GSF SEMINAR

'Cyber Defence: The Biggest Challenge Facing UK National and Economic Security?'

Committee Room 3A
House of Lords

Wednesday 30th November 2011

On 30th November 2011, Global Strategy Forum (GSF) held a seminar entitled *'Cyber Defence: The Biggest Challenge Facing the UK National and Economic Security?'* The seminar took place in the House of Lords under the chairmanship of **Lord Lothian**, Chairman, GSF.

The speakers were: **Professor Michael Clarke**, Director General, Royal United Services Institute; **Gordon Corera**, Security Correspondent, BBC News; **Luke Forsyth**, Vice-President for Security and Compliance, CA Technologies; **Lord Hannay of Chiswick**, Chairman, House of Lords EU Sub-Committee F (Home Affairs); **Robert Hayes**, Senior Fellow, Microsoft Institute for Advanced Technology in Government; **Andrew Miller MP**, Chairman House of Commons Science and Technology Committee; **Professor Sir David Omand**, Visiting Professor, Department of War Studies, King's College, London; **Sir David Pepper**, Former Director, GCHQ; and **Martin Sutherland**, Managing Director, BAE Systems Detica.

The seminar took the form of an opening address by Sir David Omand, followed by two panels. Respectively, these covered the political context as seen from London and Brussels; and the industrial and media dimensions.

Speakers identified the following main themes:

OPENING ADDRESS: ***'Securing The State From Cyber Attack: An Overview Of The Emerging Cyber Threat Landscape'***

The starting point in any discussion of cyber security should be the recently published UK Government paper, '*The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.'* This presents a credible statement of current knowledge and sets out a planning basis up to 2015. For the purposes of understanding the challenge posed by the Internet, five aspects stand out.

- While cyber security is a fast-moving and inherently unpredictable subject, the central underlying point is that the Internet represents a secular development in human affairs, comparable to other "step-changes" and "paradigm shifts" in

history. Failure to master and exploit the Internet is a grave threat to national welfare.
- The time to act is now;
- The task is not just to secure information, it is to realize that any digitised material can be stolen;
- National borders offer no protection;
- The driver for cyber security will be the private sector, not government. Nonetheless the government contribution via secret intelligence will be vital.

Practical challenges include:
- While plenty of evidence exists about criminal and state-sponsored cyber intrusions, we should not be intimidated by worst-case scenarios;
- We need to think about the appropriate way to respond to cyber crime. Cold War responses, for example, the expulsion of diplomats, have little current relevance;
- Uncertainty about attribution is an ever-present factor;
- The 'self-assembling dynamic network' (swarming) dimension of social media introduces a totally novel factor in public behaviour;
- Static monitoring by governments is in place, but the potential for real-time intelligence gathering offers opportunity for manipulation by governments and markets.
- The roles of Russia and China remain opaque.

SESSION 1: <u>Cyber Security: The Politics in Westminster, Whitehall and Brussels</u>

<u>Government response</u>: All speakers believed that the emerging UK government strategy was prudently conservative, given the limitations in knowledge about how the cyber threat would evolve. It useful took the discussion beyond the 2009 original outline of government policy. Speakers in both sessions highlighted the identification of cyber as a "hub" as a useful concept. They welcomed the 1st-2nd November FCO-sponsored London Conference on Cyberspace and drew attention to recent reports from both Houses of Parliament.

The appropriate bureaucratic structures are now in place, but the challenge will be for government to prepare for a threat that crossed bureaucratic boundaries, something that traditionally neither executive agencies nor Parliamentary committees find easy to do. Government needs to recognise that the cyber threat is a continuum and that "we are all in this together" with everyone responsible for "cyber hygiene." By adopting best practice in this field, for example, by maintaining up-to-date versions of all software, well over 90% of the threat of cyber intrusion can be eliminated. Governments themselves are often bad examples of poor cyber hygiene and of adopting software updates. An analogy was drawn between the cyber threat and nuclear deterrence.

There was some discussion of whether international treaties, on the ITU model, represent an effective response or whether practical experience should allow "norms" to emerge. No definite consensus was established but all agreed that there is an urgent

need for international cooperation and mechanisms. The attraction of norms is that they raise the price to those who aim to cause infractions.

The resource question: There was discussion in both the session and in the Q&A about whether the £650 million of new money for cyber foreseen by the government is adequate. Most speakers felt that the sum was inadequate, especially as it assumed that existing cyber defences would be put into effect with current resources.

The UK and the EU: Speakers agreed that the UK leads its EU partners on cyber matters. It was agreed that EU and NATO cyber institutions needed to be strengthened and that cooperation between the two bodies should be encouraged. The best agency to take charge of EU cyber aspects is Europol, to which additional resources should be given.

Cyber as warfare: The central question is whether cyber is a weapon of war or a new dimension of war. In either case, it should be remembered that there are classic balances between offence and defence. To be effective, an aggressor had to reveal himself and attack on an industrial, systematic scale. The military is aware of these threats and has response opportunities based on intelligence. Further, society is both regenerative and resilient. The real threat of cyber warfare may be to distract government attention at times of crisis.

The private/public relationship: From industry's perspective, the key insight is that the Internet is a global phenomenon. National responses therefore need to be globally compatible. Major companies like Microsoft are themselves daily targets of cyber intrusion and so have a great deal of experience to offer. Industry tends to feel that it is constrained by a "policy lag," for example on establishing "end-to-end" trust protocols, which would help in addressing the attribution problems implicit in identifying the source of a cyber attack. Trust between industry and government is vital. Industry is aware that governments seek "comparative advantage" in cyberspace but is reluctant to assist offensive intentions. Should governments decide to take offensive actions, companies which provide the Internet infrastructure will detect such action. They are unlikely to remain silent in the light of the various agreements that are in place, for example between Microsoft and governments, about reporting anomalous activities on the Internet.

SESSION 2: Cyber Security: The View from Industry and the Media

The corporate response: Speakers regretted that too often corporate leaderships did not take responsibility for cyber defences, but assigned it to IT departments. To address this deficiency, several speakers suggested that a new language in which to frame cyber issues is needed. This should be based on risk: to cash flow, reputation, confidence, IT infrastructure and IP. Cyber defences need to become a board level concern. Corporate leaders need to recognise that cyber is not a parallel universe, but that their core business models depend on cyber technology. There is a need for companies to shed their ingrained reluctance to share information about cyber attacks and to speak more openly about them.

With losses to British industry from cyber attack now running at approximately £27 billion per annum, businesses need a much more targeted approach to the specific threat each faced. Was this, for example, from hobby activists, competitors, criminals, terrorists or nation states? A different response is required in each case.

Technology: The technology gap between sophisticated defence and professional attack is narrowing. Attacks can come from geographically and culturally close quarters. They can be state-sponsored or state-tolerated. It is no longer legitimate to assume that attackers will be technically incompetent. With advances in virtualisation and VOIP, conventional defences like firewalls will fail. Cyber criminals are acquiring greater equality of equipment and capability. Much more rigorous testing, including a willingness to accept testing that does actual damage to IT infrastructure, is needed.

Designing defences: The key is to be innovative and pro-active. Tools like cloud-based anomaly calculation engines are extremely powerful in detecting intrusions, Convergences can arise between apparently unrelated disciplines like cyber defence and the search for "green" IT. In pursuing the latter, for example, capabilities for detecting anomalies in power and bandwidth consumption – which are indicators of cyber attack – can be developed. If active defences are in place, then "zero day" responses to virus infection can be very effective.

Public opinion: While the news salience of cyber issues has risen over the past years, media coverage is still patchy. Reporters struggle to persuade editors to cover cyber. The problem is that the word "cyber" is seen as too broad: *"It is about everything and therefore about nothing."* Sometimes the subject impinges on public consciousness through conspicuous examples like Google's differences with the Chinese government or the hacking of Sony's PlayStation but, more often, the very mention of the word "cyber" is a turn-off. Both companies and government agencies, for example GCHQ, need to be more open about cyber. Alternatively, another approach may be to deemphasise use of the word. The public also tunes out because of what it perceives as "threat inflation." There are parallels here to the way in which the public has lost interest in climate change because of perceived over statement of threat. It will be a continuing problem to convince the public that it must be involved in combating cyber attack.