Cyber Doctrine
Towards a coherent evolutionary framework for learning resilience

JP MacIntosh, J Reid and LR Tyler
The Institute for Security & Resilience Studies (ISRS) at University College London (UCL) provides a hub for scholars and practitioners to address the challenges of resilience and security in the 21st Century. We bring together the public, private and third sectors to seek out ways to catalyse innovation – so that we can all better cope with, and flourish in, increasingly uncertain times.

The contents and opinions expressed in this paper are entirely and solely those of the authors and do not necessarily reflect the views or policy of HM Government or of University College London.
Cyber Doctrine
Towards a coherent evolutionary framework for learning resilience

JP MacIntosh, J Reid and LR Tyler

June 2011
Acknowledgements

The authors would like to thank the following for their invaluable advice and support during the drafting of this document:

Dr Mark Bentall, Cassidian; Prof Philip Bobbitt, University of Texas/Columbia University; Prof Steve Caddick, UCL; David Ferbrache, Ministry of Defence; Julia Harris, Oxfam; Philip Rice, Erudine; Martin Rice, Erudine; Mike Simms, Cassidian; Chris Swan, UBS; John Trundle, Euroclear; Judy Baker, Cyber Security Challenge UK.

And Dan Fox and Jas Mahrra at the Institute for Security & Resilience Studies at UCL.

Any outstanding errors, omissions and weaknesses are – of course – the fault of the authors alone.

We also take this opportunity to thank our Foundation Partners, EADS and Ultra Electronics, for their support.
Authors

Rt Hon Lord Reid of Cardowan PhD, ISRS Chair and UCL Honorary Professor

Before leaving Parliament in 2010 after 23 years as an MP, Dr John Reid had served at the highest levels of government, including as Home Secretary, Secretary of State for Defence, Health, Northern Ireland, and Scotland, and as Leader of the House of Commons.

He is a leading thinker on security and resilience and regularly publishes articles and comments on these issues in media throughout the world. He is a Principal in the Chertoff Group.

Lord Reid established the ISRS in 2008.

Dr JP MacIntosh, ISRS Director of Programmes and UCL Honorary Professor

After a decade’s service with the British Army, Jamie became a research scientist at the Ministry of Defence in 1995. Before his secondment to ISRS, he was the Chief of Research and Assessment at the Defence Academy of the UK.

He has fulfilled several advisory roles for Cabinet Ministers and senior decision-takers, in the UK and abroad. In spring 2001, he co-authored the concept of “Resilience to Crises” for the UK Government.
He has built teams that have worked in operational theatres and with many organisations facing the challenge of deep transformation – in and out of conflict. How strategies gain traction through innovation remains core to his work as ISRS Director of Programmes.

Len Tyler OBE, ISRS Senior Associate Fellow

Recently retired as a Senior Vice President at EADS, Len has, since the late 1980s, held a number of senior management positions in the technology and defence sectors, with companies such as Marconi, Nortel and Cogent.

His international experience includes growing businesses in the US, Taiwan, Netherlands, Turkey and Saudi Arabia; and with supra-national organisations such as NATO and the United Nations. Len was awarded his OBE for services to the defence industry in the 2009 Queen’s Birthday Honours List.

Over recent years, he has developed a keen interest in supporting innovation and entrepreneurship with a number of SMEs. At ISRS, he leads the promotion of our work on Cyber Security and Cyber Doctrine.
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFACE</td>
<td></td>
<td>ix</td>
</tr>
<tr>
<td>Key Findings and Recommendations</td>
<td></td>
<td>xiii</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER ONE</td>
<td>Competent Authorities</td>
<td>13</td>
</tr>
<tr>
<td>CHAPTER TWO</td>
<td>Organisation Of Capabilities</td>
<td>43</td>
</tr>
<tr>
<td>CHAPTER THREE</td>
<td>Capacity To Innovate: Scaling For Generational Change</td>
<td>65</td>
</tr>
<tr>
<td>IN CONCLUSION</td>
<td>In Conclusion: An Ethos For Learning Resilience</td>
<td>103</td>
</tr>
<tr>
<td>Acronyms And Initialisms</td>
<td></td>
<td>115</td>
</tr>
</tbody>
</table>
It has often been said that the price of security is constant vigilance. In our contemporary world that is only half the task. Today, that price must also include constant innovation; pro-active, strategically-guided but free-thinking innovation.

This year, 2011, marks the 25th anniversary of the signing into law, in the United States, of the Computer Fraud & Abuse Act (CFAA). Partly inspired by the 1983 blockbuster "WarGames" (Hollywood's early rendering of the "hacking" phenomenon), the CFAA was the first example of liberal democracy's attempts to protect itself and its citizens from what are now better understood as cyber-crimes or cyber-attacks.

Today, the reach and effect of technology bears little resemblance to the inchoate networks and unwieldy hardware of 1986. The opportunities have been (and remain) growing and incalculable. Unfortunately, so do the vulnerabilities. In the intervening quarter century since 1986 our ability to address the commensurate threats has not evolved at a similar rate. Indeed, too often, the scramble to catch up has been undermined by ill-informed action.

This booklet, *Cyber Doctrine: towards a coherent evolutionary framework for learning resilience* addresses this problem. It is the
Cyber Doctrine

inaugural publication from the Institute for Security & Resilience Studies (ISRS) at University College London. It offers bridges between law, policy, security, and technology across our highly networked individual lives. Though there is inevitably a UK focus, there are wider applications, as befits a transnational approach to this environment.

Cyberspace is a manufactured environment, comprised of ones and zeros, not bodies and mass. Its infrastructure depends on nano-scale innovation, not industrial-scale production. The rules of engagement - both civilian and military - developed for land, sea and air, over the centuries and millennia, require unprecedented adaptation.

Drawing on work and with input from cybersecurity practitioners, technology specialists, legal experts, policy makers, entrepreneurs and academics, ISRS has identified the major challenges faced by anyone seeking to ensure the security, exploitation and exploration of cyberspace. Whether a sovereign body, corporation or citizen, surviving and thriving will depend upon embracing an ethos of delivery, innovation and growth to ensure that the UK becomes a (or possibly the) trusted hub for global ventures.

The proposed Doctrine is founded on the recognition that resilience is competitiveness. It should be synonymous with entrepreneurship. At its centre is the vital principle of the easy integration of competent authorities and capabilities with the capacity to manage and innovate. Sustainable resilience in cyberspace will derive from open sources and standards, driving an internationally coordinated approach to Research & Development.
This is only the starting point. To reflect the velocity and flux of cyberspace itself, Cyber Doctrine will likely not remain a singular concept in the months and years ahead. In the meantime, we would welcome any feedback to isrs@ucl.ac.uk

Rt Hon Lord Reid of Cardowan
Chair, Institute for Security & Resilience Studies
London, June 2011
Cyber Doctrine
The aim of this document is to advance production of cyber doctrines on terms that enable the learning of resilience. The document offers a model that is open to falsification. This befits the evolutionary nature of cyberspace in which change and indeed crises – as decisive moments – are the norm not the exception.

Throughout, the document treads a careful path between cyber hyperbole and scepticism by placing concepts and evidence in an evolving context, which can enable durable learning. Alarming anecdotes and the inevitable dismissive rational backlash they invite are counterproductive. Time is wasted; learning stalls.

The concepts of resilience and its inverse – irresilience – are grounded in advances in mathematics. These enable people – decision-takers at all levels – to explore the risks and uncertainties of dynamic networks. Doing so does not just raise awareness of complex dangers; it also offers options for coherent decisive actions, which produces rather than just protects value. The challenges of cyberspace present ample reasons for optimism.

Moving beyond attempts to stop bad things from happening is vital. An overriding message emerges from the document: cybersecurity involves necessary tactics that are never sufficient to a strategic solution; whereas resilience is pragmatic and adds value because
pursuit of resilience enhances the productive forces of cyberspace promoting healthy competitiveness. This is a quite different proposition to conventional security industries.

The productive forces for trustworthy networks embody Delivery, Innovation and Growth (DIG) and sow resilience wide and deep. Whether a sovereign body, firm or citizen, the DIG ethos becomes vital to surviving and thriving in cyberspace. It offers the prospect of creating a growth industry, bringing together academia, private and public sectors – in which the UK can excel at home and abroad.

We are not an official body. We do not claim to be a competent authority. But the document does signpost how evolving doctrines can restore coherence and trust in competent authorities, the organisation of capabilities and the capacity for innovation. Indeed, for traction to be gained with the challenges ahead, the capacity for innovation – especially entrepreneurship – is the first consideration. From innovation flows the organisation of capabilities in composable ways across time that will demonstrate the competence of any would-be authority. Competent authority is not a given.

Cyberspace is a challenging environment in which there will be continuity – but that will be difficult to discern in the welter of change. Restating familiar phrases about risk, leadership and strategy is easy; abstraction adds to the disconcerting sense of unrelenting change. Yet from abstract concepts to development of doctrine we are able to offer recommendations for further consideration:

• The immediate creation of a joint cyber-resilience Task Force to include academia, government and industry.

• The Task Force should be established under a dedicated Minister reporting directly to the National Security
Council (NSC), particularly on economic, financial and market factors.

- The Task Force is to be action-oriented and focused on DIG outcomes through the:

  1. Establishment and development of cyber-doctrine in the UK, which will offer a framework for learning resilience to all (e.g. instead of arms control treaties) but also advance national competitive advantage.

  2. Design of evolving processes for meshing concepts and doctrine to demonstrate the value of blending investments in exploration (e.g. education, R&D) and exploitation (gaining market share in products and services) i.e. DIG for pragmatism.

  3. Development of transnational liaison involving public, private and third sectors, especially academia.

  4. Promotion of entrepreneurship by selecting, educating, examining and placing competent individuals for recruitment and advancement to leading posts in public, private and academic sectors vital to the continuous demonstration of competent authority in cyberspace.

  5. Incentivisation of innovation through organising incubators (e.g. Cyber Enterprise Zones) as venues for entrepreneurs from all sectors to invest in and catalyse innovations that can be spun out as Joint Ventures with equity shared appropriately.

  6. Creation of Hubs (action groups – *little platoons*) to facilitate the necessary transformation, for example, in
Cyber Doctrine

developing means of measuring and assessing the capacity for innovation vital to resilience and the development of open source tools and apps, which enable exploratory navigation and the gathering of evidence about the value of evolving capabilities in healthy markets and how insurance affects behaviour.

These recommendations are provisional. Cyber Doctrine provides a framework for learning resilience as much through failure as success. Inasmuch as what needs to be done, how and in what strength can be answered, the question of who is more challenging. In a transnational environment, clarity about who can do what and how everyone learns is vital.
Cyber Doctrine
INTRODUCTION

Preamble

1. Cyber is fashionable again. Use of the prefix cyber is proliferating: cyber-crime, cyber-tax, cyber-bullying, cyber-money and so on. In recent decades cyber-hyperbole has been followed by scepticism and confusion. The cyber-punks\(^1\) of the 1980s produced a seductive cocktail of edgy culture and technology to which a decade later was added the declaration that “Cyber War is coming”\(^2\). Today the fictional character Lisbeth Salander from Larsson’s *Millennium Trilogy*\(^3\) exemplifies the virtues of cyber-punks to a mass audience.

2. Leaders and decision-takers – elites – are however more confused about what competencies, capabilities and capacity befit the now officially recognised environment of cyberspace\(^4\). Self-evidently, the addition of the first man-made environmental domain to maritime, land, space and air is far from just a bureaucratic detail. Unfortunately, the implications can over-excite people from many different fields. Consequently, in reaction, cynics and sceptics are once again poised to dampen enthusiasm and unwittingly frustrate learning. Other pundits can profit from building a story up as well as knocking it down\(^5\). The mounting confusion and neglect that ensues only further undermines the prospects for shaping resilient networks.


Cyber Doctrine

3. The aim of this document is to advance production of coherent Cyber Doctrines on terms that enable the learning of resilience.

Concepts: Bounds and Assumptions

4. Cyberspace may be the first man-made environment but it brings us back to nature with an almighty thump. As Burns succinctly put it centuries ago, “Nae man can tether time nor tide”. Rational measures to master nature at sea, on land, in the air and space have not ended in systemic control. Instead, networks have been created that proliferate and evolve fast. They morph temporal and spatial dimensions that impact all environments, putting patches of control into a welter of evolutionary change.

5. Cyberspace presents this in abundance. This awakening to the nature of cyberspace – whether or not you live in a wealthy or economically developed community – affects everyone:

- From the Neo-Taliban’s propaganda front nurturing a cyber-Ummah out of the borderlands of AfPak, sometimes with skills learned in Yorkshire schools and colleges;

- To High Frequency Traders, un-chastened by the Great Recession or the Flash Crash, profiting through processes operating near the speed of light;

- From the raw statecraft experienced by Google and Morgan Stanley as the Chinese seek to shape the future;

- To paedophile “grooming” of children and their use of proxies; and


6. Cyberspace abolishes neither time nor space; it just makes good and bad evolutionary forces more dangerous to ignore. The examples cited above do not imply that only the malevolent can innovate or have the fitness for cyberspace. Rather these are important competitive benchmarks. Gaining advantage over such competitors cannot rely entirely on old assumptions. Rational attempts at control tend to assume that time can somehow be stopped and cut up into short-term static chunks, systems can be disconnected and that rewarding those that solve tame problems based on these assumptions has no consequences. These assumptions do work – sometimes. Cyberspace makes those occasions increasingly rare.

7. It is not hard to imagine how easy it is to exploit cyberspace. The internet was not originally designed to be a global infrastructure for the world’s human population online. It is easily scaled but anyone with malicious intent can abuse the network.

8. As game-changing technologies drive the global web, with the internet seen as free, open and neutral, issues are mounting. These are diverse and range across the spectrum of national security and commercial concerns – from the continuing and growing risk from cybersecurity threats in both Communications and Information Systems (CIS) currently used by military, government and commerce to the Industrial Control Systems (ICS) used by organisations such as utilities. These affect citizens everywhere.

9. Some are of specific concern in military and defence affairs; there is, for instance, the growing need for interoperability for coalition operations, inter-agency and improved C4ISTAR\(^9\) coupled with the need to put in place predictive protection rather than reactive.
10. But in a wider sphere, governments are also moving towards enabling technologies to plug in solutions from any vendor – Open Source / Standards – which drives the need for a co-ordinated R&D agenda. However, the recession-imposed budget constraints for Governments in Europe, US and some other key economies are reducing opportunities for new business. Cuts and efficiency measures alone can cut deadwood but still be done in ways that crowd out innovation and growth. Austerity must be complemented with innovation and growth, gaining greater value from legacy capabilities and providing the gateways for future migration to new technologies. Mishandled austerity will lead to complications being layered on complications.

11. Old realists are fond of saying deal with the world as it is rather than as you would wish it. Cyberspace requires a natural pragmatism. In this document we strive to deal with the world as it evolves through the coherent development of Cyber Doctrines. We do not assume reality is static or that a static ideal is attainable. In a transnational world, coherent doctrine development has to be a pluralistic, multilateral and evolutionary endeavour. As jurists understand, the principles that evolve through doctrine rather than details fixed in codified law (treaties, statutes etc) makes such endeavours realistic.

12. We do assume that the capacity to innovate is fundamental to fitness in cyberspace. Developing doctrines can enable the productive uptake of innovation. We believe that this potential for a deep, innovative resilience is made manifest in the span of capabilities that can be integrated and in the competence of decision-takers to catalyse timely, coherent actions of enduring merit. These measures are a vital supplement, not a substitute; they complement routine and standard security practices by focusing on the gaps. It is here that gains can achieve increasing rather than diminishing returns on investments.
Purpose and Proposition

13. Cyber Doctrine offers a framework for enabling coherent decisive actions because it makes learning the core enduring activity from which the capacity to innovate germinates. It is a framework for learning resilience that is open to multilateral debate from a plurality of perspectives. The provisional framework is addressed to all citizens: senior decision-takers, security professionals, strategists, innovators, service providers and users. Cyberspace now involves and embroils us all. So must the development of evolving doctrines and concepts.

14. Cyber Doctrines are for good days and bad. Beyond the Great Recession, cyberspace is the environment that will spur growth. The content created through the rich interactions cyberspace enables in education and research move seamlessly into the production of mass and open innovation and the distribution of goods and services through networks that reach all consumers. This is far from one-way traffic. The distinction between users and developers is blurring like so many other boundaries in cyberspace. Cyberspace provides an environment for everyone to contribute to the challenges ahead as active citizens not just passive consumers.

15. Growth on these terms can be peaceful. But – as ever – it would be naïve to assume that those bent on crime and conflict\textsuperscript{10} are not just as eager to feed on innovation. Learning resilience is vital whether the the circumstances are favourable or not.

Design: Form and Flow of Reasoning

16. As Einstein is reputed to have said: “Everything should be made as simple as possible, but not simpler”\textsuperscript{11}. Cyberspace confounds many prevailing assumptions when it is least helpful. That can tempt an upsurge in noise and jargon with an
**Cyber Doctrine**

**Diagram 1**
Evolutionary learning through developing cyber doctrines

<table>
<thead>
<tr>
<th>Cyber Doctrine: A coherent framework for learning resilience</th>
<th>Proactive</th>
<th>Reactive</th>
<th>Integrative</th>
<th>Fragmentary</th>
<th>Evolutionary</th>
<th>Rapidly outdated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competent authority</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organisation of capabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity to innovate: scaling for generational change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Diagram showing the evolution of cyber doctrines with axes for Proactive, Reactive, Integrative, Fragmentary, and Evolutionary. The diagram highlights Tractability and Composability, with a timescale showing De Jure or De Facto standards in evolving architectures.
inevitable simplistic backlash. This document will strive for simplicity without descending into the simplistic or pointless complications. As laid out in Diagram 1 (left), the body of the document is in three parts, each addressing a major challenge:

a) Competent Authorities. Explains the various stakeholders and their needs, agendas and world views and how these will influence future strategies;

b) Organisation of Capabilities. Considers how doctrine can work to enable the integration of evolving capabilities; and

c) Capacity to Innovate. How a Cyber Doctrine works to promote the requisite variety for resilience in depth.

17. Under each of these headings, developments relevant to cyberspace will be assessed as tending to be either:

• Reactive, fragmentary and easily overtaken by events; or

• Proactive, integrative and cultivating evolutionary strength.

18. This assessment will range from: (in)coherent decisive actions, weak strategies, policy and slow legal developments (part 1); the challenge of composing a wide variety of evolving capabilities in “satisficing”\textsuperscript{12} ways (part 2); and, finally, outlining the depth and requisite variety required for bodies to thrive on innovation (Part 3). This extends from Research and Development (R&D) to growing on healthy terms the cybersecurity sector and the economy as a whole that relies upon it through the uptake of innovation.

Cyber Doctrine

19. The document’s design is simple not least because the doctrine outlined here is provisional. It extols evolutionary forces, and those apply as much to the development of the doctrine as to the topic of cyberspace itself. The document is designed to provoke learning, and signposts an agenda for action.

20. Resilience requires moving forward rather than just “bouncing back”. Meshing concepts and doctrine needs focus on Composability (concerning the pragmatic permutations for integrating capability options across the flow of time) and Tractability (concerning gains and losses of power in evolving combinations of capability options running with the flow of time). Steering through the spate of uncertainties demands no less.

Innovations and Undertakings for Consideration

21. Our considerations take place against a backdrop of cyber activity and engagement at government, corporate, technological and social levels; in turn, these exist as national, international and transnational networks. Some of the more significant are worth mentioning.

22. In the published US National Strategy for Cyberspace (Dec 2008), building partnerships with the private sector was seen as key and crucial. It saw the critical infrastructures as energy, finance, the converging information and communication sectors and central/local government. By effectively improving cybersecurity it offered the opportunity to rethink how government operates and could build collaboration across organisational boundaries. These themes have been underscored and somewhat elaborated upon by the White House’s 2011 “International Strategy for Cyberspace”.

23. In the UK there are obvious parallels being considered, with cybersecurity and assurance at the centre of government future
investment strategies. Government is also under pressure to rationalise the many systems that it uses to identify its employees and contractors, and its dealings with citizens, residents and visitors, in order to cut costs, reduce fraud and improve national security.

24. For some, the evolution of Cloud computing over the past few years is potentially one of the major advances in the history of technology. Securing the infrastructure is becoming ever more essential against the impacts of disruptions and cyber attacks\textsuperscript{14}. Governments and commercial enterprises are further committed to ensure a level playing field for Open Standards\textsuperscript{15}. The US DOD has already moved in this direction on the SIPR Net with an open framework. (This enables the US Air Force to plug in solutions from any vendor and more importantly to overlay with multilayered threat protection). This is cited as evidence of legislation not impeding innovation rather than advancing corporate interests\textsuperscript{16}.

Strategic Importance To The United Kingdom

25. The appropriate handling of cyber issues is now being publicly identified as a matter of worldwide strategic importance in economic and security terms. In the UK, Peers\textsuperscript{17} and the retiring Minister of State for Security (Baroness Pauline Neville-Jones) have stressed the importance of having governance regimes that makes the UK’s networks the indispensible choice for internationally trusted operations.

26. We strongly support this view. We believe that the failure to create and enforce such governance regimes will lead to the UK inevitably becoming overly reliant on systems over which it would have little or no serious influence\textsuperscript{18}. Moreover, we contend that if the UK is to retain its reputation for trustworthy and reliable networks there is no room for complacency. Strategies need to evolve fast, based on the learning of resilience that Cyber Doctrine can enable. Doing so is of immediate and enduring value:

---

\textsuperscript{14} See, for example, a German security researcher has used a program that runs on Amazon’s Cloud Computing system to run through possible passwords to see if they allow access to the network, “Cloud Computing Used to Hack Wireless Passwords”, 10th January 2011, Networked World available at http://www.networkworld.com/news/2011/011111-cloud-computing-used-to-hack.html?page=1 accessed 12th Feb ’11.


Cyber Doctrine

- **Commercial security** – businesses would be immensely better protected against loss of Intellectual Property and can continually gain competitive edge in global markets;

- **IT enabled productivity gains** – not least through smarter utilisation of highly scaleable hardware and software resources and from enhanced business agility including mobile interactive applications that respond in real time to user requirements;

- **Public service improvement** – greater confidence would be engendered in public service transactions, thus enabling efficiencies and economies from the migration towards a national ‘Computer Cloud’; PwC estimate that if every currently off-line adult moved just one contact a month with government to on-line, the savings would total £900m per annum19;

- **Competitive edge for firms and nations** – inspiring the growth of work forces that drive the uptake of innovation vital to the advance of sustainable economies; and,

- **Cyber crime and the economics of security** – playing a crucial role in countering cyber crime, which it is currently estimated cost the UK alone, £27 Billion per annum20. Estimates of costs worldwide vary but there tends to be a consensus that cyber-crime involves all other forms of organised crime and terrorist funding.

27. These do no more than begin to indicate the potential benefits and savings to us all as citizens, achievable through injecting resilience into the public, private and voluntary sectors of the fast changing systems and networks we all increasingly rely on. But is there enough direction and leadership from Competent Authorities?

---


Cyber Doctrine
28. “A competent authority is any person or organisation that has the legally delegated or invested authority, capacity, or power to perform a designated function”. What competent authorities do stems from an understanding of the context. The more uncertain, dynamic and prone to unexpected events a context is, the wiser it is to underpin competent authorities with doctrine. Doctrine provides guidance where codified knowledge gives out. Cyberspace is exactly such an arena. In such circumstances friction at the interface between politics and law can be lubricated with doctrine. This is particularly important in the overlap between peace and war. We return to the direct issue of competent authorities having clarified how doctrine lubricates learning where friction is at its worst.

What is Doctrine?

29. The rule of law is fundamental doctrine for many, foremost because it is believed to be a bulwark against the arbitrary exercise of power. The rule of law may even be a universal principle everybody can adhere to; yet the arbitrary exercise of power remains desirable to some21. To wish it otherwise is fanciful.

30. Irrespective of any desire for arbitrary power, rule of law stalwarts need to differentiate law-upholding from law-making, rather
Cyber Doctrine

than subsume the latter to the former. Over time the rule of law will be found inadequate if based exclusively on upholding existing law\textsuperscript{22}. That inadequacy cannot be satisfactorily filled by the judiciary making legal precedent\textsuperscript{23}. The rule of law includes the politics of law-making\textsuperscript{24}. Such politics and principles ranges from constitutional to civil matters; a span that for some veers more to protectionism than competitiveness\textsuperscript{25}. Doctrine in the sense developed here is multilateral and plural, offering the prospect of more graceful evolutionary learning processes than may otherwise happen. Doctrine works with the politics and learning from evolving principles.

31. Cyberspace poses many challenges for the rule of law. Those challenges will be aggravated, if the rule of law principle only affirms the upholding of existing law, the slow advance of judicial precedent, for example, through Customary International Law (CIL), notwithstanding. There are incontrovertible reasons for not politicising the upholding of the law, whether along partisan or autocratic lines. However, to assume the rule of law as a whole is apolitical is fallacious. If the law trumps politics on the exclusive basis of law-upholding, then politics will be lured into states of exceptionalism\textsuperscript{26} and decisionism\textsuperscript{27}. This usurps the rule of law because it invites the arbitrary use of power. To contend that competent authorities are affirmed by the arbitrary use of power is not only undemocratic but also retards learning, which consistently leads to catastrophic errors.

32. The dangers of exceptionalism and decisionism are not new but are amplified in cyberspace by two features:

   a) the pace of change throws up cybersecurity challenges – real and imagined – that will be readily construed as states of exception to existing legal frameworks; and

   b) in addition to sovereign bodies, non-state actors and networks will more often have the power to perceive and act in exceptional ways, too\textsuperscript{28}.

22. See, for example, Tikk, E (2011) Ten Rules for Cyber Security, Survival, Vol. 53, No. 3, 119 – 131, in which a thorough map of existing laws is boiled down to a baseline of ten rules for improving the upholding of existing laws; an effort that explicitly excludes consideration of the evolving politics and technology.

23. It has been asserted that judges are using the European Convention on Human Rights (ECHR) to introduce a “backdoor” privacy law, which is an affront to UK sovereignty because it sidelines the elected lawmakers of the UK’s Parliament. See, for example, “Mail Editor Accuses Mosley Judge”, 10th Nov ’08, BBC News available at http://news.bbc.co.uk/1/hi/uk/7718961.stm accessed 12th May ‘11.


26. The concept of exceptionalism stems from the German romantics JG Herder and JG Fichte. Their claims for the uniqueness that makes a people exceptional have been taken up by several Great Powers including the US (see, for example, Leven, A (2004) America Right or Wrong, HarperCollins: London). Exceptionalism extends to exceptional circumstances or states of emergency in which decisiveness is seen as an imperative, albeit arbitrary. This couples exceptionalism with decisionism.
27. Decisionism is a politico-legal concept that focuses on the authority to decide rather than substance of the decision. This convenience is viewed as necessary in states of exception but can become the default for exceptional states. Carl Schmitt provided the logic of decisionism for the Third Reich (see, for example, Schmitt, C (1985) Political Theology: Four Chapters on the Concept of Sovereignty, (trans) Schwab, GD, MIT Press: Boston MA, original publication: 1922, 2nd edn. 1934). Albeit, exceptionalism and decisionism are not exclusive to Fascist states. The culminating point of David Frost's Nixon interview is a decisionist gem. Nixon candidly admits that as President he believed what he uttered as a decision is law. The lure of decisionism and exceptionalism is also evident among Neo-Conservative scholars, see, for example, Strauss, L (1995). "Notes on Carl Schmitt, The Concept of the Political". (English trans. by J. Harvey Lomax of "Anmerkungen zu Carl Schmitt", 1932.) In Heinrich Meier, Carl Schmitt and Leo Strauss: The Hidden Dialogue, trans. J. Harvey Lomax. Chicago University Press: Chicago.

28. Tikk, E (2011) op cit, makes the interesting point that the rule of self defence can be invoked under the UN Charter and the domestic criminal law of nations. Whilst it is unclear how cyber attack would amount to "armed attack" under the UN Charter, it is also unclear how much asymmetric force an individual exercising self-defence might unleash and whether that could be contained within a domestic jurisdiction.


33. In cyberspace, decisionism is not the monopoly of sovereign bodies. Competent authorities will be evidenced by their capacity to learn. Such learning could not be more vital than at the interface of politics and law. But the apolitical rule of law is doctrinaire and self-defeating. Doctrine, on the other hand, does not exclude the political in either peace or war. Accepting politics as the overriding friction on these terms does not necessarily invert Clausewitz’s dictum that “war is the continuation of policy by other means”²⁹, nor does it imply or require the militarisation of cyberspace (although we can learn from historical military developments and use of doctrine). Evolving doctrines can offer coherent ways forward that avoid the needless and reckless slide to exceptionalism and decisionism. This is not a Kantian “pious wish”; it is unashamedly pragmatic. Paradoxically, strategic nuclear doctrine and military doctrine more generally offer sound reasons and precedents for such a move.

34. Doctrine can hold and handle contradictions in healthy tension. For example, the use of Dumdum bullets in war against combatants is illegal. These bullets were judged cruel and disproportionate in the Hague Convention (1899). Yet they are legal for law enforcement purposes.

35. The precedent of Dumdum bullets is at odds with the legality of threatening or using nuclear weapons. There is no definitive judgement on nuclear weapons³⁰. Their menacing presence in peace is undoubted but it avoids being judged aggressive enough to be a crime against peace. Whilst in war a nuclear exchange might be proportionate, it is hard to doubt any such grim proportionality would outweigh the indiscriminate cruelty using such weapons would inflict. Yet legal judgements remain vague and inconclusive. Nuclear doctrines have played a vital role in filling the void between sovereign powers and the rule of law.
Cyber Doctrine

36. For the British, military doctrine comprises evolving principles by which action is guided; it is authoritative but requires judgement in its application. The use of doctrine accepts the contingency of circumstances and constantly adapts by learning lessons\(^1\). Among these has been a fresh realisation that conflict is saturated in politics; and that fact is affirmed by and affirms the need for doctrine to engage and enable more services than just the military. The need for a comprehensive approach that includes many civil agencies has become manifest. Doctrine is helping bring coherence to these diverse activities – an approach endorsed by the United Nations publishing doctrine on these terms in 2008\(^2\). Doctrine is also being invoked from an interdisciplinary perspective that brings social, technical and economic behaviour into a coherent framework for cybersecurity\(^3\).

37. In using doctrine the British military have always been wary about any slide from doctrine into being \textit{doctrinaire}.

38. That concern is not necessarily diminished by seeking a “comprehensive approach” to the uncertainties of conflict or disaster zones. Or by the more general assumption that the development of any such new approaches will inevitably or automatically lead to the development of doctrine. The creation of the Civil Contingencies Secretariat in the UK’s Cabinet Office a decade ago reinforces the need for caution here. Although it has for some time been accepted – and remains clear – that the concept of resilience to crises is vital to network societies, it was always intended that that concept would be articulated through an evolving doctrine\(^4\). However, the post Cold War era left a variety of legislative loose ends, stemming from, for example, the 1926 General Strike and contemplation of a post-nuclear strike era. The Civil Contingencies Act (CCA) of 2004 tidied such loose ends in preparation for a doctrine of far greater use to citizens, organisations and leaders.

\(^1\) See, for example, http://www.mod.uk/DefenceInternet/MicroSite/DCDC/OurTeams/Doctrine.htm for a broad definition of doctrine accessed 12th Mar ’11.


39. But the UK’s resilience doctrine has never been produced to fulfil the concept, despite the fact that resilience now being taken up with alacrity around the world. Such a doctrine would support sowing resilience wide and deep. Precisely as it does for the UK military, doctrine would enable distributed decision-taking and coherent action, not least when uncertainties are at their most challenging. The CCA may be a necessary contingent but its use would be made a more remote and exceptional prospect if a resilience doctrine were enacted. This is not an unimportant issue; the CCA already empowers the Government to switch off the internet to the UK, a point missed by Liberty despite their approval of the consultation process ahead of the Act. In a moment of crisis, the UK Government could find itself in as awkward a place as Senator Joe Lieberman found himself during the Egyptian uprising. It was not a good time to be legislating to pull the plug on the internet in the US just as Mubarak tried the same, in January 2011.35

40. Agreed doctrine provides a way to avoid the pitfalls of both legalism (i.e. adherence to law as it stands rather than face the politics of law-making necessary for evolving fitness), and the twin perils of exceptionalism and decisionism. Doctrine can restore confidence in competent authorities – whether sovereign bodies or not – because doctrine renders principles accessible and enables active learning. This section goes on to detail why that is even more vital when contending with the operational and strategic challenges of cyberspace and cybersecurity.

35. The CCA is enabling legislation, which is a category of legislation that rightly excites wariness in democratic societies. Albeit, the legislative programme supporting the White House (2011) International Strategy for Cyberspace, op cit, is not enabling legislation, its claims for protective jurisdiction in the name of the “people” does not necessarily reconcile legalism with decisionism and exceptionalism.

Heterogeneous Worldviews

41. Cyberspace is transnational. This does not mean that borders are erased but nor does it take the long view of history to see borders are porous and mutable, even for people or physical goods; witness the emergence of mass migration or the traffic in drugs. So much more in things
Cyber. The categories national and international remain; but to assume most people’s lives are conducted within a nation untouched by the outside and that only the elite few need trouble themselves with relations beyond their borders is untenable: witness the effect of electronic communications in the social upheavals in the Middle East and North Africa. With networks, events tend to do far more than just spill-over the closest boundary. Interactions through networks reach into each of our lives opening up our capacity to affect powerful forces and be affected by them across many boundaries; witness the effect of the social upheavals referred to above on surging oil prices, in turn complicating a fragile recovery from the Great Recession. In such a networked world truly no man, woman or country is an island to themselves.

42. And so it is with economic and financial affairs. Capital flows have had a lead role in opening up transnational connectivity. The integration of financial systems under the banner of globalisation owes much to the emergence of cyberspace. This globalisation has not produced uniform political-economies based on tidy territories occupied by one people, paying tax and managing their debts to provide the services they need for themselves. Nor have the different ethnicities that make up most nations stayed static. Networks enable people to travel, migrate, mix, settle and move on. Many peoples now have diasporas abroad. These form globally-linked, local clusters. They are not just imagined communities; they act and those actions can be amplified by networks.

43. Similarly with social consciousness. For some people, ethnic and territorial affiliations are but one aspect of their characters. Employment with a Trans-National Corporation (TNC) or engagement with a cause through Non-Governmental Organisations (NGO) may define what moves them more. We do not inhabit a homogenous global space. In cyberspace our lives are conducted through a kaleidoscope of global and local relations, which coalesce and dissipate as diverse glocal38. Great Powers continue to rise and fall but globalisation produces many worldviews,
challenging and contesting what constitutes competent authority. It is not self-evident that sovereign bodies can monopolise claims to be competent authorities. If these involve core competencies for government, sovereign bodies will need to retain the competitive edge, offering citizens an indispensible service they value, and which justifiably retains their confidence. Such a competitive ethos extends to attracting non-citizens and businesses to the trusted networks governments – like the UK – nurture more or less directly.

Cybersecurity Puzzle

44. The multiplicity of the challenges we face could be argued to centre in the domains of Information and Communications and are affected by economic, political, physical and social-human dimensions. Indeed, the US Centre for Strategic and International Studies (CSIS) recent paper – ‘Cybersecurity Two Years Later’ – still refers to the overriding problem of security as being intrinsically complex involving national security, commercial interests and privacy concerns.

45. Schematically, the cybersecurity puzzle can be reduced to a Rubik’s Cube. The puzzle appears solved (Diagram 2, below) but this is an illusion. The protective security principles of information assurance are on one face (grey). This surface highlights how risks are mitigated by considering the confidentiality, integrity (including authentication and non-repudiation) and availability of data throughout systems (CIA). However, in the case of Industrial Control Systems (ICS), although subject to many of the same concerns as other IT systems, they traditionally put availability before integrity and confidentiality (AIC). Internet security was not a concern for ICS because it was not directly or obviously linked to the global web. However, the benefits of connectivity will now drive them towards being more directly and inextricably connected.
Diagram 2
The cybersecurity puzzle
(adapted from Paddy Francis, Cassidian Systems)
46. On the red face of the cybersecurity Rubik’s Cube, we see the entities that collect data, process information, communicate and store knowledge. This too often feeds the assumption that more Data inexorably leads to more Information, Communication and hence Knowledge. The ease with which data deluge turns into expensive data cemeteries, testifies to the dangers of the DICK trap\(^{40}\). Too few systems integrators, let alone users, appreciate the minimalism that Shannon’s definition of information continues to offer. From the perspective of any particular user (not just the most expert), “unexpected change”\(^{41}\) provides a definition of information that cuts down on needless fog and friction in systems. This is not to say the benefits of avoiding the DICK trap are evident to even – or particularly – the most sophisticated of users or developers.

47. Perhaps the pros and cons of Facebook or other social networks open such issues up for debate. Employers do find useful background that can reduce the risks of recruitment. Conversely, individuals may compromise themselves or their company with rash or easily misconstrued disclosures made in an instant or over protracted periods of time. Our credibility and character is presented through these complex flows of data.

48. Finally, the composability of capabilities, systems and architectures is neatly arranged on the blue square.

49. Each surface of the cybersecurity puzzle is deceptively simple and solutions to the puzzle illusory. There are many players of the puzzle with differing worldviews. The priorities they place on each square, let alone surface, will differ. Trust is more vital than ever but difficult to maintain and all too easily lost. For example, differences of perception may arise and/or develop between and within governments and enterprises. There is almost a limitless capacity for them to see things quite differently. Both can claim to be risk-aware and able to safely operate in compromised environments but will act in

---


different ways, which will not complement one another by default. And this is merely one set of players – there are – of course – far more players of the cybersecurity puzzle.

50. Their worldviews will colour their perspectives and often jar with one another, to the extent that players may suffer different forms of colour blindness – with all the complexities of the various views on how they see what the resolution to the problem might be. They differentiate some squares but not others and can match squares from different faces. Partial solutions can look fine from different worldviews.

51. The starkest contrived solutions come when it is presumed that law trumps politics or vice versa, obscuring the salience of cyberspace’s transnational character. This overriding characteristic creates complex interactions between the jurisdictions of sovereign bodies that breed uncertainty, friction and potential flashpoints. Little wonder legal frames of reference tend not only to polarise between war and peace but then skew considerations towards conflict and war in what seems the bulk of commentaries. The question of competent authorities then reveals more about incompetence of state and non-state actors in such a challenging dynamic environment. The anticipation of events and crises does not necessarily urge caution. For some, the profits to be made from sensational commentary are the upside of an unsolvable cybersecurity puzzle.

Competent Authorities and Atomisation

52. This is the context in which competent authorities now exist. As mentioned above, “a Competent Authority is any person or organisation that has the legally delegated or invested authority, capacity, or power to perform a designated function”\(^{42}\). While local cybersecurity does matter, the very nature of cyberspace means that

---

the global will intrude. No single nation can secure it and any strategy centred on domestic action alone will be inadequate to address the global challenges. Indeed, unless cybersecurity permits entities to interact they are soon rendered non-viable. Nevertheless, the local protective security practices of firms and citizens will encounter a scale of security with a qualitative difference—sovereign bodies. Their constitution and view of national security will tempt exceptional claims. The presumption that global governance supersedes the powers of sovereign bodies is easily falsified.

53. Conversely, cyberspace does not give sovereign bodies an easy ride as competent authorities. Through much of human history, it might be assumed that only sovereign bodies were competent authorities. The rational Enlightenment, reinforced by Positive Jurisprudence and the complications it adds over time, seems only to embed the assumption that competent authority flows solely from the sovereign body rather than emerging from the state of nature. It is an assumption that can still be read into the definition of competent authority offered above, albeit the phrase “or power to perform a designated function” opens the issue of competent authority to challenge from sources other than sovereignty. Indeed “power to perform” in an environment prone to disruptive innovations may well precede the “designation” of a competency by anyone let alone a sovereign body saddled with bureaucratic inertia. Cyberspace does not preclude sovereign bodies from being competent authorities but such a dynamic environment will soon make a mockery of any pretence of monopolising such a claim. Fitness as a competent authority is now a highly competitive business. Retrospective norms may only produce evolutionary-drag, which tempts exceptionalism. Particularly when acting in the name of the people, it is worth remembering the dark side of democracy that can too easily entail.

54. The state of nature to which cyberspace returns, is not the preserve of sovereign entities alone. Individuals may—
Cyber Doctrine

– view themselves to be competent authorities in their own right and take a worldview that conflicts with orthodox practices of power. For example, Dan Kaminsky’s actions in 2008 are exemplary; he not only discovered a massive risk in the internet but with the utmost secrecy assembled the volunteers to fix it. He has earned the accolade of being one of the seven keyholders of the internet, trusted as a competent authority to act wisely in the event of an Internet meltdown. Conversely, Chinese and Russian cyber-militias could be under competent authorities. Yet such non-state or para-state bodies often learn their power invests its own authority and undeniably begin to advance their own business interests. The maritime history of privateers as state proxies evidences how readily such bodies blur into transnational criminal organisations. These can thrive in cyberspace as the Russian Business Network (RBN) demonstrates.

55. Transnational Corporations (TNCs) well understand that laws cannot be harmonised across every form of jurisdiction (territorial, citizens, protective, passive and universal) or type of law (public, criminal, civil, corporate etc). Nonetheless, TNCs depend on networks operating in a variety of circumstances. They know the cost of incoherence and unreliability. Some jurisdictions operate with patchy to non-existent cyber-laws. Others with burgeoning cyber-laws which are no less prone to being outdated. This is deeply troubling. Particularly so when issues of sovereignty and partisan politics lurk menacingly over the question of whether cyber-laws are already too arcane or yet to be established. Diagram 3 (right) summarises the intractable complexities that ensue.

56. Competent authorities in cyberspace – such as they are – are atomised or just absent. This can be seen as the inevitable outcome of legal or regulatory or governance specialisation, stripped of politics and history. For some, the resulting divergence of sovereignty and legality is dysfunctional and the misconception of presumed competencies that can ensue is at the heart of violence. It is little


Chapter One
Competent Authorities

Diagram 3
Cyberspace sovereign body array

<table>
<thead>
<tr>
<th>Types of Jurisdiction</th>
<th>Types of Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>War</td>
<td>International</td>
</tr>
<tr>
<td>Peace</td>
<td>Public</td>
</tr>
<tr>
<td></td>
<td>Criminal</td>
</tr>
<tr>
<td></td>
<td>Corporate</td>
</tr>
<tr>
<td></td>
<td>Civil</td>
</tr>
<tr>
<td>Territorial</td>
<td></td>
</tr>
<tr>
<td>Citizen</td>
<td></td>
</tr>
<tr>
<td>Passive</td>
<td></td>
</tr>
<tr>
<td>Protective</td>
<td></td>
</tr>
<tr>
<td>Universal</td>
<td></td>
</tr>
</tbody>
</table>

Cyberspace populated by a 5x5 array for nearly 200 Sovereign Bodies
wonder that commentators are so often drawn to discussing cybersecurity in terms of the International Humanitarian Laws of Armed Conflict (IHL) rather than peacetime bodies of law at home or abroad. Beyond sovereign jurisdictions, relevant peacetime bodies of international law exist. The International Telecommunications Union (ITU) addresses the technical infrastructure in which data is stored and flows. The World Trade Organisation (WTO) and World Intellectual Property Organisation (WIPO) are the obvious focuses as cybersecurity concerns move on to the value of content and the contribution of Intellectual Property to competitiveness. None of which seems to prevent the atomisation and friction among would-be competent authorities. The combinatorial array (Diagram 3) gives a sense of the potential for friction.

57. Clarity about the boundary conditions between peace and war is hard to achieve and perhaps getting harder as the nature of evolving forces elides tidy categorisation. It is not as easy to distinguish armed from other forces\(^49\) that can nonetheless be asymmetric and decisive. Albeit, data on conflicts – their intensity and duration – points to their declining in number and lethality\(^50\), it is hard to imagine that downward trend being extrapolated either to zero or even just (significantly) downwards. Meantime, the effect of global and 24-hour media coverage of conflicts worldwide makes the current declining trend in conflicts counter-intuitive, too. The challenges ahead are daunting. Whatever the level of conflict or the nature of forces involved, the “glocalisation” referred to above will not permit the insulation of conflict from those parts of the world otherwise enjoying their own continuing peace. Peace and war will continue simultaneously. And one will intrude upon the other. Contriving neat separations between these is already difficult.

58. Cyberspace will make it more so. For example, it is easy to understand the perception that supplying tangible goods (like ammunition) potentially compromises the neutrality of a third

---

49. See, for example, Schmitt, MN (1999) Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 37, pp. 885 – 939. Albeit the ground covered by these thorough “thoughts” are worth recalling, more than a decade later the presumption that normative jurisprudence provides a pragmatic way forward is doubtful.

party in the eyes of one or other belligerent party. Arguably, the targeting data for any ammunition is even more important. Use of the internet will inevitably compromise the neutrality of many parties – wittingly and unwittingly. There is a contrivance to push tame solutions for the boundary conditions between war and peace, which will be found wanting when least helpful.

59. There are several fundamental questions about competent authorities in the event of cyber war or conflict using forces that may defy easy categorisation. Critics fulminating about warmongers stoking such debate miss the point. The eminent jurist Martti Koskenniemi’s\(^{51}\) assessment of legal fragmentation\(^{52}\) needs careful consideration, not blind faith in Kant’s “pious wish” for “perpetual peace”\(^{53}\) as a deontological duty, whilst waiting for the ensuing cynical plea to “Give War a Chance”\(^{54}\) in cyberspace. Cyber Doctrine has to be more pragmatic and forward looking than just awaiting retrospective norms to emerge after the fact.

**In Practice**

60. Legality is ultimately tenuous unless grounded in practice. In these terms, it is indeed evident that legal institutions have proliferated since the end of the Cold War. The functions of these bodies often overlap and boundaries between them are ambiguous. (Some go so far as to allege that fragmentation is the intended rather than mistaken design of these bodies because it suits the Great Powers\(^{55}\)). The narrow functionality of any one institution disables less powerful sovereign bodies from coalition building. The transaction costs for bringing coherence to fragmented legal bodies are too high. And these inadequacies make it easy for sovereign bodies to blame legal ones as events unfold. The frustration with incoherence and ambiguity among legal bodies may well be more of a concern for sovereign bodies than legal scholars realise.
61. Fixating on the IHL is not helpful. As already mentioned, one peacetime body of law that could complement study of the evolving IHL is the Constitution and Convention of the International Telecommunication Union (ITU). Indeed, it is the ITU – along with the United Nations Office on Drugs and Crime (UNODC) – that has been proposed as the body to address cybersecurity and cybercrime. The WTO will in due course be another as the issue of content comes more to the fore. Building on the draft Code of Crimes against Peace and Security of Mankind (1996), a road map to the ITU’s 2010 quadrennial plenipotentiary conference was plotted. At the 2010 World Economic Forum (WEF), the Secretary General of the ITU could not have stated the stakes for a cyber accord more clearly given his sense of the prospects for interstate cyber conflict: “the framework would look like a peace treaty before a war.” A peacetime body of law reaching into the province of the IHL is not necessarily a bad thing.

62. The ITU’s quadrennial plenipotentiary conference convened in Guadalajara, Mexico for three weeks in October 2010. Cybersecurity was high on the agenda. The High Level Expert Group (HLEG) that prepared the ground for the conference’s consideration of cybersecurity had already recognised that regional, let alone national, approaches to cybersecurity were inadequate. Furthermore it was noted that the Council of Europe’s Cyber-Crimes Convention (2001, updated and revised 2008) failed to keep pace with change. This no doubt reflected Estonian frustration with the breakdown of law enforcement cooperation in their attempts to investigate the 2007 attacks perpetrated against them. If nothing else, Russia brought home to Europe that legality and sovereignty would continue to clash regardless of a detailed – if already dated – convention. Assuming that normative jurisprudence is a given is rash. Western powers would be wise to pay more heed to the sources of jurisprudence.


57. En route the ITU launched the Global Crime Agenda (GCA) in May 2007 and in order to assist the ITU in developing strategic proposals, a global High-Level Experts Group (HLEG) was established in October 2007. This 100 strong group made detailed recommendations in 2008.


59. Also known as the Budapest Convention it enjoys continued support from the White House (2011) International Strategy for Cyberspace, op cit, as had the HLEG previously.

among rising and other longstanding powers. The ITU conference did not resolve matters.

63. The final acts of the Guadalajara conference expose the cybersecurity puzzle as unsolved. Resolution 181 of the plenipotentiary conference had the option of writing cybersecurity into Article 1 of the ITU Constitution and an appropriate clause of the Convention, reflecting the fundamental importance of cyberspace. The alternative option for Resolution 181 was to adopt the resolution by acknowledging the importance of the technical definitions which appear as a footnote\(^\text{61}\) to the final acts. Taking the footnote option reinforced Resolution 130, which emphasised that the ITU is to focus on its core mandate. This excludes “areas related to Member States' application of legal or policy principles related to national defence, national security, content and cybercrime, which are within their sovereign rights”\(^\text{62}\). Peacetime international law aspiring to address the transnational asymmetric forces of cyberspace was firmly put in its place.

64. This highlights the question and the quandary. The practice of vacillating between national sovereignty and international legality is doing more to reveal incompetent authorities. The blame for fragmentation can no doubt be shared. This will not necessarily promote the required learning. Competent authorities will have to come to terms with the world of transnational networks\(^\text{63}\). The nature of these networks and the forces that can act through them is the real challenge.

Where Are TWAIL?

65. Great Powers cannot monopolise the asymmetric forces cyberspace channels. The cost, and the technical and institutional barriers that hitherto excluded smaller powers

---

61. International Telecommunications Union (ITU) (2011) “Final Acts of the Plenipotentiary Conference”, Guadalajara, 2010 available at http://www.itu.int/plenipotentiary/2010/index.html accessed on 28th Feb '11. The footnote p. 428 cites Recommendation ITU-T X.1205 stating that: "Cybersecurity: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality,"


(state and non-state) from the use of decisive or strategic forces, are eroding. This does not catalyse a free for all; the uptake of innovation can be a struggle for rising as well as incumbent powers. Competent authority is no one’s divine right and may be in anyone’s gift. Again, it is important not to assume asymmetric forces are synonymous with the armed forces of a sovereign state or “armed attack” as defined in the UN Charter (Article 51). This re-opens debates about what constitutes force. It does so on terms that are in greater accord with the lines of argument the Third World and Non-Aligned Movement tried to advance during the Cold War. Then the Great Powers could narrow the definition of force to exclude hard power dimensions, such as, economics and geostationary orbits for satellites. From now onwards, such presumptions may be counterproductive.

66. Third World Approaches to International Law (TWAIL) is an umbrella term for a diversity of legal schools. These schools (their different jurisprudence and methods) share an overall concern about the interaction between international law and formerly colonised peoples. This has in large measure been defined by the uneven or unjust power dynamic between the First and Third World. TWAIL scholars provide fresh perspectives on the rule of law. They draw similar conclusions to Koskenniemi on the dangers of doctrinaire approaches and will be extremely wary of managerialism. Great Power attempts to place cyberspace within an arms control framework may well be viewed with alarm.

67. TWAIL perspectives on cyberspace could well endorse an evolving doctrine rather than a treaty. TWAIL scholars are as suspicious of legal fragmentation across incoherent international bodies as they are about (what they perceive as) disingenuous treaties upheld only when convenient

64. The Bogata Declaration (1976) of equatorial nations tried to exert sovereignty over geostationary orbits (35,786.56km) for equatorial countries but has so far come to nothing. See, for example, Gorbiel, A (1978) “The Legal Status of Geostationary Orbit: Some Remarks”, Journal of Space Law, Vol. 6, No. 2, pp. 171 – 177.

for the powerful\textsuperscript{66}. In a multipolar world, TWAIL scholars can provide invaluable insights on how non-aligned states will perceive international treaty manoeuvres. Cyberspace provides an opportunity for multilateral coherence to emerge from doctrine rather than treaties that engender friction in a multipolar world.

\textbf{Asymmetric Forces In Networks}

\textsuperscript{68}. Setting aside the states of exception that could define cybersecurity misses what is most salient about cyberspace. This does not tip the issues at stake towards consideration under either the banner of sovereignty and conflict through exceptionalism or legality through peacetime norms with limited reach or no force of law when it matters in practice. The test of a competent authority will be its resilience to crises (thwarting exceptionalism and decisionism); and crises abound in networks. Here, crises are defined, as in the Shorter Oxford English Dictionary, as “decisive moments, turning points for better or worse”. ISRS defines resilience as:

\begin{quote}
\textit{“...the enduring power of a body or bodies for transformation, renewal and recovery with the flux of interactions and flow of events”}.\textsuperscript{67}
\end{quote}

\textsuperscript{69}. Resilience to crises is the product of pragmatism. It deals with networks as they evolve\textsuperscript{68}. Evolutionary perspectives offer neither nostalgia for an idyllic past in which norms or values ruled nor false precision too readily extracted from what is easy to count. Both approaches are static and renounce time; this is not only nonsense in evolutionary terms but bad economics too\textsuperscript{69}. Even as the healthiness of eco-systems becomes a consistent characterisation of cyber-resilience, evidence that the
transformative sense of the concept is becoming manifest lags somewhat. Having invoked ecosystems the default into standardisation, automation and speed\textsuperscript{70} perhaps evidence how hard it is to overcome narrow rationalist habits. Evolutionary thinking about resilience to crises is fit for purpose\textsuperscript{71} but not necessarily easy as major scholarly efforts evidence\textsuperscript{72}.

70. Nevertheless, evolutionary forces cannot be ignored in either the short or long term as cyberspace makes plain. The ITU’s deliberations in Guadalajara acknowledged that mention of cybersecurity in Article 1 of the constitution could be troubled by constant revisions. And, as already mentioned, the HLEG ahead of the conference also pointed out that Europe’s regional (Budapest) convention is failing to keep up with technological developments. The institutional urge to codify and instil norms seems only to add to backlogs and learning bottlenecks.

71. On orthodox terms, how to make these problems tractable is perhaps a moot point. The nature of networks throws up qualitatively different challenges. Understanding the difference between transnational and international or national is just the beginning. Advances in mathematics and modelling are revealing uncertainties in evolving networks that defy conventional approaches to risk and decision support\textsuperscript{73}. This is not to say that established approaches are obsolete. They have some continuing utility but greater care is required to prevent them being used in error. Meanwhile, competent authorities need to learn why a variety of mathematics and models matter and how to use the tools developed from these insights.

72. To reduce asymmetric forces in networks to a parable of David and Goliath can be very misleading. Size is not the issue, particularly not as a one-shot deal. Networks do permit


\textsuperscript{71} Some have gone so far as to seek a multi-disciplinary approach to resilience based on a more integrated approach to risk. This includes risk taking not just risk mitigation and protective measures. See, for example, Council on Competitiveness (2007) Resilient Enterprise Paradigm, report prepared for US Department of Commerce, Technology Administration. However, in seeking reconcile competitiveness with security, resilience is poorly defined, albeit eco-systems and complexity are again mentioned. The simple point that competitiveness and resilience are synonymous because transformation is the lead characteristic is missed.


\textsuperscript{73} See, for example, Dorogovtsev, SN & Goltsev, AV (2008) Critical Phenomena in Complex Networks, Review of Modern Physics, Vol 80, pp. 1275 – 1335.
the proliferation of knowledge and reduce the barriers for acquiring and using capabilities that were once the preserve of Great Powers. As an example of continuity and change, Estonia is planning to conscript cyber experts, who can be mobilised in times of national emergency\textsuperscript{74}. This approach acknowledges that competencies necessary to exert sovereignty are not necessarily produced or sustained under the authority of the State. Nonetheless, dynamic networks rich in content enable symmetry-breaking events to become everyday. This is both good and bad.

73. Asymmetric forces permit Small World Clusters, for example, bringing together the worlds best health labs to address the challenge of SARS in weeks not years. The combination of video teleconferencing, robotics, distributed databases etc all enable learning to happen at a hitherto unprecedented pace\textsuperscript{75}. However, Small World Clusters also add to the nightmare of biological weapons proliferation\textsuperscript{76}. To assume that cybersecurity is synonymous with the Internet Protocol is flawed. Content matters, not just infrastructure; and content will impact all environments, not just cyberspace.

74. Asymmetric forces can also permit runaway effects that discover or use Scale-Free Networks. This may amplify dangers, bringing on catastrophic contagion and irrecoverable defeat in war; or it may deliver greater entrepreneurial success through the economics of increasing returns\textsuperscript{77}. The former is not scaremongering or limited to the prospect of a solar flare. Whilst it is right to say that the first Internet Protocol was designed to maintain mission critical services, such design intent does not vouchsafe the Protocol’s evolution since. Patches and connections to different bodies of code build up complicated layers that introduce wrinkles and holes. These

---


76. See, for example, Roberts, B (Ed) (2000) Hype or Reality? The “New Terrorism” and Mass Casualty Attacks, The Chemical and Biological Arms Control Institute: Arlington, VA.

may lie concealed never to be discovered or are revealed, for example, by the simulation methods developed at Oulu University (Finland)\textsuperscript{78}. Major developments in what maths and modelling are revealing – not least Scale-Free Networks for better or worse – is yet to underpin the acts of competent authorities in cyberspace\textsuperscript{79}.

75. The recent discussion between Andrew Haldane (Bank of England Executive Director for Financial Stability) and Lord May (former Government Chief Scientific Advisor), of systemic risk in banking systems, is more promising\textsuperscript{80}. It neatly underscores the point that asymmetric forces in networks can be good and bad but are always evolving. Conversely, the Organisation for Economic Co-operation and Development’s (OECD) recent systemic cybersecurity risk report comes to the evolutionary point through resilience too late\textsuperscript{81}. The confidence to explore and exploit asymmetric forces in networks as evolutionary systems is vital. Using the wrong methods and tools for the challenges of cyberspace is incompetent. Tradition, habit or institutional strictures are no excuses for missing the turning points for better and worse. The stakes are too high both in terms of gains and losses. This is why a framework for learning resilience is vital.

Managerialism or Doctrine

76. The evidence for the approach to cybersecurity being reactive, fragmentary and overtaken by events is overwhelming. The more specific the details, the more obvious that conclusion becomes (see Diagram 4 below). The UK as but one sovereign body illustrates how patchy competent authorities are.

78. See, the work of Finland’s Oulu University Secure Programming Group at https://www.ee.oulu.fi/research/ouspg/ accessed 20th Apr ’11.
79. See, for example, Dorogovtsev, SN and Mendes JF (2003) Evolution of Networks: From Biological nets to the Internet and WWW, Oxford University Press: Oxford.
CHAPTER ONE  Competent Authorities

77. In October 2010, the UK Government created the National Security Council (NSC), and published the NSS, together with the Strategic Defence and Security Review (SDSR). The NSC was a means of ensuring collective, co-ordinated and informed decision-making. It further alluded that, for the first time, lead Ministers would be accountable to this body. There are several national bodies, including at the time of writing: Office of Cyber Security Information Assurance (OCSIA), Centre for Protection of the National Infrastructure (CPNI), Get Safe Online Campaign (GSOC), Cyber Security Operational Centre (CSOC) and the Defence Cyber Operations Group (DCOG). Linked are a great number of key departments, emergency services, GCHQ, counter terrorism bodies, and UK Trade & Investment (UKTI) etc, together with a larger number of associated agencies and advisory boards.

78. These organisations are highlighted in Diagram 4 as the outer structure which borders the various cyber threats that translate at a national level. At the centre of the cloud is the citizen, dependent upon critical infrastructures and network services from public, private and voluntary sectors. As in the US, there appears to be a distinct lack of integration, and chain of command and actions seemed to have moved to individual agencies.

79. One of the US recommendations was for clear authority to mandate better security in the critical infrastructures and develop new ways to work with the private sector. It is perhaps not surprising how our evolved society has followed the true tradition of liberalism, a combination of individual consumer choice and the protection of the State, resulting in the individual choosing not to do anything in the misconception that the State will. For example, the surge in identity theft and fraud and in particular its impact, could be seen as the result of the

82. Green, A (2010) Cyber-Defence: Threats and Opportunities to UK Business, A|D|S: London. This report also provides a good overview of the existing cyber security market.

83. CSIS (2011) op cit.
mis-match between individual consumer choice and the protecting State, in which privacy gets caught up a ‘free for all’ in data mismanagement.

80. There are now powerful antibodies to cybersecurity initiatives that appear to infringe on consumer privacy and civil liberties. Recent developments with super-injunctions in the UK underscore how powerful the issues and interests at stake are. The importance of these issues will increase as there is a move to active defence and Cloud computing. The Cloud’s economies of scale and flexibility bring further and mixed concerns for security and regulations. The connectivity of legacy data stores and information systems associated with diverse bodies – not just the Cloud vendor – will make for major management challenges. The pros and cons need to be carefully considered; taking public confidence for granted would be unwise.

81. In the aftermath of the Great Recession, the UK government is determined to drive down costs and drive up efficiency in the public sector. The scope for rationalising the many systems that identify its employees and contractors, and deliver public services to the UK’s citizens, residents and visitors offers the prospect of significant savings. A coherent public policy framework for trusted collaborative identity governance is fundamental. Allowing the citizen access to a safer internet experience and to entitlements, including being able to inspect their own data and eliminate identity fraud are outcomes not to be compromised. These are demanding requirements; Cloud computing could offer ways to achieve them simultaneously.

82. Inevitably public bodies will have to consider the consequences of surrendering a certain amount of control to the Cloud provider. Similar issues will arise for corporate and third sectors. Private and public sectors seem to be leaving gaps in security and resilience, not just individual citizens. See, for example, House of Lords, European Union Committee (2010) “Protecting Europe Against Large-Scale Cyber-Attacks” op cit.

Diagram 4
Competent authorities in clouds of fog and friction

- Finance
- OGD
- Energy
- Cabinet Office
- Insider
- Health
- CT
- NSC
- Manufacturers
- Citizen
- Emergency services
- Organised crime
- SIS
- Communication
- OCS
- Data protection
- GCHQ
- Transport
- Terrorists
- CPNI
- MoD
- Other

Client state?
sector bodies as data comes together on any particular Cloud. The liberation of “big data” will have major consequences for every citizen. Combining sensors harvesting massive streams of data (such as, smart phones not only tracking geographic position but also who the device holder is in proximity to and how they are interacting) with business analytics in real time, may present marketeers with a dream but could prove a nightmare even to the least privacy conscious. Freeing “big data” is a major step forward into the post-bureaucratic age but opening up government’s data cemeteries could prove a horrifying prelude to “data determinacy”. Dazzling statistical precision can be misused to extrapolate bogus certainties about people’s lives that foreclose chances for change.

83. Conversely, the uncertainties inherent to the uptake of innovation could also make Cloud-based resilience achievable on healthier terms. The lessons from early adopters of Cloud computing – largely in the private sector – need to be learned. The benefits realised earn most from going with the grain of users’ skills and aspirations. Doctrines can support and enhance education and experimentation to propel such innovation on the healthiest terms. From private citizens to larger organisations, the development of doctrine can enhance learning and improve the chances of successful innovations’ uptake. This extends to the empowerment of critical infrastructure providers and broadening and deepening their understanding of dependable software and reliable systems. Doctrine enables pragmatism on the largest and smallest scale for actors in cyberspace.

84. The sense of pragmatism on cybersecurity given voice by the UK’s Foreign Secretary, William Hague, is to be welcomed. His use of principles that are open to debate accords with the use of doctrine jurist and educators advocate. Such

86. See, for example, the app by a Silicon Valley start-up called Color, reported in the Financial Times, p. 11, 6th May 2011 under the headline “A binary goldmine”.

87. Foreign Secretary, William Hague’s Speech at the Munich Security Conference, op cit.
principles readily embrace security and competitiveness where the re-use of complicated and fragmented laws as rules may veer protectionist. Resilience stems more from the former than the latter. Cyberspace can doubtless learn from the evolution of the medieval Law of Merchants and the more recent UN Convention on the Law of the Sea (UNCLOS). Both involve activities in environments outwith or cutting across many sovereign jurisdictions, where the state of nature has been little tamed. However, acknowledging the reality of an evolving environment offers the prospect of seeking more organic approaches to change. This is crucial to turning the discord between sovereignty and legality into something more proactive, integrative and evolutionary. This does not necessarily pit politicians and security services against lawyers and civil society. Incompetent authorities – servants of the state or global citizens – do us all a disservice and in cyberspace the stakes are only getting higher by the day.

85. To be fair, this is recognised within the legal fraternity itself. Koskenniemi does not spare his own community of jurists from criticism. The fragmentation of bodies of law and institutions has been compounded by their succumbing to “managerialism”. This he characterises as apolitical, ahistorical and asocial. The sterility of legal managerialism ultimately serves no one. Again to be fair to the legal profession, the learning myopia Koskenniemi and Carty diagnose are common traits found outside the ranks of their own profession. They impede organisational transformation and sap resilience. It is somewhat reassuring that legal scholars arrive at conclusions similar to strategists and practitioners dealing with complex challenges in the military and the UN. They agree not only on the diagnosis but on the way forward; doctrine is needed to overcome dogma. This admits politics is

88. Tikk, E (2011) op cit, perhaps overplays the upholding of existing law boiled down to ten rules, which will just as simply be ignored by those for whom the rule of law has less mean than raw power.


Cyber Doctrine

endemic, practices are the product of time, and that elites cannot exclude wider society.

86. This is why cyber doctrine offers a framework for learning resilience. Throughout we acknowledge that the development of doctrine is a multilateral process in which a plurality of doctrines will co-evolve. Doctrine has strong strategic and military associations. These can be built on but the overriding sense in which we are using doctrine combines legal principles (rather than codified statute) and educative material to spur the uptake of innovation not just training in well codified practice. Rather than undermining coherence, diversity on all these terms acknowledges reality and can open doctrine development to more productive learning. The question now is “how?”. The next two sections are grounded more in the evolving material base and the practices thereby enabled.
95. For details summarising the distinction between exploration and exploitation and the harm done to enterprises by the latter squeezing out the former, see, March, J. G. (2006). "Rationality, foolishness, and adaptive intelligence." Strategic Management Journal 27(3): 201-214. Also see, Chakravarthy, B & Lorange, P (2010) Profit or Growth? Why you don’t have to choose, IMD: Switzerland for a more recent variation on the theme in which exploitation is synonymous with profitability and exploration with growth.


97. Incremental innovation does not have to be at odds with disruptive or transformational innovation. The former can lead gracefully to the latter. However, incremental approaches can create a false sense of security to vested interests. Ignoring disruptive innovation is a regular symptom of firms on the brink of demise as new entrants to the market embrace innovation on a scale incumbents tend to resist. See, for example, Ernst and Young (2011) Competing for Growth, available at http://www.ey.com/GL/en/Issues/Business-environment/Competing-for-growth--how-business-is-growing-beyond-boundaries accessed 19th May ’11

Networks-in-Being: Asymmetric Credibility

87. We do not suggest that doctrine is a universal panacea. It can provide a framework for learning, which brings coherence to many strands of otherwise discordant activities. These range from the strategic to the tactical, encompassing the organisation of capabilities through entire life cycles. Without undermining or obscuring the value of drills, cyberspace and cybersecurity presents doctrine with fresh challenges.

88. Hitherto, doctrine has had a sharp focus on principles for the present and near future, leaving concepts to consider more protracted generational change. This has some accord with the differentiation in the business literature between exploitation of capabilities and the exploration\textsuperscript{95} of dynamic or meta-capabilities\textsuperscript{96}. Exploitation is at ease with weak innovation\textsuperscript{97}; exploration much less so. It can trigger innovation on a massive, disruptive scale, particularly for incumbent organisations’ capabilities. Cyberspace is an environment in which any sharp demarcations between these characteristics will work less well.
Synchronising generations of capabilities with very different life-spans is becoming a persistent challenge. The framework for learning that Cyber Doctrine needs to develop, must enable concepts and doctrines to mesh better as an evolving mix on various interacting timescales. The variety of interacting timescales underscores the need to rework the distinction between capabilities and meta-capabilities. Otherwise, the ever more intensive and extensive uptake of innovation will only spur unhealthy competition and co-operative cartels.

Moreover, during any given or anticipated life-cycle, the use-value of a capability is seldom smooth. Instead, volatility is growing. Entering service, the costly teething problems of a capability and its integration dice with early termination, perhaps on the cusp of beginning to pay-off. In-service capabilities fluctuate from obsolescence to invaluable re-uses as they are recombined in unanticipated ways. The evolving assemblages that swarm through cyberspace challenge existing distinctions between the exploitation of capabilities and the exploration of meta-capabilities. Concepts and doctrine need to mesh better.

Evolutionary-drive and drag will create turbulent currents. Rather than seeing these challenges as insurmountable there is much to be gained from learning to steer through them. As a man-made environment it is not only possible to launch better designed vessels into cyberspace but also shape how some of the currents flow. Although cyberspace is an open system by nature, this does not mean that closed systems assumptions are always unfit for the environment. Like the sea, cyberspace offers real advantages to the Fleet-in-Being, moving targets that are hard to detect, easy to misperceive and difficult to mimic. Cybersecurity can embrace the concept of Network-in-Being for peaceful and other purposes. For example, they can help make

---


99. An open system is one that continuously interacts with its environment. Whilst the system has a boundary, it is permeable and mutable. Open systems can be viewed from different disciplinary perspectives; they may be thermodynamic, biological, social and / or ecological. In either case energy, information and matter are exchanged between the system and its environment. A closed system does not permit exchanges between the environment and the system. The interdependence of information and energy systems is made clear where energy consumption for Cloud, grid and supercomputing becomes a defining issue for the viability of such systems and services. See, for example, Lefèvre, L & Orgerie, A-C (2010) Designing and evaluating an energy efficient Cloud, Journal of Supercomputing, 51, pp. 352 – 373.

100. The Fleet-in-Being is a naval concept involving a small number of forces able to tie up far larger numbers of forces. This may be by staying safely in port or by manoeuvring in ways that make detection unreliable. See, for example, Virilio, Paul (1986) Speed and Politics: An Essay on Dromology. New York: Semiotext(e) on Nuclear Submarines as fleets-in-being.

content difficult to steal, particularly when conventional protective measures are costly and unreliable.

92. This section and the next will consider how Cyber Doctrine can provide a framework for learning resilience on these terms. Networks-in-Being are an example of how capabilities can be organised across and through time to produce resilience. Measures for meshing concepts and doctrine better will need to focus on composability and tractability:

- **Composability** concerns the pragmatic permutations for integrating capability options across the flow of time.

- **Tractability** concerns gains and losses of power in evolving combinations of capability options running with the flow of time.

93. Composability and tractability are linked not just in terms of the capabilities selected for integration but also the potential options that emerge and remain to be exercised. This avoids misconstruing cyberspace as anything other than an open environment in which capabilities, systems and architectures can evolve as healthy mixtures of open and closed systems adhering to de facto or de jure standards as appropriate. Albeit the first man-made environment, the evidence is thin that cyber strategies are achieving such coherence. The forces of evolutionary-drive and drag in cyberspace create great turbulence through which it is hard to steer. This is particularly so if vacillating between an overweening urge for control on the one hand, and profiteering from weak or no regulation on the other. Repetition of the word “interoperability” can evidence falling into either or both traps. Composability offers a more modest, contingent and realistic goal in an evolving environment.
94. Systemic risks are aggravated by such idiosyncratic confusion. Alarming anecdotes accompanied by lists of counter-measures and numbers loaded with partial precision do not help. These analyses may attempt to rank-order threatening attacks but the selection of protective measures gets no easier. Each new catalogue tends to only add more threats of attack and one or more protective measures to be taken. This adds to the need for interoperability without making it any easier to deliver. The OECD has recently provided another lengthy list, albeit the product of a critical assessment determined not to exaggerate the risks\textsuperscript{102}. It cites “security doctrine” as the first of the four remedies it suggests needs development for reducing systemic cybersecurity risk. In connection with which the word resilience is used repeatedly, too. It is worth examining more closely.

95. The OECD’s path to recognising a need for doctrine goes through four phases. The first is a technical tit-for-tat in which technical problems are matched with technical solutions. Next, audits are used to raise standards. Then invocation of risk management covers the realisation that absolute security is unattainable. Finally, use of the term “information assurance” comes to embrace a wide array of “softer” issues, including people, organisation and business economics. These phases can be associated with the OECD’s uptake of the term resilience. Unfortunately their understanding of the latter seems confined to only the narrow engineering sense – bounce back, rather than move forward through innovative learning from the experience. Just as worryingly, the four phases are consistent: reaction outweighs the proactive; there is little evidence that integration is made easier; and developments continue to be outpaced by events.

96. The OECD report does underscore a few basic points. It restates the now commonplace conclusion or assumption that with the attribution of acts in cyberspace being problematic, deterrence

as a strategy fails\textsuperscript{103}. Events will happen; they cannot be deterred. This is irrespective of events being intentional acts or attacks, or free of any intent. Resilience in the narrow sense of absorbing impacts and shortening recovery times is offered as the fallback by default. Yet the nature of cyberspace makes the notion of bouncing back to the \textit{status quo ante} risible. There is perhaps a hint that the OECD team understand a narrow sense of resilience is inadequate but innovation fuelled by research and education comes only as an afterthought. In fact, innovation born of research and education is how resilience is sown deep and wide for today and the rapidly unfolding futures.

97. Furthermore, resilience as a fallback (because deterrence fails as a strategy) misses the equally important concept of irresilience. Circumventing deterrence as the mainstay of strategy – or strategic stalemate – opens up novel defeat mechanisms or vectors for catastrophic failure. Deterrence remains a tactic and may even be a key manoeuvre in operational art on occasion but is no longer the capstone of strategy it was in the Cold War. In part, OECD’s critical cyberwar refrain only obscures the danger of irresilience. Had they been more precise about differentiating cyber combat from war rather than confusing and conflating them, it would have been helpful. They are right that a decisive blow in battle will seldom mark defeat. However, campaigns are designed to integrate many capabilities and under the banner of the “comprehensive approach”\textsuperscript{104} those are far from limited to combat forces.

98. This is where their acceptance of the “perfect storm” becomes important. A pattern of events (simultaneous and sequential) can discover irresilience, act on it and force catastrophic failure. Such perfect storms need not be confined to the domain of cyberspace itself; as the OECD acknowledges, cyberspace readily connects all environments. This underscores the imperative for deep and broad assessments, which explore the potential for resilience


and irresilience spreading through all environments. In turn, it makes composability and tractability key measures of the capacity for innovation. Innovation is vital whether at war, in the business of healthy competition or indeed healthy co-operation. The OECD signposts for doctrine offer little insight on how appropriate innovation is to be achieved from concepts to capabilities.

99. Idiosyncratic risks – filtered or otherwise – do not necessarily add up to systemic risks. It is the symmetry-breaking or asymmetric risks of events and how they amplify or quell in networks that needs to be addressed. These events and the forces that propel them may be good and bad. There are advantages to be gained both in terms of harnessing asymmetric forces and competing with them. Like several recent reports embracing the concept of resilience in eco-systems, OECD’s tends to view the issue from the wrong end of the telescope. Doctrine and resilience come as insights after a long and difficult journey through systemic risks, looking out to even more distant prospects. Here, we intend to swing the telescope round, bringing what is most salient into closer focus and making the prospect of moving forward more rewarding than daunting.

What are Capabilities?

100. The very networks that make the challenge of cyberspace and cybersecurity manifest also spur innovation,\(^{105}\) vital to the continuous learning of resilience. Two propositions underpin the pragmatism here:

a) first, the composability of capabilities is alert to our bounded rationality\(^{106}\) (inasmuch as cyberspace connects us to arrays of new sensors and immerses us in flows of data but rationality is still limited by time that bounds a decisive moment) and how


that compounds known pathologies of organisational learning\textsuperscript{107}; and

b) second, aspirations\textsuperscript{108} and variety\textsuperscript{109} (too often repressed in the pursuit of efficient exploitation) are nonetheless vital to any organisation’s longevity (and these attributes can pick up on the economics of increasing returns).

101. This is cause for neither optimism nor pessimism. The challenges are just as daunting, albeit with the prospects of desirable outcomes much improved because resilience is not undermined by driving brittle optimisation onwards to catastrophic failure. Rather, to make these propositions viable the definition of capabilities needs to be enhanced in its evolutionary sense:

• \textit{Capabilities can be understood as evolving ecologies of competencies and technology.}

102. This links the definition of capabilities as “routines” that “confer decision options”\textsuperscript{110} with meta-capabilities or “capabilities to acquire capabilities” also known as dynamic capabilities\textsuperscript{111}. It is a move in keeping with open and mass-innovation\textsuperscript{112} making Schumpeter’s creative destructiveness\textsuperscript{113} more not less insistent because change is more continuous than intermittent. Raising aspirations, investing in variety and being poised to exploit the economics of increasing returns are essential characteristics of this process and need positive stimulation; we cannot rely on the residual covert learning that bureaucratic managerialism fails to eradicate\textsuperscript{114} in its quest to squeeze out exploration in favour of exploitation only. Yet it would be rash to assume that times of austerity will catalyse such productivity gains for cybersecurity or for economies or economic systems increasingly reliant upon cyberspace.
103. Doctrine can facilitate good design of capabilities to scale, not least by avoiding security and resilience being left as afterthoughts that then herald hideous costs. It can also support the selection of permutations of capabilities as befits fast-changing circumstances. This is the issue of composability. In the next section the question of how to assemble and compose the appropriate span of capabilities moves on to the gaining or loss of traction, from generation to generation through time.

104. These may seem abstract notions. However, as the UK military is discovering, the consequences of a stream of Urgent Operational Requirements supporting “transformation in contact” (some perhaps peculiar to one operational theatre) does not always easily—or automatically—mesh with the through-life acquisition of systems over generations (the latter of variable life-spans and usage ranges). For better or worse, the budgetary consequences are significant and impact far sooner than hitherto. Tending to the minutes does not always adequately provide for, or accord with providing for, the hours.

105. Less obvious, but more pernicious, is the degrading of capability integration and capacity that ensues from ephemeral “transformation in contact”. Competencies and technologies become mismatched. Learning the wrong lessons from shallow transformations will further undermine prospects for productivity gains. This is not just an issue for defence but for service providers at large. Whilst the spectre of conflict and irresilience cannot be dismissed, Cyber Doctrine is concerned more widely, with how integrating capabilities enhances their use-value not just as cybersecurity services but for economies at large, themselves increasingly dependent on cyberspace for growth. This will be done by focusing on meshing “exploitation and exploration” or “profitability and growth” within and between organisations rather than being waylaid in shallow transformation.


106. Hackers are not new to the experience of exploitation squeezing out exploration, or even to profitability undermining growth. Nor is their environment *a tabula rasa*; cyberspace has a history stretching well back, well beyond William Gibson’s coining the term in 1982. For over half a century, cybernetics has been the banner under which fundamental research and development in computing, information and communication systems has been conducted. During the nineteenth century, the French unified discipline of government was known as *cybernetique*. The concept of an oarsman (kyberion) steering through turbulent waters has been a metaphor of government and leadership contending with uncertainty since the ancient Greeks. Transformation is, and long has been, an enduring and profound issue.

107. The travails of cybernauts, cyborgs or cyberpunks evidence how challenging these uncharted and turbulent waters can be. They echo themes from the philosophy of science debate between Lakatos and Feyerbend, for and against method. The assumption that hackers hinder deeper and more durable transformations needs to be questioned, as do the results of two hacker crackdowns. We can learn from those experiences in the development of doctrine.

**Hacker Crackdown 1: For Or Against Method**

108. The term *hacker* has more than one sense. Before hacking and hackers became synonymous with gaining unauthorised access to systems, the word referred to anyone who cut code. It can be argued that the 1970s and 80s saw the onset of not one “hacker crackdown” but two. The experience of both is relevant to the development of Cyber Doctrine. Developing software always relies on the skills of software and systems engineers in what for many people are abstract and arid codes of logic and management. Hacker and systems skills are easily mismanaged.

---


109. The process of producing code on a large scale is prone to being very wasteful, the individual brilliance of hackers notwithstanding. As systems grew larger and more complicated, hordes of hackers needed to be formed into teams. Cutting code to ready-made designs seemed the obvious way to cut wasted energy. Methods for achieving hacker compliance were developed that built on classic economics of specialisation. From 1983, Structured Systems Analysis Design Methods (SSADM) was mandated for use on UK government projects and programmes. Albeit, not all projects or programmes are about software production, SSADM underpinned the development and implementation of PRojects IN Controlled Environments (PRINCE) in 1989, the use of which now extends to far more than software development. The uptake of these and similar methods have been backed by Governments around the world. This is less an affirmation of how invasive and pervasive software is and more a baleful reflection of how over reliant bureaucratic management can be on the presumption of control. Ready made templates for the production of libraries of code and system components have some undoubted merit. However, dynamic systems are breeding grounds for innovation that defy simplistic or complicated controls. Evolutionary approaches are more natural.

110. There is no denying that the tighter control of costs, quality and delivery deadlines can be productive, but there are limits. Indeed, the very titles of the methods suggest that their developers understood these limitations. “Structured”, “Analysis” in “Controlled Environments” make it pretty clear where waterfall assumptions might work. By 1995 even the software enthusiasts for SSADM had become cautious about just how useful version 4.2 would be. There have been no further versions released. Projects and programmes on many scales continue to demonstrate that whatever patches of control there are in cyberspace, these are at sea in an environment that soon makes nonsense of overweening control. Hackers can and do offer a healthy response to the realities of their environment.


122. Projects or programmes adhere to the waterfall profile when their phases run in a tidy sequential series from requirements capture to design, implementation and in-service maintenance. Beyond the purchasing of kit a whole life approach to acquisition may be summarised as CADMID (Concept, Assessment, Demonstration, Manufacture, In-service and Disposal). Waterfall projects find change difficult; once requirements are captured they struggle to stick to plans with cost overruns and delivery slippage a persistent problem. Evolutionary and Incremental approaches to the acquisition of capabilities can offer ways round the well known problems of waterfall projects.
111. Despite the compliance crackdown, the hacker ethos lived on in small and distributed systems design (including parallelisation of code for supercomputing). As the pace of change intensified, big projects and programmes often became too complicated. Requirements capture took so long that they were out-dated once – or long before – agreed. Unfortunately, that did not prevent projects or programmes going ahead. A clear pattern emerges in projects and programme. Slippages appear inevitable (masked with a few change requirements to rationalise costs and delays). Outputs are all too consistently delivered late – both in terms of the plan but more importantly the real practical need. The requirement fulfilment persists in the paperwork only; reality has long since moved on.

112. Dynamic Systems Design Method (DSDM), for example, enables users and developers to work together more productively. This is not just at small scale. Distributed teamwork enables such methods to be used extensively and with an intensity that goes with the grain of organisational learning. That can include the most challenging of software engineering challenges – the production of an Operating System (OS). Linux was produced on just such terms. It demonstrated that hackers could work as distributed teams and produce open source code that competes with proprietorial code, particularly on reliability. Moreover, Linux has now come to replace Unix as the predominant OS for the parallel and distributed high performance architectures of supercomputing\(^\text{123}\). These hacker virtues are spreading\(^\text{124}\).

113. The annotations that supported the distributed and dispersed production of software – wikis – are now a mainstay of social software. The kinds of organisational learning they promote are proliferating from cutting code to networking and content production. Open source code, systems and architectures enable hackers to compete with conventional methods and the organisations that use them inappropriately. Methods such as DSDM can bring out the good in the hacker ethos for all to

---

123. See, for example, Top 500, Supercomputer site data on Operating Systems use and performance over time available at http://www.top500.org/overtime/list/32/os accessed 30th May ’11.

124. It is worth noting that the Open Source Code community could do a great deal more to make their developing knowledge accessible. The profit motive does seem to encourage proprietal vendors to provide training packages that make their wares accessible to more than the tenacious.
share. These methods are not perfect but they are far less prone to “exploitation squeezing out exploration”.

Hacker Crackdown 2: Infections and Inoculations

114. The more familiar “hacker crackdown” hit the digital underground from the 1970s onwards. Before the convergence of telecommunications and computer processing, those who freeloaded on telephony systems were known as “phreakers”, whilst hackers in the narrow sense gained unauthorised access to computer systems. Towards the end of the 1970s, their activities began attracting attention and were deemed unacceptable. It is disputed whether the combination of cutting code and using it to explore how to access systems is entirely a bad thing. Hackers (and their supporters) like to split themselves into “black hats” and “white hats”. Black hats hack for profit or to do damage. White hats do it for the challenge and often see it as a civic duty to test the reliability of systems.

115. Within the security community, “Penetration Testing” offered a white hat service that was nevertheless frowned upon. The reluctance to test protective measures in the 1990s was surprisingly strong. For some in the security establishment, using offensive techniques to test the efficacy of protective measures was at that time anathema. “Pen” Testing is now routine practice and integrates many techniques, not just software attacks. In particular, social engineering is among the most powerful, if indirect, ways to gain unauthorised access to systems. This recapitulates the importance of the human errors or “cribs” that were vital to Bletchley Park’s hacking of Nazi ciphers during World War Two. Beyond human error it also underscores the continuing importance of human sources in cyberspace.

116. Managerialism will always be tempted to crackdown on hackers. In turn, black hats and those – like Feyerbend before them – that repudiate methods in favour of reckless individualist experiments will
lend managerialist urges legitimacy. However, history teaches us that we should learn from – sometimes especially from – our opponents; hackers have shown themselves capable of developing distributed network communities that embody and thrive on organisational learning. They signpost ways to avoid “exploitation squeezing exploration”. This ethos extends to mash-ups that overcome the restrictive practices that Intellectual Property can inflict, restrictions that stymie rather than protect innovation. The resurging interest in parallel and distributed supercomputing may also herald a refreshing outbreak of competitiveness based on innovation spurred by the deep puzzles hackers relish rather than vendor lock-ins. As Lakatos envisaged, research programmes can explore and exploit evolving methods for tackling evolving puzzles. Cyberspace enhances such empiricist processes but escaping bureaucratic managerialism is neither easy nor inevitable.

**Pragmatic Composability: Escaping Brittle Optimisation**

117. British politicians left and right have been eager to proclaim the onset of the Post-Bureaucratic Age\(^\text{125}\). A new era is dawning in which ease of data collection, assessment and communication will radically reduce the need for bureaucrats or the organisations in which their ethos thrived. Choice and user-driven innovation affirms the dawning of the new era. A shift marked by increasing consumer choice moves on to enabling more people to be “prosumers\(^\text{126}\)”, eager to work with developers to improve existing as well as shape subsequent generations of products and services. Cutting the supply of public services that are hard up against the law of diminishing returns is not enough. The goal is to sustain cuts not postpone their inexorable rise. The upward trend in public spending and taxation is to be driven through an inflexion point, not a temporary plateau. For that to happen, consumption cannot merely be stalled or displaced. Citizens need to become active in propelling innovation, which more often taps into the law of increasing returns. Discerning but passive consumers cannot bring the Post-Bureaucratic Age to life.

---

125. The phrase and its implied criticism are attributed as much to the current UK Prime Minister David Cameron as it is to the former Prime Minister Tony Blair.

118. There are many trends and drivers making the Post-Bureaucratic Age attractive. Poor productivity gains perhaps caps them all\(^\text{127}\), particularly when aggravated by failed IT projects, that are bedevilled by inappropriate use or non-use of methods. Of course, as talk of the Post-Bureaucratic Age and the prospects for open or mass-innovation grows, it is worth remembering that the one-size-fits-all products and services of mass consumerism have delivered what would otherwise have been beyond the reach of many citizens. It is not ingratitude but aspiration that leads to greater expectations today, especially since citizens have a good sense of what productive forces are now capable of. That dynamic itself owes much to cyberspace and its relations with all other environments (maritime, land, air and space).

119. The pattern of change unleashed by these productive forces seems perplexing but can be simplified. The previous pattern of large economies of scale and narrow economies of scope, with only intermittent innovation between long production runs, is no longer the only or prevailing mode of production. Short production runs open to incessant innovation are now prevailing. These changes are most pronounced in and through cyberspace; they affect users/consumers and producers.

120. Changes in productive forces also morph organisational topographies, as longstanding studies of the firm predict\(^\text{128}\). Large hierarchies persist but are far less self-contained. They rely increasingly on networks across their entire enterprise, including “glocal” nets of suppliers, customers and finance. Hierarchies and networks have always been interrelated\(^\text{129}\). For example, during the industrial era the growth of British hierarchical firms depended on maritime trade networks, assured by protection and indemnity clubs ashore in the City, and the presence of the Royal Navy at sea. Prevailing organisational topographies are shaped by the costs of collecting data and constraints on communicating. Where data is expensive to collect and hard to communicate (for example, in the era of press barons and print unions), hierarchical organisations and anti-markets tend to prevail. Where collection of data is cheap and easy to


communicate (for example, with the rise of the Huffington Post), networks or markets prevail. However, that does not mean that a “Post-Bureaucratic Age” affirms the efficient market hypothesis.

121. Orthodox economics can make cyberspace more, not less, prone to irresilience, as the systemic risks that led to the Great Recession make clear. In the aftermath of economic crises the imperative to achieve productivity gains tends to be dominated by efficiency through cuts. Productivity gains through innovation suffer just when needed most. Vigilance in cutting waste is always vital but savings have to go deep enough to create the headroom for growth investments. Streamlining organisations, capabilities and technical systems is an issue of composability. Too often streamlining merely optimises for the interoperability of uniform components stripped of innovative grit: headroom is not created from which to drive innovation by selecting from creative diversity. Evolutionary-drag makes narrow adaptation seem efficient and effective; evolutionary-drive is too often crowded out until too late. Skills are too thin to make composability durable.

122. Working harder but not smarter will reinforce the brittle optimisation of systems. Incumbents are recurrently prone to the failure that ensues. It is arguable whether Cloud computing will address composability in ways that produce resilience or irresilience. Claims for dramatic increases in utilisation of networks through Cloud computing will have a significant appeal, particularly where IT project mismanagement has blighted so many careers. Advocates of Cloud computing will doubtless talk up “seamless” composability: they may even stretch to cryptographic “universal” composability to underline their security credentials. But composability will only ever be partial as systems inevitably evolve. A pragmatic approach to more organic composability has real merits, including:

• upfront design that forestalls obvious compromises on security;

Cyber Doctrine

- assuring the highest levels of reliability on well-defined kernel software;

- interfaces between modules honed to meet interoperability standards;

- data libraries of reliable composable code ready for reuse;

- attention to legacy code and systems (particularly audits of encrusted patches); and

- clarity about cryptographic composability (including anti-tamper).

123. Likewise, well-codified drills that standardise competencies need to complement technical composability. This could prove more vital than ever if emergencies in the Clouds are prone to contagious spread. These drills present composability challenges, too. What state of readiness these competencies are held in, how combinations of drills are selected and how effort is sustained from a pool of too often rare skills are important considerations. Capabilities can always be improved; capacity doubtless needs to grow substantially. Discovering that surge capacity is unattainable in emergencies is unhelpful, to say the least.

124. There is, thankfully, some evidence of improving transnational coherence and mutual assistance, including:

- increasing numbers of Computer Emergency Response Teams (CERTs);

- Forum for Incident Response and Security Teams (FIRSTs) may provide a better focus on learning lessons and coordination of mutual assistance; and
125. Greater coordination of available capabilities will encourage convergence on more common standards. These make training easier to scale. However, evolutionary-drag factors cannot be discounted. For example, in cyberspace it would be wrong to assume that technical specialists hail from a common heritage (see Diagram 5 on the next page). There can be significant differences which, if obscured, complicate training matters to the detriment of security and resilience.

126. Industrial Control Systems (ICS) and Communication & Information Systems (CIS) communities see cybersecurity quite differently. They may share adherence to the information assurance principles but the former prioritises Availability before Integrity and Confidentiality and the latter reverses that order. This perhaps made sense when both communities dealt with seemingly separate architectures. But these have long since converged in cyberspace. The habits of the ICS and CIS communities are formed through training and experience based on different orientations to information assurance principles. Education needs to provide more evolutionary flexibility for diverse communities. This accords with the development of coherent doctrines rather than succumbing to being doctrinaire.

127. Training is the easiest part of individual and organisational learning and can be overdone. Education is harder but offers more enduring rewards. Whereas training can make the execution of codified procedures happen with unthinking and replicable precision, education takes the value of learning further. Principles can guide the adaptation of drills and alter the permutations in which these are assembled and integrated during use; concepts go deeper and wider by enabling people and organisations to recognise circumstances changing to a degree that makes some or all existing drills inappropriate and heralding the
Diagram 5
ICS and CIS Topographies

Industrial Control Systems

- Mechanical/Analogue/Digital with increasing use of CIS COTS Technology
  - Programmable Logic Controllers
  - Sensors
  - Remote Telemetry Units

Communications - IP/Serial/Wired/Wireless

- SCADA
- Data Historian
- Distributed Control Systems

Availability - Integrity - Confidentiality

Business Drivers

Human skills base

Communications & Information Systems (CIS)

- Communications & Computer Hardware/Software
- Data Storage
- Communications - IP/Serial/Wired/Wireless

Availability - Integrity - Confidentiality
requirement for new capabilities – perhaps in unprecedented configurations. Common standards favour training over education. Doctrine provides the syllabuses needed to support both training and education.

128. One downside of training may be held in check by the powerful undercurrents of sovereignty. Shared interests in common standards will seldom be universal. Composability in terms of technical interoperability or codified skills will conflict with competitive interests at some point. A transnational world makes these limits more not less apparent. The dynamics of “glocal” networks mixes open and closed architectures with de jure (statutory and treaty based) and de facto (emerging from markets and civil society) standards. Organising capabilities with these complex dimensions of composability will be no mean feat (in or outside of emergencies).

129. The danger of over-striving for composability is that brittle optimisation sets in through myopic learning. Incumbent organisations tend to learn less well than up-starts. Unfortunately, the latter includes black hat hackers. For example, there is evidence that the circulation of vulnerability notices and the mismanagement of security patches enable black hats to learn faster. Since bureaucracy has always been less of an issue for them, their capacity to innovate is different and perhaps better. Any move to the Cloud needs careful consideration on these terms too. “Virtualisation” in the Cloud may be little more than a smokescreen for maximising utilisation rates for software, bandwidth and processing power. Well before such a utility computing model reaches maximisation a host of dangers threaten to materialise. For example, the untimely but inevitable discovery that the limited capacity for computer forensics is thwarted not only by technical virtualisation but also Clouds conveniently spanning multiple jurisdictions. At worst, Cloud computing could be offering the kind of security-through-diversification the banking sector was offering on the brink of the crash, i.e. bogus.

130. The composability challenges Cloud computing seems to resolve could be down to short-lived expediency not pragmatism. The

---


133. Cyber criminals are “spear phishing” as a more targeted approach than phishing whole networks with generic messages. Spear phishing involves, for example, spoofing vulnerability notices, virus and malware alerts, and news alerts for events, such as, the Royal Wedding and Osama bin Laden’s death to hook the unwary. Cyber-criminals are also manipulating Search Engine Optimisation. These gambits all evidence their innovative agility. Conversely, it is not clear that automation – removing humans from the loop – will enhance the resilience of bodies or systems in cyberspace. See, for example, Department of Homeland Security (DHS) (2011) Enabling Distributed Security in Cyberspace: op cit, which does not necessarily address the more robust eco-systems issues raised by Frei, S, Schatzmann, D, Plattner, B & Trammell, B (2009) Modelling the Security Ecosystem - The Dynamics of (In)Security, available at http://www.techzoom.net/security-ecosystem accessed 16th May ‘11.
Cyber Doctrine

advertised promise of Cloud computing echoes that of supercomputing, although expectations for the Cloud seem to obscure challenges supercomputing continues to explicitly wrestle with\(^{134}\). A prior assessment of resilience could map performance bottlenecks, latencies and anticipate the emergence of hubs or “superspreaders” of contagion. Obviously, these hubs will not be the same as the banking sector; albeit the overlap between financial services and cyberspace is almost complete\(^{135}\). Rather, an assessment of where the drive for composability necessary to deliver Cloud computing becomes dangerous is vital. Re-usable libraries of code and interoperable interfaces can combine clones with easy transmission routes for contagion. Clarity about drills, standards, codes, modules, interfaces etc is always vital but remains tactical. Overworked tactics can give a false impression of proficiency, flexibility and diversity. Hybrids of bespoke supercomputing may offer vital diversity to the otherwise commoditised uniformity Cloud computing seems to rely upon.

131. Not being prescriptive makes doctrine workable, particularly with a pragmatic sense of what is composable across and through time. It is not clear that either SSADM or DSDM makes composability pragmatic. Moreover, the project and programme management methods applied to either conventional procurement or Urgent Operational Requirement (UORs) only seem to amplify composability problems. It is little wonder that cybersecurity experts are calling for a radical change of ethos\(^{136}\) and for far more attention to be paid to the economics of security\(^{137}\). This is of immediate and enduring consequence. Expectations for the Post-Bureaucratic Age are reasonable, as up-starts – black or white hat – make evident through mass or open innovation. This makes the practical limits of cybersecurity less to do with composability of technology (software, devices, systems, architectures etc) than the incentives of agents in networks\(^{138}\).


\(^{135}\) See, for example, Tett, G (2011) Beware the disquieting threat from cyber hackers, Insight, Financial Times, 10 Jun ‘11, p. 30. In this case, Nonghyup, a large South Korean Bank crashed leaving thousands of customers stranded for days. South Korean military sources believe the “attack” is the work of the North Koreans trying to sow customer panic. The term attack may be used loosely but the potential for electronic and financial networks to become new fronts for conflict not just competition is daunting.


Cyber Doctrine
What is Innovation?

132. The definition of resilience (paragraph 68) places the enduring power of a body for transformation before renewal or recovery. This sharpens the focus on what competencies really matter in cyberspace, not least looking through the right end of the telescope, so that what really matters is more than dimly discerned at an impossible distance. The previous section underscored the primacy of deep and wide transformation in the evolving organisation of capabilities. To do otherwise only leads to optimisation that introduces irresilience against the nature of cyberspace. This section will clarify how the capacity for innovation is vital to cybersecurity and resilience. Cyber Doctrine – which meshes concepts with doctrine – can act as a guide in how innovation is taken up on the healthiest terms.

133. Innovation is much discussed by policymakers, consultants, financiers and industrialists. Growth is not feasible without innovation, particularly for highly developed economies. Behind talk of innovation and growth is the pragmatic reality that Research and Development (R&D) underpins both. Managing R&D is a restive process; as far back as 1912 and onwards, Schumpeter detailed two key reasons why. Firstly, researchers may thrive on invention but evidence more reluctance to drive beyond invention
to the market uptake that defines successful innovation. Secondly, innovation is not just routine management or even leadership; it requires entrepreneurship. Entrepreneurs personify innovation. Cyberspace is a natural environment for innovation embodying technology and competencies as entrepreneurship.

134. Given the challenges innovation throws up, it is little wonder that five generations of approaches to R&D management can be mapped since the 1950s\textsuperscript{139}. Much of that history is bound up with defence and aerospace. With each successive generation, calls for innovation grow more insistent; many lessons are identified but fewer are learned. Schumpeter is no innovation romantic; however much he shares Marx’s views on the power of the historical forces that propel innovation, he does not underestimate the resistance to innovation that works at all levels of organisations – bosses and workers. Whatever the additional value produced in new combinations of capabilities, processes and systems, it is far from inevitable that evolutionary-drag will be overcome by evolutionary-drive. Resistance is particularly hard to overcome for incumbents of formerly successful niches.

135. Expanding on the Schumpeterian definition of innovation as \textit{new combinations that create value}, a further six characteristics are:

- the spark for innovation comes from the creation of knowledge, which may involve unlearning existing habits as much as learning how to be more productive with what is new;

- to create value, the knowledge must herald:
  - an emerging capability or capability gap; and

an emerging market (among leading users or non-users ill-served by existing markets);

it is not necessarily derivative to mimic activities detected through horizon scans and benchmarking because fresh contexts may spur further creativity and innovation rather than localised adaptation;

reliable investment flows are the vital lubricant at the interface between the emerging capabilities and markets;

the incentives for any middlemen at that interface need careful consideration; and

mapping the innovation pathway to viable and mature markets is important not only to speed the delivery of innovation but also by making innovation safe to fail by “failing fast”.

136. These assumed characteristics are worth recalling because hyperbole about innovation can obscure them. Private sector experience of the innovation challenge makes plain that it is hard to achieve, but vital. It is also acknowledged that a number of associated displacement activities masquerade as innovation and do not add value:

• damaging rivalry aimed primarily at protecting and increasing market share;

• cost reductions through optimising or outsourcing established processes;

• communication campaigns for customer loyalty;
Cyber Doctrine

- mergers and acquisitions; and
- cutting away marginal business units.

137. These activities may or may not be necessary in any given case; they may bestow benefits; but they can also absorb management and decision-taking, distracting attention and energy from entrepreneurship. A variety of middlemen can profit from these gambits both within and outwith a firm but they are not necessarily entrepreneurs and often sidestep the direct challenge of innovation. Overall they may push-up transaction costs and add bureaucracy that works hard against the law of diminishing returns. This seldom enhances desirable outcomes.

138. To now, defence, aerospace and higher education spending has been crucial to innovation in developed nations. Doubtless the yield on such spend might have been significantly better. Beyond the diagnosis of “disruptive innovation” in the 1990s, the advent of more user-driven open and mass-innovation only underscores how vital the capacity for innovation is to the security and resilience of cyberspace. The tension between industrial strength SSADM and user-driven DSDM begs interesting questions regarding which ethos better fosters entrepreneurship among users and developers.

139. Incumbent organisations (public, private and third sector) in developed nations may reaffirm Schumpeter’s findings on resistance. It is not evident that any transnational Defence Industrial Base (DIB) is ready to transform its relations with Small and Medium Enterprise (SME) networks to produce the needed capacity for innovation. Similarly, most universities still favour creativity over innovation and entrepreneurship; and government attempts to replicate geographic innovation “clusters”, like the UK’s Silicon Fen\(^\text{140}\), are proving wasteful almost everywhere.

140. Silicon Fen is regarded as the most significant innovation cluster in Europe. UK Government efforts to leverage that success, led by Gordon Brown from 1998, in the guise of the Cambridge MIT programme achieved many results but not the overall goal intended; namely, enhancing the coupling of invention to innovation. See, for example, Simmonds, P, Stroyan, J & Clark, J (2009) An Evaluation of the Cambridge-MIT Institute, Prepared for the Department for Innovation Universities and Skills (DIUS), Technopolis Group.
140. As funding for higher education and defence stalls and goes into decline, it is not clear that there will be unleashed the innovation and entrepreneurship that advances cybersecurity and resilience in ways, or on the scale, that our dependence on cyberspace warrants. If the Big Society is the reciprocal of the shrinking State, the security and resilience of cyberspace could well throw up the Big Society’s acid test. Moreover, any belated growth in the capacity for innovation in cybersecurity and resilience will need to overcome major deficiencies in leadership, management and the participation of citizens.

Mad Stalemate: Ogarkov’s Breakthrough

141. It is claimed in some presently fashionable business literature that incumbent firms rarely – if ever – have the capacity for “disruptive innovation”. Sovereign states are not firms but their monopoly provision of key public services (including the use of armed force, law enforcement, intelligence, tax and revenue collection etc) and predilection for bureaucracy might suggest the curse of incumbency can affect them, too. That hypothesis is – in part – supported by the uptake of the Revolution in Military Affairs (RMA) in the US during the 1990s and the Soviet Union from the late 1970s. The experience of RMA in the USSR and US heralds what “disruptive technology” or “disruptive innovation” means in cyberspace. The examples are illustrative.

142. Marshall of the Soviet Union NV Ugarkov can be seen as one of the real fathers of cyberwar. He became Chief of the General Staff in 1977, the same year that President Brezhnev made his Tula Speech in which he officially acknowledged that the utility of nuclear weapons was limited to Mutually Assured Destruction (MAD). This did not mean that all Soviets strategists viewed themselves as locked into a MAD stalemate. (Although some concluded
that the Soviet military saw nuclear weapons marking the “end of history”\textsuperscript{142}, they only made that mistake a little earlier than Fukuyama.) There were other schools of Soviet strategy that merely dropped nuclear contingencies for limited war or pre-emptive strike, but they continued to explore how to breakout from the MAD terror of total peace.

143. Ogarkov\textsuperscript{143} readily agreed that any use of nuclear weapons would escalate. However, true to the more hawkish tendency that had dominated Soviet strategic thought from 1965, he led the development of concepts that would create new capabilities for waging war. Ogarkov’s stance dismayed the high priests of deterrence; for them, MAD made the strict rational balance of power plausible. Disruptive innovation was most unwelcome. Ogarkov advocated the integration of capabilities to produce the Recce-Strike-Complex. He postulated that this would be decisive in the earliest stage of any war, particularly in the crowded European theatre. It would range deep into the enemy’s formations, not just its first echelon but second, third and rear. In particular, precision targeting of Command and Control nodes as well as sowing deception and confusion with Radio Electronic Combat (REC) would be tantamount to the impact of nuclear weapons. The shock and surprise inflicted by the tempo of operations would be amplified by the networks disrupted and destroyed. Such a concept did not need nuclear weapons to have decisive affect.

144. Having argued for increased funds to further develop the capabilities to fulfil his concept of the RMA, Ogarkov was transferred to other duties in 1984\textsuperscript{144}. His military colleagues did not disagree with Ogarkov but there was a growing sense that whilst nuclear weapons were a dead end, military transformation needed Perestroika for funds. However coherent, his ideas were too uncomfortable, unsettling and demanding of resources.

\textsuperscript{142} Fitzgerald, MC (1987) The Soviet Leadership on Nuclear War, Center for Naval Analyses: Alexandria VA.


\textsuperscript{144} General Secretary Chernenko was not prepared to cut social programmes to fund these developments. Ogarkov cited Chernenko on the need to overcome the forces of "conservatism and stagnation".
145. The irony is that Ogarkov was responding to NATO’s integration of advanced technology. This western drive was aimed at off-setting the Warsaw Pact’s larger numbers of conventional forces, which were enhanced by the strategy and operational art which NATO lacked. It was also aimed at addressing nuclear force disparities too, in that whilst many citizens of NATO made it clear that use of nuclear weapons was unacceptable, NATO’s leaders could not be sure that the Soviets shared such repugnance at any use of such weapons. In response to these dilemmas, the US (supported by the UK) drew on the same schools of operational art and strategy that informed Ogarkov. This produced US Air-Land Concept from 1976 to 1983 for NATO, which became known (or notorious) as “shock and awe”, as exhibited in the 1991 Gulf War. Ogarkov had anticipated how concepts and capabilities would evolve out of the MAD stalemate. Strict rationality and balance of power did not put an end to history.

146. The US capacity to innovate with the RMA concept did not last long. Whereas Ogarkov understood the concept was only part technological, vested interests in the US made it entirely technological because that was more profitable and could off-set the commercial losses of the “peace dividend” augured by the end of the Cold War. The capacity to innovate stalled, on both sides.

147. Early triumphs in combat operations did not carry through to winning wars – or better – winning the peace. And now, the multipolar world, that the Cold War advocates of deterrence thought MAD would keep at bay, has erupted. Cyberspace is a network world in which expenditure on technology will seldom erect enduring cost or technical barriers. Instead, more often than not, cyberspace will enable knowledge transfer and innovation to happen, undercutting prices and delivering innovation where it might otherwise not reach.
Cyber Doctrine

148. Ogarkov’s concerns had been roused by military systems needing generational redesign every 10 to 12 years. His RMA was not just technological; he knew that concepts, doctrine, organisational design and learning were just as important as technology. But the torrent of innovation now – and likely into the future – must daunt even him. Without a focus on how people will or will not take up innovation, expensive mistakes will be made in cybersecurity; mistakes that bedevil national, international and transnational security in what is now a multi-polar world. These trends and drivers underscore Philip Bobbitt’s historic warning that the victors of epochal conflicts tend to merely be the second to lose\textsuperscript{147}, unless they redouble their efforts to learn.

Sovereignty: Dig for Pragmatism

149. In retrospect, Ogarkov’s mistaken legacy is to confuse war with combat. His RMA, and that of the US, focused exclusively on military operations and the purchasing of hardware. War is not about combat \textit{per se} or stockpiling kit. Winning war, and winning the peace, are about innovation; they are, in reality, continuous processes\textsuperscript{148} saturated in politics large and small. In a transnational world separating these winning activities (their preparation and conduct) is impossible, unless defeat is to be accepted as the end product.

150. This is true of spheres far removed from war, though crucial to security whether personal, national, international or transnational. Tidy categorisations that would insulate, for example, intelligence\textsuperscript{149}, criminal justice, economics and finance from how an innovation enables the winning of war \textit{and} peace\textsuperscript{150} are futile and dangerous. This is not to advocate anything as grand as nation building in the aftermath of combat operations or to urge governments into trying their luck as venture capitalists, stock-picking and lubricating innovation in the economy at large.


\textsuperscript{149} See, Herman, M (1996) Intelligence Power in Peace and War, Cambridge University Press with the Royal Institute of International Affairs (Chatham House): London.

However, abdicating responsibility in the face of the perplexing challenges arising from cyberspace is unacceptable too.

151. Sovereignty matters, not just to elites but to the peoples of nations. It even matters to corporations when life beyond their niches reveals how fragile thoroughbred firms can be, adrift in cyberspace and assailed by upstarts affirming disruptive innovation. Networks-in-Being place entrepreneurs in their element. In a transnational world, sovereign states that bank on their monopoly positions are inviting failure as much as incumbent firms that indulge anti-competitive practices to fix markets. This is not an exhortation to reckless rivalry; it recognises that ecosystems are about growth and decay and protectionism can forestall neither for long. These classes of challenge are not intractable, particularly in cyberspace.

152. Whilst organisational learning is better where aspirations are held high\(^{151}\), notions of “information superiority” or “knowledge dominance” may go too far, even for the US. The generations of innovation the US aspires to master in these terms is, in all probability, beyond even the only remaining superpower. Mass-innovation occurs on so broad a front and on such variable timescales that even if several generations of disruptive innovation could be mastered in any one area integrating these strands across time in the short or longer term will be less than tractable and perhaps self-defeating to attempt. A far more organic and evolutionary approach is necessary to gain and sustain traction. Such a process needs concepts and doctrine to mesh and demonstrate the value of blending investments in exploitation and exploration. This can be summarised as Delivery-Innovation-Growth (DIG). The DIG process need not build on orthodox economic assumptions, which too often underpin hubris or resignation. Heterodox economics can avoid two traps:

---

Cyber Doctrine

- It can alert organisations when the self-inflicted harm of suppressing aspirations - which firms are in the habit of doing as efficient adaptation to narrow niches becomes myopic – is getting dangerous; and

- It can improve the selective targeting of investments by always keeping the dynamic blend of investments open to variety and attuned to the aspirations of users despite the known organisational learning constraints.

153. With cyberspace being an environment encompassing peace and war and a hotbed for innovation in either circumstance, old ideological economic positions are unworkable. Healthy DIG will be jeopardised by neoliberal loose regulation predating a shrinking state as much as by Neo-Keynesian tight regulation seeking to dampen risk and uncertainties, when risks need to be taken and uncertainty explored. The former may produce patchy profits or profiteering in cybersecurity; the latter bureaucratic inefficiencies and procurement white elephants or cyber-Maginot lines. Between these poles pragmatism is not only feasible but essential.

154. Our recent past offers signposts for a pragmatic approach to sovereignty. The spirit of innovation at Bletchley Park so vital to winning WW II did not die afterwards. The invention of Public Key Encryption (PKE) is of massive consequence to the security and resilience of activities in cyberspace. It was invented by James Ellis at GCHQ in the late 1960s. Early stages of innovation needed the 1972 breakthroughs of Clifford Cocks and Malcolm Williamson, then at Cambridge but who later moved to GCHQ. Rather like Alan Turing and so many others, Ellis was characterised as something of a quirky misfit\textsuperscript{152}, underscoring that innovation and entrepreneurship are easily mismanaged. Misfits or not, Ellis, Cocks and Williamson produced perhaps the most significant breakthrough in twentieth century cryptography. Like their Bletchley

Park forbears the credit owed to them came too little and too late. The history surrounding the invention of PKE points up enduring issues for interfaces between the public, private and third sectors. It is a story worth retelling in some detail because of what it illustrates for the pursuit of the common good and its sometimes awkward relationship with innovation and entrepreneurship.

155. Cocks and Williamson were somehow able to learn of the Ellis PKE concept whilst still at Cambridge. They then cracked the first steps along the innovation pathway but agreed to PKE remaining secret. That agreement held when Whitfield Diffie and Martin Helman at Stanford University, and Ronald Rivest, Adi Shamir and Leonard Adleman at MIT published their PKE discoveries in the mid-1970s. When Diffie-Helman applied to patent the invention in 1977, some on the GCHQ team wanted the patent blocked. A heavy public hint about the real inventors of PKE from a US National Security Agency (NSA) chief (Bobby Inman) caused Diffie real concern. He eventually met with James Ellis in 1982 but Ellis confirmed nothing about his invention. Ellis and Diffie remained firm friends.

156. Eventually however, in 1987, the UK Government began marketing GCHQ’s security wares beyond their long-standing defence and diplomacy clients. Publicising the invention of PKE would have been any marketeers dream. But that gambit was pulled because of the publicity around Peter Wright’s “Spycatcher”. In 1991, Philip Zimmermann took PKE another massive step down the innovation pathway by launching Pretty Good Privacy (PGP) on the internet. Ellis’s invention had become a mainstay for e-commerce. Public acknowledgement of the contribution made by Ellis, Cocks and Williamson was to come at a 1997 conference. Ellis died a month before the event. Diffie disclosed one comment Ellis had made in 1982: “you did a lot more with it than we did”\textsuperscript{153}.
157. The challenge of innovation and entrepreneurship may well encourage some to think it is easier to outsource or rely on the private sector. Indeed, private sector dependence on cyberspace could not provide a greater incentive for producing and using cybersecurity services. However, as a minimum those services need regulation in ways that equal or exceed the challenge for the financial sector. More substantially, any pretence to strategic or operational sovereignty will need more substance. Private firms will naturally tend to cherry-pick only the niches they can service profitably. They will not generally pick up the tab for R&D or education in the depth and breadth that cyberspace will demand, irrespective of the economic imperative.

Financing Innovation or Ruining Futures

158. Innovation needs to be lubricated with well run finance at the interface between innovative producers and innovative users. In bringing the capacity for innovation to the heart of winning the peace (or war), it may seem that cyberspace encompasses just too much. However, the tidy separation of various areas of government and other businesses is unworkable. Small World Clusters happen and can trigger contagion in Scale Free Networks for better or worse. Investment criteria and measures of value are key.

159. The recent outbreak of fraud and theft in the EU Emissions Trading System (ETS) is another case in point. Cybersecurity basics were compromised from the outset by permitting separate registries to be run in each of the ETS participating States. Local registries would have been acceptable, were it not for the inconsistent application of routine security measures. Incoherent security measures meant that the pattern of infiltration into these registries became apparent too slowly. Meanwhile, criminals had the time to make the innovative leap between stealing certificates and
coupling their onwards sale to Carousel Value Added Tax (VAT) fraud. Interpol estimate €5bn has been lost to the tax scam\textsuperscript{154}. Returns on investment for innovation are clear to some.

160. Whilst criminal gain may have been the only motive for the ETS raids, it is not the first time that cyber attacks\textsuperscript{155} have been employed that discredit climate change initiatives. The disclosure of the University of East Anglia (UEA) climate change e-mails was not an accident. It involved sophisticated and protracted attacks on and through academic systems with links to Russia. These affects may not be scale-free \textit{per se} but are setbacks of lasting consequence to climate change. Conversely, the gains for the Siloviki\textsuperscript{156} elite of a rentier economy suffering a lack of economic diversification are an easy topic for speculation. However, between these uncertainties the time lost and overall damage to the planet could prove irrecoverable. The damage to the planet less immediately so.

161. Reconciling Russia’s repeated wish for a cyber treaty akin to arms control with the growing strength of cyber-criminals and cyber-patriots is easily misconstrued. An arms control treaty keeps cyber issues close to the threshold for sovereign bodies to invoke exceptionalist and decisionist claims. This does not detract from the real comparative advantage nuclear arms control has. As strategic capabilities, nuclear weapons for the most part have large verifiable footprints. Verification of nuclear arms control does get difficult as these capabilities approach abolition. But, in stark contrast to nuclear arms control, the verification of cybersecurity arms control would be a farce from the outset.

162. If it could be taken seriously, cyber arms control would make nuclear disarmament verification appear a trivial challenge. The (perhaps convenient for some) difficulties of verifying cyber capability treaty compliance contrast sharply with the feasibility of co-operation on cross border evidence gathering in pursuit of

\textsuperscript{154} This underscores the confusion of jurisdictions, where crime and matters of national security will overlap and the scale of an attacks significance is hard to discern in the short term. See, for example, the confusion arising in House of Lords, European Union Committee (2010) “Protecting Europe Against Large-Scale Cyber-Attacks” op cit.

\textsuperscript{155} Not to be misconstrued or conflated with “armed attack” as defined by Article 51 of the UN Charter.

\textsuperscript{156} The Russian term for those with a KGB heritage, particularly FSB past and present, with links across defence and security services.
criminal justice. With the RBN the only organised crime body listed as a threat by NATO\(^{157}\) and credited with a 40% slice of the $100bn taken by cybercrime in 2007, Russia’s preference for an arms control treaty rather than cooperation on cybercrime can be put in an unflattering light. Funding innovation in cyberspace is anything but a challenge for some; it is highly profitable.

163. It is easy to allege that cyber-crime, cyber-patriots and cyber-terrorists have a worrying capacity for innovation. They give some indication of the darker side of transnational Big Society in the Post-Bureaucratic Age as demonstrated by degeneracy “After Virtue”\(^{158}\). If the Aristotelian turn advocated by Big Society thinkers translates – and it is a big if – into substantive policy, then tight regulation and ends defined by hard standards could emerge. Teleological thinking\(^{159}\) will be confounded by the pace of evolution in cyberspace. Although a smaller less bureaucratic state is laudable, it is imperative that such a State has demonstrable competitive fitness for the realities of an evolving environment. Faith in telos is not pragmatic\(^{160}\) policy for cyberspace. The real issue is the capacity for innovation among those who would compete with cyber-crime and proxy militias. For states (more developed ones in particular) the aftermath of the Great Recession presents a real challenge for the funding of innovation.

164. This difficulty is not a straightforward issue of money being tight (though it is). Cyber capabilities are relatively inexpensive. However, even smaller amounts of money expended in anything like established procurement practices could prove to be a disastrous waste. The UK’s 1998 Strategic Defence Review (SDR ’98) said a great deal about Smart Procurement. Whatever the advances, it would be difficult to claim that the eventual merger of logistics and procurement coupled with talk of the Through Life Acquisition of Capabilities led to consistently smart outcomes. The financing of routine procurement and urgent operational

---

159. For a recent example, see, Fukuyama, F (1992) The end of history and the last man, Free Press.
requirements has tested the limits of credibility. Such travails are far from limited to the UK, or to defence. Cybersecurity and resilience presents a challenge for how best to use capital to invest in the capacity to innovate right across public, private and third sectors. The Critical National Infrastructure (CNI) of any developed country makes plain how these are now inextricably linked, since today’s CNI is less and less confined to either tangible assets or those under government control or ownership.

165. And more and more, financial integrity and security are enmeshed. We can identify five legacy mechanisms for structuring finance that illustrate the challenges:

- Opaque financial arrangements have already demonstrated their potential for harm. It is important that lessons are learned now rather than glossed over. There is much to learn from the migration of Project Finance from North Sea oil exploration to the public sector as Public Finance Initiatives (PFIs) and Public Private Partnerships (PPPs). Oil industries are better at running engineering projects than raising capital. This made Project Finance a value-adding service for the oil industries. Its attraction for the public sector is not so clear. A tax base gives governments very strong and versatile finance mechanisms, irrespective of poor project and programme management skills. Whatever the intent, PFIs (sometimes rebranded as PPPs) have three outstanding features – not necessarily advantages. First, they bundled finance, fixed capital and facilities management into large sums that were taken “off-balance-sheet”. Second, the public sector developed expertise in complicated financial arrangements rather than delivering projects. And finally, these projects meant that not only public servants but all those involved in PFIs became part of arrangements that repudiate the coupling of Delivery-Innovation-Growth (DIG).

Whatever their benefits, PFI contracts based on long term commoditised items of expenditure are almost hard-wired to reject innovation and flexibility. The transparency hangover that PFIs will undergo as International Financial Reporting Standards (IFRS) are complied with should be welcome but may squeeze innovation further. New approaches to financing innovation need to be shared across the public, private and third sectors, if cybersecurity and resilience is to be a healthy enterprise.

• Far from marginalising the human or ecological, cyber-space revitalises our awareness of the state of nature. In terms of capital, it becomes difficult to avoid considering what human or intellectual capital is; narrow financial capital is inadequate to measuring value. This is a pragmatic point. Better Returns on Investment (RoI) are achieved through locking the uptake of technology with the learning of competencies. In the UK, defence lines of development under the rubric of TEPID OIL (Training, Equipment, Personnel, Information, Doctrine, Organisation, Infrastructure and Logistics) offers some basis for locking technologies and competencies or human capital together. However, TEPID OIL on its own evidences little more than superficial evolutionary integration in routine peacetime procurement, akin to “transformation in contact” on operations. Any notion that TEPID OIL has enhanced RoI is overshadowed by a £38bn “bow wave” of unfunded commitments. Moreover, the financial retrenchment required to address the bow wave is unlikely to result in TEPID OIL widening and deepening the capacity for innovation through research and education as some have warned is vital.

TEPID OIL may be an advance on Other Government Departments’ (OGDs) procurement thinking but that


164. Wolf, A (2010) “Defence research must be protected from cuts”, Financial Times 20th June, a noteworthy article if only because Prof. Wolf, although at King’s College London is not part of the War Studies Department but Public Sector Management.
does not mean it is an adequate basis for achieving good RoI for cybersecurity capabilities as some suggest\textsuperscript{165}.

- Influential voices in the US are focusing attention on the “human capital crisis in cybersecurity”\textsuperscript{166}. They suggest that the US currently has 1000 cybersecurity professionals of the calibre required but needs between 10,000 and 30,000. The skills gap listed is worrying but also technical and tactical. It may be reassuring that the size of the required workforce estimate is so wide a variable. The gap perhaps affirms how exploratory capacity building sensibly has to be. However, job creation schemes based on alarming anecdotes are not necessarily the way to spur creative enterprise. The agility, versatility and stamina required for cybersecurity and resilience capabilities need accounting standards that measure value as befits the environment. The role of inadequate accounting standards in the Dot.Com bubble has not been addressed. It may be that the first market bubble in cyberspace seems trivial in the aftermath of the Great Recession but it is also arguable that the Keynesian measures taken for a soft landing in 2000 only compounded the moral hazard and problems in 2007 – the mega-bubble continued to inflate based on assets (e.g. property) securitised and leveraged with debt in increasingly exotic and ultimately toxic ways. Accounting standards need to be addressed not only for cybersecurity and resilience industries but also for economies utterly dependent on cyberspace\textsuperscript{167}.

- The three legacy challenges above are none too encouraging. However, they affirm the nature of the overall challenge of financing innovation. The last two legacies offer more positive prospects for possible action. Implicit so far in much consideration of financing projects and


programmes is the assumption that flexibility, agility, surge capacity, etc only incur greater costs. Thus, the cheap certainties of fixed requirements and commoditised standards are hard to resist. This is despite the fact that these certainties are largely fictional[^168]. Faced with these realities, Evolutionary Real Options[^169] offer a useful approach to the kinds of uncertainty inherent to cyberspace. It builds on systems engineering to offer a design process that values flexibility as circumstances change for systems and projects. It does so by using decision support models to explore the evolving combinatorial real options, working with the bounded rationality of decision-takers to exploit satisficing (sub-optimal but good enough)[^170] realities rather than pretending global optima are achievable. This is not only a pragmatic integration of concepts but can switch investments between low and high yield options to deliver composable capabilities which other design processes cannot. Cybersecurity and resilience capabilities need such innovative approaches to finance and valuation.

Sounding a final note of cautious optimism on legacy mechanisms for finance, is the salutary tale of Admiral John Poindexter’s Directorship of DARPA and the rise of VIX, the Chicago Board Options Exchange Market Volatility Index. VIX is a measure of implied volatility over the next 30 days for the S&P 500 index options (financial rather than real). Invented in 1993 by Prof Robert Whaley as a “fear gauge”[^171], VIX went live in March 2004. It has since gone from strength to strength. One day of trading in March 2011 saw one million contracts changing hands as the consequences of news of unrest and natural calamity from the Middle East and Japan sunk in[^172]. Tradable notes are now being linked to


the VIX. This thriving market provides a powerful hedge for uncertainties. Ironically it does so on almost exactly the terms John Poindexter advocated before retiring abruptly in August 2003 for suggesting a similar mechanism to better price and hedge for the risks and uncertainty thrown up by a networked world. The VIX and its development of traded notes offer another approach to pragmatic financing when facing massive degrees of uncertainty in which sentiment rather than rationality can be decisive.

166. The legacy mechanisms cited above are far from a comprehensive assessment of how to invest for cybersecurity and resilience capabilities. These examples merely signpost how robust an evolutionary approach needs to be. The kinds of risk and uncertainty under consideration are not entirely new. In the early twentieth century Frank Knight prepared the ground for a more pragmatic approach to risk and uncertainty (including non-actuarial or business risk), not least through his attention to how people behave and learn. UK experience of the near collapse of terrorist insurance markets as a result of “spectacular” bombings lead to the creation of Pool-Re, a development that offers some insights into the difficulties of sustaining viable markets for insuring such risks. More recent work on cybersecurity insurance suggests the role of insurance will be anything but straightforward. Not only are the risks and uncertainties difficult to measure but any insurance product may do more to create moral hazard. Again the behavioural and evolutionary dynamics are vital considerations for cyberspace.

167. Investing in composable and innovative capabilities whilst building the capacity for innovation will require greater competence with dynamic portfolios of investments (including insurance). As innovative users and developers will need challenging but trusted relationships – not cosy corporatist relations laced with moral hazard...
Cyber Doctrine

that span public, private and voluntary sectors and are open to continuous learning. Anti-markets or anti-competitive practices retard learning. Combining markets with aspirations for strategic and operational sovereignty is not easy and can be intractable, particularly if predicated upon the efficient market hypothesis. Heterodox rather than orthodox economics (Neo-Classical or Neo-Keynesian) can underpin a more tractable approach. At the heart of any such approach will have to be a consideration of the behavioural and emotional\textsuperscript{177} incentives finance entails.

168. Middlemen of all sorts are a concern in any enterprise (market or anti-market) but financial intermediaries are a particular concern. Dynamic portfolios of investments that link current capabilities with the capacity for innovation could create another arena for bewildering activities and perverse rational incentives. Financial engineers seem largely unchastened by the economic crises they helped trigger with opaque products and services. The Flash Crash of May 2010 and the recent emergence of Credit Derivative Swaps for junk bonds again evidence how innovation can be unhealthy. Cybersecurity and resilience is not a monopoly of any one sovereign body. The public, private and third sectors will form evolving “glocal” clusters. How all these market participants will value cybersecurity and resilience will differ and be changeable.

169. Measuring the value of investments in dynamic portfolios of cybersecurity and resilience capabilities challenges existing measures and preconceptions. That challenge will intensify as the convergence of banking (utility and investment), securities and insurance deepens and widens. The reality is that conventional risk measures are inadequate for the uncertainties that networks nurture, not least financial networks.

170. These uncertainties can be good and/or bad. Assuming that measuring RoIs in constant flux can be achieved through existing

accounting standards would also be rash. The Dot.Com bubble and Enron debacle should have been warning enough but some lessons have yet to be heeded. Nor is the question of value limited to the profit-seeking private sector. Cyberspace provides an environment for multilateral partnering. How contracts (not least non-actuarial insurance), ownership and value work in cyberspace needs fresh consideration. Assuming that established practices work in changed circumstances is unwise.

Resilience And The Origins Of Wealth

171. Convergence in cyberspace has been discussed for over a decade in terms of telecommunications, computer processing and interactive multi-media content. This marks an important milestone in the evolution of the cyberspace environment; but that evolution is not at an end. The outcomes of such a technical convergence are far from predetermined, as uptake in the use of mobile devices affirms, for example, across the Arab world when combined with doctrine.  

172. Cyber, bio and nanotechnology are also morphing into one another. These uncertain developments, building on the question of financing innovation, open a broader economic question in which cybersecurity and resilience are not just a service but are the services underpinning trust and confidence in an environment that touches all others. Indeed, cyberspace creates the environment in which the externalities of orthodox economics become increasingly untenable. Woven together through cyberspace, productive forces are transforming all environments, forcing profound questions about the origins of wealth.

173. These questions could not be more urgent for developed economies struggling with the aftermath of the Great Recession and on-going economic crises. The Chairman of the US Joint Chiefs is
Cyber Doctrine

incisive: the economic crises and recession are the greatest challenge to US national security and are therefore of great transnational consequence. This point is only underscored by the throw away remark of a major bank CEO in the City of London, “I cannot tell if we’re a bank or IT firm”\(^{181}\). Little wonder given that the integration of financial networks under the banner of globalisation owes so much to technical convergence. However, the integrated networks that support finance and trade have produced economic structural imbalances\(^{182}\). A great divergence has set in with the over indebted consumers at one end and overproducing savers at the other. Both need one another but their unhealthy (even abusive) relations need to undergo a different sort of convergence\(^{183}\). This could be less than graceful, a point the US Joint Chiefs clearly grasp.

174. Economic convergence in the aftermath of the Great Recession comes on top of financial convergence (of banking, securities and insurance) and the technical convergence (of computing, telecommunications and content). The stakes for cybersecurity and resilience could not be higher. Graceful economic convergence will depend on cyberspace being a trusted environment enabling growth. It is not clear that the incumbent defence and security firms are yet ready for the DIG challenges overtaking them. The Financial Times has expressed real doubts about how incumbents are placed to innovate for cybersecurity and resilience\(^{184}\). Similar assessments for the biggest defence market on the planet are emerging from the US\(^{185}\). The question posed cannot be directed at the supply base alone; customer relations are two-way and need to be intelligent throughout. With the UK’s Office of Government Commerce (OGC) renewing its advocacy of SSADM and offering nothing other than PRINCE 2 for projects and programmes, bureaucracy and transaction costs will work against innovation for both developers and users alike. The State will continue to find the productivity gains achieved elsewhere with the uptake of innovation eludes them. Security and resilience will then only suffer further.

181. Private conversation with Authors.


175. If cybersecurity is built on these terms and methods, it is reasonable to expect something akin to another weak RMA: this time will be worse than the last. Since the 1990s dependence on cyber-space has grown, some potential adversaries have invested heavily but any Western budget will now be far tighter. This is emphatically not just a military matter. Budgets across government may only address in a very limited way what is understood of current or lagging capability requirements. Another lacklustre RMA is in prospect rather than concepts and doctrine meshing to gain traction with the challenges ahead on all security and resilience fronts. This is all the more discouraging because resilience offers healthy growth for all enterprises (public, private or voluntary).

176. Cloud computing could make matters worse. Cheap options are likely to be seized upon narrowing evolutionary real options. The hardsell on maximising the utilisation of slack processing power, minimising software needed on each device, making interoperability through standardisation easy and liberating organisations from the need to have IT departments build to a compelling proposition. In the short-term, this will flatter to deceive. As utilisation goes up, and interoperability thrives on clones, the brittleness of optimisation will, for a while, be obscured by profitability. Innovation will tend to be killed off. When things go wrong vendors of Cloud architectures may be reassured that computer forensics are seriously challenged by the Cloud. Learning lessons, even when innovation becomes imperative, will be hampered. With the Great Recession, the questionable dependability of the infrastructure is only part of the concern.

177. Around the time of US Presidential Decision Directives (PDD) 62 and 63 in 1998, debate on matters cyber was already moving on from infrastructure per se to insider threats and protecting content. Cyber espionage was already a concern. Today, thefts of content are again a major source of anxiety, threatening privacy, property, intellectual property rights and national security, among other
things. The emphasis on protecting content – whether public, private or third sector – also begins to shift attention deeper than privacy issues and onto how knowledge and concepts shape the future. Given the under investment in cybersecurity, particularly research, it is almost flattering that counter-intelligence has much work left to do other than close the door after the horse has bolted. However, invention and innovation are limitless rather than scarce resources, so it is vital to stop security being an afterthought and move the uptake of the resilience concept forward in its more radical sense. Bouncing back is inadequate; competitiveness on terms fit for cyberspace requires us to bounce forward and thrive on innovation.

178. The recognition that content is far more than a privacy issue is important. There is a growing acknowledgement that cyberspace is the environment – weaving together all others – through which growth will happen. Not only are large amounts of money and time sunk into research but, whatever the time and money involved, knowledge is the fuel for innovation and entrepreneurship. This knowledge provides competitive advantage that is even more vital in developed economies where growth is otherwise up against a law of diminishing returns.

179. Economic convergence will make the comparative advantage of cheap labour in developing countries alter with time. For now, the few TNCs that do not out-source to tap into these human resources struggle to survive long. Global economic convergence will not be a smooth passage. Exporting jobs abroad is never popular but a jobless recovery from the Great Recession will make matters far worse. This outcome could cement in the limits of growth some developed economies are veering towards being locked into. Cybersecurity and resilience offers many innovative paths out of such limitations, not just for security and resilience service providers but by enabling service users too. Such agility and stamina is not financial capital intensive, knowledge and human capital yields most value.
Non-rivalrous in consumption

Diminishing returns

Rivalrous in consumption

Increasing returns

Diagram 6
Strict rationality boxed into a corner

Known unknowns

Unknown unknowns

Known knowns

Unknown knowns

CHAPTER THREE Capacity To Innovate
180. Nonetheless, knowledge and human capital cannot be presumed the preserve of the developed economies. Economic convergence is evidencing how quickly developing economies and emerging markets move on from the most simple commoditised products and services towards far more complex outputs. Calls for protectionist measures will gain a hearing, particularly when the consequences of content theft become known and understood. There is already mounting frustration with TNCs in developed economies moving inventions and innovations (often stemming from public funding) off-shore earlier in production runs. Confidence in the resilience of economies is vital, if economic convergence is not to be far less graceful than it might otherwise be.

181. Orthodox economics places a great deal of weight on the assumption that economies tend towards equilibria. This is why exploitation is favoured over exploration. The consequences are teased out in the three Quads of diagram 6. The bottom left Quad is adapted from Charles Perrow’s “Normal Accidents” and summarises how the nuclear accident at Three Mile Island happened\textsuperscript{186}. The bottom right Quad is a Johari Window\textsuperscript{187} made famous by Donald Rumsfeld’s fine epistemological riposte\textsuperscript{188}, more often unwittingly cited as “out-of-the-box-thinking”. Above these two, is a Quad comparing and contrasting consumption and returns. Strict rationality leads to brittle optimisation, which tends to box economic activity in the bottom left of each Quad. This ultimately produces irresilience, which is not the healthiest way to come to terms with creative destruction.

182. Evolutionary economics\textsuperscript{189} accepts bounded rationality and all its perverse affects, particularly through poorly designed incentives. In terms of security, Perrow’s Quad may have dealt with a closed system at Three Mile Island but even it revealed that assuming things were decoupled and could not interact in


non-linear ways was unwise. The same assumption brought both Value at Risk (VAR) and Dynamic Stochastic General Equilibrium (DSGE) modelling into disrepute through the recent economic crises. Had exploration been encouraged and equilibria assumptions appropriately challenged, the chances would have improved for not only discovering and preventing costly things from going wrong but also in creating an ethos better attuned to adding value in entrepreneurial ways. This is the key to resilience as being first and foremost transformative.

183. Resilience contributes to the creation of wealth, it is not an overhead. Cyberspace is rich in networks that are tightly coupled. Swift recall or retrieval of unknown knowns involves data management that does not turn data deluge into data cemeteries. Instead, it enables ready navigation of complex cross indexes with imaginative connections – very much the unique contributions humans bring. Systematic or programmatic research of known unknowns becomes more not less vital. And out of these coherent, combinatorial and co-evolutionary activities comes serendipity, which can and does provide emergent insight into the unknown unknowns. This is not a luxury. Optimisation that kills exploration produces irresilience.

184. The Economist 2007 Survey on Innovation summarises the importance of the final Quad very simply in its last sentence: “The one natural resource that the world has left in infinite quantity is human ingenuity”\(^{190}\). The cost of collecting and communicating electronic data fuels that “infinite quality” – it is non-rivalrous in consumption. Moreover, disruptive innovations amplify that quality further by operating with an economics of increasing returns\(^{191}\). Disruptive innovations may be rarer than incremental innovations or limitless ideas but the value added exceeds the costs of failed exploration. Overall, the dynamic Blend of


Cyber Doctrine

Investments (BoI) can prevent the dire consequences of irre-silience and sustain confidence in innovation to propel growth.

185. There is evidence that such heterodox economics is informing US cyber strategy. President Obama appointed a Cybersecurity Coordinator “to provide White House leadership on cybersecurity issues”. In particular, Cybersecurity Coordinator Howard A. Schmidt’s remit, supported by the National Security Staff, makes strategic links with economics through the Office of Management and Budgets (OMB), education, science and technology. This explicit linking of the material base to the policy superstructure is vital. In the UK, on the other hand, irrespective of the continuing security and resilience impact of the Great Recession, the NSC essentially divorces itself from matters economic. Furthermore, in recognising that the sums earmarked for cyber-security contain little for education or R&D, the UK NSC is content that the private sector has the incentives and wherewithal to fill the gap.

186. In the UK, on the other hand, irrespective of the continuing security and resilience impact of the Great Recession, the NSC essentially divorces itself from matters economic. Furthermore, in recognising that the sums earmarked for cyber-security contain little for education or R&D, the UK NSC is content that the private sector has the incentives and wherewithal to fill the gap. The discrepancy between UK and US approaches and their grounding in economics asks serious questions about the viability of any strategy.

187. The Chancellor, George Osborne’s speech to the Google Zeitgeist conference may offer something more promising. He laid great emphasis on cyberspace enriching rather than just endangering our lives. He did so whilst acknowledging


security threats. It remains to be seen whether his determination to liberate government “big data” as part of the Post-Bureaucratic Age agenda and advocacy of entrepreneurship amounts to a recipe for resilience embodying DIG. But it is nonetheless a promising statement with which evolving cyber-doctrines may find strong accord.

Leadership: Enabling Entrepreneurs And Innovators

188. The development of Cyber Doctrine is intended for an arena rich in uncertainties – i.e. the realities of cyberspace. It does not overturn the need for drills or standard operating procedures nor is there any pretence that bureaucracy and optimisation can or should be eradicated. Indeed, doctrines strive to enunciate the principles that permit the healthy selection and assemblage of well defined and ready-made components but also marks the limits at which certainties begin to breakdown and options need to be created as well as executed. It is important to be clear about when certainties can be relied upon and when the assumptions underpinning them will work. Clinging to inappropriate certainties is unhealthy, though. Cyberspace can make the consequences of misplaced confidence all too apparent.

189. Having reiterated that the development of cyber doctrine is pragmatic, sticking to drills when they work but being clear when they do not, there remains a question of what personalities or characteristics are most fit for the environment. Tactical cybersecurity will place a great premium on high grade technical skills. These may well be complex and difficult to acquire. They will certainly require stamina and an insatiable willingness to learn because tactical techniques develop fast in cyberspace. Distributed and dispersed teams working on abstract challenges with variable timescales obscuring the fast and slow onset of
Cyber Doctrine

events or crises, will challenge individual skills at all levels but will also pose significant leadership challenges. Mismanaging such talent is unhelpful and could trigger one of the biggest dangers in cybersecurity – i.e. the trusted but disgruntled insider. Mismanagement could stem from both over and under-attentiveness to talent. The key to resilience is organisational learning.

190. Organisations that do not support tactical learning will, of course, aggravate cybersecurity and resilience problems. But while tactical capacity cannot be neglected, practitioners at all levels need to be committed to life-long learning. Moreover, the challenges go much deeper and wider. Building up a cybersecurity workforce will not address the deeper and wider issues of creating the necessary and sufficient capacity to innovate. This involves a very particular form of leadership – entrepreneurship. Such characters are ill-fitted to inflexible hierarchical structures fixated on exploitation. As organisations flatten and disperse into networks, the Post-Bureaucratic Age will not by default nurture healthy innovation and entrepreneurship. Selection, education, mentoring and evaluation will need to be developed to bring on personalities with the right ethos for the evolving environment.

191. Classic psychometrics methods are geared towards replicating archetypes\textsuperscript{194}, in particular strict rationalists. Cyberspace has niches for such predispositions but they are narrow and prone to change or collapse. Leadership that can deal with profound and unrelenting change does not fit standard templates. Here we can only flag the issue and offer some tentative signposts for how characters can be selected for development as entrepreneurs or people who relish driving DIG. Again evolutionary science offers pragmatic ways forward because it is alert to evolutionary-drag as well as drive.

\textsuperscript{194} See, for example, Myers-Briggs Type Indicator (MBTI) based on Jungian archetypes.
192. Modernity has bequeathed us two forms of homogenisation: the atomised sands of individualism and the concrete bloc of solidarity. Neither permits healthy evolution; both are prone to crumbling under the pressures of change. Cognitive paradigms attuned to strategic resilience are beginning to be the focus of research attention\(^{195}\). These offer insights into peoples predispositions towards innovation. It is clear that we are all ambivalent about uncertainty. Some are more often than not fearful of losing the benefits of the status quo. Others are more often than not fearful that sticking with the status quo is a prelude to catastrophic losses. Characterisations are not polarised; different circumstances will elicit different personae from people in different combinations along a full spectrum. Nonetheless, understanding how the uncertainties of innovation will be perceived and acted upon is important for leadership and strategic resilience.

193. The Schumpeterian concept of entrepreneurship is also attracting fresh research into its evolutionary nature. This affirms the capacity for innovation as vital to strategic resilience but goes further into the relationship between the entrepreneur and organisations, particularly through evolving networks\(^{196}\). Building on Simondon’s concept of individuation, that relationship is able to break with atomising individualism and the ossifying solidarity. The insights offered on the entrepreneur clarify how they behave differently and how those behaviours can be healthily incentivised. It does not suggest that everyone becomes an entrepreneur or that people with such inclinations or experience are special. What such research does do is present key questions about how to select, educate and research with entrepreneurs. Unless a flare for entrepreneurship is valued the capacity to innovate simply goes elsewhere.

---


194. Accommodating a few token misfits in established organisations is unlikely to achieve the necessary capacity for innovation. Whilst some continuity is inevitable hard questions need to be asked about precisely who adds what value to organisations in the Post Bureaucratic Age. Ducking such questions will undermine strategic resilience. For too long, developed nations have relied on migration for fresh entrepreneurial verve. In the US, the cohort of post-doctoral mathematicians, scientists and engineers owes too much to Asian foreign students choosing to stay after their studies. Now many are moving on to the rising powers of the East. This includes younger and more experienced researchers and innovators. Some are merely following the outsourcing of production which US TNCs are exploiting.

195. The existing pool from which the cybersecurity workforce is drawn cannot be taken for granted. Enabling entrepreneurs is an issue for all organisations but particularly those charged with cybersecurity and resilience. As the embarrassing hack on HBGary – a cybersecurity firm – by Anonymous demonstrated in February 2011, the talent is out there. It can be mobilised to campaign for Wikileaks and if threatened with unmasking by a cybersecurity firm has the ingenuity and wherewithal to inflict reputational damage and more. Attracting and growing such entrepreneurial flare is more than a leadership question about remuneration and career structure, it is about ethos. Without an attractive ethos the capacity for innovation will be diminished for cyber resilience and all that depends on it.

Tractability: Concepts And Doctrines Mesh

196. The past demonstrates war is man’s most infernal engine of innovation. War must not be confused with combat. Winning the peace is as much an issue of innovation as winning

war. Cyberspace makes coming to terms with that unending paradox more of an imperative. Peace and war will co-exist in cyberspace. Whatever the virtues of open or mass innovation it can be used as an engine for both. Contaminating cyberspace with militarism is undesirable but, just as confusing combat with war is wrong, assuming militarism is the preserve of the military is flawed too. Militarism fixates on the certainties of drills and the execution of these under pressure. That fixation can eradicate the capacity for innovation, bringing on a particular processes early demise. It tempts the narrowing of innovation to states of exception. Public servants obsessed with a process rather than enhancing their capacity for innovation through diversification and selection are prone to their own peculiar militarism.

197. Militarism and totalising concepts have a shared affinity, which is a problem for all institutions (public, private and third sector) not just the military. An unhealthy reading of Clausewitz produced the concept of total war. An unhealthy reading of Kant turned the horrors of total war into the terror of total peace enforced by the menace of nuclear weapons. For all the pieties of the Kantian “wish” for “perpetual peace” it needs MAD to underpin it. The MAD stalemate provided the certainty both sides needed. Perpetual peace was bought at the price of a rational pact based on a ruse – a MAD bluff - that could easily have backfired through misperception as bluff and counter-bluff sunk into an infinite existential regress. Sheltering under the MAD ruse, the Defence Industrial Bases (DIB) could achieve two things:

- Over-engineered procurement projects based on massive upfront R&D from which major spin-off benefits were derived for the wider economy; and

Global market share for products and services that subsidised production costs for a DIB parent nation and provided client nations with kit that was hard to use.

198. In these, cost, technical and training barriers all had a beneficial affect. And capabilities were too precious and horrifying to use. This reinforced MAD for those outside the nuclear armed club too. The conventional weapons they bought tended to require lengthy training programmes and even if capabilities attained operational readiness the cost of losing precious capabilities or paying for surge capacity in the event of war was financially unrealistic. The MAD umbrella sheltered defence industries that supplied capabilities that were more attractive to buy than use. They shared some of the prestige affects of nuclear weapons as well as being ruinously expensive if capabilities were used in earnest. Such wider deterrence affects have been undermined by asymmetric forces in networks.

199. MAD is a risky game for two; in a multipolar world it is no longer a strategy but an error-prone tactic, at best. Asymmetric forces in network can readily out-flank cost, technical, training, research and sustainability barriers. They can also avoid categorisation as armed force and may be unattributable if used. Dual-use capabilities and the proliferation of knowledge now ranges well beyond the defence and security services of States. Barriers to open and mass-innovation are down. This is what makes cyberspace such a challenging environment in peace and war. Evolutionary Blends of Investments are dynamic whether spurred by healthy competition based on boundless ingenuity or man’s most infernal engine of innovation. The pace and intensity of change means that doctrines and concepts have to mesh in coherent co-evolutionary ways.
200. This affirms the power of Networks-in-Being in which the fitness of bodies can be charted with cladistics\(^{199}\) tracking and anticipating evolving powers. Such genealogical charting applies to sovereign bodies as much as firms. Cladistics put any claims for protective security or the protective state into perspective. The rise and fall of powers and firms demonstrate how pernicious an overweening fixation on certainty has always been. Cyberspace returns us to a state of nature in which we have real options, in particular avoiding the calamities strict rationality will inflict through brittle optimisation. On these terms it is more than academically arguable that cybersecurity is an oxymoron. However, cyber-resilience is pragmatic; for example it can embrace proactive learning from failure:

- Advanced mathematics and modelling can detect emerging *single points of failure*, small world clusters and scale-free networks (e.g. across supply chains in the aftermath of the Japanese tsunami);

- *Fail safe* requirements can learn from Perrow’s Quad to enhance the readiness to act in the event of simultaneous events that confound conventional risk calculus;

- Alertness to good or bad hubs or “superspreaders” in systems that can be designed as *safe to fail* because they decay and grow gracefully; and,

- Striving for cyber-resilience can develop the trust that exploring a rich variety of options need only discover a few asymmetric “superspreaders” to pay-off overall and therefore be confident that many options can and must *fail fast*.

201. Learning from failure is among the most potent ways to learn but under a dominant regime of exploitation, any

---

199. Allen, P (2010) *op cit.* Cladistics is a method of mapping the evolutionary characteristics. In contrast to other methods it is claimed to be more parsimonious and open to falsification.
failures are more likely to result in the blame game than learning\textsuperscript{200}. Meshing concepts with doctrines needs a healthier attitude to failure. The capacity to innovate needs to thrive on failure rather than just talking up success in predictable fashions\textsuperscript{201}. Learning from failure or its anticipation promotes resilience because it spurs the creation of diversity and selection options vital to propelling innovation. The traction gained owes much to developing the confidence to confront our fears. Cyberspace provides little or no shelter from uncertainties. Meshing doctrine and concepts to gain traction and the confidence to learn through innovation is vital.

\textsuperscript{200} For a neat summary of these points, see, The Economist (2011) Schumpeter: Fail Often, Fail Well, p. 75, 16th Apr – 22nd Apr.

\textsuperscript{201} National Audit Office (2009) Helping Government Learn, Report by the Comptroller and Auditor General and also, see, former Head of the Office of Government Commerce (OGC), Sir Peter Gershon’s comments on project and programme management reported in, for example, “UK IT projects must pull up socks, says hefty maven: Public sector is ‘swirling mass of unprioritised initiatives’”, The Register, 22nd Oct ‘10 available at http://www.theregister.co.uk/2010/10/22/gershon_government_it_failures/ accessed 31st Apr ‘11.
Summary

1. **Cyber is a new domain throwing up unprecedented challenges for traditional elites.** Interactions through networks reach into each of our lives opening up our capacity to affect powerful forces and be affected by them across many boundaries. Networks have transformed our economic, financial, political and social affairs; even our social consciousness has been transformed. Traditional levers of power are being rendered less effective, appropriate and legitimate. Orthodox views on questions of competency and sovereignty are being challenged. The distinction between users, consumers and developers is blurring.

2. **Cyberspace is transnational, diffuse and subversive of traditional power structures.** Crises – decisive turning points - are now the norm, not the exception. Leaders and decision-takers – elites - are confused about what competencies, capabilities and capacity befit cyberspace and how, and even whether, to control the cyber domain with traditional, orthodox approaches. This is particularly true when it comes to considering who or what are the competent authorities, how evolving capabilities can be integrated and organised, and how we can incorporate within these the ever more essential capacity to innovate.
3. This unprecedented novelty causes people’s responses to swing between alarmism and scepticism, potentially frustrating our capacity to learn the right lessons. In many ways, we are failing. Partly this is due to attempts to meet the new challenges with approaches, concepts, constructs and institutions inherited before the official recognition of cyberspace as an environment. They are inadequate for the task. They may be necessary, but are altogether insufficient; they are patching over challenges, rather than organically developing with them.

4. But within cyberspace itself, there is the potential for developing a sustainable resilience that will supplement existing practices by focusing on the gaps. In doing this, we need to avoid approaches that are reactive, fragmentary and easily overtaken by events; and to promote those that are proactive, integrative and cultivating evolutionary strength.

5. And there are pre-existing tools and approaches that are more befitting and rewarding when meeting the challenges of the Cyber Age. These are attuned to the productive forces of today and into the future.

6. Key to this is the question of developing concepts and doctrines. Based on accessible principles and active learning, an evolutionary approach to doctrine can act as a bridge between (and avoid the pitfalls of) a more static “legalism” and ill-informed action. The former relies on adherence to law as it stands rather than embracing the politics of law-making necessary for evolving fitness. The latter, especially when taken arbitrarily and in emergencies, throws up the twin perils of exceptionalism and decisionism.

7. Based on this, we can develop a greater depth of resilience for the challenges presented. Resilience to crises is the product of pragmatism. And it is dynamic. It deals with networks as they
evolve. Evolutionary perspectives avoid a nostalgic (or lazy) reliance on past approaches and the fixation on false precision, drawn from what is easy to count today.

8. Cyber Doctrine can provide a framework for learning resilience on these terms. Resilience requires moving forward rather than just “bouncing back”. Meshing concepts and doctrines requires focus on:

- Composability (concerning the pragmatic permutations for integrating capability options across the flow of time); and

- Tractability (concerning gains and losses of power in evolving combinations of capability options running with the flow of time).

9. Such an approach assists in reducing systemic risk, irre-silience and waste, and spurs innovation and exploration (as opposed to mere exploitation of existing capabilities). Doctrine can facilitate good design and scaling of capabilities. It can also support the selection of permutations of capabilities as befits fast-changing circumstances (the issue of composability) and cautions against the dangers of addressing the minutes at the cost of the hours (inherent in “transformation in contact” approaches and managerialist practice).

10. These changes and challenges are compounding, even as we write. Not least in productive forces and relations introduced by networks; across producers suppliers, consumers, finance and distribution; in data and information flows and collection; in investment research and development; in economic reasoning; in training and, especially, educational needs. All of which demand an even greater emphasis on creativity, innovation and entrepreneurship (actual and
cultural) in value creation and productivity, when short-term expediency and present-capability-optimisation is the norm. In short, in thinking “outside the box” (for the box walls have fallen) for everyone.

11. If the Big Society is the reciprocal of the shrinking State, the security and resilience of cyberspace could well throw up the Big Society’s most acid test. Here again, an innovative and evolving doctrine-based approach offers a framework for meeting the challenge and embedding resilience.

12. Fortunately, there are some general lessons that signpost the most fruitful way ahead. The fabrication of certainty in cyberspace through over-codified treaties and increasing reliance on conventional risk calculus makes the challenges of cyberspace incompressible and intractable for anybody – big or small. Uncertainty is ultimately irreducible, making decisions unavoidable.

13. The challenges of cyberspace are not necessarily intractable. Cyber doctrine offers a framework for enabling coherent decisive actions because it makes learning the core enduring activity from which the capacity to innovate germinates. Learning is an uncertain business. But composable ecosystems of capabilities can be assembled across and through time.

14. It may be that cybersecurity is illusive while Cyber Resilience is realistic and pragmatic. Success will owe much to designing evolutionary processes that are fail safe, safe to fail and fail fast. This makes productive the blending of exploitation and exploration.

15. These general principles have important implications for the UK (or any other country grappling with these challenges). The appropriate handling of Cyber issues is now being publicly
identified as a matter of worldwide strategic importance in economic and security terms. Cybersecurity (and information assurance) is now at the centre of Government future investment strategies. In the UK, Baroness Pauline Neville-Jones, as the then Minister of State for Security, has stressed the importance of having governance regimes that makes the UK a location of choice for internationally trusted operations. The failure to create and enforce such governance regimes will lead to the UK inevitably becoming overly reliant on systems over which it would have little or no serious influence.

16. Moreover, we contend that if the UK is to retain its reputation for trustworthy and reliable networks at home and abroad, there is no room for complacency. Strategies need to evolve fast, based on the learning of resilience that developing Cyber Doctrine can enable. Doing so is of immediate and enduring value, for reasons including:

- Better safeguards against loss of Intellectual Property
- Business gains in competitive edge in global markets (commercial security).
- Benefits from IT efficiencies.
- Greater confidence in public service transactions.
- Wise efficiencies and economies from migration towards a national ‘Computer Cloud’.
- Development of a work force confident with the uptake of mass and open innovation.
Cyber Doctrine

- An advancing economy grounded in evolutionary capabilities that underpin the competitive advantage of firms and nations;

- A crucial role in countering Cyber Crime.

17. These do no more than begin to indicate the potential benefits and savings achievable through building trust in Government, commercial and private networks based on learning resilience.

Recommendations

18. The nature of the challenges outlined in this paper requires urgent and significant action. In recent years the daunting challenge of responding to the new, ever-changing implications of cyberspace has presented severe challenges to government and institutions, corporate and individual, private and public, national and transnational. The response so far has been piecemeal on many fronts.

19. The pattern of reactive and fragmentary actions is consistently overtaken by events cascading through networks. Perhaps understandably so. Cyberspace is transnational yet thinking in most bodies remains national and / or international. Cyberspace is more diffuse and invasive, entailing simultaneous actions in many dimensions and levels. The cyber environment envelopes all sections of society, making coherent cross-societal actions essential. Since cyberspace constantly evolves, so must the behaviours of bodies in this environment. It is a daunting challenge. There is no route map for this journey.
20. But we can use tools for navigation. In this paper we have tried to supply a framework for using navigation instruments. Doctrine. We do not pretend that this is fully comprehensive, sufficient or near completion. A unitary, uniform or exclusive doctrine will be inadequate. To provide a framework for learning doctrine has to emerge from multilateral debate that welcomes plurality. By its nature cyberspace would make a mockery of anything less. Multilateral, plural and coherent doctrines are feasible. They are necessary. And their support for continuous learning urgent. Even on a journey whose destination is as yet unknown we need a concrete starting point. For the UK, we recommend:

- The immediate creation of a joint Task Force to include Academia, Government and Industry
- The Task Force should be established under a dedicated Minister reporting directly to the National Security Council (NSC).
- The Agenda for the Task Force must be action orientated.
- It must have the capability and expertise to and be recognised as the authority for thought leadership
- Specifically, it should be tasked with:

  (1) The establishment and development of Cyber Doctrine for the UK, which will offer a framework for learning resilience to develop greater depth and breadth to capabilities and capacity for the challenges ahead, not least advancing national competitive advantage.
Cyber Doctrine

(2) Meshing concepts and doctrines to demonstrate the value of blending investments in exploitation and exploration. Develop innovation growth for pragmatism.

(3) Developing transnational liaison, involving the public, private and third sectors (especially academia).

(4) Encouraging entrepreneurship by selecting, training, educating, and examining competent individuals for recruitment and advancement to posts in public, private and academic sectors vital to the continuous demonstration of competent authority in cyberspace.

(5) Incentivising innovation through organising incubators (Cyber Enterprise Zones) as venues for entrepreneurs for all sectors to invest in and catalyse innovations that can be spun out as Joint Ventures with equity shared appropriately.

(6) Creating Hubs (action groups or little platoons) to facilitate any necessary transformations.

(7) Developing (via Hubs) means of measurement and assessment that instrument the capacity for innovation and the production of resilience as a value, not least in terms that insurance can use appropriately to incentivise healthy behaviours.

(8) Developing (via Hubs) open source tools and apps that evidence the value of information sharing by enabling the mapping of evolutionary capabilities (as ecologies of competencies and technology) across and through time.
21. These recommendations may be UK centric but are situated within a clear understanding that cyberspace is a transnational environment. Frameworks for learning resilience must be the product of multilateral debate that welcomes plurality. Evolving concepts and doctrines produce the syllabuses for continuous learning that enhances the capacity for innovation. They are also the embodiment of principles that keeps the politics of lawmaking true to a healthy pragmatic course avoiding the rock and the hard place of legalism and exceptionalism. Together, evolving syllabuses and legal principles can offer desirable and measurable outcomes for the betterment of everyone immersed in cyberspace.
Cyber Doctrine
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BoI</td>
<td>Blend of Investments</td>
</tr>
<tr>
<td>CIL</td>
<td>Customary International Law</td>
</tr>
<tr>
<td>CIS</td>
<td>Communications &amp; Informations Systems</td>
</tr>
<tr>
<td>CNI</td>
<td>Critical National Infrastructure</td>
</tr>
<tr>
<td>CPNI</td>
<td>Centre for Protection of National Infrastructure</td>
</tr>
<tr>
<td>CSIS</td>
<td>Centre for Strategic and International Studies</td>
</tr>
<tr>
<td>CSOC</td>
<td>Cyber Security Operational Centre</td>
</tr>
<tr>
<td>DCOG</td>
<td>Defence Cyber Operations Group</td>
</tr>
<tr>
<td>DIB</td>
<td>Defence Industrial Base</td>
</tr>
<tr>
<td>DICK</td>
<td>Data, information, communication, knowledge</td>
</tr>
<tr>
<td>DIG</td>
<td>Delivery-Innovation-Growth</td>
</tr>
<tr>
<td>DOD</td>
<td>US Department of Defense</td>
</tr>
<tr>
<td>DSDM</td>
<td>Dynamic Systems Design Method</td>
</tr>
<tr>
<td>DSGE</td>
<td>Dynamic Stochastic General Equilibrim</td>
</tr>
<tr>
<td>ETS</td>
<td>Emissions Trading System</td>
</tr>
<tr>
<td>GSOC</td>
<td>Get Safe Online Campaign</td>
</tr>
<tr>
<td>HLEG</td>
<td>High Level Expert Group (for the ITU plenipotentiary conference 2010)</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td>IFRS</td>
<td>International Financial Reporting Standards</td>
</tr>
<tr>
<td>IHL</td>
<td>International Humanitarian Laws of Armed Conflict</td>
</tr>
<tr>
<td>IP</td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunications Union</td>
</tr>
<tr>
<td>MAD</td>
<td>Mutually Assured Destruction</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Governmental Organisation</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NSC</td>
<td>National Security Council</td>
</tr>
<tr>
<td>OCSIA</td>
<td>Office of Cyber Security and Information Assurance</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OGC</td>
<td>Office of Government Commerce</td>
</tr>
<tr>
<td>OGD</td>
<td>Other Government Department</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budgets</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PDD</td>
<td>Presidential Decision Directive</td>
</tr>
<tr>
<td>PFI</td>
<td>Private Finance Initiative</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PKE</td>
<td>Public Key Encryption</td>
</tr>
<tr>
<td>PPP</td>
<td>Public-Private Partnership</td>
</tr>
<tr>
<td>PRINCE</td>
<td>PRojects IN Controlled Environments</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and development</td>
</tr>
<tr>
<td>RBN</td>
<td>Russian Business Network</td>
</tr>
<tr>
<td>REC</td>
<td>Radio Electronic Combat</td>
</tr>
<tr>
<td>RMA</td>
<td>Revolution in Military Affairs</td>
</tr>
<tr>
<td>RoI</td>
<td>Returns on Investment</td>
</tr>
<tr>
<td>SDSR</td>
<td>Strategic Defence and Security Review</td>
</tr>
<tr>
<td>SIPRNet</td>
<td>Secret Internet Protocol Router Network</td>
</tr>
<tr>
<td>SMEs</td>
<td>Small and Medium-Sized Enterprises</td>
</tr>
<tr>
<td>SSADM</td>
<td>Structured Systems Analysis Design Methods</td>
</tr>
<tr>
<td>TEPID OIL</td>
<td>Training, Equipment, Personnel, Information, Doctrine, Organisation, Infrastructure and Logistics</td>
</tr>
<tr>
<td>TNC</td>
<td>Trans-National Corporation</td>
</tr>
<tr>
<td>TWAIL</td>
<td>Third World Approaches to International Law</td>
</tr>
<tr>
<td>UKTI</td>
<td>UK Trade &amp; Investment</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>UNCLOS</td>
<td>UN Convention on the Laws of the Sea</td>
</tr>
<tr>
<td>UNODC</td>
<td>UN Office on Drugs and Crime</td>
</tr>
<tr>
<td>UOR</td>
<td>Urgent Operational Requirement</td>
</tr>
<tr>
<td>VAR</td>
<td>Value at Risk</td>
</tr>
<tr>
<td>VIX</td>
<td>Volatility Index</td>
</tr>
<tr>
<td>WEF</td>
<td>World Economic Forum</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organisation</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organisation</td>
</tr>
</tbody>
</table>
Cyber Doctrine

‘Cyber Doctrine: towards a coherent evolutionary framework for learning resilience’ is the inaugural publication from the Institute for Security & Resilience Studies (ISRS) at University College London. Drawing on work and with input from cybersecurity practitioners, technology specialists, legal experts, policy makers, entrepreneurs and academics, it identifies the major challenges faced by anyone seeking to ensure the security, exploitation and exploration of cyberspace.

"Cyberspace both enriches and endangers our lives in unprecedented ways. Today, constant vigilance is only half the task in affirming our freedom and security. The greatest rewards will flow from unrelenting innovation – and the healthy competition and cooperation it inspires. This is the key to resilience: thriving on bouncing forward, and not simply bouncing back."

Rt Hon Lord Reid of Cardowan, Chair, ISRS.