previous participants include: Lord Eatwell, *Professor of Financial Policy, University of Cambridge*; Sir Terry Leahy, *CEO, Tesco*; Lord Turnbull, *former Cabinet Secretary and Head of UK Civil Service*; Dr John Jenkins, *HM Ambassador to Iraq*; Sir Samuel Brittan, *Financial Times*; Dominic Casserley, *Managing Partner, McKinsey & Co. UK & EMEA*; Chris Saul, *Senior Partner, Slaughter and May*; David Strachan, *Director, Financial Stability, FSA*; Peter Horrocks, *Director of BBC World Service*; Lord Wilson, *former Cabinet Secretary and Master, Emmanuel College, Cambridge*; Will Hutton, *The Work Foundation*; Tony Wright MP; Peter Kellner, *President, YouGov*; Matthew Taylor, CEO*, RSA, former Chief Adviser on Strategy to the Prime Minister*; Robert Chote, *Director of Institute for Fiscal Studies*; Paul Skinner, *former Chairman Rio Tinto, Chair Infrastructure UK;* Lord Macdonald of Tradeston, *Senior Adviser, Macquarie*; Ray O'Rourke, *CEO, Laing O'Rourke Group*.

In addition to acting as a forum for the exchange of views on a range of major and global concerns, the Rustat Conferences provide outreach to a wider professional, academic and student audience through the publication of reports in a variety of media. The conferences are held at Jesus College, Cambridge, one of the colleges of the University of Cambridge, and are named after Tobias Rustat (d.1694), an important benefactor of Jesus College and the University. Tobias Rustat is best remembered for creating the first fund for the purchase of books for the Cambridge University Library.

On behalf of Professor Robert Mair, we would like to thank all speakers and chairs at the Cyber Security conference, as well as the following for their advice: Professor John Naughton, Professor Jon Crowcroft, Professor Ross Anderson, Lord Macdonald of Tradeston CBE PC, Sir Richard Dearlove KCMG OBE, Jon Moynihan OBE, Dr Steve Marsh, Professor Paul Cornish, Dr Steven J. Murdoch, Dr Ian Brown, Richard Abel, Dr Rex Hughes, David Liebler, Jeff Bauer, and Olivier Grouille.

Rustat Conferences

Rustat Conferences

Cyber Security - An Assessment of the Threats to National, Economic and Individual Security

Jesus College, Cambridge   Thursday, 3 February, 2011

Jesus College
Cambridge

Conference Participants

Professor Robert Mair CBE FREng FRS	*Chair, Rustat Conferences, Master, Jesus College, Cambridge, Professor of Geotechnical Engineering and Head of Civil and Environmental Engineering, University of Cambridge*
Richard Abel	*Managing Director, Macquarie Infrastructure and Real Assets*
Dr Robin Andrew	*Ministry of Defence*
Professor Jean Bacon	*Professor of Distributed Systems, Computer Laboratory, University of Cambridge, and Fellow, Jesus College*
Jeff Bauer	*Senior National Security Specialist, NATO Joint Intelligence Operations Centre Europe*
David Bond	*Director and Producer, Green Lions; director of Erasing David*
Dr Ian Brown	*Oxford Internet Institute, Oxford University*
Rory Cellan-Jones	*BBC Technology Correspondent*
Nick Chaffey	*Head of Defence and Security, PA Consulting Group*
Mark Chesterman	*Managing Director, Chase Security Solutions Ltd*
Professor Howard Chivers	*Director of the Centre for Forensic Computing and Security, Cranfield University*
Professor Roberto Cipolla	*Professor of Information Engineering, University of Cambridge, and Fellow, Jesus College*
Dr Richard Clayton	*Security Group, Computer Laboratory, University of Cambridge*
Dave Clemente	*International Security Programme, Chatham House*
Paul Collacott	*Deputy Director for Cyber Policy, GCHQ*
Jennifer Cole	*Cyber Security Programme, Royal United Services Institute*
John Cornwell	*Director, Science & Human Dimension Project, Jesus College, Cambridge*
Ned Cranborne	*Director, Samos Investments*
Professor Jon Crowcroft	*Marconi Professor of Communication Systems, Cambridge University*
Kerry Davies	*Director, Information Protection and Business Resilience, KPMG*
Sir Richard Dearlove KCMG OBE	*Master, Pembroke College, Cambridge, former Chief, Secret Intelligence Service*
Tim Dowse	*Director, Intelligence and National Security, Foreign & Commonwealth Office*
Chris Durbin	*Head of Cyber, Northrop Grumman Mission Systems Europe*
Euros Evans	*Chief Technology Officer, Airwave Solutions*
Vincent Geake	*Infrastructure UK, HM Treasury*
Olivier Grouille	*International Relations, University of Cambridge; Research Associate RUSI, and Rapporteur, Rustat Conferences, Jesus College, Cambridge*
Chris Hardy	*Regional Director Central Government, Defence & Security, McAfee Security*
Wg Cdr Shaun Harvey	*Officer Commanding Force Generation Wing, 90 Signals Unit, RAF Leeming*
Robert Hayes	*Director, Microsoft Institute for Advanced Technology in Governments, Microsoft Research*
Dr Rex Hughes	*Visiting Fellow, Cyber Security, Wolfson College, University of Cambridge*
Christopher Joyce	*Eastern Europe and Central Asia Directorate, Foreign & Commonwealth Office*
Kweilen Kimmelman	*Corporate Strategy Manager, BAE Systems plc*
Lord Gus Macdonald CBE PC	*Senior Adviser, Macquarie Infrastructure and Real Assets, former Minister of Transport and Cabinet Office*
Dr Steve Marsh	*Deputy Director, Office of Cyber Security OCSIA – Cabinet Office*
Alex Michael	*MoD Defence Academy and Office for Security and Counter Terrorism, Home Office*
Jon Moynihan OBE	*Executive Chairman, PA Consulting Group*
James Muncie	*Head of Cyber Policy, Centre for Protection of National Infrastructure*

Dr Steven J. Murdoch *Security Group, Computer Laboratory, University of Cambridge, and Fellow, Christ's College, Cambridge*

Professor John Naughton *Professor of Public Understanding of Technology, OU, Fellow, Wolfson College, Cambridge*
Sir David Omand GCB *Former Director, GCHQ, Visiting Professor, King's College London*
Wg Cdr Tom Parkhouse *Cyber Policy Staff Officer, Ministry of Defence*
Mark Ploszay *EMEA Defence and National Security Programme Manager, i2 Ltd*
Craig Pollard *Principle Advisor, KPMG*
Mike Prettejohn *Director, Netcraft Ltd*
Dr Tristram Riley-Smith *Centre for Protection of National Infrastructure*
Dr Michael Rutter *Head of Energy Resilience, Department of Energy and Climate Change*
Guillaume Tissot *VP Product Marketing, i2 Ltd*
Alex van Someren *Amadeus Capital Partners, founder nCipher*
Dr Timothy D. Wilkinson CEng *Reader in Photonic Engineering, University of Cambridge, and Fellow, Jesus College*
Jonathan Cornwell *Rustat Conferences, Jesus College, Cambridge*