The Foundation for Information Policy Research

Response to

The Joint Committee on the National Security Strategy

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

FIPR has the following comments to make in response to the questions asked by the Joint Committee on the National Security Strategy in its call for evidence of July 24th. It appears logical to tackle the questions in reverse order.

1. We welcome the committee's question of how broadly 'national security' (NS) should be defined. For many years, it has been used as a universal get-out clause. The Court of Appeal remarked that it is a protean concept, 'designed to encompass the many, varied and (it may be) unpredictable ways in which the security of the nation may best be promoted'. Secretary of State for the Home Department v Rehman [2003] 1 AC 153.
2. Yet the ECHR and the case law flowing from it make clear that NS exemptions must be proportionate, necessary and predictable in their effects, while some prohibitions (such as that on torture) may not be overridden under any circumstances. We suggest that a good starting point is the Johannesburg Principles, as elaborated in the Article 19 discussion at http://www.article19.org/pages/en/national-security-more.html.
3. The Article 19 discussion notes that one of the main roles of the state in a post-imperial age is to act as a guarantor of human rights. It points out that NS restrictions, even in democratic countries, are often 'impermissibly vague or respond to statements which pose only a hypothetical risk of harm, making them ideal instruments of abuse to prevent the airing of unpopular ideas or criticism of government.'
4. The Scottish referendum underlines its argument that national unity is better safeguarded by democratic process, and that NS should only be invoked when the threat to unity comes from force or the threat of force. It should not be invoked for local or isolated threats to law and order.
5. It is also argued by the security and intelligence agencies, when lobbying for an enhanced role in protecting critical national infrastructure, that the state also acts as an insurer of last resort. When banks started to fail in 2008, voters looked to the Government to do something, and the same would be the case if a network-based attack were to take down the National Grid, or a computer worm to break the Internet.
6. But it does not follow from this that protecting all manner of (mostly privately-owned) infrastructure from sabotage should come within the definition of NS, even where such crimes could be of sufficient consequence to have a material effect on the economy.

7. The Security Service Act 1989 says that the service's function shall be [1(2)] the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means [1(3)] to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands [1(4)] to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.
8. The prevention of crimes such as sabotage of the National Grid is thus clearly seen as a national security mission only if the attack is performed by a foreign government (in which case it falls under 1(2)). Sabotage by non-state actors falls under 1(3) if they are outside the UK and 1(4) if they are domestic extremists.
9. The recent history of such attacks ranges from the attempt by PIRA to blow up three of London's supergrid substations in 1996, to more recent occupations of generating plant and other sites by environmental activists. In every case, the attackers were domestic.
10. The Intelligence Services Act 1994 similarly sets out a threefold purpose for SIS in 1(2), namely national security, economic well-being, and supporting the prevention and detection of serious crime.
11. These issues have been discussed extensively by Parliament, not just during the passage of the above Acts but also in the debates on the Interception of Communications Act 1985 and the Regulation of Investigatory Powers Act 2000. Ministers have assured Parliament that although boundaries are difficult to draw, the engagement of the national security apparatus should be restricted to serious matters (E.g. Lord Bassam of Brighton HL Deb, 12 June 2000, c1496).
12. This settled disposition is now being challenged by two facts. First, critical infrastructure in Britain and elsewhere is becoming dependent on networked computer systems, and the protection of systems for electricity, water, communications, financial services, and even healthcare – against even petty crime – are becoming a matter of information security mechanisms as well as of the more traditional physical security.
13. Second, GCHQ's protective arm, CESG, has been designated the National Technical Authority for cybersecurity, putting it in pole position for advising not just the military and intelligence communities but also the full range of civil government departments. Thus we find CESG managers and experts involved in setting security policy for smart meters at DECC; advising the DoH on acceptable mechanisms for the anonymisation of health records; instructing the DWP how to go about authenticating people who lodge welfare claims online; and telling the Bank of England and other financial regulators what should be considered acceptable resilience in financial networks.
14. This represents an enormous expansion of the scope and scale of national security activities, and is objectionable on quite a number of grounds.
15. First, there is competition. Britain has many information security firms who would love to advise government departments on how to protect their systems, ranging from the big international consultancies down to small specialists. Why is the (Conservative-led) Government engaged in a creeping nationalisation of this industry?
16. Second, there is quality. Good security engineering tends to build on a deep understanding of the tradecraft of the application area; for example, banks know quite a

lot about payment fraud, while DWP has a lot of experience of people trying to fiddle benefits and HMRC understands carousel fraud against the VAT system.

17. Third, there is resource. Both the Security Service and GCHQ are small, and must perforce focus on major threats. As a result, GCHQ's work on smart meter security tackles only those threats that might bring down the grid (for example, by switching millions of meters off remotely) rather than the much more numerous and diverse threats from routine criminal activity (householders stealing electricity by manipulating meters, energy companies defrauding customers or colluding to commit competition offences).
18. The national security apparatus is not in a position to take over, or even to coordinate and supervise, the work of all the UK's police forces and regulators. In fact, while the law give the agencies the role of supporting the police in investigating serious crime; it wisely does not grant them any role in crime prevention at all.
19. Fourth, there is openness, which is an ideal in engineering as almost everywhere else. National security is frequently used as an excuse for companies to entrench monopolistic abuses. To take just one example, suppliers of railway locomotives and signalling equipment in the UK increasingly escape the EU "right to repair" rules by keeping key technical documentation secret from their customers, using national security as an excuse. Vendors can thus low-ball supply contracts in the knowledge that they can make more money out of maintaining a train, over its lifetime of 30–40 years, than from the initial sale. This ends up costing us real money, both as railway users and as taxpayers.
20. The extension of 'national security' to larger and larger parts of the UK infrastructure will multiply the opportunities for abuses of this kind, and help entrench monopolies and oligopolies that not only impose direct economic costs but also impede innovation.
21. Innovation requires open platforms on which market entrants can build new products that leverage existing infrastructure. For example, YouTube built a business starting in February 2005 and in October the following year sold the firm to Google for $1.65bn. This was possible because there were already hundreds of millions of people with PCs and broadband connections who could download and enjoy video clips. By comparison, the smart meter deployments made so far (for example, in Ontario, Italy and Spain) are locked down, so third-party developers cannot write applications that use their data. In consequence, the hoped-for market in energy service firms that would offer innovative energy-saving advice to consumers has simply not happened (and the UK smart meter programme, advised by CESG, looks set to go the same way).
22. Sectors that fall under the national security umbrella have many other factors that impede innovation. For example, if suppliers need staff with security clearances, this creates a catch-22 where a new market entrant can't get a sponsor for the clearance process until they have a customer, but can't get a customer until they have a clearance. There are also serious issues with nationality, as the UK does not produce anything like enough software engineers and in consequence most of the staff at tech startups are foreign. Adding clearance costs to the existing costs and uncertainty of visas is a good way to steer entrepreneurial small companies away from a sector.
23. In short, the locked-down national-security mindset is incompatible with the open standards, interfaces, labour markets and platforms required to support innovation in the information age.
24. It is therefore of grave concern that current policies are drifting towards incorporating much of the UK's infrastructure into a national security framework.

25. This is starting to affect one sector after another. Financial regulators, for example, pressure banks to hire former intelligence agency staff and CESG-approved security consultants to do penetration testing, with the result that the agencies not only learn a lot more than they perhaps need to about financial systems' vulnerabilities, but a clique of their former staff establish unjust market power in security consultancy. The same regulators neglect their proper duty of ensuring that victims of financial fraud are made whole. This is the same pattern seen in the smart metering project (and elsewhere).
26. There is a clash of incentives: for example, 'security' means different things for a bank and a bank customer. Their goals are in conflict, and the proper government body to arbitrate them is not an intelligence agency but a financial regulator or a court of law.
27. There is also a clash of cultures: the missions of 'national security' and consumer protection are also in conflict, as the latter requires openness.
28. Even national security itself may be compromised. Will agency staff be motivated to reduce risks, or merely to maximise compliance? As more and more firms in the security industry feel it prudent to get former senior agency staff (or ministers) on their board of directors, will rent-seeking cloud perceptions of the national interest at the policy level?
29. The protection of civilian infrastructure, such as the railways, the banks, the NHS, the utilities and the Internet itself, should not therefore be primarily regarded as a national security matter. The national-security apparatus may have some role to play (in respect of possible hostile state action) but its role must never be the leading one. It must be limited to that which is proportionate and necessary, leaving appropriate responsibilities to the companies' directors, to the regulators and to the police.
30. Moving now to the earlier questions in the consultation, we doubt that a twenty-year planning horizon is appropriate for the digital aspects of national security. While the product cycle of warship and warplane builders may be fifteen years, the computer industry's is more like 15 months. Looking back at 1994, IBM dominated the industry; the Internet was an academic ghetto, used by mathematicians to exchange learned papers; Microsoft's market capitalisation was only $20bn; and firms like Google and Facebook had not even been founded. (Mark Zuckerberg was only ten years old.)
31. The emphasis should not be "Should the UK plan to maintain its global influence?" but "How will the UK continue to prosper in a globalised world, where we are no longer in a position to set the terms of trade?"
32. We must make policy for the twenty-first century, not hanker for the nineteenth.

Ross Anderson FRS FREng
Professor of Security Engineering
Computer Laboratory
University of Cambridge

Ian Brown
Professor of Information Security and Privacy
Oxford Internet Institute
University of Oxford

September 27th 2014