Political Studies Association

politics

POLITICS: 2013 VOL 33(4), 299–310

doi: 10.1111/1467-9256.12035

The Future of Cyber-Resilience in an Age of Global Complexity

Lewis Herrington and Richard Aldrich

University of Warwick

This article seeks to discuss two key challenges in the area of cyber-resilience. First, it asks: who owns UK cyber-resilience? Some 80 per cent of the UK's critical national infrastructure is in private hands and the last decade has seen efforts to legislate away some of the problem of resilience by creating legal duties for service providers. This has contributed to a new ecology for intelligence, security and resilience consisting of complex state–private citizen partnerships. However, it is unlikely that populations will accept this approach to risk-shifting when systems fail. Second, it considers what constitutes genuinely robust cyber-defence after the Stuxnet event of 2010. Arguably, any system that depends on information technology, however well protected, is now vulnerable. There is a dawning realisation that the best technical solutions offer only partial assurance. Paradoxically, in an era when the Internet seems ubiquitous, a mixture of analogue and manual systems – often called systems diversity – offers a solution. However, mixed or diverse systems are a declining legacy and not the result of design. We close by discussing the immense challenges that the growing prevalence of electronic systems will bring.

Keywords: resilience; security; surveillance; cyber-war; Stuxnet

Cyber-events reverberate upon national resilience with increasing frequency. The cyber-attacks on Estonia in 2007, the WikiLeaks release of State Department cables in 2010, the Stuxnet attack on the Iranian nuclear programme during the same year and the interplay between social media and the recent 'Arab Spring' all underline both the growing importance of 'cyber' as a concept for international security and its complexity. However cyber is defined, it looms large in the current UK National Security Strategy, driven by anxieties about risk and resilience. Cyber-attacks are considered a Tier One threat; in other words they are among the four risks that the UK National Security Council considers the highest priority (UK Cabinet Office, 2010b, p. 27).

This article examines the future landscape of UK cyber-resilience.[1] It argues that in the electronic realm, intelligence, security, risk and resilience have hybridised. In the short term, this presents an already familiar problem of governance within the UK system, both in terms of ownership and also of public–private co-operation. Britain's national technical authority for information assurance is the Communications–Electronics Security Group based in Cheltenham. This is part of Government Communications Headquarters (GCHQ), the UK's largest intelligence agency. An obvious problem is that some of the hitherto most secret parts of the state now need to be connected to some of the most public. Moreover, there are a bewildering number of stakeholders both in and outside government. No one knows how the increasingly complex ecology of cyberspace should be governed or who should own it.

In the medium term, the problems are of a different order. It is an established orthodoxy among information security specialists that the main impediment to system security is human beings, not the systems themselves (Arce, 2003). The majority of serious security breaches are deemed to be the result of poor personnel security, not technological failures. However, the appearance of Stuxnet, a sophisticated computer worm used to attack Iranian nuclear centrifuges, means that this now stands in need of revision. The discovery of sophisticated malware that spies on and subverts industrial systems has prompted widespread reflection about the future of cyber-security. In the era of Stuxnet, in which even the most protected of systems have been breached by external technical attacks, the answer to cyber-resilience lies somewhere within a hybrid of mixed or diverse systems controlling a proportion of national infrastructure. There is an argument for retaining an inner core of old-style manual and analogue control systems.

Long-term trends threaten this systems diversity approach. Over the next two decades the main driver of information and communications technology will be ever closer connectivity between the Web and the individual. The ultimate goal of commercial technology enterprise is a seamless joining of human beings and the Internet. Currently this manifests itself in more powerful portable devices partnered with cloud technology. However, the future of advanced connectivity between the individual and the Web is direct computer–brain interface, an area where the field of medical technology already pushes the boundaries (Dornhege et al., 2007). The consequences of this development for cyber-resilience are of some importance. When the first person sends an e-mail by 'thinking and then blinking' cyber-security will be of even greater importance than it is now. The protection of our infrastructure will require a determined effort to resist both cultural and commercial pressures towards over-dependency on electronic systems.

Who owns cyber?

In 1941, the American press woke up to the growing importance of intelligence for national security. An enterprising reporter asked President Franklin D. Roosevelt which of the many US government departments with security responsibilities was actually in charge of intelligence. Potential candidates for this included the US Army, the US Navy, the State Department, the FBI and several components of the Treasury. 'They all are – within limits' responded Roosevelt brightly. This flippant response was nevertheless true. Each organisation owned a bit of US intelligence in the mid-twentieth century (Andrew, 1990, pp. 89–90). Deciding on the ownership of intelligence and evolving a structure for governing these matters required the repeated shock of major reverses in several conflicts over many decades. Indeed, it has taken the US more than half a century to identify an authority that commands, rather than merely co-ordinates, intelligence (Aid, 2009, pp. 286–309).

The UK and the US now confront similar problems with cyber. The recent UK Security and Defence Review underlined the new importance of cyber. Indeed, in outlining the nature of Britain's current and future security challenges the word 'cyber' occurred no less than 79 times in just 75 pages (UK Cabinet Office, 2010a). But the location, direction, governance and ownership of that challenge appeared uncertain. This is hardly surprising since 'cyber' means different things to different types of government official. For Defence it suggests a new kind of net-centric warfare which the UK finds difficult to afford at a time of retrenchment (Ministry of Defence, 2010, p. 55). For Business, Industry and Skills (BIS) it means trying to interest the captains of industry in aspects of business continuity that senior managers are often determined to ignore (BIS, 2011). For the intelligence and security agencies it conjures up new technologies that conceivably put the Chinese and the Russians out in front

(Norton-Taylor, 2010). For the Cabinet Office, cyber is something that the core executive feels it ought to own because of its importance, but which at the same time evokes a visceral fear precisely because it means political risk.

At first glance the UK architecture for cyber-security appears to be straightforward. In May 2011 responsibility for cyber-security was moved to the Cabinet Office. The Cabinet Office National Security Secretariat now hosts the Office of Cyber Security and Information Assurance (OCSIA). This supports the Minister for the Cabinet Office and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and co-ordinates action relating to enhancing cyber-security and information assurance in the UK. Spending in this area is reviewed by a National Cyber Security Programme Strategic Investment Board. This new architecture was finalised amid the creation of the National Security Council in 2010 by David Cameron and a blizzard of reviews and new strategy documents (UK Cabinet Office, 2011).

These arrangements underline that the core executive wishes to own cyber-strategy. Meanwhile, GCHQ – successor to the wartime Bletchley Park – boasts an accompanying Cyber Security Operations Centre. GCHQ has also harnessed UK universities, identifying eight as centres of cyber-security excellence and creating a Cyber Research Institute at Imperial College in March 2013 which will attempt to create fresh technologies that effectively detect vulnerabilities in software (Willetts, 2012).

The National Cyber Strategy declares that much of Britain's provision is secret, yet in the same breath it declares that a resilient electronic infrastructure requires a holistic approach involving co-operation by government, industry, universities, the third sector and private citizens. Many of the more informed commentators on information technology note a further paradox: namely that GCHQ, the organisation now in charge of making electronic security more secure, is the same organisation that wishes it to remain porous for intelligence-gathering purposes. This amounts to a bureaucratic conflict of interest or at least an element of schizophrenia that has always existed between the offensive and defensive elements of UK government supervising communications and computer security (Bowden and Akdeniz, 1999).

GCHQ also has competition. On 27 June 2011 the Ministry of Defence announced the creation of its own Defence Cyber-Operations Group with Joint Cyber Units located at both Corsham and Cheltenham provided by a melange of staff from military units and major defence contractors such as Fujitsu, BT, Cassidian, EADS, Babcock and Paradigm (UK House of Commons, 2012). The Home Office has a growing interest in cyber because of its requirement for communications interception, now extended to embrace all our Internet activity including gaming. BIS is a further key contributor because of its responsibilities for e-commerce and it boasts a sizeable budget for cyber-security research. In 2011, the waters were further clouded when significant Internet responsibilities were transferred from BIS to the Department of Culture, Media and Sport.[2] BIS has retained responsibility for the sponsorship of telecoms equipment manufacturing and the wider electronics, IT services and software sectors. In short, the prospect of multiple competing systems for cyber-security now beckons, a possibility increased by the fact that cyber remains one of the few areas attracting new government expenditure.

All these different departments liaise with a further interdepartmental unit called the Centre for the Protection of National Infrastructure (CPNI) which belongs to the Security Service.

This is the operational hub of the UK's information exchanges and works closely with Internet service providers (ISPs) and network providers. Just like everyone else it cannot superintend the UK infrastructure but it does enjoy close relationships with the backbone providers. It maintains the main Computer Security Incident Response Team (CSIRT-UK), the front-line defensive organisation for the private sector. One of its tasks is to take warning material from closed sources and reshape it for public distribution (National Audit Office, 2013). It provides infrastructure operators with guidance on protective security, and oversees an information exchange group for the security of industrial Supervisory Control and Data Acquisition (SCADA) systems. However, some infrastructure operators lack the expertise to implement this guidance.[3]

The UK governance of cyber-security is rendered more complex by two additional developments. The first is Europeanisation and the second is growing public–private partnerships. Many have argued that cyber-security governance is classic intergovernmental territory that is far better organised at a regional level. Europe currently enjoys its own cyber-authority: the European Network and Information Security Agency (ENISA) based in Cyprus. UK BIS is a member of the management board of ENISA and has helped to develop the revised EU Electronic Communications Framework which is now being implemented (ENISA, 2012, p. 15). In practice, ENISA co-ordinates regulation and encourages convergence but has little operational capability. Rather like EU counter-terrorism functions, its cyber-security apparatus is, as yet, a 'paper tiger'. Nevertheless, most ICT businesses take a favourable view of ENISA, asserting that one set of regulatory practices for Europe is preferable to 26 (Bures, 2006).

The scope and scale of the telecoms industry mean that it is they – not government – that have the larger operational capacity and indeed the expertise to deliver meaningful cyber-resilience. Companies like Vodafone, Verizon, AT&T and British Telecom are thus the real drivers of transformation. Britain's GCHQ has struggled for more than 50 years to retain high-grade staff in the face of competition from commercial providers offering more lucrative salaries. In the current climate this has not changed and GCHQ's resilience team aims to retain staff for five years before their training and expertise is siphoned off by the private sector, a target that in practice is rarely met.

Arguably, the ISPs and the major telecom companies, together with the banks and airlines, are also the intelligence and security agencies of the twenty-first century. The focus of intelligence gathering has increasingly shifted towards the agglomeration of private and protected information culled from the Internet. Unlike the government agencies, ISPs are less regulated in this realm or else have legal immunity explicitly extended to them (Williams, 2008). As a result, the ISPs and telecom companies now help to determine the boundaries between security and privacy – indeed they have even begun to shape the national surveillance architecture.

In 2008, then Home Secretary Jacqui Smith sought to introduce a communications data silo that would capture and record the majority of the UK's Internet activity in one place. Designed to help combat domestic terrorism by enabling data mining and active monitoring of mobile phones and Internet traffic, opponents condemned the proposal as 'Orwellian'. One of the key impediments to the initial version of the communications data scheme was the ISPs, which had voiced concerns about privacy and also technical feasibility. At a more fundamental level, they were worried about the degree of confidentiality that they would be able to extend to their commercial customers. The Home Office database was cancelled in favour of greater ISP data retention. On one level this is reassuring, but on another level one is forced to conclude that some of those who mediate between resilience, cyber-security, intelligence and privacy do not reside in government but in the boardroom (Whitehead, 2009).

Risk and blame in the new resilience ecology

Less than 30 per cent of UK companies have defined information and communications security policies and 90 per cent said they had difficulty in recruiting information security professionals (ENISA, 2012, p. 40). Yet government has encouraged the corporate ownership of risk and resilience. In a country that once boasted state-owned railways, telephone systems and gas and water supply, the infrastructure of the state has been radically reduced. Indeed GCHQ, the operational centre for cyber-defence and the UK's national technical authority, does not own its own building but instead leases it from a consortium through a private finance initiative (PFI) contract. This is hardly surprising, for within the hollowed-out market state one might naturally expect that the burden of resilience would gradually pass to the corporate providers through regulation, something one might describe as risk-shifting by legislation (Rhodes, 1994).

Much of this risk-shifting is proclaimed to be positive. This is often explained in terms of a new ecology for resilience. The modern mantra is that government, business, the third sector and the private citizen must work together to provide an organic cyber-defence, one that is less about barriers and more about resilient self-healing systems (Feakin, 2011). This New Age language sounds reassuring – but what happens when core systems actually fail? The public are unlikely to blame the telecoms and specialist Internet providers they have barely heard of, still less fellow citizens with a relaxed approach to anti-virus protection. When the digital tsunami occurs, citizens will hold government to account for the failure of an infrastructure they no longer own or control – and which ministers do not fully understand.

The obvious targets of a cyber-attack are well rehearsed. Government requires large-scale providers of food, power and water to develop detailed contingency plans for physical and cyber disruption and these are frequently practised. But many of these providers are dependent upon secondary chains that are less well regulated. Nor are they fully protected against state espionage and disruption. Meanwhile public–private partnerships around security tend to amount to conversations and consultation rather than genuine convergence. They ensure that the wider community know each other well and are comfortable with each other but real public–private partnerships outside CPNI are underdeveloped (Sommer and Brown, 2011, pp. 66, 75).

The UK government's own investment in cyber-security is hesitant. One of the biggest problems is that in the area of cyber-security the government struggles to assess value for money. How much spending on cyber-defence is enough? A Detica study funded by the Cabinet Office asserts that the problem of cyber-crime costs the UK a reported £27 billion a year (Detica, 2011). Industrial espionage and intellectual property theft against UK businesses account for almost 80 per cent of that evaluation. In response, the new Cyber Security for Business programme has been designed to assist companies in strengthening their electronic defences. The UK spends £650 million a year on its cyber-security programme, an amount many officials suggest is inadequate against the backdrop of what Jonathan Evans, the Director-General of MI5, has called an 'astonishing' level of state and criminal cyber-attacks (Gloucestershire Echo, 2012).

Most of the cyber-crime statistics are, however, contested. Professor Peter Sommer of the London School of Economics has claimed that some recent government cyber-crime reports are merely a 'sales promotion exercise' for specialist security firms. He called the Detica report 'an unfortunate item of puffery' (Espiner, 2011). Sommer argues that that no agreement has yet been made about what to include in the calculation of losses. Tyler Moore, a Harvard University cyber-security expert, has criticised the UK government's failure to show its methodology for ascribing the probabilities, insisting that 'small changes to the probabilities could mean the true cost of cyber crime is much smaller or larger' (Moore, 2011). Moore explains that the challenge to making accurate estimates lies in the under-reporting of incidents. Victims do not readily admit to breaches in security and in some cases do not even know they have been attacked (Curtis, 2011).

Currently one of the major gaps in cyber-resilience stems from a failure to develop IT security education on a sufficient scale. The volume of graduates produced by UK universities in this area is surprisingly low. Cultural change is also required since few IT experts end up on company boards outside the technology sector, and they are largely absent from the highest realms of the civil service. British companies still regard IT security as a backroom function, and indeed resilience and business continuity as a whole is regarded as a mundane subject of secondary importance. Within government the numbers of senior civil servants who understand the Internet or cyber-security are remarkably small.

The consequences of limited in-house government expertise have already manifested themselves. In 2005, the UK Cabinet Office decided to embark on SCOPE 2, an extension of the intelligence messaging service for core departments. Combining a multi-level protected database with secure messaging, SCOPE 2 was intended to be the next generation to its predecessor, SCOPE 1. Implemented by one of the world's top computer companies, SCOPE 2 proved to be an embarrassing and expensive failure. The UK Intelligence and Security Committee confessed they were 'appalled' that the system had been scrapped. The Cabinet Office had been forced to write off £30 million – some 28 per cent of its intelligence spend – and was pursuing a legal claim to recover £40–50 million exhausted on the project (National Audit Office, 2009, p. 24).

Spending on Internet security presents similar problems, but on a much bigger scale. A hugely expensive and risky area, no one truly wishes to own it and no one in government has the expertise to manage it. Yet the Internet is vitally important and the need to provide for its security commands almost universal consensus. Intrinsically transnational in nature, indeed often used as the very signifier of globalisation, European Union agencies such as ENISA also confront many of the same problems of complexity and entropy that baffle national government. Perhaps the most alarming aspect of cyber-resilience is that it is a moving target. Government projects and programmes have failed in the past not only because they were 'big-bang' solutions with little capacity to embrace emerging technology, but also because the private sector moved faster than the public sector. What we know for certain is that the world of information and communications technology is accelerating and the issues that confront government are growing in their size and complexity.

Cyber warfare and human security

Cyber-warfare is not a new concept. The first e-mail was sent in 1971 and within five years later so-called 'Tiger Teams' were attempting to conduct attacks on ICL and IBM machines under the auspices of a UK Ministry of Defence experimental information security programme. Much of this subject is clouded in government secrecy but it is increasingly clear that we have as many as 40 years of cyber-warfare history to draw upon in terms of lessons learned and policy advice, albeit this is often described in outmoded terms as information security or computer security (Ministry of Defence, 1976; Warner, 2012).

Propagated by the Pentagon in the early 1990s, the term 'cyber-war' was initially greeted with considerable scepticism. After the Cold War, defence budgets were in steep decline. Many security commentators regarded talk of 'cyber-war' as a slightly desperate attempt by defence bureaucracies to protect flagging budgets. This convenient new threat required expensive research and development that parliaments poorly understood. Scepticism over the reality of a genuine 'cyber-threat' increased significantly as a consequence of the apparently limited impact stemming from the Y2K millennium bug and has persisted into the twenty-first century (Arquilla and Ronfeldt, 1993; Rid, 2012).

Claims that cyber-warfare represents the fourth dimension of conflict have been confirmed. Arguably, the first cyber-war took place in Estonia in 2007 and the second in Georgia in 2008–2009 (Deibert, Rohozinski and Crete-Nishihata, 2012). Cyber-sceptics were further confounded by the Stuxnet worm used successfully to disable Iranian atomic centrifuges in 2010. Iran suffered a cyber-attack based upon a very sophisticated computer worm targeting an explicit configuration of Siemens industrial equipment. Two of the world's leading anti-virus companies, Russian Kaspersky Labs and Finish F-Secure, both concluded that the attack could only have been conducted with nation-state support. Officially the creators of Stuxnet remain unknown; unofficially both the United States and Israel, perhaps working together, have been widely accused (the United States Cyber Command, co-located with NSA, enjoys a budget of $3 billion per annum but little is known about its activities). Several aspects of Stuxnet were remarkable. First, it showed extraordinary intelligence, selectively infecting few computers outside Iran. Second, it showed the ability to bridge sophisticated air gaps and other defences employed by the Iranian authorities. Third, the Stuxnet worm made use of not one but several 'zero-day' exploits (Farwell and Rohozinski, 2011, p. 23).

Cyber-war contains an alarming paradox. The advanced societies that have developed these capabilities are precisely the ones most vulnerable to electronic warfare. By contrast a cyber-offensive against Cuba, which has one of the lowest rates of computer usage in the world (17 users per 1,000 people) and little digital infrastructure, would have relatively little impact. Organisation for Economic Co-operation and Development (OECD) countries increasingly depend on digital systems for the management of their vital infrastructure (Press, 2011). Aspects of water, power, transport and communications can all be managed remotely by SCADA systems that are designed to regulate industrial processes. Stuxnet was designed to attack a SCADA system; it has demonstrated beyond any doubt that some of these systems can be degraded with potentially grave consequences. Moreover, the precise scale of the threat and the required defence remains opaque.

Hitherto officials have embraced the idea that the critical infrastructure of advanced countries can be defended by ever more elaborate technical solutions. However, Stuxnet has reminded us that most digital systems, however well defended, are porous. What then is real cyber-resilience in the era of Stuxnet? Oddly, some officials are concluding that we might have to consider embracing the simple 'Cuban defence'. The only way to protect against cyber-warfare will be to retain a certain proportion of national infrastructure that is under dual control. In other words cyber-resilience may require the ability for a residual proportion of water supplies, power and other key utilities to be controlled by analogue systems, or even by humble human beings turning wheels and pulling levers. Anxiety over the possibility of cyber-attacks on civilian nuclear power plants has already resulted in deliberate 'system diversity' with a mix of digital, analogue and manual systems. Yet in the twenty-first century it is remarkably difficult to do this across our core infrastructure since engineers have turned to digital solutions to improve operational efficiency (Zhang, 2010).

The UK's infrastructure cannot be turned off like a light switch, partly because it still has a degree of 'systems diversity'. This is partly the result of legacy systems and partly the result of accident. The danger is that this unintended but valuable source of resilience will be eroded in the name of cost-cutting and efficiency. The widespread introduction of smart-metering is an example of a universal system that contains a vulnerability driven by the desire for greater effectiveness and efficiency.

'Systems diversity' is thus the new buzzword in cyber-defence. Resilience in fact requires an increasingly complex mixture of physical security, personnel security, procurement control and system hardening together with further measures to prevent unauthorised or unintended modifications to safety system design. Moreover, the introduction of a mixture of analogue and human fail-safe systems has overturned the accepted wisdom of information security. Hitherto, information security experts have largely been preoccupied with cyber-crime, typically sophisticated efforts to penetrate the security systems of banks and large businesses. The conclusion drawn from more than 10 years of operations in this field was that most security failures resulted from a mixture of human incompetence and human malignancy (Stolfo, 2008, p. 1). However, with the threat of serious state-based cyber-war now looming, experts view human beings together with 'heritage theme park' systems as the last line of defence against a sophisticated cyber-attack.

Gaming the future

The future of resilience is partly about human beings as an antidote to the vulnerabilities of the Internet. However, while the new logic of systems security suggests the need for diversity and even perhaps a wary separation, the broad trend in information technology is towards convergence of human beings and computers. Perhaps the most visible manifestation of this is in the world of gaming where we have seen a drive to draw human and machine together in a simulated topography (Der Derian, 1990). Sophisticated 'gaming' is increasingly embraced by providers of military training to conjure up diverse training environments. Whether for military or recreational purposes, reality and cyberspace increasingly converge, with the next challenge being seamless brain–computer interface.

The most common experience of this can be found in modern gaming technology that uses image recognition to translate human gestures into commands. The Microsoft Xbox Kinect system allows players to interact with a game through physical movement captured by video camera. Clearly the Xbox therefore requires physical motion. However in 2009 Mattel launched 'Mindflex', a game that took its inputs directly from the brain. The inputs were relatively primitive since the player was unable to steer the device consciously. Instead the game read electromagnetic pulses (EMP) emanating from the brain and the player had to learn to direct the game by manipulating their EMP. Under laboratory conditions subjects have been taught to dial a mobile phone using EMP alone. All of these devices, while primitive, nevertheless point the way to the future of technology and the potential offered by computer–brain interface.

An obvious application of the growing connectivity between humans and the Internet is pre-emptive health care. Medical scientists are increasingly interested in small chips that monitor vital signs and can indicate the early onset of heart problems, strokes and other conditions (Michael and Michael, 2005; Streitfield, 2002). Early diagnosis and intervention before these conditions strike materially improves the chances of successful outcomes. This technology is already here. Making use of emerging technologies, for example GPS-enabled smartphones, we can now measure key life signs, how long we sleep for, where we drive to, what we eat and drink and how we spend our day. Having collected these data, obsessive self-watchers place the data in the 'cloud'. The latest example is 'Fitbit', a tiny device that can be attached to your clothing and sends medical data wirelessly to a website that creates graphs of the subject's activity.

The most important developments have occurred in the medical technology intended to treat military casualties. Higher rates of survival on the battlefields of Iraq and Afghanistan combined with life-changing injuries caused by improvised explosive devices (IEDs) have increased the demand for more sophisticated prosthetic limbs. The challenge has been to connect advanced prosthetics to the nervous system to achieve something much closer to natural control by the patient. Over the last five years we have seen radical developments in terms of the ability to connect microelectronics to the human nervous system. The results have been remarkable. The fine motor control these devices offer is almost indistinguishable from that provided by real limbs. Scientists expect that this research will lead to the creation of whole-body neural prosthetic devices aimed at restoring full, essential mobility functions to paralysed patients. In short, the challenge of connecting the electronic messages delivered by the human brain and microelectronic systems will be overcome in the next 10 years (Lebedev and Nicolelis, 2006).

Few scientists doubt that direct computer–brain interface lurks just around the corner. What are the likely consequences for cyber? This sort of enhancement will bring significant economic, social and political implications. Human beings who are constantly connected to the Internet in a more fundamental way will be more capable – but will also think and act differently. The option to be connected and therefore to be in 'constant touch' will represent one of the most fundamental decisions awaiting human beings in the middle of the twenty-first century.

The looming question is how to achieve cyber-resilience in a world in which human beings become increasingly synonymous with the Internet? The possibility conjures up alternative visions that are either utopian or dystopian. It might be that the increasing connectivity between 8 billion human beings and the Web at last delivers a cyberspace that genuinely represents a global commons – a shared virtual topography based on mutual ownership, respect and trust. Alternatively, this new environment might produce greater global risk and uncertainty.

The advent of computer–brain interface will also herald the final collapse in the divide between cyber-security and intelligence. Voluntarily, we place vast amounts of data on the Web and so many of our mundane activities leave an electronic trail. Our public–private data set contains a wide spectrum of information and includes everything from our credit card purchases and library books to the 'status updates' we readily publish across social media platforms. The CIA calls this the 'electronic exhaust fumes of our lives' (Erlanger and Ewing, 2013). Over the last 10 years one of the most important advances in surveillance activity has been the ability to data-mine these vast dust hills of seemingly trivial data to produce intelligence of growing value. Tellingly, the technical intelligence services are now investing less money in cryptography and more money in data storage and large-scale data processing. These are the same national technical authorities that govern cyber-security in both the UK and the United States.

In 1998, David Brin published an intriguing book entitled *The Transparent Society*. Under-recognised when first published, this minor classic provides one of the more intriguing discussions on our digital future. It suggests that while privacy is coming to an end, we should not be unduly concerned. What really matters, he insists, is who owns the data and how they are governed. Universal data potentially hold governments as well as citizens to account. In short, Brin was an optimist and insisted that we were not that far from a radically improved society. More information everywhere could, he insisted, encourage greater civility, even a redistribution of power. In such a future, it would not matter that the state demanded transparency of its citizens as long as the state offered transparency in return (Brin, 1998). Will Brin's *Transparent Society* eventually materialise or will we encounter something rather more dystopian? Bruce Schneier, respected cyber-security expert and sometime security chief for British Telecom has offered a sceptical riposte, insisting that the ownership of these data is unlikely to be even enough to facilitate the collective human accountability that Brin envisages (Brin, 2008; Schneier, 2008). Whichever oracle proves correct, the future is rapidly approaching and, when it arrives, our current systems for Internet governance and cyber-resilience are unlikely to be able to cope.

About the Authors

Lewis Herrington is completing an ESRC-funded doctorate on 'Radicalization and British Counter-Terrorism Policy' in the Department of Politics and International Studies at Warwick University and also holds an M.Eng in Computer Science. He has also served as a research assistant on a project on 'Prime Ministers and Intelligence', supported by Warwick's Institute of Advanced Study. Using interviews with police and former jihadists, together with recently obtained court transcripts, he is currently examining the role of the UK Islamist Movement on the emergence of British Islamic terrorism since 2001. His most recent paper on this subject was given at the ISA conference in San Francisco in April 2013. Lewis Herrington, Department of Politics and International Studies, Social Sciences Building, University of Warwick, Coventry CV4 7AL, UK. E-mail: *l.herrington@warwick.ac.uk*

Richard J. Aldrich is Professor of International Security at the University of Warwick and Director of the Institute of Advanced Study. He is the author of *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (2010). His articles have appeared in *International Affairs*, *Foreign Polic*y and the CIA's in-house publication *Studies in Intelligence*. He currently serves on the Cabinet Office Consultative Group on Intelligence and Security Records, the UK Information Assurance Advisory Council and the UK Ministry of Defence Academic Advisory Forum. Richard Aldrich, Department of Politics and International Studies, Social Sciences Building, University of Warwick, Coventry CV4 7AL, UK. E-mail: *r.j.aldrich@warwick.ac.uk*

Acknowledgements

This article draws partly on the AHRC project 'Enhancing Openness, Explaining Secrecy'. We would also like to thank the anonymous reviewers.

Notes

[1] Here we define cyber-resilience to mean robustness' and 'survivability' measured in terms of performance and sustained availability. It also implies elements of both confidentiality and integrity.

[2] This transfer included: telecoms policy (including implementation of the EU framework); broadband policy and delivery; Internet policy and governance (including implementation of the Digital Economy Act); spectrum (the airwaves used for transmitting radio, television and mobile phones).

[3] CPNI also houses GovCERTUK which performs a similar task for government networks.

References

Aid, M. (2009) *The Secret Sentry: The Untold History of the National Security Agency*, New York: Bloomsbury.

Andrew, C. (1990) *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*, London: Harper Collins.

Arce, I. (2003) 'The Weakest Link Revisited', *IEEE Security and Privacy* 1(2), pp. 72–76.

Arquilla, J. and Ronfeldt, D. (1993) 'Cyberwar is Coming!' RAND Corporation RP-223.

BIS (2011) 'Cyber Security Guidance for Business', September. Available from: http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive [Accessed 2 September 2013].

Bowden, C. and Akdeniz, Y. (1999) 'Cryptography and Democracy: Dilemmas of Freedom' in Liberty (ed.), *Liberating Cyberspace: Civil Liberties, Human Rights, and the Internet*, London: Pluto Press, pp. 81–125.

Brin, D. (1998) *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?*, Reading, MA: Addison-Wesley.

Brin, D. (2008) 'David Brin Rebuts Schneier in Defense of a Transparent Society', *Wired News*, 12 March.

Bures, O. (2006) 'EU Counterterrorism Policy: A Paper Tiger? Terrorism and Political', *Violence* 18(1), pp. 57–78.

Curtis, S. (2011) 'Government Cyber Crime Report Debunked', *Tecweek Europe*, 22 February.

Deibert, R.J., Rohozinski, R. and Crete-Nishihata, M. (2012) 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War', *Security Dialogue* 43(1), pp. 3–24.

Der Derian, J. (1990) 'The (S)pace of International Relations: Simulation, Surveillance, and Speed', *International Studies Quarterly* 34(3), pp. 295–310.

Detica (2011) *The Cost of Cyber Crime: A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf [Accessed 2 September 2013].

Dornhege, G., Millan, J., Hinterberger, T., McFarland, D. and Müller, K. (2007) *Toward Brain–Computer Interfacing*, Cambridge, MA: MIT Press.

ENISA (2012) *United Kingdom Country Report*. Available from: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/UK.pdf [Accessed 23 June 2012].

Erlanger, S. and Ewing, J. (2013) 'Differing Views on Privacy Shape Europe's Response to US Surveillance Program', *New York Times*, 14 June.

Espiner, T. (2011) 'Cybercrime Cost Estimate is "Sales Exercise", Say Experts', *Znet*, 18 February. Available from: http://www.zdnet.com/cybercrime-cost-estimate-is-sales-exercise-say-experts-3040091866/ [Accessed 2 September 2013].

Farwell, J.P. and Rohozinski, R. (2011) 'Stuxnet and the Future of Cyber War', *Survival* 53(1), 23–40.

Feakin, T. (2011) 'UK Perspectives on Security in an Age of "Shock and Aftershock" ', *European Perspectives on Security Research* 1, pp. 45–45.

Gloucestershire Echo (2012) 'GCHQ Leading Fight against Cyber Crime', 6 September.

Lebedev, M.A. and Nicolelis, M.A. (2006) 'Brain–Machine Interfaces: Past, Present and Future', *Trends in Neuroscience* 29(9), pp. 536–546.

Michael, K. and Michael, M.G. (2005) 'Microchipping People: The Rise of the Electrophorus', *Quadrant* 49(3), pp. 22–33.

Ministry of Defence (1976) 'Working Group on Testing of Computer Security', 1976/7 (D/DCCIS/56/8/5/4), DEFE68/287, TNA.

Ministry of Defence (2010) *Equipment, Support, and Technology for UK Defence and Security*, Cm 7989. London: The Stationery Office.

Moore, T. (2011) 'Why the Cabinet Office's £27bn Cyber Crime Cost Estimate is Meaningless'. Available from: http://www.lightbluetouchpaper.org/2011/02/17/why-the-cabinet-offices-27bn-cyber-crime-cost-estimate-is-meaningless/ [Accessed October 2011].

National Audit Office (2009) 'Cabinet Office Performance Briefing: Briefing for the House of Commons Public Administration Select Committee', October. Available from: http://www.parliament.uk/documents/upload/cabinetofficeperform20091.pdf [Accessed 2 September 2013].

National Audit Office (2013) *The UK Cyber Security Strategy: Landscape Review, Report by the Comptroller and Auditor General*, 11 February, London: The Stationery Office. Available from: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf [Accessed 2 September 2013].

Norton-Taylor, R. (2010) 'Titan Rain: How Chinese Hackers Targeted Whitehall', *The Guardian*, 5 September.

Press, L. (2011) 'The State of the Internet in Cuba', unpublished research paper, som.csudh.edu/fac/lpress/cuba/chapters/lpdraft2.docx?.

Rhodes, R.A.W. (1994) ‘The Hollowing Out of the State: The Changing Nature of the Public Service in Britain’, *Political Quarterly* 65, pp. 138–151.

Rid, T. (2012) ‘Cyber War Will Not Take Place’, *Journal of Strategic Studies* 35(1), pp. 5–32.

Schneier, B. (2008) ‘The Myth of the “Transparent Society” ’, *Wired News*, 6 March. Available from: http://bakerinstitute.org/publications/ITP-pub-PlanksOfUSInternationalCyberPolicy-052112.pdf [Accessed 2 September 2013].

Sommer, P. and Brown, I. (2011) ‘Reducing Systemic Cybersecurity Risk’, OECD/IFP Project on ‘Future Global Shocks’, 14 January. Available from: http://www.oecd.org/internet/46894657.pdf [Accessed 2 September 2013].

Stolfo, S.J. (ed.) (2008) *Insider Attack and Cyber Security: Beyond the Hacker*, Boston, MA: Springer.

Streitfield, D. (2002) ‘First Humans to Receive ID Chips; Technology: Device Injected under the Skin Will Provide Identification and Medical Information’, *Los Angeles Times*, 9 May.

UK Cabinet Office (2010a) *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, Cm 7948, London: HMSO.

UK Cabinet Office (2010b) *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Cm 7953, London: HMSO.

UK Cabinet Office (2011) ‘The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World’, November. Available from: http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf [Accessed 29 January 2012].

UK House of Commons (2012) ‘Supplementary Written Evidence from the Ministry of Defence, Following the Private Evidence Session on 18 April 2012’, HC106, Defence and Cyber-security, DCS 001a.

Warner, M. (2012) ‘Cybersecurity: A Pre-history’, *Intelligence and National Security* 27(5), pp. 781–799.

Whitehead, T. (2009) ‘National Database Dropped but All Our Communications Will Still be Monitored’, *The Telegraph*, 29 April.

Willetts, D. (2012) ‘Oral Statement to Parliament, UUK Conference: “A World without Boundaries” (BIS)’, 13 September. Available from: https://www.gov.uk/government/speeches/uuk-conference-a-world-without-boundaries [Accessed 2 September 2013].

Williams, C. (2008) ‘BT’s Secret Phorm Trials Open Door to Corporate Eavesdropping: Government Bumbling Exposes Oversight Gap’, *The Register*, 17 April. Available from: http://www.theregister.co.uk/2008/04/17/ripa_phorm_shambles/ [Accessed 24 August 2012].

Zhang, D.J. (2010) ‘Integrating Cyber Security into Nuclear Digital I&C Safety Systems’, ASME Conference Proceedings 18th International Conference on Nuclear Engineering: Vol. 1/Instrumentation and Controls (ICONE18).