Conference report

Cyber security: managing the risk
Monday 18th – Wednesday 20th October 2010 | WP1056
"In the mind of the public and much of the political class, cyber crime has come to encompass everything bad that happens on the internet."

Conference report

Cyber security: managing the risk
Monday 18th – Wednesday 20th October 2010 | WP1056

Key points

- The scale of the cyber challenge ranges from crimes against individuals to threats to state security. The number of electronic attacks on the UK has tripled in recent years and internationally, one estimate for the scale of e-crime equates it to 1% of global Gross Domestic Product (GDP).

- Cyber crime can be seen as the perpetration of age-old crimes, using new techniques. However, there are criticisms that enforcement agencies are slow to respond to the growing on-line threat.

- There is considerable discussion about the need for global regulation but, while it is accepted that some type of governance is inevitable, there is no consensus as to what form it should take.

- Public campaigns to raise awareness of the need for better ‘online hygiene’ could do much to reduce cyber crime. However, there are concerns that individuals are increasingly being expected to assume responsibility for the risks associated with online transactions.

- Attribution in the virtual world is particularly problematic and has implications for the ways in which states respond.

- The internet is estimated to be growing at 60% and governments and industry are increasingly reliant on e-commerce and on-line services. Effective partnerships will be indispensable in tackling the challenges which lie ahead.

The cyber challenge

1. Politicians and policy makers in the UK and elsewhere have been grappling with the actual scale of the cyber challenge. It is difficult to ensure perspective on the risks posed and credible estimates range from relative calm to talk of a ‘Cyber Pearl Harbour’. The conflation of a variety of different activities under the banner ‘cyber’ has further complicated efforts to achieve perspective. In the mind of the public and much of the political class, cyber crime has come to encompass everything bad that happens on the internet.

2. Regardless of the precise definition, the threat emanating from the increased use of the internet and other electronic networks is growing at a considerable rate. The internet is estimated to be growing at 60% a year. The number of electronic attacks on the UK has tripled in recent years and the theft of intellectual property (IP) continues to increase in both the commercial and national security space. Online banking losses increased by 132% in 2007-8 and one botnet attack alone stole the details of 12.7 million banking customers. Internationally, one estimate for the scale of e-crime equates it to 1% of global Gross Domestic Product (GDP).
3. Amidst the conflicting analysis of the current cyber threat there is an even greater divergence in opinion over the medium term risks. A conservative reading argues that while ‘cyber’ represents a new means, the actors and their desired ends are not so different. Stealing is still stealing and the methodology should not be a distraction. Alternatively, ‘cyber’ may be analogous with global warming. In other words, discussions may be focusing too much on the weather, when, in fact, it is the climate that is changing. Digitisation and growing reliance on electronic networks represent a qualitatively new way of organising the world. The extent of decentralisation of power and information will have profound long-term effects that cannot be fully understood at this time. However, they will have major implications for security.

“In the UK, 2-3 million e-crimes are committed each year in comparison to approximately 1 million conventional crimes.”

4. Of the cyber activity directed against the UK and its citizens, approximately 80% is e-crime. While there is variation, it is largely high volume and relatively unsophisticated in nature. The other 20% is made up of more targeted attacks, the sophistication of which has grown to the extent they can no longer be countered by defensive means alone.

5. In response to the dramatic growth of e-crime impacting individuals and businesses, governments are accused of being slow to re-orientate themselves. In the UK, 2-3 million e-crimes are committed each year in comparison to approximately 1 million conventional crimes. However, the vast majority of policing resources remain targeted at the latter. Intelligence agencies too are accused of a lack of urgency in relation to types of cyber activity which, while mundane in nature, impact large numbers of citizens and businesses. While there is acceptance of the need for a degree of cultural change at agencies traditionally concerned only with the integrity of the state, there is also a determination that good general awareness and basic computing hygiene will free resources to deal with high end threats.

6. With the roll out of super high-speed broadband, continued growth in processing power and the move from a web of documents to a web of data are converging with likely consequences for e-crime. E-criminals will be able to collate data and target large numbers of people much more effectively and efficiently raising the prospect of e-crimes of such an order of magnitude that they regularly become genuine national security threats.

7. Cyber will change the face of warfare. Estonia may already mark the defining moment. These new dynamics are placing tremendous strain on traditional political and operational decision making processes. For collective defence, the real world test was the ability to hold the border for 72 hours whereas collective cyber defence may mean the ability to secure networks for 30 seconds.

E-crime, national security and cyber warfare heading

8. Hacking, the exfiltration of data, has undergone considerable transformation from its early days when it was intended to be conspicuous proof of the perpetrator’s skill. As the hacking community has become cross-pollinated with the organised crime world hacking has become highly commoditised. Hackers now often act in a mercenary fashion stealing data to order at the instruction of others. More recently, hackers have begun to distribute hacking tool kits which can be used by relative novices. A competitive black-market industry has grown up around these products and some even boast 24 hour customer service for buyers.

9. Prices across the cyber black market, for hacking tool kits or access to botnets, has fallen markedly in the last 12 months suggesting an oversupply of hacking skills relative to the other ‘professional services’ which support organised crime groups. For law enforcement pursuing other more fragile aspects of the criminal supply chain, such as money laundering, this may cause greater disruption to efforts to ‘drain-the-swamp’.

10. Contrary to popular belief hackers, operating mostly out of the developing world, are often well educated and operating within highly organised enterprises. What often appear clumsy scatter-gun attempts at fraud are based on advanced social engineering
 techniques exploiting condescending attitudes to the developing world or plain greed. The most successful hackers have become skilled in identifying synergies with other organised crime groups. In Nigeria, hackers are known to work with kidnap gangs, targeting passenger data from airlines to identify potential victims as they arrive in-country. They are also known to engage in intelligence gathering via insiders deliberately placed in target organisations around the world.

**An international understanding on cyber**

11. The world's major powers recognise the necessity of establishing an international order. However, the nature of that order is the subject of much contention with even closely allied western powers pursuing different approaches. Russia and China have called for international treaties to govern state's behaviour in the cyber domain. The US administration is divided on the question but the UK is of the view that the formulation of international treaties could have perverse outcomes, generating a new layer of international law which would likely be exploited and flouted by adversaries. Rather, the UK is advocating the establishment of internationally recognised norms of behaviour and more effective use of the relevant body of international law which already exists. The UK's preferred end-state is of a cyber global commons freely, accessible and without areas of sovereign cyberspace.

12. As major powers have developed their respective cyber capabilities governmental discussions on cyber space have been marked by reticence and vagueness. Concerns have been ill-defined and complaints largely limited to talk of ‘incidents’. This had led to questions about the current status of the cyber domain. Is it playing host to the next phase of inter-state competition or are states embroiled in a kind of low intensity warfare?

13. Episodes such as “STUXNET” are adding impetus to an extremely sensitive international dialogue on cyber. Discussions are highlighting cultural differences and uncomfortable truths for all parties. Varying conceptions of intellectual property and privacy are proving difficult to reconcile, as is the shift of power from West to East which should have been reflected in a contemporary global order. The construction of global cyber regime, if truly representative, would have to look quite different from the existing international order which was shaped and dominated by the West. Governments are inclined to map cyberspace to existing power relationships creating the impression of a plot to preserve Western hegemony.

14. The UK is committed to leveraging its membership of international institutions such as the European Union (EU), the Commonwealth and the Organisation for Security and Co-operation in Europe (OSCE) to exert influence on the development of a cyber regime.

15. In addition to the vast majority of countries which are ‘online’, there are also at least 20 international organisations claiming some regulatory responsibility for the internet. This clamour for cyber relevance has made for a fractious environment where cooperation is poor and duplication of efforts commonplace. The result is a poor use of what is a limited body of international expertise. Much of this activity is driven by the interests of vendors and requires urgent rationalisation.

**Public awareness and the ownership of risk**

16. In the UK and the US there have been frequent calls for increased levels of awareness from the online public. Better hygiene, the updating of anti-virus and the patching of systems are routinely cited as preventative measures through which a significant amount of cyber crime could be prevented. Accordingly, individual users are increasingly being expected to assume responsibility for the risks associated with their online transactions. Currently, 44% of Britons who are the victims of electronic fraud do not get their money back-up from 14% just a few years ago. However, the received
wisdom around educating users and users’ ability to protect themselves has been called into question.

17. The ‘Ghost Net’ attack on the Dali Lama’s office is a good example of the sophistication of modern ‘phishing’ and ‘spear phishing’ attacks against which the public cannot realistically be expected to defend themselves. According to this line of argument, the banks and other financial institutions are actually in a massive process of ‘risk dumping’ whereby they accrue the savings of online transactions without assuming any of the associated risk thanks to a culture of ‘train and blame’.

18. The unfairness of these practices for consumers are compounded by the structural failings of the software security market which tends towards monopolies and features largely indistinguishable security products which do not meet consumers needs. Attempts to redress the balance for the consumer are taking various forms. In Australia Internet Service Providers (ISPs) have been tasked with ensuring security across their networks. While they have welcomed the responsibility in private, they required the political cover of government intervention and guarantees of a level playing field between providers, before they could act.

19. In the US, it may be through litigation that consumers eventually hold security vendors and software providers to account. The prospect of class action lawsuits by shareholders is similarly forcing corporations to invest and address problem such as weak authentication.

Law enforcement, cyber crime and attribution

20. From the perspective of UK law enforcement, cyber crime is the perpetration of age-old crimes committed through new techniques. Fraud, theft and extortion lie at the heart of all cyber criminality. However, prosecution is complicated by the multi-national nature of conspiracies (crimes investigated by Serious Organised Crime Agency typically span 3-4 countries), and the degree of anonymity which criminals can depend upon. Law enforcement is developing new tools and international mechanisms in response to the threat from cyber crime, but these are cumbersome.

21. The prospects for law enforcement in the face of cyber crime appear quite bleak. Improving international connectivity and increasing bandwidth will play into the hands of criminals. Cyber crime is currently the preserve of high-tech unit which can quickly become swamped. In the face of the growing threat, there is a strong argument for mainstreaming policing responses to cybercrime in the same way that counter-terrorism and money-laundering, once niche capabilities, are now on the radar of large numbers of officers.

22. Law enforcement would welcome some international treaties or conventions which facilitated the transfer of information and the pursuit of police investigations across borders.

23. In the future, concrete attribution for actions in cyberspace is likely to become extinct. Attributing an act or a threat to a state or a non-state actor will increasingly have to be done on the basis of probability rather than certainty. This has implications for the response to incidents and also the way in which responses are interpreted. In the absence of irrefutable proof of identity, accusations of guilt will be contested and retaliations inevitably viewed as illegitimate. The prospect of conducting international relations and formulating deterrence policy on a probable basis is unnerving for policy makers. It could be that the global community is destined for a shady future international environment which longs for the relative certainties of now.

The internet, governance and popular culture

24. A distinctive culture has grown up around citizens and their use of the internet. Part subversive, part idealistic and part anarchic, understanding the roots of this culture and
reconciling it with commercial and nation-state imperatives is a challenge to
governments around the world.

25. Basic state assumptions are very different in the physical and cyber worlds
respectively. In the ‘real’ world the State’s right to inspection is largely assumed while it
is the individual’s right to privacy which dominates online life. At the heart of
government’s dilemma is the question of whether the internet should be governed and
whether governance is feasible. Governance and policing historically take place by
consent and on the basis of some form of social contract. It is not clear that citizens are
willing to extend this social contract to the cyber domain.

26. While there will be push-back on efforts to roll out governance to what has appeared a
largely ungoverned space, the current arrangement may be unsustainable. Arguably,
the internet cannot continue to be free and bound by the assumption that people expect
to live their lives communally by a set of rules until they go online in their homes. As the
online and the physical worlds converge, such expectations become increasingly
unrealistic.

27. If it is accepted that some form of governance is inevitable, authorities will have to work
much harder to develop a shared understanding with people who currently inhabit
ungoverned spaces on the internet. There is considerable, understandable suspicion of
official efforts to normalise and commoditise the internet.

28. If efforts at governance from traditional sources of authority fail, there is the prospect of
de facto governance from some other source—perhaps by virtue of one organisation’s
dominance online. If projections around ‘Facebook’s’ future potential were realised it
would be an obvious candidate. Expedience dictates that it currently operates within the
rules of various real-world jurisdictions. What if it didn’t?

Espionage, government/industry cooperation and the protection of infrastructure

29. The UK views the cyber threat posed by other states as an asymmetrical one. While all
states with the requisite capability seek a military advantage in cyber space, the UK
does not engage in economic espionage.

30. Service denial through cyber-attacks remain a rare occurrence. However, state
sponsored economic espionage against the West has grown dramatically in recent
years. The sophistication of these attacks is growing and they are highly targeted, for
instance against firms in mergers and acquisitions negotiations. Fifty percent of
espionage activities directed against the UK are now thought to be cyber in nature.
Definite attribution of these activities can be difficult but investigations into them are not
limited to the cyber domain and real-world intelligence is very important. It is currently
thought unlikely that terrorist groups hold the capability to launch cyber-attacks.

31. Most developed and developing countries now have a plan to place the digital economy
at the heart of their future prosperity and to use high-quality, resilient digital
infrastructure to attract investment. While Government’s in developed countries have
been in a dialogue about security with infrastructure operators for a number of years,
the emergence of a pervasive cyber infrastructure and the impact of cyber on existing
infrastructure are necessitating a new kind of dialogue with a much broader spectrum of
the private sector.

32. The biggest impact of cyber on existing infrastructure has been to make it significantly
more interdependent than was historically the case, and arguably more interdependent
than is currently realised. Research suggests that additional complexity and the
potential for cascading failures have changed the profiles of infrastructure to such an
extent that current risks may be underestimated by one to two orders of magnitude.

33. Government find large sections of industry still sceptical about the threat from cyber
and the implications of data losses. A sophisticated and widely recognised vocabulary
has grown up around efforts to sell new areas of work and exploit the advantages of online commerce. However, security experts have largely struggled to articulate equally compelling arguments for the need for adequate risk management. As such, the costs of properly securing new types of activity often only become apparent in the wake of security incidents.

34. Even in the wake of serious incidents and huge exfiltration’s of data, executives are often unwilling or unable to place an economic value on what they have lost and fail to acknowledge the business case for better security. To date the UK government, for instance, has preferred to help industry manage risk through dialogue and light touch regulation. However, there is a growing feeling that security and resilience can be a source of market failure and that new levers are required if that failure is to be addressed.

35. In addition to the new cyber threat to existing infrastructure operators, the growth of e-commerce and the delivery of government services electronically are suddenly making whole new sections of industry operators of critical infrastructure. This in turn means the need to open up dialogue with sections of the economy who are not accustomed to thinking about high-end security and view it simply as an impediment to dynamism and competitiveness.

36. To date, government has rarely sought to provide support directly to businesses. It can help by providing context about the cyber threat in advance and with clarifying attribution after an attack. More often, it acts in an advisory capacity and seeks to facilitate intra and inter-sector information sharing. Successful partnerships with industry are based on rapport and personal relationships. The activity requires high levels of trust and, as in the case of the Centre for the Protection of the National Infrastructure’s (CPNI) information exchanges, can take years to become productive.

37. Securing the requisite investment of time and resource for this type of activity from the new breed of cyber infrastructure operators will not be easy. Government will have to develop a wider range of nuanced arguments and toolkits as resorting to cosy conversations about ‘national interest’ becomes less realistic.

38. The view that ‘government has the intelligence, if only it would share it’ is now considerably out-dated. Private-sector networks are now the primary battleground in the competition to secure advantage through the cyber domain. Government is increasingly aware that it cannot impose additional, unjustifiable cost on the private sector. However, for governments and the private-sector alike, effective partnerships will be indispensible going forward.

Anthony McGee
Wilton Park | November 2010

Wilton Park reports are brief summaries of the main points and conclusions of a conference. The reports reflect rapporteurs’ personal interpretations of the proceedings – as such they do not constitute any institutional policy of Wilton Park nor do they necessarily represent the views of the rapporteur.

Should you wish to read other Wilton Park reports, or participate in upcoming Wilton Park conferences, please consult our website www.wiltonpark.org.uk

To receive our e-newsletter and latest updates on conferences subscribe to www.wiltonpark.org.uk/news