



Defence Academy
of the United Kingdom

The Global Cyber Game

The Defence Academy Cyber Inquiry Report



Professional Skills for Defence & Security

About the Defence Academy

The Defence Academy provides education and training in a broad range of subjects - including command & staff, leadership, defence management, languages, acquisition and technology - for members of the UK Armed Forces and Defence Civil Servants. The Academy is also the MOD's primary link with UK universities and international defence educational institutions. Our work serves to enhance the understanding, skills and competences of our Service and civilian personnel so that they are able to respond swiftly and imaginatively to the challenges of an increasingly uncertain world. Our teaching is underpinned by cutting-edge research by our academic partners, ensuring that education at the Academy is vibrant, current and relevant.

In delivering education and training, it is our responsibility to prepare senior decision makers for the uncertainties and complexities of the challenges ahead. To that end, we recognise the value of research that has the potential to enhance our own thinking. "*The Global Cyber Game*" report is a good example of this. The Academy's Research and Publications Portal provides a single point of access to a wealth of research material as well as links to Subject Matter Experts and Communities of Practice and can be accessed via our website: www.da.mod.uk

The open source Cyber Inquiry underlying this Report is characterised by its independence of approach and the spread of contributions drawn from UK and internationally. Specifically, the Report proposes *The Global Cyber Game* as a tool of strategic, policy and operational analysis. As an Academy, we will consider ways to draw on the ideas in this report to enrich the education of our students and contribute to the Game's further development in the coming year. If you would like to do the same, or simply increase your understanding of the work done so far, contact details for the team that produced the Report are provided in this document. For further information about educational and training opportunities at the Defence Academy please visit our website.

The Defence Academy Cyber Inquiry Report

The Global Cyber Game: Achieving strategic resilience in the global knowledge society

Report author: Hardin Tibbs

Cyber Inquiry Team: Susan Ambler-Edwards,
Michael J Corcoran, Hardin Tibbs

This report presents a synthesis of the findings of the Defence Academy Cyber Inquiry. This programme of work, based entirely on open source material, was designed to respond to a strategic research question posed by the Ministry of Defence. The Inquiry's overall remit was first to consider the broad question 'how should the cyber domain be conceptualized?' and in the light of that to examine the implications for security strategy generally, the issues raised for state actors in the Internet age, new power relationships, possible sources and modes of future conflict, and the steps that need to be taken to prepare for a range of plausible possibilities. This report gives an overview of the Cyber Inquiry's big-picture conclusions. It represents a cross-section through a highly multi-dimensional field of research and, inevitably, at this level of detail cannot do justice to the depth of research by the Inquiry into the many specific areas that contribute to a full understanding. Nevertheless, the Cyber Inquiry team believes that what is presented here is a balanced strategic assessment of the emerging meaning of security in the cyber era, clarifying the new meaning of security in a world that is now pervaded by networked digital computers. It does this, in part, by proposing the idea of the Global Cyber Game and Cyber Gameboard as a framework that can be used for practical thinking about cyber strategy, and it hopes this template may be persuasive and useful enough to be widely adopted and further developed.

Publisher's Note

The views expressed in this report are entirely and solely those of the author and do not reflect or represent the policy or official thinking of either the UK Ministry of Defence, or any other department of Her Britannic Majesty's Government of the United Kingdom. Further, such views should not be considered as constituting an official endorsement of factual accuracy, opinion, conclusion or recommendation of the UK Ministry of Defence, or any other department of Her Britannic Majesty's Government of the United Kingdom.

Acknowledgments

The Defence Academy Cyber Inquiry team would like to express its appreciation and thanks to the large number of people who assisted in the process of information gathering and discussion that comprised the overall process of the Inquiry and contributed to developing the findings included in this report. The Inquiry was greatly helped by the generosity and enthusiasm of all those who participated, and by the breadth of expertise and experience they provided.

Contact Information

The Defence Academy Cyber Inquiry team can be contacted at cyber@synthstrat.com.

Conditions of Supply—Full Rights

This document is supplied to MOD in accordance with Contract No DSTLX-100064380. The document comprises information proprietary to Synthesys Strategic Consulting Limited and whose unauthorized use may cause damage to the interests of Synthesys Strategic Consulting Limited.

This document is supplied to MOD as a FULL RIGHTS VERSION under the terms of DEFCON 705 (Edn 11/02) and, except with the prior written permission of Synthesys Strategic Consulting Limited, MOD's rights of use and dissemination in the document are limited to those set out in that Condition and the Contract for the use of Full Rights Versions of Technical Deliverables.

Requests for permission for wider use or dissemination should be made to Hardin Tibbs at Synthesys Strategic Consulting Limited at htibbs@synthstrat.com.

Copyright Hardin Tibbs © 2013

ISBN 978-1-905962-99-0

Contents

Executive Summary	2
Preface	3
The Global Cyber Game	4
The Cyber Game and the Internet	6
The power dimension of the Cyber Gameboard	14
The information dimension of the Cyber Gameboard	18
The Cyber Gameboard	31
How the Global Cyber Game is being played	42
Scenarios for the future of the Cyber Game	71
How the Cyber Game relates to cyberspace	81
National strategic priorities for the Cyber Game	91
Recommendations: How to play the Cyber Game	103
Conclusion	107

	Connection Physical data handling domain	Computation Virtual interactivity domain	Cognition Knowledge and meaning domain	
Cooperation Integrative social power (Infopolitik)	7	8	9	<i>Power as positive social reciprocity</i>
Co-option Economic exchange power	4	5	6	<i>Power as balanced social reciprocity</i>
Coercion Destructive hard power (Realpolitik)	1	2	3	<i>Power as negative social reciprocity</i>

Information hardware Information software Information wetware

Graphic: © H Tibbs, 2013

The Cyber Gameboard

Executive Summary

This report presents a systematic way of thinking about cyberpower and its use by a variety of global players. The urgency of addressing cyberpower in this way is a consequence of the very high value of the Internet and the hazards of its current militarization.

Cyberpower and cyber security are conceptualized as a 'Global Game' with a novel 'Cyber Gameboard' consisting of a nine-cell grid. The horizontal direction on the grid is divided into three columns representing aspects of information (i.e. cyber): connection, computation and cognition. The vertical direction on the grid is divided into three rows representing types of power: coercion, co-option, and cooperation. The nine cells of the grid represent all the possible combinations of power and information, that is, forms of cyberpower.

The Cyber Gameboard itself is also an abstract representation of the surface of cyberspace, or C-space as defined in this report. C-space is understood as a networked medium capable of conveying various combinations of power and information to produce effects in physical or 'flow space', referred to as F-space in this report.

Game play is understood as the projection via C-space of a cyberpower capability existing in any one cell of the gameboard to produce an effect in F-space vis-à-vis another player in any other cell of the gameboard. By default, the Cyber Game is played either actively or passively by all those using network connected computers. The players include states, businesses, NGOs, individuals, non-state political groups, and organized crime, among others. Each player is seen as having a certain level of cyberpower when its capability in each cell is summed across the whole board. In general states have the most cyberpower.

The possible future path of the game is depicted by two scenarios, *N-topia* and *N-crash*. These are the stakes for which the Cyber Game is played. *N-topia* represents the upside potential of the game, in which the full value of a globally connected knowledge society is realized. *N-crash* represents the downside potential, in which militarization and fragmentation of the Internet cause its value to be substantially destroyed. Which scenario eventuates will be determined largely by the overall pattern of play of the Cyber Game.

States have a high level of responsibility for determining the outcome. The current pattern of play is beginning to resemble traditional state-on-state geopolitical conflict. This puts the civil Internet at risk, and civilian cyber players are already getting caught in the crossfire. As long as the civil Internet remains undefended and easily permeable to cyber attack it will be hard to achieve the *N-topia* scenario.

Defending the civil Internet in depth, and hardening it by re-architecting will allow its full social and economic value to be realized but will restrict the potential for espionage and surveillance by states. This trade-off is net positive and in accordance with the espoused values of Western-style democracies. It does however call for leadership based on enlightened self-interest by state players.

Preface

The Defence Academy Cyber Inquiry was set up to provide *a strategic overview and assessment of the new nature of security in a world that is increasingly enabled by and dependent on networked digital computers.*

The result is an open source strategic assessment, not merely of what security ‘in cyberspace’ might mean, but of the way security is being transformed more generally in a world of ubiquitous computation and connectivity. Cyber security is interwoven with other security concerns, so the Inquiry’s findings as summarized in this report are relevant to everyone who is interested in the overall development of security issues.

The Inquiry’s working method combined a variety of qualitative strategic research tools, to explore the ‘future anthropology’ of the cyber domain. These included interviewing, sense making, and futures thinking (both horizon scanning and scenario development), as well as decision framing and strategic thinking.

The Cyber Inquiry started by taking the widest possible view of the value of the ‘global information sphere’ and from this worked back to discover what security issues it raised. This approach produces a different perspective than starting with a question about what ‘cyber’ might mean for ‘national security’.

The global information sphere now largely shapes the strategic environment for all geopolitical players. It does not simply add information to the existing situation, it essentially transforms the situation, undercutting many customary assumptions. To understand how this should reset security priorities means projecting the future path of the global situation, and reflecting on the way different assumptions about strategic interests may lead to significantly different outcomes.

This report looks across a variety of scales of observation, to consider how geopolitical players are struggling to transition from the old industrial world into the new information era, the cyber-enabled trends that are operating within the field of security itself, and the new strategic imperatives that are emerging because of these changes.

By thinking about the forces that are transforming security this way, a fresh strategic perspective can be formed. This perspective provides a foundation for assessing the overall significance of the cyber challenge, for determining how well-adapted we are to the emerging conditions, for considering the implications for national security (broadly framed), and ultimately for deciding how cyber capability should be used, by whom, under what circumstances, and for what purpose.

Overall, this report offers a wide strategic review of the cyber question, aiming to present it in a way that is both balanced and proportionate, and at the same time adequately reflecting cyber as a major driving force of future change. What it does not do is discuss cyber security at a technical level, or in terms of practical actions to be taken by individual computer users, as both have been extensively covered elsewhere. This report’s focus is strategic.

The Global Cyber Game

There are many possible analogies for what is happening internationally in the cyber domain, but an illuminating one is that a new kind of global game is being played out. The idea of a game covers a span of meanings from open-ended play to competitive sport, in which skill, strength or luck may determine the outcome. It also invokes the idea of game theory, in which the interactions of groups of people are studied and the results of different kinds of play may be worked out in advance. Games also range from open ended puzzles, such as the tangram, to contests with a clear winner. A game can be finite and time-bound, or infinite and universal, with echoes of Herman Hesse's *Glass Bead Game*. The beauty of the game analogy is that it captures the highly multidimensional and still puzzling nature of the cyber domain, as well as its clear evolution into an arena for business competition and geopolitical power plays.

The Global Cyber Game, as envisaged here, is a worldwide effort to achieve information-enabled advantage. It is a contest to gain a competitive edge through the most effective application and orchestration of knowledge and information capability. The Cyber Game spans the infrastructural, computational and cognitive aspects of information. The game has come to prominence, indeed been made unavoidable, by the advent of digital technologies and cyberspace, although it is as much about a mode of organization as it is about technology.

The game can be considered as a 'competition' because although it may involve physically violent conflict, it does not need to do so, and quite probably will usually not do so, given the global trend away from violent conflict. Nevertheless, the Cyber Game spans several distinct modes of 'competition', running from new forms of interstate war, through new types of criminal activity, to new forms of civil society struggle, and even new forms of constructive civil society interaction.

The game analogy is helpful for framing cyberpower and cyber strategy because it allows the possibility of striking a constructive balance between competition and cooperation, and because it clarifies the various components involved in a game, highlighting the key features of what is otherwise a very complex strategic puzzle.

The first component of a game is a playing field or, in this case, a 'Cyber Gameboard' which is global, and formed from the intersection of power and digital information processing and exchange. Second, there are players, who range widely: from nations, to ordinary citizens and consumers, to businesses, to politically- and ideologically motivated non-state actors, to serious organized crime networks. All have relatively unconstrained access to the Cyber Gameboard, though with varying degrees of technical sophistication. Third, there are the rules of the game, which are just beginning to emerge, though until now it has been something of a free-for-all. Fourth, there is the nature of play and the objective of the game, which is where the emerging outlines of cyber strategy can be discerned.

The Cyber Gameboard provides a framework for thinking about the global information space formed by the entire nexus of computers and telecommunications networks, including their

hard and soft infrastructures and their associated flows of information, and human cognitive interaction with the information.

Play on the Cyber Gameboard implies the use of cyberpower—power exerted through or against information. This is feasible thanks to the new information infrastructure which, perhaps unintentionally, has the side-effect of allowing continuous threats to and from information.

Information is not merely susceptible to power; power and information form a reciprocal relationship on the gameboard. Power is able to act against or through information, but at the same time information helps to build power, producing some subtle interdependencies that will be explored later.

If the Cyber Gameboard is envisaged as an arena for the exercise of cyberpower, it logically has a ‘cyber’ or information related dimension and a power dimension. Together, these two dimensions form a conceptual framework, the gameboard as described later, that allows various types of cyber gameplay to be analysed. Interpreting the resulting implications for cyber strategy, meaning strategy for the exercise of cyberpower, is one of the main aims of this report.

Before looking at the structure of the gameboard and the game in detail it is helpful to understand what makes the Cyber Game significant, namely the very high value of the Internet and the potential hazards of its current militarization by states.

The Cyber Game and the Internet

The principal reason the Cyber Game is an issue of rising global concern is its potential impact on the Internet.

The Internet is the information processing system that networks almost all the world's computers together into a single interactive medium via global telecommunication systems. The Internet is based on the Internet Protocol (IP) software which addresses and routes small packets of information across the network of networks without requiring a dedicated communication line (the IP is also the basis of isolated networks, not accessible from the public Internet, which also form part of the Cyber Game). This innovation from the 1970s allows the Internet to leap far beyond the capacity of the old circuit-switched telephone system.¹ That depended on switching in an inefficient dedicated link between any two parties who wanted to communicate, the equivalent of connecting them with a private road. The Internet, in contrast, carries a continuous stream of packets between all communicating nodes, and can re-route around blockages, rather like the flow of cars on a public highway. This has allowed exponential growth in information exchange and interaction, accompanied by an equally rapid rise in stored information content, and an enormous proliferation of information services and applications affecting all areas of the economy and culture.

The spread and success of the Internet was not expected, though the very great efficiency with which it uses communication channels might have made this predictable from a technical point of view. From its early experimental beginnings it has gone on to become a major global asset shared, essentially, by all of humanity. The fact that it is human-made, unlike many other shared resources, means it also needs to be actively kept in being by continued cooperative decision making among its stakeholders. This in turn depends on a widespread appreciation of its value.

The public Internet, and the World Wide Web it enables, link the whole world together, quite literally, into a single shared communication space. This has unleashed enormous creativity and initiative, producing solutions for a world of seven billion people that could not have been provided by any other means.

The Internet is now the primary enabler of the world's globalized economic system. It is relied on for financial transfers and exchange, market and commercial transactions, coordination of transport and supply chain logistics, distributed manufacturing systems, engineering and design teamwork, management communications, geographic positioning, infrastructure services such as power and water, news reporting, weather forecasting, advertising, product documentation and instructions, customer feedback—in short just about everything that makes the globalized economy work.

The value of the Internet

The exact value of the enabling and coordinating role of the Internet is hard to assess, as without it the economy as a whole could not function at its current level of transactions. However, research by McKinsey in 2011 showed that when Internet consumption and

¹ John Naughton, *A Brief History of the Future* (London: Phoenix Paperbacks, 2000), p.123

expenditure is measured purely as a sector of the economy, it is now bigger than agriculture or energy. On average, for the 13 countries covered by the research, it now contributes 3.4 percent to GDP, and its total contribution worldwide is equal to the GDP of Spain or Canada, and growing faster than Brazil. In relative terms, the United Kingdom was in second place, with an Internet contribution to GDP of 5.4 percent, behind Sweden, but ahead of the United States in fifth place with 3.8 percent.²

The Internet is a major source of economic growth. The McKinsey study found that, on average, the Internet had contributed 21 percent to growth in mature countries during the five years to 2009, up from 10 percent for the previous 15 years. It contributed 3 percent to growth in rapidly growing countries. A recent study by the Boston Consulting Group (BCG) expects the Internet economy to grow by more than 10 percent a year, and that it will contribute a total of \$4.2 trillion to the G-20's total GDP by 2016. In other words, if it was a national economy, it would rank among the world's top five. In developing markets, the Internet economy will grow at an average annual rate of 18 percent, and is expected to grow at about 11 percent a year in the UK.³

The Internet is also important for jobs and profitability. Among 4,800 small and medium-size enterprises surveyed for the McKinsey study, use of the Internet created 2.6 jobs for each job lost to technology related efficiencies, and increased profitability by 10 percent on average. In addition, most of the extra economic value is not in the technology sector but in more traditional industries, which capture 75 percent of the benefits. Overall, businesses using web technologies grew twice as fast as others, brought in twice as much export revenue as a percentage of total sales, and created twice as many jobs.

Use of the Internet also correlates with national resilience and the ability to weather a financial crisis. An analysis by David and Matthew Cleevely compares 10 year government bond rates for 15 countries against BCG's e-intensity index, which is based on adoption, expenditure and use of the Internet and e-commerce. This shows that countries with high e-intensity, such as the UK, have far lower bond rates than countries with low e-intensity, such as Spain or Portugal. In other words, this suggests that countries with high e-intensity have also either eliminated or minimized underlying structural problems, or created a flexible and robust economy that can respond more flexibly to shocks and crises, or both.⁴

In the words of the BCG report, 'no one—individual, business, or government—can afford to ignore the ability of the Internet to deliver more value and wealth to more consumers and citizens more broadly than any economic development since the Industrial Revolution.' As things stand, the United Kingdom is well positioned to be a leader in gains from this economic potential.

² http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/internet_matters accessed 18/02/13

³ https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/ accessed 14/02/13

⁴ <http://www.thenbells.com/2012/02/font-face-font-family-cambriap.html> accessed 14/02/13

An analogy with world trade

The value of the Internet is directly comparable with the value of world trade. The principle of comparative advantage has long been the rationale for open markets, with each region specializing in what it does best and exchanging the results. This produces a much more prosperous whole than if each nation struggled to provide all of its own needs, including those it is ill-suited to manufacturing or producing. In an Internet context, goods are not the currency in play; information is. Some of this information is exchanged simply in support of trade in goods and services: contracts and specifications are emailed across the world and credit card payments made for services. These efficiencies alone would be large enough to justify protecting the unity of the network to protect trade, a logic most nations are familiar with. But beyond this there is a second effect. One of the primary impacts of the Internet is a global increase in the quality of decision-making because of the ease with which experts on any topic can be located and consulted. This applies equally to academic collaborations, business decisions, policy deliberations, and personal life.

Although hard to quantify, given the extremely decentralized nature of the effect, the long term impact of generally better decision-making at every level due to the ability to source expertise from anywhere in the world on an as-needed basis cannot be overstated. A typical example is medical outsourcing, in which X-rays taken in San Diego are read by highly trained doctors in Bangalore. The same effect is used in software outsourcing, design agencies operating online and many other areas. But this is simply the commercial aspect of a much wider phenomenon, found when people are debugging or configuring software and looking for help on the Internet, or wondering up how to look after a particularly tricky species of tropical fish.

The help accessed is seldom local. If the Internet were to be Balkanized or subdivided, the odds of finding help on a particular question would drop very quickly, and accumulating mistakes would silently be made all over the world. This may sound abstract, but this kind of passive cooperation is a huge part of the ordinary everyday economic utility of the internet: searching for answers to practical questions. As more expertise is documented, as better tools connect people to the knowledge resources or embodied expertise they need, the more valuable the global network becomes. Over the course of a few decades, this phenomenon is likely to transform human endeavour in invaluable and completely unexpected ways.

Internet vulnerability

However, for its economic and social potential to be realized, Internet connectivity must be capable of growing very significantly, in terms of connected nodes and traffic carried, and remain stable as it does so. Internet traffic growth is accelerating exponentially, and according to Cisco was up 42 percent in 2011. Cisco estimates that Internet traffic could grow from its 2011 level of about 300 Exabytes a year to about 1300 Exabytes a year by 2016 (an Exabyte is a million Terabytes).⁵ Unfortunately the Internet was not designed with the expectation of current or expected traffic levels, or security threats, and has a number of

⁵ http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html accessed 14/02/13

known, and no doubt unknown, vulnerabilities that make it potentially liable to sustained catastrophic outage.

The risks of failure include online actions that can affect the whole Internet, such as the fundamental weakness in the Domain Name System (DNS) discovered by Dan Kaminsky in 2008, that would have allowed takeover of the entire Internet had he not revealed it publicly, allowing immediate steps to be taken to fix it.⁶ Similarly, so-called communication ‘black holes’ that already exist in the Internet could either begin to multiply spontaneously through sheer overload, or could be deliberately triggered, for example by deliberately overloading routers, as in the Internet-wide ZMW-style online attack described by Max Schuchard at the University of Minnesota.⁷ Widespread loss of the Internet through physical damage is also possible, as with the 90 percent reduction in Chinese and Southeast Asian Internet service for several weeks in 2006 after an earthquake in the South China Sea severed six undersea cables 15 kilometres south of Taiwan. Internet failure could also be caused by widespread computer damage, say from an electromagnetic pulse (EMP) burning out all unshielded computers in a very wide area, either caused by a bomb-like device or a major solar flare such as the 1859 Solar Superstorm.

The consequences of prolonged Internet failure would be severe. As Su Tzu-yun, a Chinese military analyst, put it in 2001, ‘as soon as its computer networks come under attack and are destroyed, the country will slip into a state of paralysis and the lives of its people will grind to a halt.’⁸ A study in Finland by Leena Ilmola of the International Institute for Applied Systems Analysis (IIASA) showed that total loss of Internet services in the country would lead to a failure of the food supply within two days.⁹ In short, the Internet is a critical component in the global life support system. It is not an exaggeration to say that the lives of a large proportion of the world’s population depend on it.

Internet insecurity

The Internet was not originally designed with its own security in mind and, as a result, individual nodes (connected computers) are vulnerable to online incursion and attack.¹⁰ Message traffic can be intercepted and the Internet as a whole can be used as a medium for online theft or manipulation of information assets or destructive attacks on information related or real-world assets such as critical national infrastructure (CNI).

The level of online attacks has been rising rapidly for some years and, in the words of Jonathan Evans, the head of the UK’s Security Service, MI5, ‘Vulnerabilities in the Internet are

⁶ An attack known as DNS cache-poisoning, largely prevented by vendor patches that implement source port randomisation in the nameserver <http://www.kb.cert.org/vuls/id/800113> and <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html> accessed 30/03/13

⁷ <http://www.newscientist.com/article/dn20113-the-cyberweapon-that-could-take-down-the-internet.html> accessed 18/02/13

⁸ Frank Gaffney, *War Footing* (Annapolis: Naval Institute Press, 2005)

⁹ Leena Ilmola, presentation at a Strategic Foresight conference at Wilton Park, 13th-17th August 2012

¹⁰ <http://technet.microsoft.com/en-us/library/cc959354.aspx> accessed 14/02/13

being exploited aggressively not just by criminals but also by states,' and 'the extent of what is going on is astonishing.'¹¹

Symantec, a US computer security company, reported that a total of over 5.5 billion malware attacks were blocked by its software in 2011, an increase of 81 percent over 2010. They also reported that web based attacks increased by 36 percent in 2011 with over 4,500 new attacks each day.¹² The definition of 'attack' in such statistics can sometimes include 'pings', which are Internet Protocol (IP) 'echo request packets' sent as probes. These usually fall short of being attacks, so some care is needed in interpreting the data, but clearly the level of the problem is increasing.

Kaspersky Lab, the Russian computer security company, reported that in 2011 the number of browser-based attacks increased from 580,371,937 to 946,393,693 and the number of web-based attacks was 1.63 times the total for 2010. Although this is an extremely steep increase, they comment that it 'points to a much slower rate of growth than we have seen over the course of the past three years. In 2010, we recorded a far greater surge in the number of attempted infections—8 times as many as in 2009.' They say this was because there were no fundamentally new mass-infection methods in 2011.¹³

During 2011 two new black market exploit collections (hacking kits), BlackHole and Incognito, became popular with online criminals. BlackHole appeared in 2010 and costs \$1,500 for an annual license.¹⁴ Black market sales of such kits, and other resources for online crime such as stolen credit card information, are made through online business structures based on elaborate value chains reminiscent of legitimate online commerce.¹⁵

The direct and indirect cost from all types of online crime are hard to estimate but are substantial, roughly in the hundreds of millions of pounds a year in the United Kingdom and in the billions worldwide.¹⁶ The indirect costs tend to be several times larger than the direct costs, since online crime makes consumers and businesses tend to avoid online transactions, imposing costs from loss of the economic benefits already discussed. Clearly this is a serious and growing problem that requires fresh approaches and more focused resources.

There is also the threat of online espionage or attack by state actors. A number of countries around the world are reputed to have a military malware (sometimes called milware) capability, although they have mostly avoided making any official announcements. However, in June 2012 the German government confirmed that its military has an operational top secret 'cyberwarfare' unit.¹⁷ On the same day Google announced that it would be warning

¹¹ <http://www.bbc.co.uk/news/uk-18586681> accessed 07/03/13

¹² <http://www.symantec.com/threatreport/> accessed 14/02/13

¹³ http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011#8 accessed 14/02/13

¹⁴ <http://www.allspammedup.com/2012/07/blackhole-exploit-kit-used-in-conjunction-with-spam-emails/> accessed 14/02/13

¹⁵ Chris Grier et al., 'Manufacturing Compromise: The Emergence of Exploit-as-a-Service' *The Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS)*, (October 2012)

http://www.imchris.org/research/grier_ccs2012.pdf accessed 26/02/13

¹⁶ http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf accessed 14/02/13

¹⁷ <http://www.securityweek.com/germany-admits-existence-cyberwarfare-unit> accessed 14/02/13

Gmail users when it believes their accounts are being targeted by state-sponsored attacks.¹⁸ And in July 2012, President Obama urged support for the proposed Cybersecurity Act of 2012 by describing a dramatic scenario of online attack against US critical national infrastructure (CNI): 'Across the country trains had derailed, including one carrying industrial chemicals that exploded into a toxic cloud. Water treatment plants in several states had shut down, contaminating drinking water and causing Americans to fall ill. Our nation, it appeared, was under cyber attack. Unknown hackers, perhaps a world away, had inserted malicious software into the computer networks of private-sector companies that operate most of our transportation, water and other critical infrastructure systems.'¹⁹

State actors may even act against the Internet itself, something criminals have no intrinsic interest in doing. For example, governments under pressure may be prepared to shut down the Internet in local areas or even in the whole country. This happened in 2011 during the revolution in Egypt, when the Egyptian government ordered local Internet Service Providers to withdraw border gateway protocol (BGP) advertisements. These are needed for online connections to be made, and withdrawing them led to the failure of routing throughout Egypt, which disabled the Internet even though the infrastructure apparently stayed up. The outage lasted for five days and, according to an OECD estimate, caused an immediate loss of \$90m to the Egyptian economy, plus longer term costs due to loss of trust that Egyptian networks will remain reliable.²⁰

Similarly, in late 2012, the Internet was also temporarily shut down in Syria, with 77 networks, 92 percent of the country's total, reported to be offline on November 29th.²¹

Iran has also announced plans to develop a national data network and disconnect itself from the rest of the Internet, not surprising given the level of attacks that have been directed against the country. They also intend to export this kind of online isolation to other countries around the world.²² Arguably, a desperate enough nation could disconnect, and then launch a structural attack on the rest of the Internet, while preserving its own internal network. Of course disconnection would also make it vulnerable to an attack on its entire internal network, without risk to the rest of the Internet.

Ironically, given it is the country that leads the Internet supply ecosystem,²³ the United States itself is reported to be responsible for triggering this attempt to Balkanize the Internet, by

¹⁸ <http://googleonlinesecurity.blogspot.co.uk/2012/06/security-warnings-for-suspected-state.html> accessed 14/02/13

¹⁹

<http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?KEYWORDS=Obama+cybersecurity> accessed 14/02/13

²⁰

<http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm> accessed 14/02/13

²¹ <http://www.wired.com/dangerroom/2012/11/syria-offline/all/> accessed 30/03/13

²² <http://www.haaretz.com/news/middle-east/report-iran-seeks-support-to-censor-internet-disconnect-from-global-network-1.425602> accessed 14/02/13

²³

<http://www.mckinsey.com/~media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technolog>

allegedly using the Stuxnet worm to attack the Iranian uranium centrifuge plant at Natanz. (This intrusion is discussed in more detail later, in the context of games that are played on the Cyber Gameboard.)

Internet governance

At the same time as it is being militarized, there is also a global struggle underway for control of the Internet. This is partly because it was not originally subdivided along national lines. According to Vint Cerf, co-inventor of the TCP/IP protocol and now Internet Evangelist at Google, the Internet was designed to solve the military problem of allowing soldiers to communicate without letting the enemy know their location. The solution was to design the Internet to ignore national boundaries. As a result, according to Cerf, most of the Internet's problems stem from state sovereignty.²⁴ The flip side is that some of the problems of sovereign states stem from the Internet. One of the overarching themes of the Global Cyber Game is the struggle for control of the Domain Naming System (DNS), the one hierarchical aspect of what is otherwise all network. This struggle goes by the more refined name of 'Internet governance', and pits the UN's International Telecommunications Union (ITU) against the Internet Corporation for Assigned Names and Numbers (ICANN) which maintains the DNS system.

The United States and its allies would like Internet governance to stay under the control of the existing group of technical nonprofit and volunteer organizations who have been associated with the Internet since its inception, most of them based in the United States, but with many international members. ICANN is a non-profit organization with representatives from more than 100 countries on its advisory boards, but it does remain technically under the control of the US Commerce Department. This is a source of concern for a group of countries led by Russia and China, who would like to see DNS under the control of the UN's ITU. It also happens that this group of countries is interested in seeing controls over Internet content, which the United States opposes. The United States upholds the idea of Internet freedom, which former US Secretary of State Hillary Clinton describes as the right to use the Internet to 'express one's views,' to 'peacefully assemble,' and to 'seek or share' information.²⁵

The last round of talks of the World Conference on International Telecommunications (WCIT) held in Dubai in December 2012 did not resolve this issue, so for the time being there is an uneasy stalemate.

Summary

As things stand, the Internet is seriously insecure, largely the consequence of past decisions about features of its technical architecture. Internet militarization followed by indiscriminate outbreak of 'cyber war' in, or spilling into, a medium with such enormous potential and high vulnerability, clearly puts everyone's long term interests at risk.

y%20and%20Innovation/Internet%20matters%20-

%20Nets%20sweeping%20impact/MGI_internet_matters_full_report.ashx p.25, accessed 12/09/11

²⁴ <http://www.vanityfair.com/culture/2012/05/internet-regulation-war-sopa-pipa-defcon-hacking> accessed 14/02/13

²⁵ Ibid.

The ability to determine an optimal strategic approach to cyber security concerns would greatly benefit from a way of mapping the positions of the players and the kinds of effects that they can exert on each other, and on the Internet as a whole. This is the purpose of the Cyber Gameboard, which allows the Cyber Game to be analysed in terms of game-like moves.

Two dimensions, power and information, come together to form the Cyber Gameboard and the next two sections look at them in more detail.

The power dimension of the Cyber Gameboard

As already described, the Cyber Gameboard has two dimensions, power and information, reflecting the hybrid character of cyberpower. The specific features of these two dimensions in large measure determine the nature of the Cyber Game and how it can be played, and it is therefore important to consider them in more detail before looking more closely at the Cyber Gameboard itself.

The structure of power

Power is the first dimension of the Cyber Gameboard, and power in geopolitics depends on a number of factors. Geopolitical players are traditionally nations—though the Cyber Game expands this—and the power of nations is usually considered to be a function of several types of resource. The classic formula used by Ray Cline (the CIA official responsible for assessing the balance of American and Russian power during the Cold War) took into account population, territory, economic and military strength, and multiplied them all by strategy and will.²⁶ Unfortunately, this did not always produce the right answer, as it failed to capture the weakness and eventual collapse of the Soviet Union.

The idea that power derives from physical resources is convenient, as they are relatively easy to assess, but whether they are effectively deployed depends on complex social and behavioural factors that are much harder to assess. This leads to an alternative view of power as the ability to achieve preferred behavioural outcomes. According to Harvard Kennedy School Professor Joseph Nye, this concept of power as relational has three faces: commanding change, controlling agendas, and establishing preferences.²⁷ The first involves overt threats or rewards, the second attempts to restrict the strategic options considered legitimate by the adversary, and the third attempts to shape the adversary's beliefs and initial preferences.

This conception of power leads to a spectrum of power running from hard to soft. At the hard end is coercion by the use of force, and at the soft end is the possibly unnoticed shaping of the adversary's worldview. In practice a skilful player will combine both hard and soft power elements into effective strategies, an approach that Joseph Nye recommends and calls smart power.²⁸

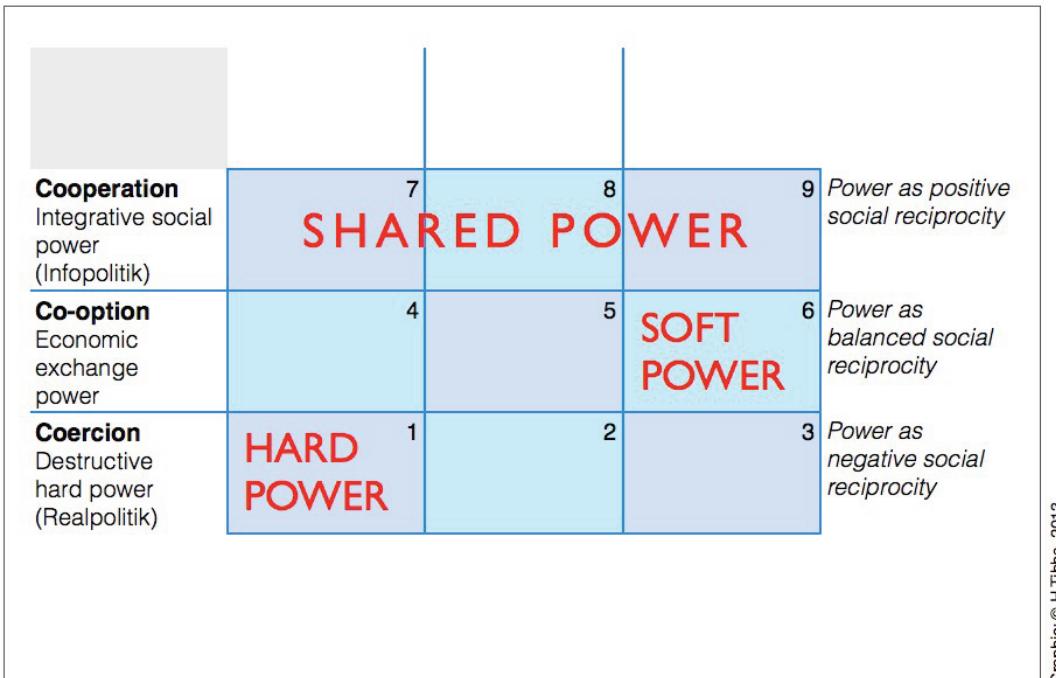
An alternative taxonomy of power has been offered by John Arquilla, Professor of Defense Analysis at the Naval Postgraduate School in Monterey, California, and his co-author David Ronfeldt. He suggests that there are three ways of thinking about power: as resources, as organization, and as 'immaterial'. The organizational and immaterial forms of power are similar to Nye's relational view of power, but seen from the 'supply' side rather than the outcome side. This suggests that power seen as immaterial is, in effect, the supply or delivery side of soft power. Arquilla and Ronfeldt's classification is useful, because it combines the

²⁶ Joseph Nye, *The Future of Power* (New York: Public Affairs, 2011)

²⁷ Ibid.

²⁸ Ibid.

resource and behavioural aspects, and also introduces the idea that power has an immaterial aspect that gives it an interesting convergence with the cognitive aspect of information. It is perhaps less clear what the immaterial aspect of power would mean in practice; in this sense it might be better expressed as psychological power.



Graphic: © H Tibbs, 2013

The power dimension of the Cyber Gameboard

In an influential 1989 study of power, economist and systems thinker Kenneth Boulding also set out a three-level model. Boulding proposed three kinds of power which, when categorized by their effects, he called destructive, productive and integrative. The three behaviours that produce them he called threat, exchange and respect.²⁹

The destructive power category corresponds to military power and the spectrum of coercive power. The productive power category refers to economic power, involving production and exchange. Integrative power introduces the idea of social power, the power to create identification with a social grouping to which people voluntarily give their loyalty.

Integrative power differs from traditional ways of thinking about geopolitical power. Nye, and Arquilla and Ronfeldt, for example, both regard power as essentially coercive. Nye's definition of power is the ability to cause the antagonist to behave in a way preferred by the protagonist. So even soft power involves subtle and possibly unconscious coercion. This coercive principle also appears to apply subtly to Arquilla and Ronfeldt's notion of power as immaterial. Boulding proposed, in contrast, that not all power consists of 'power over' and that there is an important field of shared power based on 'power with'.

²⁹ Kenneth E. Boulding, *Three Faces of Power* (Newbury Park: SAGE Publications Inc., 1989)

This distinction is subtle but important. Austrian cyber analyst Alexander Klimburg, for example, describes a spectrum of power running from hard to soft that he terms ‘coerce, co-opt or convince’.³⁰ Yet even the soft power notion of ‘convince’ at root involves the assertion of one party’s will over another. In contrast, integrative power is built when behaviour is not motivated by self-interest but by goodwill and genuine respect for the other, and a mutual willingness to act for the common good.

Institutions that are primarily based on integrative power include the family at its best, non-governmental organizations (NGOs), charitable and most religious organizations. These organizations are held together primarily by a sense of legitimacy, which is at the core of integrative power. Many other organizations, such as corporations and, at a pre-global stage, nations, attempt to use a degree of integrative power to improve morale and performance, even though they are primarily based on threat or exchange power, but these efforts are increasingly viewed as not fully legitimate. In a period of globalization, when people identify less with their country³¹ and more with global issues, and they network freely with friends around the world, it may well be that legitimacy and ultimate integrative power is moving to the global level. This alone makes integrative power a particularly useful extension to the traditional ways of thinking about geopolitical power.

Boulding’s three types of power also align with a continuum of human interaction recognized by anthropologists. They correspond roughly to three points on the spectrum of social reciprocity, a concept that Boulding does not explore but which is important in cultural anthropology. The anthropologist Marshall Sahlins identified three forms of reciprocity: negative reciprocity, where each party tries to gain at the expense of the other; balanced or symmetrical reciprocity, where people expect a fair and specified return; and generalized (i.e. positive) reciprocity, where giving and receiving is not measured and there is no specified expectation of balance over time.³² Negative reciprocity aligns with destructive power, balanced reciprocity with productive power, and positive reciprocity with integrative power.

Boulding’s formulation is interesting in several ways. First, it is comprehensive, in the sense that it spans the resources underlying power, the behaviours involved in exercising it, and the effects produced. Second, it captures the idea of a spectrum of hard to soft power. Third, it extends beyond the concept of power as necessarily coercive and allows for the power of social solidarity. This is important when a shared global information infrastructure is at stake. Fourth, the three types of power capture the full spectrum of human social reciprocity relationships, important in view of the rising power of networking.

³⁰ Alexander Klimburg, ‘The Whole of Nation in Cyberpower’ *Georgetown Journal of International Affairs* (Special issue, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity, 2011), pp.171-179

³¹ ‘Foresight Future Identities – Executive Summary’ *The Government Office for Science*, 2013
<http://www.bis.gov.uk/assets/foresight/docs/identity/13-524-future-identities-changing-identities-summary.pdf> accessed 08/03/13

³² Marshall Sahlins, *Stone Age Economics* (Abingdon: Routledge, 2011), pp.193-195

Power on the Cyber Gameboard

These different ways of thinking about power all contribute to an understanding of the power dimension of cyberpower. Reflecting insights from all these perspectives, and particularly Boulding's threefold formulation of power, the power axis of the Cyber Gameboard is sub-divided into three types of power: Coercion, Co-option, and Cooperation.

The information dimension of the Cyber Gameboard

Information, the second dimension of the Cyber Gameboard, has always played a role in human affairs, but in the last few decades it has become much more important, as a consequence of the so-called ‘information revolution’. The advent of electronic computers and the ability to network them globally, and now to put one in everyone’s pocket, has transformed the information context in which we all live.

Before the era of electronic computers, information consisted mainly of written or printed documents, and paintings. Recorded information was static, passive, scarce, and relatively inaccessible, and, until the telegraph, there was no technology for sending it instantly over long distances. Now there is a seamless information environment, formed from an underlying electronic infrastructure that creates a connection domain in which information of all types (data, text, sound, and image³³) is stored, processed, and flows freely. This instant multi-way connectedness and digital processing has given information quite new characteristics: now it is dynamic, interactive, abundant, and ubiquitously accessible.

The global information infrastructure in its current form has come into being over the last 50 years, with the most significant developments in just the last 20 years. The physical information infrastructure consists of the totality of telecommunications networks (the cables, satellites, wireless links, switches, routers, storage devices, and servers) that together link the vast number of computers of all sizes distributed throughout the world. Running on this hard infrastructure is the soft infrastructure of the Internet and the applications it supports and, in combination, they conjure up the global information realm usually known as cyberspace, or C-space later in this report.

The essence of the information revolution is that electronic computers and digital communications are acting as powerful amplifiers and multipliers of information. They are driving a fundamental shift from scarce to abundant information that is transformative: as information becomes abundant, the logic of how it acts in situations is flipped. Information has gone from being an output or representation of physical situations to something that dominates and determines them. Abundant information is a game-changer: it is an evolutionary acceleration factor that is transforming the whole global situation, for social, economic and government players alike.

The information revolution

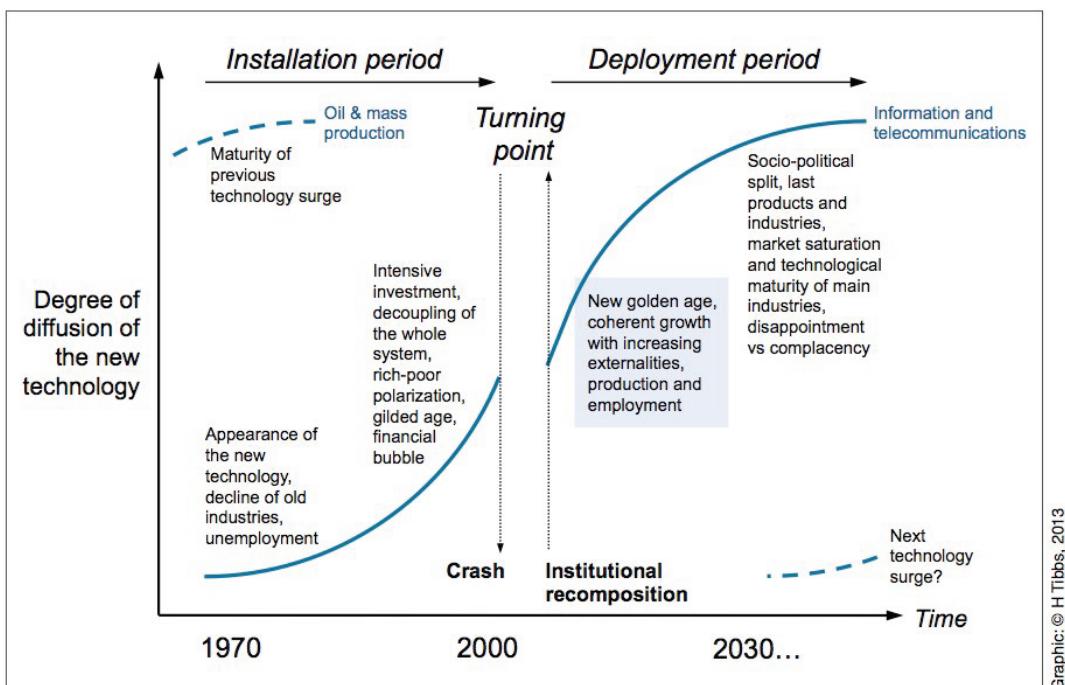
The information revolution is, according to an analysis by Carlota Perez, the latest of five major technological revolutions since 1770.³⁴ Its core technology is the microprocessor, which has been developing exponentially since the 1960s. This growth was predicted by Moore’s Law in 1965, which originally stated that the number of transistors on a semiconductor chip would double every eighteen months (the actual figure turns out to be closer to 24 months), and this has turned out to be remarkably predictive for 50 years. The growing power of microprocessors enabled a similar growth in the power of computers and in the amount, and availability, of information.

³³ Stan Davis, *Lessons from the Future* (Oxford: Capstone Publishing Ltd., 2001) (see a useful diagram on p.35)

³⁴ Carlota Perez, *Technological Revolutions and Financial Capital* (Cheltenham: Edward Elgar Publishers, 2003)

As listed by Perez, the successive technological revolutions are: the industrial or machine revolution starting in 1771; the age of steam and railways starting in 1829; the age of steel, electricity and heavy engineering starting in 1875; the age of oil, the automobile and mass production starting in 1908; and now the age of information and telecommunications starting in 1971.

Based on the typical trajectory of the previous technological revolutions, the resulting 'information economy' is probably halfway through an S-shaped growth curve and will mature sometime between the 2020s and the 2040s. In other words, the first half of the information revolution is now complete and the second half has just begun. Historically, the first half of a major technological revolution, the 'installation stage,' involves the installation of new infrastructure and the transformation of productive activity, while the second half, the 'deployment stage,' involves the transformation of socio-economic organization necessary to fully release the potential of the new technology. The mid-point of the S-curve is also its steepest stage, so the information revolution is now at its maximum rate of growth and just about to enter its most transformational phase.



The Information Revolution

(Source: Adapted from Carola Perez, 2002)

The installation stage of the information revolution was focused on technology, and its adoption and installation around the world led to an exponential increase in computing power, storage and bandwidth. The second half, the stage of full deployment, will be focused on social organization, leading to a fundamental reform of organizations and institutions, for the first time enabling society as a whole to harness the full power of the new technology.

The deployment stage, although it is past the halfway point of the whole revolution, involves the most transformative change for society as a whole. The old institutional structure of centralized hierarchical pyramids with functional compartments has been disrupted, while a new networked institutional structure is becoming clearer and is beginning to diffuse across the system.

The benefit of being part of a network is captured by Metcalfe's Law, which states that the value of a network is proportional to the square of the number of its users. There is some debate about the exact multiplier value of Metcalfe's Law,³⁵ but in broad terms, as more people join the value increases rapidly. This suggests that, setting aside security and other possible limiting factors, the natural economic endpoint is universal connectedness. This forces all players to reorganize in network compatible form, obliging them to devise and adopt corresponding new industry structures and business models.

Eventually there will be a new socio-economic pattern encompassing the entire range of organizations and institutions, spanning global, national and local governments, as well as business and civil society. The deployment of the new pattern will trigger a wave of transformative wealth-creation and social development unattainable in the earlier structure.

Existing organizations and institutions are, therefore, on the threshold of an acute challenge which may not yet be apparent to them. The first stage of the information revolution has been about installing information technology and this may appear to be enough. Now they face the need to fundamentally reconstitute themselves, which means understanding and adopting the new organizational forms and strategic models that will be essential for continued viability and development.

One aspect of the information revolution has become familiar: accelerating, exponential growth in computational power, stored content, traffic levels, and number of participants. But the character of the revolution is about to shift as it is on the threshold of triggering deep socio-cultural changes, which are likely to prove far more disorientating than the purely technological changes that paved their way. Gaining an understanding of the coming changes will, however, rely on a deep appreciation of the effects flowing from the new infrastructure of information that has been installed during the first phase of the revolution.

Information as a game-changer

As already noted, computers and communications are acting as powerful amplifiers and multipliers of information. They are driving a fundamental shift from scarce to abundant information that is transformative because information has some idiosyncratic properties that are becoming more pronounced as information becomes more abundant. These properties demand new thinking and adaptive changes by institutions and organizations, if they are to develop effective strategies for cyberpower and excel in the Cyber Game.

Information abundance and accessibility are progressively altering the whole context in which strategy plays out, changing the nature of actors and how they organize and interact,

³⁵ <http://spectrum.ieee.org/computing/networks/metcalfe-s-law-is-wrong/0> accessed 28/03/13

and giving rise to entirely new modes of economic value creation, social communication, and national power, all of which are reshaping the security landscape.

Some of the changes are clearly apparent and have been widely reported. The new information environment has a number of characteristics that alter the tempo and dynamics of the geopolitical game. These include:

- Speed of information transfer—information is now instantly available between any two points around the world, removing the time buffer that once existed and, in many cases, necessitating an instant response.
- Breadth of information transfer—information can be instantly replicated and distributed to any number of pre-identified network nodes.
- The death of distance—instant global transfer of information eliminates the isolating effect of geographic distance and the autonomy it once conferred.
- Empowerment of individuals—near-zero cost access to one-to-one, one-to-many, and many-to-one communications is giving individuals unprecedented power to influence and organize.
- The rise of networks as an organizational form—networks have always existed in human society, but instant multi-way communication at zero marginal cost is giving networks a relative advantage over up-down hierarchies, which had the edge when message transmission was expensive and it made sense to concentrate information and decision-making at the top.
- Rapid propagation of reactions to information—the phenomenon of news and ideas ‘going viral’ is a consequence of speed combined with empowerment of individual communications.
- Volume of information—automated processing and sending of information, and the rapid growth of Internet connections, is resulting in an exponential rise in the amount of information being generated, stored and consumed. Effort is increasingly being focused on extracting hidden patterns from this data—the ‘Big Data movement’.
- Complexity of processing—information in many forms (numeric, text, audio, image) can be processed and combined in increasingly sophisticated ways to produce ever more complex outputs and new capabilities.
- Openness of information—information about all aspects of society, that was once scattered and hard to access, is now readily available (this includes such things as inconsistent statements made by, for example, diplomats in different contexts).
- Transparency—the ease of copying and distributing information, combined with inherently poor Internet security, means that whistleblowers have a powerful new tool, as WikiLeaks demonstrates. Players must expect even covert actions to become known and that malware will proliferate.

All these characteristics have direct implications for Cyber Game players: responses must be fast, thinking must be holistic and global, decisions must be made in the context of information abundance and transparency, powerful actors will range from organizations to individuals, and capabilities will be relentlessly surprising.

These effects largely arise from the technical attributes of the new information infrastructure, and its acceleration and amplification of information. Although this report does not explore each of these characteristics in detail, it is important to keep them in mind, as they condition the pace and nature of Cyber Game play, and set the context for all interactions on the Cyber Gameboard.

The information dilemma

At the heart of information's idiosyncratic effects there is a fundamental dilemma related to the value of information, which cannot be eliminated by any purely technological advance; indeed it is being intensified by technology.

To be useful, the information environment needs to be as open and interconnected and robust as possible to maximize its network value, both economically and socially and, at the same time, as secure as possible to guarantee the safety of financial transactions, proprietary knowledge and private communications. All users would like these conditions to apply to their own communications, so any lack of these conditions affects all users. No one, not even the most powerful of states, is exempt. At the same time there is a temptation for some powerful users to want these rules to apply to their own communications but not to those of others.

As Stewart Brand famously said, 'information wants to be free.' What is less well known is that he added,

'Information also wants to be expensive. Information wants to be free because it has become so cheap to distribute, copy, and recombine—too cheap to meter. It wants to be expensive because it can be immeasurably valuable to the recipient. That tension will not go away. It leads to endless wrenching debate about price, copyright, 'intellectual property,' the moral rightness of casual distribution, because each round of new devices makes the tension worse, not better.'³⁶

Brand is saying that not only can the tension not be eased by technology, but that advancing technology is actually intensifying the problem.

This is a textbook dilemma. Information needs to be shared to become useful. If it is never used or seen by anyone, it has no value at all. On the other hand, it is also true that the distribution of information must be restricted if it is to have economic value, at least in terms of conventional economics. If it is distributed freely it cannot also be charged for, no matter how valuable it may be to the recipient. Its utility, however, may be unaffected by being freely distributed, indeed it may be increased, as with scientific knowledge.

³⁶ Stewart Brand, *The Media Lab: Inventing the Future at MIT* (New York: Viking Penguin, 1987), p.202

The coding community know the information dilemma in their bones. In the words of one contributor to the Inquiry, contrasting the cyber age with the industrial age, 'Techies understand scarcity completely differently. Talent and connectedness are scarce, code is free. Since the birth of the computer age, software has circulated in a commons.'³⁷ The pressure of the information dilemma is what explains the free software movement, which finds economic value elsewhere.

It is sometimes said that dilemmas cannot be solved, they must be resolved. Somehow the standoff must be transcended by moving to a new position, not by trying to argue for one extreme or the other. Strategic problems can seem intractable when they take the form of dilemmas consisting of two incompatible alternatives, when ideally both would be true at the same time. Finding resolutions is likely to require a reframing of existing thinking.

Policy or strategy needs to be based on the discovery of a new vantage point outside the frame of each dilemma which, when adopted, allows both poles of the dilemma to coexist, even if not in their pure form. This type of resolution allows society to gain the greatest overall benefit, as societies that get jammed at one or the other end of a dilemma tend to become dysfunctional. This stance lies at the heart of several institutional innovations from the Enlightenment period, such as patents, which allow a period of monopoly on inventions in exchange for disclosure (avoiding the less advantageous extremes of either an unlimited monopoly or disclosure which could undermine the economic incentive for exploitation). Arguably, these innovations contributed significantly to the rapid material development of Western nations and indeed the entire globe.

Some problems may be more complex than dilemmas, as in the case of trilemmas³⁸ where three different alternatives would all ideally be true. Nevertheless, the same generic mode of resolution still applies. One management author refers to this type of thinking as 'integrative'³⁹ and makes a case that it is a hallmark of all effective leaders.

Once a strategic resolution is found, its technical implementation in software may well require some ingenuity, but the important point is that technical design should be guided by resolving the tension between fundamental principles, not just by technical convenience. If the idea of 'technical design' is extended to include design of policy and strategy, this can and should be determined in the same way.

The inherent information dilemma between free and expensive—where free has several appealing connotations and expensive signifies various kinds of restricted access—is growing in intensity as a side-effect of information abundance. As Stewart Brand said, technology is making it worse not better. Abundance is a challenge to the core of economics, a discipline based on scarcity from its inception and traditionally defined as 'the allocation of scarce resources among competing wants'. The abundance and accessibility of information therefore undermines many of the forms of scarcity on which traditional economic models

³⁷ From commentary submitted to the Inquiry by Vinay Gupta

³⁸ For example see 'The Shell Global Scenarios to 2025- The future business environment: trends, trade-offs and choices' *Shell International Limited (SIL)*, 2005

³⁹ Roger Martin, *The Opposable Mind* (Boston: Harvard Business School Press, 2009)

and economies have been built. This is beginning to prompt a search for alternative conceptions of economics not based on scarcity. If the technological potential for abundance continues to be obstructed by the chronic instability and failure of existing financial institutions, this search is likely to intensify.

So far, our age has acquired a global technology of infinite instant free⁴⁰ duplication of information: information is now abundant. But abundance goes further. With the advent of information-enabled 3D printers combined with a 'closed loop' of materials we are about to have a technology of precise physical duplication too.⁴¹ When it is fully developed this will be the ultimate technology of abundance, the dream of humans since the dawn of history. But without question this threatens power and business based on certain types of scarcity and, thereby, many of the hallmark institutions of the industrial age. The overarching strategic challenge is therefore to achieve the benefits of abundance while coping with the legacy aspects of the system.

The benefits of abundance cannot be realized if the global-scale flow of information is blocked. This is fundamental. This implies that the highest security priority is the integrity of the global information infrastructure, the most important infrastructure of all in an information age. The security of the critical national infrastructure (CNI), while important, forms a subset of the larger concern. Governments do need to assure the security and connectedness of all the nodes of the Internet physically within their borders, but this involves any other parts of the network which are interacting with those computers, which quickly becomes the entire Internet. This globally extended national interest is the 'critical international information infrastructure'. If governments and defence organizations are wondering what to defend in the information age, this would be it.

The global knowledge commons

Most information does now exist as a vast flow of digital signals in an electronic infrastructure. But information's highest strategic role in the Global Cyber Game is its contribution to the knowledge of humanity as a whole. We now tend to think so instinctively of information as an attribute of technology that it is easy to lose track of its contribution to knowledge, which has its ultimate value in the human mind.

The intangible sphere of human knowledge is, in effect, a 'global knowledge commons,' a domain of social, cognitive and cultural development made possible by ubiquitous knowledge availability and exchange.⁴²

The abundance and accessibility of information is driving enormous worldwide advances in human knowledge. This may present an unwelcome challenge for some incumbent players, but the overall benefit means they are likely to gain more by adapting to and enabling abundant and accessible information than from trying to control and restrict it. Governments can gain influence and prestige to the extent that they open up to and protect information

⁴⁰ Approaching zero marginal cost per copy

⁴¹ *The Economist*, 'The Printed World' 12 February 2011, p.75

⁴² This is similar to the cyberspace component of the global commons concept explored by the 2011-2012 round of the US-managed Multinational Experiment (MNE-7)

flows. Economic players can gain customers by adapting their business models to coexist with maximum information flows. And social players will expect and ultimately demand that government and business do these things as anything else will seem retrograde.

A rapidly increasing part of the world's population now live in a globally connected knowledge society, with an economy that is primarily enabled by digital computers and information processing, and a subordinate industrial economy based on maximizing material production. The transition to knowledge society has high potential value for humanity as a whole, because it promises eco-efficiency innovations that can free us from dependence on industrial-style use of material resources, which will otherwise impose environmental limits, economic constraints, and a risk of global system collapse⁴³. Unlike matter, knowledge is not a finite resource, but its further expansion does depend on the continued abundance and accessibility of information. Seen in this light, the global connectivity enabled by information technology is essential to the future continuity of human civilization.

The information revolution of the last half-century, which enormously expanded the global knowledge commons, also contributed directly to the emergence of global society as a meaningful reality. Global human connection is being forged, not though politics or hard power, but through a spontaneous recognition of interdependence and the oneness of human culture, despite all its diversity and individual differences. This long run trend is reshaping the strategic environment in which national governments interact, and is gradually obliging them to take a 'whole world' perspective, if only from a stance of enlightened self interest.

Digital communications technology therefore represents a key part of the developmental potential for the whole human race and, to a large extent, governments are the custodians of this potential. In the current global period, the ultimate continued justification of national governments is their shared responsibility for facilitating global development, not their competitive defence of restricted patches of geographic territory. Those governments that cling to a zero-sum view of international relations are likely to find themselves sidelined in the Cyber Game much faster than those willing to pioneer a non-zero view of international coexistence and cooperation. This need for a revised strategic positioning is due to information abundance changing the rules of the geopolitical game.

Powershift to knowledge society

A significant aspect of the Cyber Game is that the predominant type of power used by Cyber Game players is gradually shifting as all countries move out of the industrial era and join the global knowledge society. In other words, this move signals a shift in the preferred type of power used, from destructive, through productive, to integrative power.

Knowledge society can be thought of as comprising a knowledge-based economy plus a digitally connected and empowered population. In the industrial period, which still tends to condition perceptions, the economy was based on chemical energy and mass production,

⁴³ Hardin Tibbs, 'Sustainability' *Deeper News publications* (Global Business Network) vol.10, no.1 (January 1999)

and communications relied on one-way broadcast mass media. In knowledge society, the economy is primarily enabled by digital computers and information processing, and communications are based on interactive multi-way networking.

In the industrial economy the classic factors of production were land, labour, raw materials and capital; these have not disappeared, but now they are all trumped by knowledge. This is because knowledge, when appropriately deployed, reduces the requirement for any of the other factors of production.⁴⁴ In other words, a knowledge-based economy is one in which knowledge dominates the other factors of production.

This is significant for the Cyber Game, because it means that the source of power is also shifting to knowledge itself. In any given technological era, the dominant means of production is also the dominant source of geopolitical power. In the industrial era, power was derived from mass production capability, the capacity to produce very large numbers of tanks, planes, trucks, guns and bombs, and the ability to use them to project maximum levels of kinetic power. In contrast, any strategic competition within global knowledge society will tend to focus on knowledge itself as the key source of power, because of its ability to achieve the effects of industrial-era power while simultaneously reducing the actual amount of industrial power required.

In terms of hard power, in the industrial era the military objective was a bigger bang for the buck, whereas in the knowledge era the aim is a more precise bang for the buck, meaning that there is a smaller bang overall. In technical terms, this is equivalent to saying that the mass- and energy-intensity of geopolitical power projection is being reduced, while the knowledge intensity is increasing.

A well-publicized example is that the addition of information technology to weapons makes them far more accurate. This is illustrated by a historical comparison. By the 1990s, one F-117, flying one sortie and dropping one smart bomb, could achieve the same 'hit probability' as 44 B-52 bombers dropping 176 dumb bombs during the Vietnam War, or 3,024 sorties by B-17s dropping 9,070 dumb bombs during World War II.⁴⁵ Today, the ratio of information technology to the mass and energy of weapons has shifted even further, with ever-smaller drones rapidly evolving into remote assassination weapons, capable of killing targeted individuals from thousands of miles away.

Increasing knowledge intensity has paradoxical consequences for traditional notions of hard power. If the essence of hard power is the application of kinetic coercive force, then increased knowledge intensity reduces the kinetic force required to achieve a given effect. It reduces the 'hardness' of the power delivered, despite the weapon becoming more effective. This overturns thinking about total war that goes back to Clausewitz, who wrote: 'War is an act of force, and to the application of that force there is no limit.'⁴⁶ Adding intelligence to weapons

⁴⁴ Alvin Toffler, *War and Anti-War* (London: Warner Books, 1994)

⁴⁵ Richard P. Hallion, Precision guided munitions and the new era of warfare, *APSC Paper Number 53*, (1995) <http://www.fas.org/man/dod-101/sys/smart/docs/paper53.htm> accessed 30/03/13

⁴⁶ Karl von Clausewitz, *On War* (New York: Random House Inc., 2000) p.266

means that the use of maximal achievable kinetic force is no longer the inevitable tendency in war.

Greater precision also demands more thoughtful targeting (e.g. 'full spectrum targeting', that tries to take into account systemic effects) because although the amount of kinetic force is getting smaller the relative effect is increasing, making the meaning of any strike within the surrounding information environment more significant. Much closer attention must therefore be paid to the perceived significance and possible unintended systemic consequences of any kinetic (or cyber) strike. The soft power context is becoming more important. This is, in effect, increasing the ratio of strategic thinking to kinetic force demanded in knowledge-era conflict, another aspect of increasing knowledge intensity. Making weapons smarter does not make antagonists smarter, but it does push them in that direction.

As information progressively shifts from being subsidiary to physical situations, to determining and dominating them, it changes both the context and significance of all physical action. This is why making weapons smarter changes their primary impact from the physical to the informational context.

It is also why there is a trend, described by Joseph Nye, from hard power to soft power as a result of the shift in relative advantage from coercion to persuasion in an information-rich environment.⁴⁷ This trend is apparent in an analysis by Javier Noya of public survey research in Spain, to identify the form of power associated with what he calls pre-modern, modern and post-modern countries. The power of pre-modern countries is seen to derive from geographic size and population; the power of modern countries to depend on their economy, technology and military; and the power of post-modern countries is seen as based on factors such as culture, democracy, language and international aid and cooperation.⁴⁸

Against the background of an ongoing trend from modernity to post- or trans-modernity,⁴⁹ the 'cyber powershift' is contributing to a gradual global shift from realpolitik, the past reality that purely physical power is dominant, to what might be called 'infopolitik,'⁵⁰ in which future power will increasingly be wielded by means of the information environment. Of course for some time to come, the actual situation will be a mix of these two realities, and perceptions are likely to be confused as to which has the upper hand. This is because not all Cyber Game actors are equally far advanced in their development of information era capabilities, as is indicated by the BCG's e-intensity index discussed earlier. State actors form a cohort in transition towards global knowledge society, but with a wide distribution between the trailing and leading edge players. In geographic terms, the Cyber Gameboard is a patchwork of uneven development, and infopolitik will supplant realpolitik for some issues and in some parts of the world faster than others.

⁴⁷ Nye, *The Future of Power*

⁴⁸ Javier Noya, 'The Symbolic Power of Nations' (Translation from Spanish) *Elcano Royal Institute Working Papers* vol.2005, no.35 (2005)

⁴⁹ Hardin Tibbs, 'Changing Cultural Values and the Transition to Sustainability' *Journal of Futures Studies* vol.15, no.3 (March 2011), p.13-32

⁵⁰ Arquilla and Ronfeldt have suggested the more exotic word 'noopolitik' for this new mode

Information becomes reality

The final point to be made about information is that our conception of its nature is shifting. Instead of thinking that information is about things, some scientists are starting to think that things are the result of information.

According to biologist Gregory Bateson, a brilliant early proponent of cybernetic theory and systems thinking, the essence of information is the detection of difference. As he pointed out, the sensory systems of biological organisms are tuned to respond only to change or difference.⁵¹ When nothing changes, nerves don't fire. Similarly, in Shannon's information theory information is essentially surprise, the appearance of a new pattern of differentiation, the opposite of undifferentiated disorder or entropy.

Differences, as it happens, are created by power, that other dimension of the Cyber Gameboard. When difference is detected it becomes information. In the hands, or mind, of an intelligent player, this information then guides the next application of power. Hence knowledge is power, as Sir Francis Bacon observed in 1597. But what if this equivalence runs much deeper?

If your idea of information is something captured by quill on parchment, you have a very different sense of it than if you have witnessed a virtual reality simulation or seen the portrayal of future immersive virtual reality, for example the holodeck on Star Trek, or the Matrix in the film of that name. It is a small step (at least in retrospect) from the idea that a simulacrum of 3D reality can be created entirely from information, to the idea that reality itself may be a simulation of some kind generated from information. What if this actually works as physics? Since the 1990s it has been possible to explain the universe scientifically as a giant quantum computer that essentially computes itself.⁵² In this still radical view, we would be part of an enormous holographic computer output in which the Planck time (the shortest possible time according to physics) is the refresh rate of the display, and the Planck length (the shortest possible length) is the pixel⁵³ size, assuming, that is, that the computer turns out to be digital⁵⁴.

This type of thinking shifts the centre of gravity of our understanding of information from being something derivative to being something generative. And this generativity, this creativity, has its source at the level of cognition and ideas, giving weight to the view that ideas shape reality. This now becomes demonstrable, more evidently obvious, thanks to the new abundance and dynamism of information, which allows us to see how it actively shapes outcomes. The intangible now determines the tangible. The software in the avionics system determines the flightpath of the plane. Big data determines what a business communicates to a customer. The real value, the lasting strategic advantage, lies in using knowledge to shape new outcomes. It does not lie in disrupting the flow of information that is sustaining existing outcomes, or in damaging or endangering the infrastructure that is allowing the

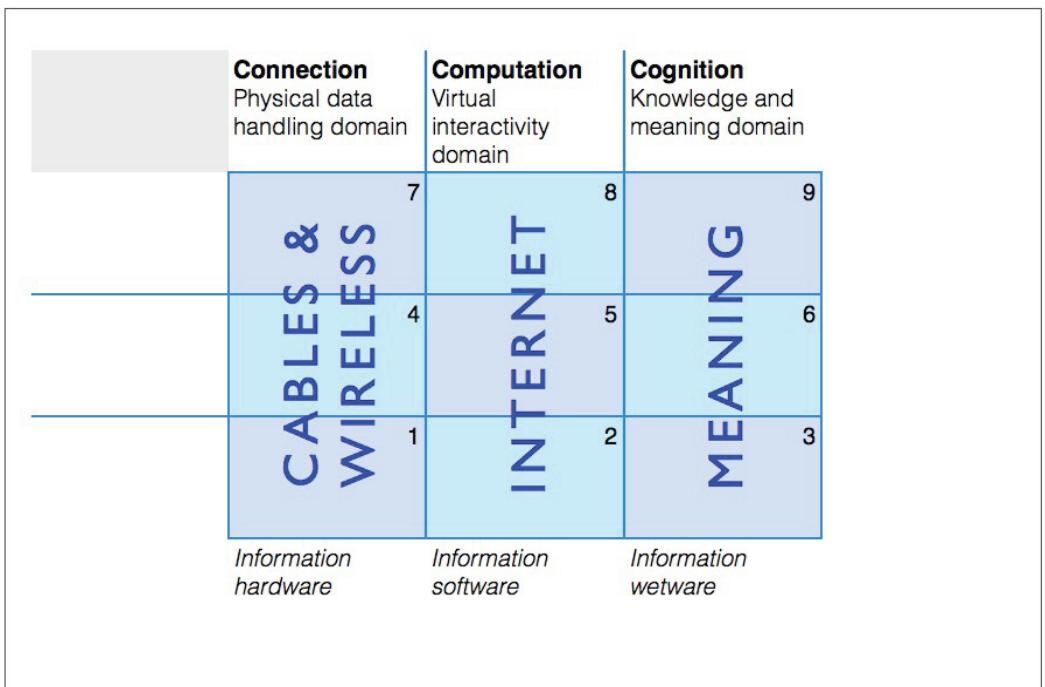
⁵¹ Gregory Bateson, *Mind and Nature, A Necessary Unity* (New York: Bantam, 1988)

⁵² Seth Lloyd, *Programming the Universe* (London: Vintage, 2007)

⁵³ Or more precisely, voxel (3D or volumetric pixel)

⁵⁴ David Tong, 'The Unquantum Quantum' *Scientific American* vol.307, (December 2012)

information to flow, or in interdicting individuals who are creatively advancing the information environment. Creativity is the high ground of the information terrain.



Graphic: © H Tibbs, 2013

The information dimension of the Cyber Gameboard

Information on the Cyber Gameboard

What then is the nature of the computationally networked world, the information component of the Cyber Gameboard?

At a physical enabling level, it is *connection* across the network. At the level of social and economic transactions, it is empowerment by networked interactivity, enabled by *computation*. At the highest level of *cognition* and cultural meaning, it is the expansion of a society in which open communication of knowledge has become a ubiquitous and transformational resource.

The full spectrum of the information domain runs from hardware, through software to what has been called ‘wetware’, the realm of knowledge in the human brain and mind. This expands the understanding of ‘cyber’ from simply being about technology to having its greatest value in the form of knowledge. The ultimate impact of ‘cyber’ is similar to the long-standing example of science as the model of open enterprise, involving collaboration and free sharing of information to improve the quality and accelerate the development of new knowledge.⁵⁵ Global society as a whole now has access to the same kind of developmental potential, and it is in the common interest of all nations to ensure that this potential is

⁵⁵ http://royalsociety.org/uploadedFiles/Royal_Society_Content/policy/projects/sape/2012-06-20-SAOE.pdf
accessed 14/02/13

protected and enhanced. Even if some players hold a narrower view, it is, quite simply, the highest strategic asset in the Global Cyber Game, and the highest priority for cyber security.

These different aspects of information all contribute to a full understanding of the information dimension of cyberpower, which on the Cyber Gameboard is therefore subdivided into three types of information: Connection, Computation, and Cognition.

The Cyber Gameboard

As already described, the Global Cyber Game is envisaged as a worldwide contest to achieve information-enabled advantage. It involves the exercise of cyberpower to gain a competitive edge through the most effective application and orchestration of knowledge and information capability. In keeping with the game analogy, the game is visualised as played on a 'Cyber Gameboard' which embodies the two dimensions of cyberpower, information and power.

The Cyber Gameboard is presented here as a three-by-three grid, with a 'cyber' or information related axis, and a power axis. The three subdivisions of each axis follow from an analysis of information and power, as already described.

	Connection Physical data handling domain	Computation Virtual interactivity domain	Cognition Knowledge and meaning domain	
Cooperation Integrative social power (Infopolitik)	(7) Open source hardware (e.g. mesh networks)	(8) Open source code, social software (e.g. Linux, GitHub)	(9) Shared knowledge and narrative (e.g. Wikipedia)	<i>Power as positive social reciprocity</i>
Co-option Economic exchange power	(4) Dominate hardware market (e.g. Cisco, Huawei)	(5) Dominate software market (e.g. Microsoft, Apple)	(6) Knowledge services, marketing, PR, advertising, spin	<i>Power as balanced social reciprocity</i>
Coercion Destructive hard power (Realpolitik)	(1) Kinetic attack on information infrastructure	(2) Malware attack, IP theft (e.g. Stuxnet, China?)	(3) Threats, disinformation, psyops	<i>Power as negative social reciprocity</i>

Information hardware Information software Information wetware

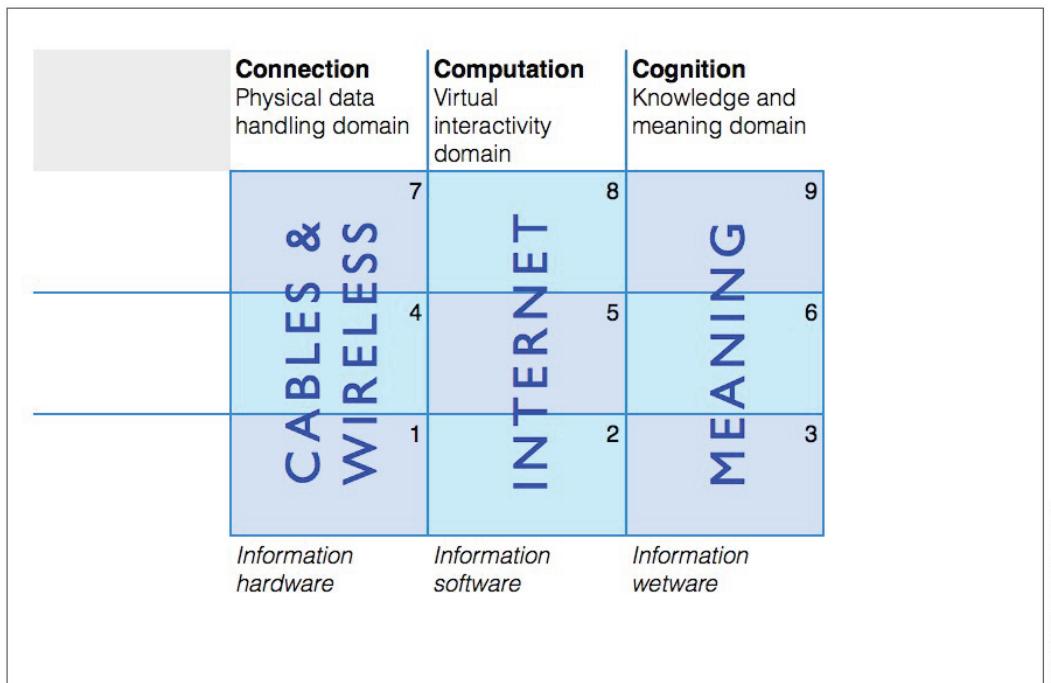
Graphic: © H Tibbs, 2013

Cyberpower on the Cyber Gameboard

The three subdivisions or domains⁵⁶ of the information axis follow the hierarchy of information from its transmission as data to its contribution to knowledge in the human mind. The three domains are: Connection (the physical infrastructure of cables, switches, satellites, etc.), Computation (the software and processing which enables networked interactivity), and Cognition (knowledge and meaning). The distinction between these is not always clearcut, as in the case of the Internet which is a combination of hardware and software. And the second domain is usually broken down into more detailed technical subdivisions, such as in the OSI Model and the TCP/IP stack. Nevertheless, the threefold

⁵⁶ This is consistent with the definition of 'domains' in MoD doctrine. See: 'Campaigning - Joint Doctrine Publication 01' MoD DCDC, December 2008, p.93

subdivision captures the three broad ways that information is susceptible to power: in terms of hardware, software, and 'wetware'.



Graphic: © H Tibbs, 2013

The information dimension of the Cyber Gameboard

The three subdivisions of the power axis reflect economist Kenneth Boulding's formulation of power (destructive, productive and integrative), discussed earlier. The three fields of the power dimension of the Cyber Gameboard are: Coercion, Co-option, and Cooperation. The distinction between these is not sharp; in practice they form a continuous blend.

The combination of the two axes produces a nine-cell grid, with power on the vertical axis, and information on the horizontal axis. This allows a very wide range of Cyber Game plays to be considered. To make the explanation clearer, the cells are numbered, starting from the bottom left corner, so that the bottom row runs from cell 1 to 3, the middle row from cell 4 to 6, and the top row from cell 7 to 9. In this way, the numbering runs from hard power acting on physical infrastructure, in cell 1, to its diagonal opposite, the cognitive results of cooperative power, in cell 9.

The bottom row, from 1 to 3, corresponds to Boulding's 'destructive' hard power, and the hard power end of Joseph Nye's spectrum of hard to soft power, also discussed earlier. This is the traditional realm of military strategy.

The middle row, from 4 to 6, corresponds to Boulding's productive or exchange power, the domain of economics. It also roughly corresponds to 'organizational power' as proposed by John Arquilla and David Ronfeldt, discussed earlier, and to the soft end of Nye's spectrum of

hard to soft power. This is the realm of economic power, traditionally regarded as a major ingredient of national power.

Cooperation Integrative social power (Infopolitik)	7	8	9 <i>Power as positive social reciprocity</i>
Co-option Economic exchange power	4	5	6 <i>Power as balanced social reciprocity</i>
Coercion Destructive hard power (Realpolitik)	1	2	3 <i>Power as negative social reciprocity</i>

Graphic: © H Tibbs, 2013

The power dimension of the Cyber Gameboard

Taking the bottom and middle rows together, reading from bottom to top, and somewhat from left to right, roughly corresponds to Nye's spectrum of hard to soft power. Counterinsurgency provides a comparative example, with the principle of lethal targeting in operations towards the bottom left, cell 1, and non-lethal targeting towards the top right, cell 6.

The top row, from 7 to 9, corresponds to Boulding's integrative social power, and has some similarities to Arquilla and Ronfeldt's concept of immaterial power, the key distinction being that it is non-coercive. This is relatively neglected as a component of national power but it is a potent factor in the information-intensive Cyber Game. Not coincidentally it captures the essence of 'Internet culture', with its emphasis on open source software and information sharing.

The first column, cells 7, 4 & 1, addresses information hardware, the basic infrastructure that enables communication and connectedness, as acted on by the three types of power.

The middle column, cells 8, 5 & 2, addresses information software, the capacity of the information infrastructure for interactivity, networking, processing and amplification of information, as influenced by the three types of power.

The third column, cells 9, 6 & 3, addresses information 'wetware', the realm of knowledge in the human brain and mind as shaped by the three types of power. Although distinct, Cell 9

has some echoes of what Arquilla and Ronfeldt call ‘the view of Athena’, a combination of seeing power as immaterial and information as constitutive of matter, an idea discussed later. As Arquilla and Ronfeldt point out, this is a very interesting intersection, because here it is as if information and power become the same thing.⁵⁷

Together, these two dimensions and their subdivisions form a conceptual framework that allows various types of cyber gameplay to be analysed.⁵⁸ In the sections that follow, various possible game plays are described and discussed, and the implications and resulting options for cyber strategy—meaning strategy for the exercise of cyberpower—are explored.

How power and information interact

According to biologist and systems thinker Gregory Bateson the essence of information is the detection of difference. Similarly, according to Boulding, the essence of power is the potential to effect change⁵⁹ or difference. So there is a clear complementarity between the two. Seen one way, what the cells of the gameboard identify are the various ways that information can be impacted by power in its various forms. Seen another way, the cells identify the way effects, produced by power, turn into information when they are detected, as well as how this information can condition power.

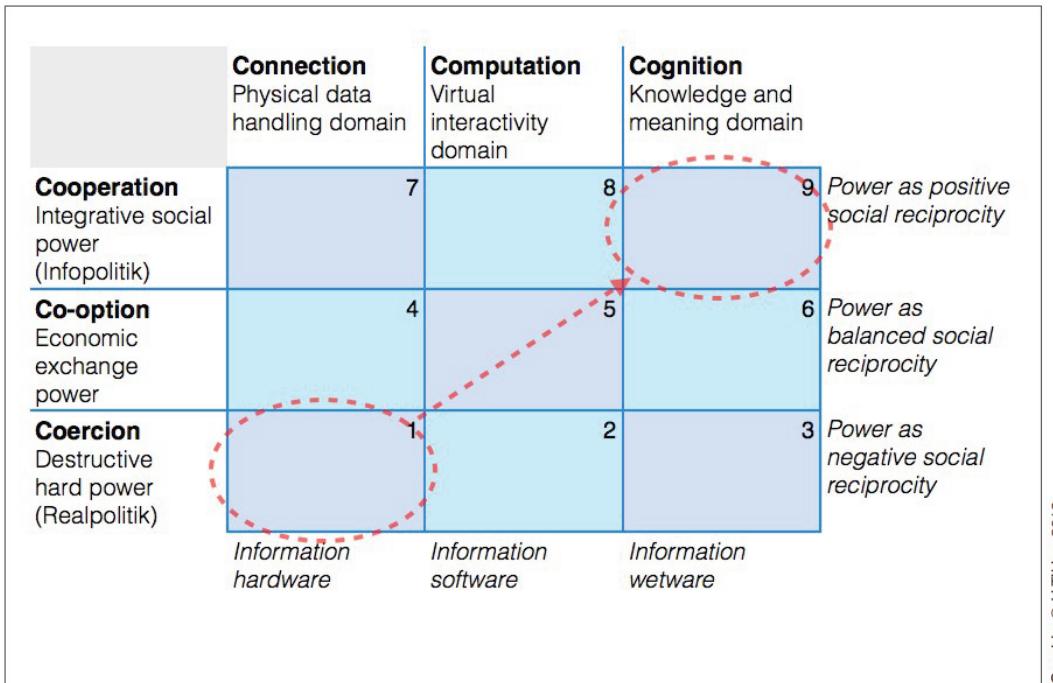
For example, information is vulnerable to coercive power through such things as damage to physical connectivity (cell 1), disruption of computational processing (cell 2), or manipulation of cognitive meaning (cell 3). But these effects produced by power are also sources of information. When a player exercises power, effects are produced that become information, and this information influences the behaviour of other players, as well as guiding the next application of power by the original player.

The Cyber Game, as opposed to the industrial-era geopolitical game, has very high information intensity. This means much greater attention will be paid to the feedback from applied power to information context, a consequence of information amplification. Over the course of several cycles of interaction among Cyber Game players, depending on their information intensity, a gravitation towards more subtle actions (towards the right and top of the gameboard) would be expected. This is because the information-rich tools of strategy-making will cause Nye’s relational concept of power to become ever more apparent. It will be ever-clearer that power’s true effect is to shape behaviour, and that behaviour is most readily shaped by information, even if the information is about a bomb that has just gone off.

⁵⁷ John Arquilla and David Ronfeldt, *In Athena's Camp* (Santa Monica: Rand Corporation, 1997)

⁵⁸ Arquilla and Ronfeldt (*ibid.*) offer a superficially similar 9-cell grid that sets power against information, but it differs in several important respects that will become apparent if the two are compared.

⁵⁹ Kenneth E. Boulding, *Three Faces of Power* (Newbury Park: SAGE Publications Inc., 1989)



Graphic: © H Tibbs, 2013

The evolution of strategy on the Cyber Gameboard

Cyber Game play

To recap, the Global Cyber Game is a contest to achieve information-enabled advantage, involving the exercise of cyberpower. The game plays out on the Cyber Gameboard, which embodies the two dimensions of cyberpower, information and power.

The Global Cyber Game started out as a friendly free-for-all, but now it is becoming much harder and faster. It has few formal rules, though they are beginning to evolve, but players are constrained in various ways.

The game is partly like a cross between chess and wéiqí. Players can make chess-like moves on the Cyber Gameboard, or gradually build up power positions. Unlike chess, some players are more or less fixed in a certain position while others are free to move. Players may be part of systemic relationships with other players that constrain their moves but form power constellations on the gameboard, while others are relatively independent.

The relative strength of players differs greatly. Some players form networked teams to play the game, increasingly necessary as play becomes more sophisticated, but loners can still make effective moves. Most players have opponents of some kind, within a power level or between levels. The game does not characterize good guys and bad guys, any more than black and white does in chess. However, some players are viewed by most other players as being legitimate, while others are almost universally regarded as illegitimate, such as organized criminal groups.

All players play for advantage of some kind, but this can vary from pure self-interest to creating advantage for all players on the board, and this can be done from any position on the board. All players are free to move at any time, but the game tends to develop through sequences of moves and countermoves, and knowledge about new types of play spreads fairly rapidly across the board. Despite the speed at which information can move on the board, many players do not keep up to date (some not even seeing themselves as in the game), creating weak nodes for opponents to exploit.

The Cyber Game, unlike most formal games, has no single agreed set of rules, though they are gradually evolving. Some players are actively trying to influence the rule-making process for future advantage. The objectives and vision of the players varies widely, as does their resolve. Some players are only just beginning to realize that the game is serious and that they become involved as soon as they use information technology. So far, hardly any players seem to appreciate that as the game gets tougher, very aggressive play could damage or even destroy the gameboard, with serious adverse consequences for all players.

Positioning moves in the game involve either changing the intensity of an existing position, or moving or extending vertically, horizontally or diagonally. Moving sideways means a shift in the type of information capability or strategic asset used, while moving up or down means a shift in the type of power interaction with other players.

The different zones of the gameboard can be characterized as follows:

Cells 1, 2 & 3:

The zone of cyber ‘game plays’ that use destructive power against information assets for the purposes of coercing another player, either at the time or later

The players in this zone of the gameboard are ones who use information related destruction for either negative or positive purposes. This includes defence departments, intelligence agencies, crime-fighting agencies, malicious hackers, and criminals.

The key to understanding this zone of the gameboard is establishing an information-centric definition of ‘destruction’. The usual meaning is physical destruction, and this is the sense used in international law for the definition of ‘use of force’, which is taken to involve serious physically destructive and lethal acts. On the other hand, in international law, espionage, an information related activity, is tacitly seen as ‘not illegal’, essentially because it is an exercise of sovereignty.

Although considerable and commendable efforts are being made to relate existing international law to cyber conflict, such as the Tallinn Manual,⁶⁰ there is an obvious disconnect in trying to assess all information related damage in terms of ‘physical destruction’. This is simply too narrow a definition to be useful in the Cyber Game.

For example, it fails to include carefully designed purely information related actions by, say, China, which sees the Cyber Game as an opportunity for winning without fighting, while

⁶⁰ Prof. M. Schmidt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013)

simultaneously arguing that cyberspace should be a conflict-free space and therefore a demilitarized zone to which the Law of Armed Conflict (LOAC) would not apply.

Part of the reason espionage may be tacitly accepted is because, in the past, information has been seen merely as an adjunct to real-world situations. In the Cyber Game, information is the substance of the game, so it needs to be central to operational definitions. If the 'use of force' criterion is replaced by 'destruction' and applied to information assets, it then can cover a range from: kinetic attack on the physical components of the information infrastructure; to intrusion into software infrastructure by hacking that destroys computational integrity, or destroys the value of information by stealing it; to the destruction of knowledge value by deception or psychological means.

It is interesting that information and damage already appear to be linked in Chinese thinking, at least in the light of their response to allegations that they were involved in hacking the *New York Times* in 2012. Asked about evidence pointing to China as the source of the hacking, China's Ministry of National Defense said, according to the *New York Times*, 'Chinese laws prohibit any action including hacking that damages Internet security.'⁶¹

Destruction of course has differing degrees of severity. For example, at the mild end of the destruction scale, the idea of damage is clearly established in law, and this is applicable to information damage, though the law sees monetary loss as the primary yardstick. Temporarily defacing or disabling a website to express outrage might be considered by some as legitimate civil protest, but if the website owner suffers loss of business and incurs costs for rectifying the situation, then in the eyes of the law this is a destructive attack causing criminal damage, even though it may not be particularly serious.

A perhaps less obvious example of cognitive manipulation in cell 3 is search engine optimisation (SEO) which, while widely regarded as acceptable, is strictly speaking a coherent, broad-based, decentralized attempt to contaminate the algorithmic processes of search engines to return misleading results.⁶²

Cells 4,5 & 6

The zone of cyber 'game plays' that use information assets to produce economic exchange power that co-opts other players

The idea of co-option here refers to the power of market share and network effects, and their ability to draw customers into dependence on successful information platforms. This puts a few very large information companies such as Microsoft, Apple, Google, IBM, Cisco, Juniper, Huawei, etc. in very powerful positions. Their strategies and innovation, as well as the start-ups that effectively challenge them, such as Big Switch Networks,⁶³ literally shape and reshape the Cyber Gameboard and often wrong-foot other players.

⁶¹ <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&r=0> accessed 18/02/13

⁶² http://en.wikipedia.org/wiki/Search_engine_optimization accessed 30/03/13

⁶³ <http://www.bizjournals.com/sanjose/print-edition/2012/11/09/tech-shift-turns-up-the-heat-on-cisco.html?page=all> accessed 18/02/13

In some cases these economic players may work with governments, to extend national intelligence-gathering capability. For instance, news reports have alleged that Huawei works closely with, and is collecting intelligence on behalf of the Chinese government.⁶⁴ Such a link, with the added support of government-subsidised finance,⁶⁵ could help a firm win business of strategic importance by bidding low in an ‘open’ market. This may have been a factor when Huawei won the contract to provide the BT Internet backbone in the United Kingdom in 2005.⁶⁶ Equally, suspicion may work against its commercial ambitions, as when the Australian government refused to allow Huawei to bid for a similar Australian contract in 2012.⁶⁷ In such cases, the economic player is likely to be regarded as an extension of the government, forming a single player that extends over the middle and bottom layers of the gameboard.

Smaller players in the economic zone of the board are very exposed in terms of cyber security. Small companies, and even ones the size of The New York Times, typically rely on so-called ‘anti-virus’ packages to protect their information systems. Yet these systems are inadequate to protect against the current level of threats.⁶⁸ Symantec, the anti-virus company confirmed this in a comment about the failure of their products to protect The New York Times: ‘We encourage customers to be very aggressive in deploying solutions that offer a combined approach to security. Anti-virus software alone is not enough’.⁶⁹ For smaller companies, however, more sophisticated protection skills or technology are out of reach. Even more problematic is the possibility that some anti-virus software may contain back doors. Similarly, in 2012 Wired magazine raised questions about Kaspersky Lab that implied a link with the Russian government,⁷⁰ although Kaspersky himself vigorously denied there was any basis for concern.⁷¹ The difficulty is that if governments do use, or are even suspected of using, commercial companies to assist with espionage, the more generalized distrust it will foster, which will indirectly impede the operations of their smaller firms which are responsible for the bulk of job creation.⁷²

Cooperative innovations, originating in the social power level of the board, can be another difficulty for economic level players, if they provide a means to freely share information that economic players regard as their intellectual property (IP). Strictly speaking, IP theft should be classed as damage to information value, making it a hard power play, but much of this innovation happened during the euphoria of the early Internet period, when there was no effective reaction, which enduringly shaped outlooks.

⁶⁴ http://www.theregister.co.uk/2009/06/12/cybersecurity_huawei/print.html accessed 18/02/13

⁶⁵ <http://ovum.com/2012/03/14/huawei-zte-hold-upper-hand-in-vendor-financing-wars/> accessed 18/02/13

⁶⁶ <http://www.huawei.com/uk/about-huawei/newsroom/press-release/hw-088555-news.htm> accessed 18/02/13

⁶⁷ <http://www.securitymagazine.com/articles/83669-huawei-proposes-australian-cyber-security-test-center> accessed 18/02/13

⁶⁸ <http://www.technologyreview.com/news/428166/the-antivirus-era-is-over/> accessed 18/02/13

⁶⁹ http://www.theregister.co.uk/2013/02/01/symantec_responds_nyt_apt/ accessed 18/02/13

⁷⁰ http://www.wired.com/dangerroom/2012/07/ff_kaspersky/all/ accessed 19/03/13

⁷¹ <http://eugene.kaspersky.com/2012/07/25/what-wired-is-not-telling-you-a-response-to-noah-shachtmans-article-in-wired-magazine/> accessed 19/03/13

⁷² http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/supporting-documents/2012/do-smes-create-more-and-better-jobs_en.pdf accessed 18/02/13

Capitalist culture accepts what economist Joseph Schumpeter called creative destruction, but it is generally assumed that this is channelled within the existing structure of business and market frameworks, as Apple did. Nevertheless, many innovations occur on the fringe almost as accidents and, in the case of Internet innovations, they frequently spread far faster than innovators expect.

During the current period, governments are organizing to crack down on this type of activity on the basis, in terms of the Cyber Game, that it destroys information value. Much of it, however, ultimately creates greater information value than it puts at risk. A better resolution would be for the state to use a calculus that balances social value gained against economic information value lost, and to foster a relationship between social and economic power players that encourages constructive channelling of innovation to convert social value into replacement economic value.

Cells 7, 8 & 9

The zone of cyber 'game plays' that use the social power of freely shared information assets to build cooperation with other players

In this zone of the Cyber Gameboard, collaborative power is created by the integrative force of respect and legitimacy. The 'Internet culture' of free exchange of information-based know-how and technology is a form of positive social reciprocity that works as a powerful binding force.

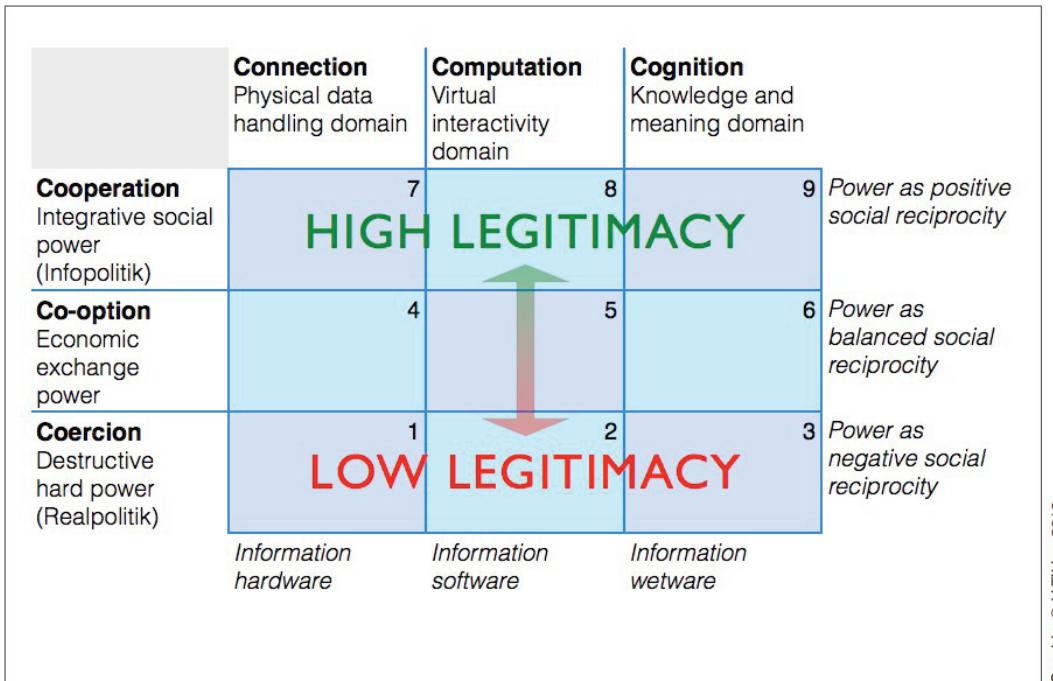
Even the exercise of coercive force depends, to an extent, on legitimacy,⁷³ so this form of power is not unique to the social power level. Internet culture has legitimacy because its values stem from this social source of power. Al Qaeda, by contrast, operates at the hard power level, with frequent destructive actions that have even lost it the support of many Muslims, who would be its natural source of integrative power.

A particular issue in the Cyber Game is how the players in the bottom and middle layers of the gameboard will generate legitimacy. The ideological power of national patriotism (an industrial era form of integrative power) is waning, and the global narrative of globality is gaining in legitimacy and integrative power. In future, state players of the Cyber Game will need to pay special attention to the source of their legitimacy.

State players are, in fact, at risk of seriously underestimating the role of legitimacy in justifying the use of coercive power in an environment of information abundance. In the section of Wikileaks containing material from the UK, there is what purports to be a leaked copy of the MoD Manual of Security, JSP-440, a restricted document (ironically a manual about how to prevent leaks, par for the course under conditions of information transparency).⁷⁴ The document identifies investigative journalists, along with extremist groups and criminals, as threats to security, and identifies unwelcome publicity of any kind as the 'enemy'. The MoD has not apparently denied the authenticity of the leaked manual, so for the purposes of the following comments it is regarded as genuine.

⁷³ Kenneth E. Boulding, *Three Faces of Power* (Newbury Park: SAGE Publications Inc., 1989)

⁷⁴ <http://www.telegraph.co.uk/news/uknews/defence/6261756/MoD-how-to-stop-leaks-document-is-leaked.html> accessed 18/02/13



Graphic: © H Tibbs, 2013

Legitimacy on the cyber gameboard

Treating journalists as threats may be justified in a tactical sense, but the problem is that investigative journalists are generally regarded as an essential and legitimate part of the democratic system, so this is hardly a holistic appraisal, let alone a holistic strategy. That a Western Cyber Game player could regard them as a threat is a view that can only be maintained if the player has limited their thinking to the hard power level of the gameboard, which will automatically lower their legitimacy when seen from the perspective of the economic or social levels.

In much the same way, the US government's widely reported coercive-power takedown of Kim Dotcom, described in the next section, not only has dubious legal validity, but definitely has lower legitimacy in the Cyber Game than Kim Dotcom himself, whose new company Mega actually quotes Article 12 of the UN Human Rights Charter on its website.⁷⁵

The dominant source of legitimacy in the Cyber Game comes through promotion of open information exchange in the global knowledge commons, scary as that might be. Only by shifting the frame of reference to the widest possible conception of the Cyber Game is it possible to identify the high ground available to all players who aspire to provide genuine strategic leadership in this new global game. Ultimately this means operating at the level of integrative power. In this part of the Cyber Gameboard, cyberpower takes on a completely new meaning.

⁷⁵ <https://mega.co.nz/#privacypolicy> accessed 14/02/13

For example, the news channel Al Jazeera has achieved substantial international credibility, greatly adding to the international legitimacy of Qatar. While commonly understood as a media channel, Al Jazeera's distribution is global because of its extensive internet presence. This means that it has achieved disproportionate status, comparable in many eyes to that of the BBC, at a fraction of the cost of building global distribution channels for its programming. Although backed by a national government, Al Jazeera gets the majority of its reach from the internet.

Wikipedia is another example of an organization with huge perceived legitimacy, entirely built online. For an organization with a tiny budget and little official backing of any kind to achieve greater dominance in reference than Encyclopaedia Britannica in less than 12 years is remarkable. Economist Yochai Benkler calls this kind of structure 'commons-based peer production' and considers it to be a breakthrough as fundamental as the assembly line or mass production itself.⁷⁶ Wikipedia's legitimacy comes from an army of volunteers and a constant process of community-based self correction, not entirely unlike peer review. The result is an enormous creation of new legitimacy not only for Wikipedia, but for the Internet as a source of free, trustworthy information which rivals or overshadows traditional reference materials. The overall impact is a direct transfer of legitimacy from state level resources to international, transnational or simply non-national resource pools as new classes of actor transform our shared intellectual space.

The same phenomenon has happened to software itself. Around 70 percent of the Internet's servers run open source software, mainly Linux, a project started in 1991 that grew slowly for its first ten years. The projects producing this open source server software are loosely regulated, if at all, and gain legitimacy by simply providing functionality for free.

Furthermore, because all source code is available for public inspection, there is a widespread belief that these operating systems and server architectures are inherently more trustworthy than closed source offerings from companies that have close relationships with their respective governments. The gold standard for credibility in software is that the software is free, the source code is free, bugs are posted publicly, patches to fix bugs are accepted from any credible source, and a strong user community keeps the software up to date at all times. It is very hard for companies to imitate all these features, as a combination of commercial and competitive pressures prevent them making their code available for inspection to security minded members of the general public.

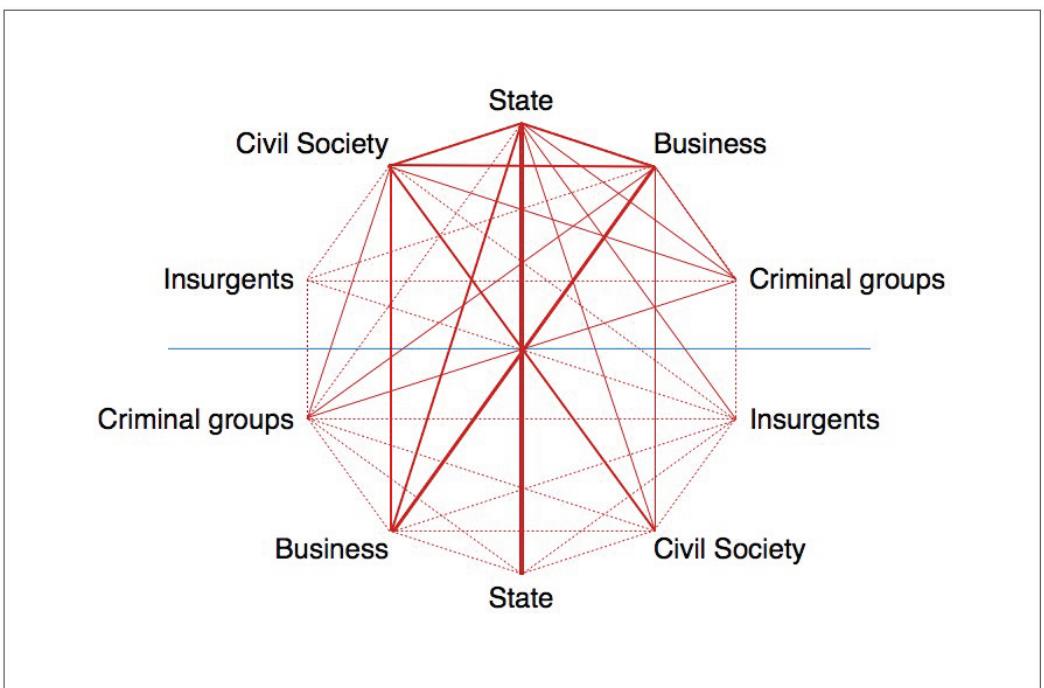
The result on all fronts is a transfer of legitimacy away from traditional channels to new, Internet-based structures with radically different characteristics from the ones that held legitimacy in the last century.

⁷⁶ Yochai Benkler, *The Wealth of Networks* (New Haven: Yale University Press, 2006)

How the Global Cyber Game is being played

The Global Cyber Game is still in its opening stages, but much can be learned from the way it has been played to date. Any new strategic phenomenon can appear puzzling or chaotic in its early stages and to make sense of what is happening requires an appropriate framework of analysis. The Cyber Gameboard, described in the previous section, provides a framework which allows the existing pattern of game-like moves by players to be mapped and better understood, which is the aim of this section.

There is a much wider range and number of players on the Cyber Gameboard than on the traditional geopolitical gameboard. The barriers to entry are so low, and the technology is so empowering, that power is diffusing widely among many smaller players who would previously have been insignificant. The various strategic actors see the Cyber Game in different terms and from dissimilar perspectives, which gives them widely varying motivations, objectives and actions.



Graphic: © H Tibbs, 2013

The Cyber Game is multiplayer

Some actors are closely associated with particular cells on the Cyber Gameboard, which places them on the board almost like chess pieces. Other actors are systematically extending their influence over many cells of the gameboard, somewhat in the way the game of wéiqí (Go) is played. This contrast in modes of play, between Western and Eastern styles, gives the game some interesting properties.

Cyber Game players can be grouped broadly into those that play on the hard power level of the gameboard, the economic level, and the social level respectively. In the hard power level

are the military and intelligence agencies of national governments and, to an extent, their police forces. These are the agencies that exercise the modern sovereign state's monopoly on the use of force. Also in the hard power level are their direct adversaries: hostile states, criminal groups and terrorists, and any other players using destructive or damaging methods.

State actors differ in their approach to the information content flowing in information infrastructures. Most Western-style 'open society' democracies value freedom of information content in support of freedom of thought, while other states believe that it is necessary to control information content. There are already signs that this ideological divide could become a primary source of conflict in the Cyber Game, as is clear from the tensions surrounding Internet governance. In practice, of course, all states agree that certain types of extreme content are unacceptable, so hopefully this divide can be bridged by avoiding highly polarised positions, although this will depend on skilful diplomacy.

O = open play (freedom of thought)
freedom of information content is a public good in itself,

V

X = closed play (information control)
control of information content is necessary for public safety

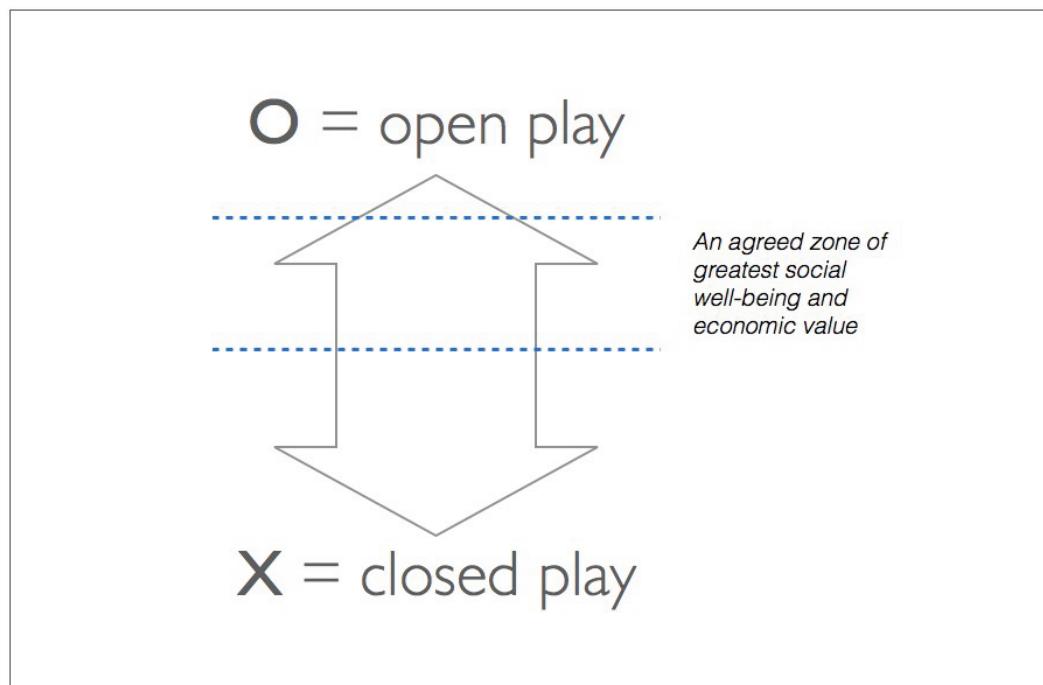
Graphic: © H Tibbs, 2013

Cyber Game play: the ideological divide

In the economic power level of the Cyber Gameboard are commercial companies, particularly those in the information business itself, such as Apple and Google. These economic power players are producing information-based economic value to create exchange power in the marketplace. Some government agencies are now using the web to transact and deliver government services, and they are also in the middle row, even though the 'exchange value' they create is levied as tax by the state. The appearance of web-based government service provision alongside commercial service provision is one way in which the state is recasting its

'business model' in terms of economic efficiency, leading to the emerging idea of the 'market state'.⁷⁷

In the social power level of the Cyber Gameboard are what might be called 'Internet culture' players who are interested in the power of cyberspace to create new capabilities and freedoms through collaboration and sharing. There are many innovative and experimental players in the social power level who are important for the evolution of the Cyber Game, but some of them play an ambiguous role. Their contribution could be considered creative by some players but destructive by others; it is what economist Joseph Schumpeter called 'creative destruction'. Placing these players appropriately on the gameboard presents an important strategic conundrum that is discussed later. Non-governmental organizations (NGOs), of which there are probably tens of millions in the world, also operate on this level. NGOs are, according to the UN definition, organized to 'address issues in support of the public good'⁷⁸ and are therefore distinct from non-state actors that operate at the hard power level and are willing to use violence.



Graphic: © H Tibbs, 2013

The Cyber Game ideological divide can be bridged

Some players move at the same pace as governments in adapting to the Cyber Game, but some are much faster. These fast players are a concern for state players, because they are the ones who can innovate and initiate faster than the time needed for adaptation by the core processes of government; they are cycling through their decision making 'OODA loop' faster

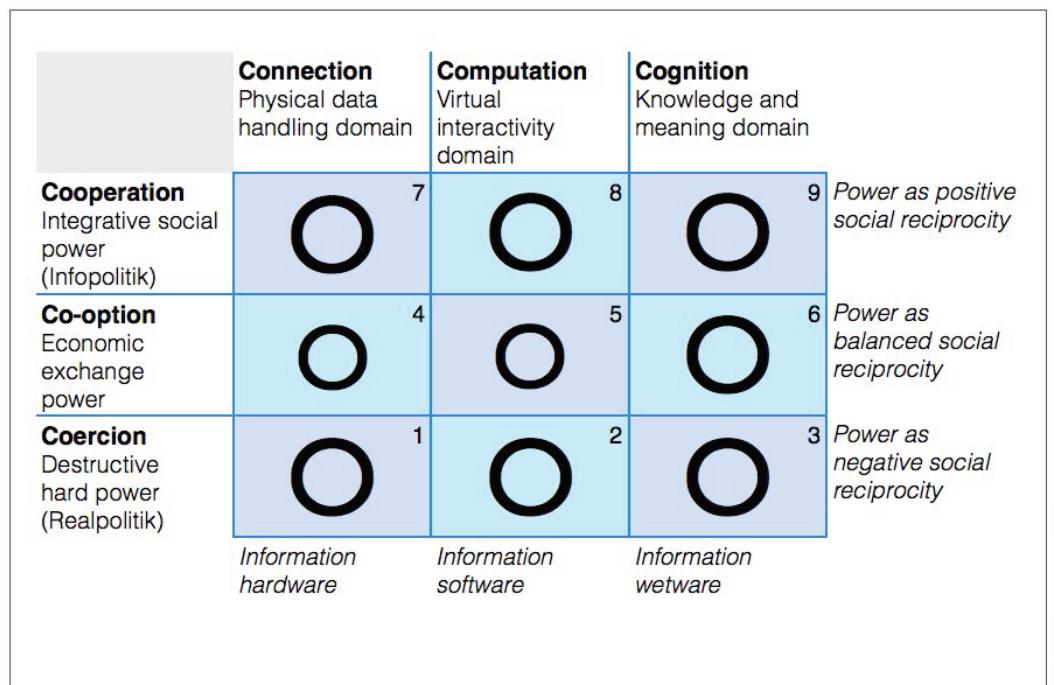
⁷⁷ Philip Bobbitt, *The Shield of Achilles* (London: Anchor, 2003)

⁷⁸ http://www.unrol.org/article.aspx?article_id=23 accessed 30/03/13

than the state and can out-manoeuvre it.⁷⁹ The fast players include rapidly innovating information industry firms, 'Internet culture' players, and criminal groups, plus some fast players on the state side, primarily in the intelligence agencies.

Player perspectives and modes of play

The different players have contrasting views of the Cyber Game, which affects how they play and is itself a source of potential cyber conflict. The biggest contrast in perspective and approaches to the game is between players is between states, business, and civil society.



Graphic: © H Tibbs, 2013

United States cyberpower (illustrative)

The perspective of national security players in native English-speaking (and Francophone) countries is that a new threat space, cyberspace, has appeared, in which all defence forces must now learn to operate. Cyberspace is viewed as a new military domain or environment that needs to be made secure for the state, commerce, and citizens by developing the capability for military operations 'in' cyberspace. A milestone in this process was the establishment of US Cyber Command in May 2010, which was charged with developing 'the required technical capability' to focus 'on the integration of military cyberspace operations'.⁸⁰

The wake-up call for the US military that prompted the establishment of Cyber Command was in 2008, when a computer worm called 'agent.bz' worked its way unnoticed into classified networks and exfiltrated large amounts of US defence information. This unpleasant surprise, despite much unimplemented anticipatory cyber thinking in defence circles, reinforced a technology-centric response. The cyber security problem now tends to be

⁷⁹ From commentary submitted to the Inquiry by Vinay Gupta

⁸⁰ <http://www.defense.gov/releases/release.aspx?releaseid=13551> accessed 18/02/13

understood primarily in terms of technical intrusion into computer networks, and offensive cyber is seen as doing something technically destructive in return, such as making a centrifuge malfunction. This approach appears to be favoured because it allows the most straightforward application of existing thinking about defence and military operations. Western players are also constrained by the need to 'operate within the rules' and try to ensure that their activities stay within the boundaries of various legal frameworks, such as the US Constitution, LOAC, or the EU cyber security directive.

In the non-English speaking world, particularly in Russia and China, the perspective is different. English-language science fiction has portrayed cyberspace as being a romantic technological frontier. For these countries it does not have the same resonance, instead they regard information itself and its political integrity as a vital strategic and economic asset and interpret information security in a far more comprehensive and anticipatory way than the West.

The United States: a strategy of pre-emptive cyber offence?

Among the earliest and most obvious applications of military cyberpower was its use for disabling and disrupting computerized control systems. It was used this way during the early cyber period, before any drawbacks were evident. Some of the issues involved can be examined by looking at the best example so far of this way of playing the Cyber Game, the US and Israeli use of military malware against Iran, mentioned earlier.

In June 2012, the *New York Times* ran a story⁸¹ claiming that the United States had been responsible for online attacks on Iran, starting under President Bush and continuing under President Obama. The story explained how the Stuxnet worm had been used by the United States and Israel to attack the Iranian uranium centrifuge plant at Natanz and had escaped onto the wider Internet due to a programming error.

This was not all. In May 2012 Kaspersky Lab had announced that a large and complex malware programme called Flame had been found on Iranian computers. The company said it believed the attack was state-sponsored, and described it as 'one of the most complex threats ever discovered'. 'Once a system is infected, Flame begins a complex set of operations, including sniffing the network traffic, taking screenshots, recording audio conversations, intercepting the keyboard, and so on,' said Kaspersky's chief malware expert Vitaly Kamluk.⁸² The size of Flame is 20Mb, 'twenty times more complicated than Stuxnet' and, according to Kaspersky, it could take as long as 10 years to analyse.⁸³ After Flame's exposure in news media, Symantec reported on 8 June that Flame's controllers had sent a 'kill' command to infected PCs to erase all traces of it. The sophistication and complexity of Flame supports claims that Flame was the work of a state actor rather than cyber criminals because of the amount of time, skill and resources needed for its creation.⁸⁴ In June 2012, The

⁸¹ http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all accessed 14/02/13

⁸² http://www.bbc.co.uk/news/technology-18238326#_jmp0 accessed 14/02/13

⁸³ [http://en.wikipedia.org/wiki/Flame_\(malware\)](http://en.wikipedia.org/wiki/Flame_(malware)) accessed 14/02/13

⁸⁴ <http://www.bbc.co.uk/news/technology-18365844> accessed 14/02/13

Washington Post claimed that Flame had been developed by the United States and Israel, citing Kaspersky's discovery that Stuxnet shared a common code module with Flame.⁸⁵

	Connection Physical data handling domain	Computation Virtual interactivity domain	Cognition Knowledge and meaning domain	
Cooperation Integrative social power (Infopolitik)	7	8	9	<i>Power as positive social reciprocity</i>
Co-option Economic exchange power	4	5	6	<i>Power as balanced social reciprocity</i>
Coercion Destructive hard power (Realpolitik)	○	✗	✗	<i>Power as negative social reciprocity</i>

Information hardware Information software Information wetware

Graphic: © H Tibbs, 2013

United States government versus the Iranian government (alleged)

More recently, in August 2012, Kaspersky Lab announced that it had found 'Gauss,' a new malware threat facing computer users in the Middle East. This is a complex espionage toolkit which shares common code with Flame. Unlike Flame, however, it is designed to steal confidential data, with a specific focus on browser passwords, online banking account credentials, and cookies.⁸⁶ Gauss may well be another part of the US government's cyber weapons programme, code-named Olympic Games. But in view of what it is designed to do, it would clearly be of interest to criminals and is an obvious target for online weapons proliferation.

If Stuxnet, Flame and Gauss, are part of the most intense state-on-state online attacks so far reported, the obvious question is whether they have been effective. The answer is not encouraging. According to IAEA data,⁸⁷ the attacks stimulated Iran to expand its production of low-enriched uranium to higher levels than before the attacks, making up the Stuxnet-

⁸⁵ http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQAxBPoV_story.html accessed 14/02/13

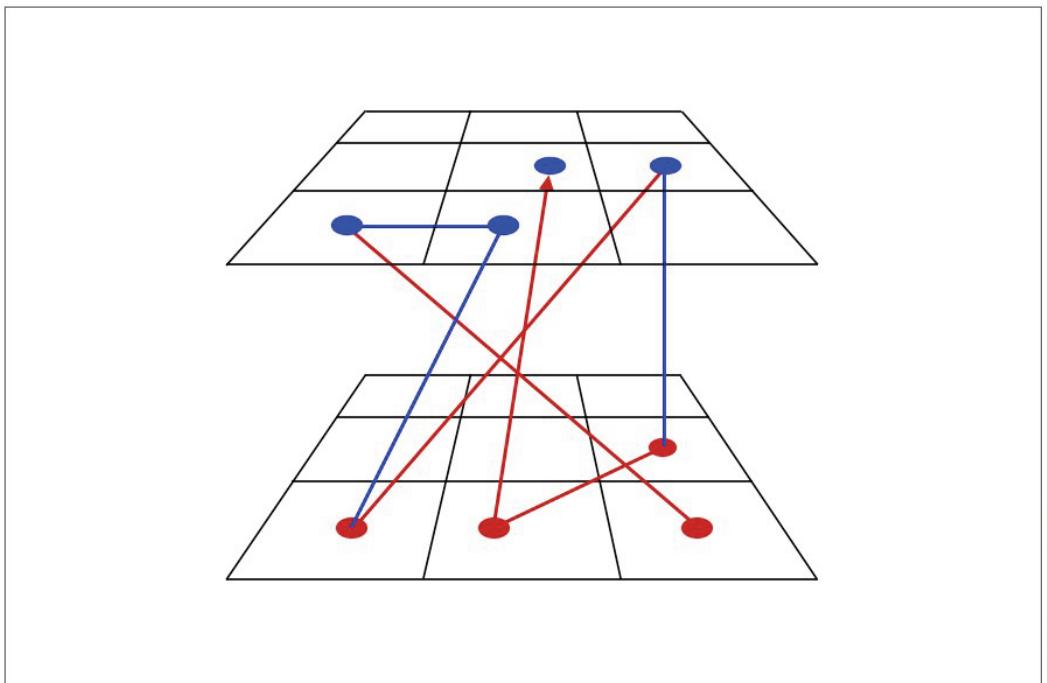
⁸⁶

http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts accessed 14/02/13

⁸⁷ David Albright et al., 'Analysis of IAEA Iran Safeguards Report' Institute for Science and International Security (ISIS), 30th Aug 2012 http://isis-online.org/uploads/isis-reports/documents/ISIS_Analysis_IAEA_Report_30Aug2012.pdf accessed 14/02/13

induced losses by March 2010, and then exceeding the pre-Stuxnet production trajectory while still under Stuxnet attack.

It could be argued that this online attack forestalled a conventional Israeli military strike and bought time for diplomacy, but, unfortunately, Iran now has even more uranium than it would have had, and trusts the United States even less, making the prospects of a diplomatic solution more remote.



Graphic: © H Tibbs, 2013

United States government versus the Iranian government (alleged)

Furthermore, the discovery of Stuxnet prompted an announcement by Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, that the Iranian military was prepared 'to fight our enemies' in 'cyberspace and Internet warfare.'⁸⁸ This was followed by a Pentagon announcement in June 2011 that computer sabotage coming from another country can constitute an act of war.⁸⁹ Then in February 2012 the US Treasury Department stated that the Iranian Ministry of Intelligence and Security (MOIS), Iran's primary intelligence organization, had 'participated in multiple joint projects with Hezbollah in computer hacking,' presumably laying the groundwork for a possible case that Iran had undertaken acts of war.⁹⁰ By its actions and reactions the United States had effectively taken online attack from an ambiguous or covert activity to being a cause of war, and had blunted its original case against Iran.

⁸⁸ http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all accessed 14/02/13

⁸⁹ <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html> accessed 14/02/13

⁹⁰ <http://www.treasury.gov/press-center/press-releases/Pages/tg1424.aspx> accessed 14/02/13

So in this case, while online attack may have been a transient tactical success, in that it physically destroyed over a fifth of Iran's 5,000 gas centrifuges, it was a strategic failure because it resulted in larger Iranian stockpiles of uranium, stimulated international proliferation of online weapons development, justified their use by the example of alleged US involvement, and brought the United States closer to the brink of declared war with Iran.

In fact Iran does appear to have hit back, aiming to disrupt economic targets, the most obvious weak point for retaliation by an Iranian cyber adversary. Starting in the last quarter of 2012 there was a wave of sophisticated large-scale attacks on leading US banks. Carl Herberger, a VP at security firm Radware said, 'The scale, the scope and the effectiveness of these attacks have been unprecedented....There have never been this many financial institutions under this much duress.' It appears that hackers remotely hijacked cloud-based data servers and harnessed their very considerable computing power to take down the American banking sites. One bank had 40 gigabits of Internet bandwidth, which is huge compared to say a midsize business that might only have one gigabit. But the flood of traffic directed at the banks peaked at 70 gigabits, 7000 times the capacity of the average household broadband connection. The amount of DDoS attack traffic flooding the American banking sites was 'multiple times' the amount that temporarily shut down Estonia in 2007, according to James A. Lewis, a former US government official and computer security expert. 'There is no doubt within the U.S. government that Iran is behind these attacks', he said.⁹¹

The US banks may have been caught in the crossfire of Internet military action, but they are not going to be the only ones. The design features of Stuxnet are now reported to be proliferating in criminal malware. To get access to computers, Stuxnet used stolen digital security certificates, something Microsoft is particularly concerned about.⁹² According to Roel Schouwenberg, a Kaspersky researcher, 'Stuxnet was the first really serious malware with a stolen certificate, and it's become more and more common ever since....Nowadays you can see use of fake certificates in very common malware.' And according to Aviv Raff, CTO and cofounder of Israeli computer security firm Seculert, 'Design features of Stuxnet, Duqu, and Flame are appearing in opportunistic criminal malware'. For example, Flame had a modular design, enabling its operators to send the parts separately to perform particular actions or attacks. Modular design makes it harder for security companies to identify and track a particular piece of malware, as they cannot see it all simultaneously.⁹³

A further concern is that there is a developing market in zero-day exploits, newly discovered weaknesses in software that malware designers can exploit. By being willing to buy these exploits, governments and other organizations are accused of boosting the market and creating what has been referred to as the 'malware-industrial complex'. According to Christopher Soghoian, a principal technologist at the American Civil Liberties Union, 'On the

⁹¹ http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=2& accessed 18/02/13

⁹² Personal communication with a senior Microsoft executive, conference in Boston: *Harvard-MIT-University of Toronto Cyber Norms Workshop 2.0* 11th-14th September 2012

⁹³ <http://www.technologyreview.com/news/429173/stuxnet-tricks-copied-by-computer-criminals/> accessed 18/02/13

one hand the government is freaking out about cyber-security, and on the other the U.S. is participating in a global market in vulnerabilities and pushing up the prices.⁹⁴

The FBI is now reported to be investigating former senior government officials who might have leaked the Stuxnet story.⁹⁵ The leak itself appeared in both *The New York Times* and in a book subtitled 'Obama's Secret Wars and Surprising Use of American Power'⁹⁶ that was released in June 2012. Interestingly, there is no indication that the story harmed the President's approval rating, which rose steadily for six months following publication.

Several points emerge from all this. Some are straightforward questions of strategic effectiveness:

- Online weapons may be unreliable or uncertain in their effects, and possibly only be tactically effective in the short term.
- Online weapons depend on secrecy, but the instant duplication and transparency effects of information technologies make it probable that they will be discovered if widely used. The more sophisticated and expensive the online weapon, the more pressure there will be to use it as extensively as possible to get value for money, which will increase the likelihood of discovery. If online weapons only have a short useful lifespan this will only add to the pressure for maximum early use.
- Use of online weapons by powerful states will justify their use by all players, who will be able to learn from the design of weapons that were originally only within reach of the best resourced actors. When the online weapons reported here were used and detected, their blueprint became available for averagely competent programmers to copy, on behalf of smaller states and non-state actors. This inherent tendency to proliferation is much greater than with nuclear weapons, which can still only be built by a handful of nations. And unlike nuclear weapons, once an online weapon has been used and detected it cannot be used again.
- Use of online weapons coupled with an explicit policy of conventional military kinetic retaliation risks rapid escalation of real-world war. This is particularly hazardous given the problem of source attribution which, although not impossible, is hedged with difficulties.
- Western adherence to a purely technological emphasis in online conflict may well provoke asymmetric non-technological responses from Russia and China, which could blindside the United States and its allies. The risk for the Pentagon, with its strong reputation as a 'technology shop,' is that an over-emphasis on technology could become an Achilles heel.

Other key points that emerge relate to the assumption that the Internet as a whole is a medium that is robust enough for destructive war fighting. Unfortunately, however, the

⁹⁴ http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/?utm_campaign=newsletters&utm_source=newsletter-daily-all&utm_medium=email&utm_content=20130213 accessed 18/02/13

⁹⁵ http://www.washingtonpost.com/world/national-security/fbi-is-increasing-pressure-on-suspects-in-stuxnet-inquiry/2013/01/26/f475095e-6733-11e2-93e1-475791032daf_story.html accessed 18/02/13

⁹⁶ David Sanger, *Confront and Conceal* (New York: Random House, 2012)

Internet is a human construct that was not designed for the enormous volume of traffic or the intense security pressures it is now being subjected to. These pressures alone may push it to the brink of failure, even without additional aggravations, including the following:

- Online attacks will tend to encourage Balkanization of the Internet, which in principle will impose disproportionate economic losses on all players. Metcalfe's Law holds that the value of a network is proportional to the square of the number of its users, and Balkanization will cause this effect to work in reverse. The value of a network will therefore drop like a stone as it shrinks. Dividing the Internet into, say, four equal sub-networks will cause their combined worth to drop to only a quarter that of the undivided network. Balkanization of the public Internet would mean, almost literally, decimation of the global economic growth potential described earlier.
- Many online weapons rely on the existence of Internet vulnerabilities, which must be kept open for the weapons to remain effective. The instinct of commercial companies is to close such vulnerabilities as soon as they are found, for the safety of their customers. Stuxnet, for example, exploited four 'zero day' (meaning that they had not been exploited before) weaknesses in the Windows operating system, which Microsoft patched as soon as Stuxnet was revealed. The designers of online weapons must continually search for new vulnerabilities and keep them secret to ensure the weapons remain useable. That means that the state is deliberately keeping the Internet unsafe, as the vulnerabilities remain open for a hostile state or non-state actor to exploit against all Internet users, including those at home. As noted earlier, even the US government is alleged to be boosting the market for previously unknown vulnerabilities known as zero-day exploits. If true, this would seem particularly short-sighted, as the United States is the preeminent worldwide leader in software products.
- This difficulty also applies in the case of online domestic surveillance. If democratic nations such as the United States ask information industry companies to build features into their products or infrastructure that facilitate domestic surveillance, those same features are then available to be exploited by an enemy against the domestic population. And if the same features are included in equipment exported from democratic countries, they will provide convenient means for repressive regimes to carry out surveillance on their own population, who will be without legal recourse.
- The public knowledge that there now exists extremely powerful state-sponsored malware, invisible to all commercial anti-malware programmes, may breed public distrust of the Internet, with potentially high indirect economic costs (as discussed earlier). As the United States is now publicly associated with creating surveillance and destruction software that parasitizes its own commercial software, the distrust this breeds will also be directed against its own economy. The loss of trust is of particular concern since an investment in maintaining trust in a society is the most important single factor in assuring resilience in the event of a crisis.⁹⁷

⁹⁷ Leena Ilmola, presentation at a conference at Wilton Park in August 2012

- As many as 100 countries are estimated to have military cyber units, and about 20 have serious capabilities.⁹⁸ If all these countries are launching covert cyber actions against each other, and possibly planting malware for later use, the result will be sharply rising combinatorial complexity which will be very difficult for any country to deal with.⁹⁹

All these points could suggest that not only is the Internet insecure, but state actors are adding to the problem without achieving a significant balancing benefit. To make this point with any certainty, however, requires a larger experience base than is currently available.

If news reports about Stuxnet are taken at face value, it could be argued that the United States is exhibiting chess-like play on the Cyber Gameboard, making discrete moves against discrete targets. Currently there is little sign of the wéiqí style of play that characterizes Chinese cyber strategy.

In the cyber arena the United States has yet to demonstrate its former mastery of integrative power. The Marshall Plan after the Second World War and the public domain sharing of space information by NASA in the 1960s gained the United States enormous worldwide legitimacy and respect. Compared to this prowess during the Cold War period, the United States is at risk of suffering a sharp loss of legitimacy if it continues its recent coercive-power cyber actions against social power players.

China's 'invisible' cyber strategy

China reputedly views the Cyber Game as centered on the 'right of controlling information,' and sees information superiority as one of the 'commanding heights' for winning any conflict. It regards information confrontation—obtaining and counter-obtaining, control and anti-control, and destroying and counter-destroying—as the key to winning a cyber era war.¹⁰⁰

Like Russia, China also sees the Cyber Game as having a social dimension. According to *Qiushi* magazine, China's information system must be independent of foreign control, and able to combat superstition, rumours, slander, and pornography that corrupt people's minds and threaten national security, and also prevent domestic use of the Internet as a subversive tool.¹⁰¹

China interprets the importance of information broadly, as does Russia, but sees it as being deployed in support of its 'peaceful rise to power,' rather than as a means to defend and restore the reputation and power of the state. The rise of China is highly significant, and forms the context for its cyber stance, so it is important to appreciate its origins.

⁹⁸ http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/?utm_campaign=newsletters&utm_source=newsletter-daily-all&utm_medium=email&utm_content=20130213 accessed 18/02/13

⁹⁹ Presentation by John C Mallory at the 2012 Workshop on Cyber Security and Global Affairs and Global Security Forum. Polytechnic University of Catalonia, Barcelona, Spain, 19th-21st June 2012

¹⁰⁰http://fmso.leavenworth.army.mil/documents/infosecu.htm#_ftnref15 accessed 18/02/13

¹⁰¹ He Dejin, 'Raise Network Security Awareness and Build Information Protection Systems,' *Quishi*, 1 November 2001. Quoted in ibid.

	Connection Physical data handling domain	Computation Virtual interactivity domain	Cognition Knowledge and meaning domain	
Cooperation Integrative social power (Infopolitik)	7	8	9	<i>Power as positive social reciprocity</i>
Co-option Economic exchange power	X 4	X 5	X 6	<i>Power as balanced social reciprocity</i>
Coercion Destructive hard power (Realpolitik)	X 1	X 2	X 3	<i>Power as negative social reciprocity</i>
	<i>Information hardware</i>	<i>Information software</i>	<i>Information wetware</i>	

Graphic: © H Tibbs, 2013

Chinese cyberpower (illustrative)

In looking towards the future, and its own role in the world, China's posture is one of 'building towards a harmonious world of lasting peace and common prosperity,' in the words of Hu Jintao at the UN General Assembly in 2005. This mirrors the way in which, almost continuously for over 2500 years, successive dynasties, each typically lasting around 300 years, maintained order in a vast territory that seemed to sit geographically in the centre of the world.

In thinking first expressed by Confucius in the 'Warring States' period around 500 BCE, earthly rule is to be achieved by securing the 'mandate of heaven,' through creating a just and harmonious society, governed by rules that mirror the harmony of natural order. Justice, according to Confucius, meant a proper harmonious relationship within a family, within a state, and between states.

China's cultural predilection is to think in terms of harmonious justice, ordered by rules, maintained by virtue of its own centrality in the world.

China is vast, but was always surrounded by potential enemies and could never hope to conquer them all, so it tended to use less direct methods for maintaining power. If possible, it sought to prevent the formation of coalitions along its borders. The fear of encirclement dominates China's strategic thinking, and is reflected in the traditional Chinese game of wéiqí, better known by its Japanese name, Go. The objective in wéiqí is to encircle the opponent in a series of simultaneous, continuously shifting power plays spanning the entire board.

Chinese strategic thinking often seeks to win by gaining sustained psychological advantage rather than by direct conflict, making it extremely subtle to the Western mind, which thinks in terms of frontal combat and decisive victory. Chinese thinking looks ahead, trying to read the direction of the evolutionary current in the strategic situation (*shi* in Sun Tzu) and turn it to advantage.

The Celestial Court of the Manchu Qing Dynasty had been ruling China for 200 years when it first came into conflict with the industrializing European powers. In 1760 the emperor Qianlong had restricted foreign trade to the southern coastal city of Canton, but by the 1780s the insatiable British taste for tea had run up a serious trade deficit. The answer was Indian opium. By 1830, 1,200 tonnes of East India Company opium were being imported into China annually, and the trade deficit had been reversed. By the mid-1830s the Qing government could no longer ignore the financial and social consequences of drug addiction and began a crackdown.

This led to growing trade frictions and, in 1840, the British government responded by sending the expeditionary force that initiated the first Opium War. British gunboats crushed mediaeval Chinese weaponry, and brought one of the world's longest-lasting civilizations to its knees. Over the decades that followed, gunboat diplomacy and unequal trade impoverished the empire and addicted its people, inflicting a lasting trauma on the Chinese psyche. A new 'warring states' period had begun, and China began the long road of adaptation to modernity.

China's own narrative of its modern history begins with gravely unfair treatment by bullying Western powers, and leads on to a 'century of humiliation' at the hands of foreign imperialists.

China now thinks that its long period of weakness has ended, and that the first twenty years of the twenty-first century represent a 'strategic opportunity period.' As acknowledged by State Councillor Dai Bingguo, writing in December 2010, the world has grown smaller, and major issues now require an unprecedented degree of global interaction. Peaceful development, he observes, is neither a ruse by which China 'hides its brightness and bides its time' nor a naive delusion that forfeits China's advantages. Other forces within China remain cautious. PLA Senior Colonel Liu Mingfu wrote earlier in 2010 that China's rise, and a peaceful world, can be safeguarded only if China nurtures a 'martial spirit' and amasses military force sufficient to deter, or if necessary, defeat its adversaries.

Whether China can grasp the 'strategic opportunity period' will depend greatly on its ability to address the significant internal vulnerabilities that exist: economic, social and environmental, each one of which could fatally fracture it. If it can master these problems, much will then depend on its ability to gain power and yet remain at peace with the rest of the global community.

Whether the militaristic or developmental current of thought becomes dominant in China will depend to a great degree on the nature of its interactions with the West, and here there is considerable scope for mutual misunderstanding. In the strategic game of establishing and

avoiding encirclement, preemptive moves are a means of deterrence. Moves that China sees in this light tend to be viewed by the West as displays of aggression, and possibly a prelude to war. Meanwhile, China is far advanced in the global game of strategic encirclement, including moves in the Cyber Game, though largely below the Western radar. Moves that the West sees as deterrent, such as the US strategic tilt towards East Asia, tend to be seen by the Chinese as representing an intolerable threat of encirclement.

It is possible to interpret China's cyber strategy in the context of its 'strategic opportunity period', though not without some residual ambiguity. Some of this may be because future cyber conflict may take many forms that are not yet familiar. On the other hand, ambiguity can be a deliberate way to create hidden strategic options, somewhat like the two inconsistent telegrams sent simultaneously by Khrushchev during the Cuban missile crisis. A strategy can also be intended to hide in plain sight, as part of its design ingenuity.

Consider therefore the following description, which is based on one possible interpretation of Chinese cyber strategy. It is a thought experiment, and something that might, in principle, be attempted by any country.

This is a hypothetical cyber strategy of enormous global ambition and audacity in which knowledge itself is directly the prize. This might well be the ultimate type of cyber 'initiative' in a global knowledge economy. One of its interesting features is the difficulty of characterizing it appropriately using the terminology currently available in English, particularly in regard to its underlying intention.

Imagine a formidable knowledge-era 'competitor', for example a powerful national government, one that is ingenious and unconstrained. This 'competitor' decides to mount a global knowledge raid on multiple coordinated fronts. At the cyber level, acting through proxies for deniability, it breaches computer systems around the world on an industrial scale, exfiltrating many petabytes of information on a sustained basis.

This raid actually goes undetected during the first few years, because initially most of the target organizations are not equipped to identify the attacks. Once it is detected, it remains eminently deniable because each specific instance is not enough to justify a retaliatory response, and the overall scale of the attack cannot be seen unless the whole picture is assembled and made public, which the target organizations are mostly unwilling to do, for reputational and other reasons. Even if the picture is put together, it still flies under the radar of international law as, at worst, it constitutes espionage, which is tacitly permitted under the Law of Armed Conflict (LOAC).

By making use of commercial competition for the implementation of its national geopolitical strategy, the 'competitor' also exploits pro-competitive economic regulation in the target economies, which are predominantly open in comparison with its own closed economy. It makes extensive state-bankrolled purchases of many critical parts of the local economies and infrastructure under the guise of independent commercial acquisitions. These include contracts for provision of national Internet backbones, and equity stakes in utility companies. These enable it to control ever larger parts of the target economies, to instal national-scale

wiretaps in domestic networks and, in effect, to place remote off-switches in elements of critical national infrastructure.

Finally, to round off the effort, the ‘competitor’ simultaneously makes a massive effort to build its own domestic knowledge industry, sending students around the world in vast numbers to learn local languages and acquire advanced technical skills. In some cases, these students even manage to obtain funding from the target country educational systems. This effort, which only pays off on long timescales, allows it to consolidate and make full use of the information it has exfiltrated from around the world.

	Connection Physical data handling domain	Computation Virtual interactivity domain	Cognition Knowledge and meaning domain	
Cooperation Integrative social power (Infopolitik)	7	8	9	<i>Power as positive social reciprocity</i>
Co-option Economic exchange power	4	5	6	<i>Power as balanced social reciprocity</i>
Coercion Destructive hard power (Realpolitik)	1	X	2	<i>Power as negative social reciprocity</i>

Information hardware Information software Information wetware

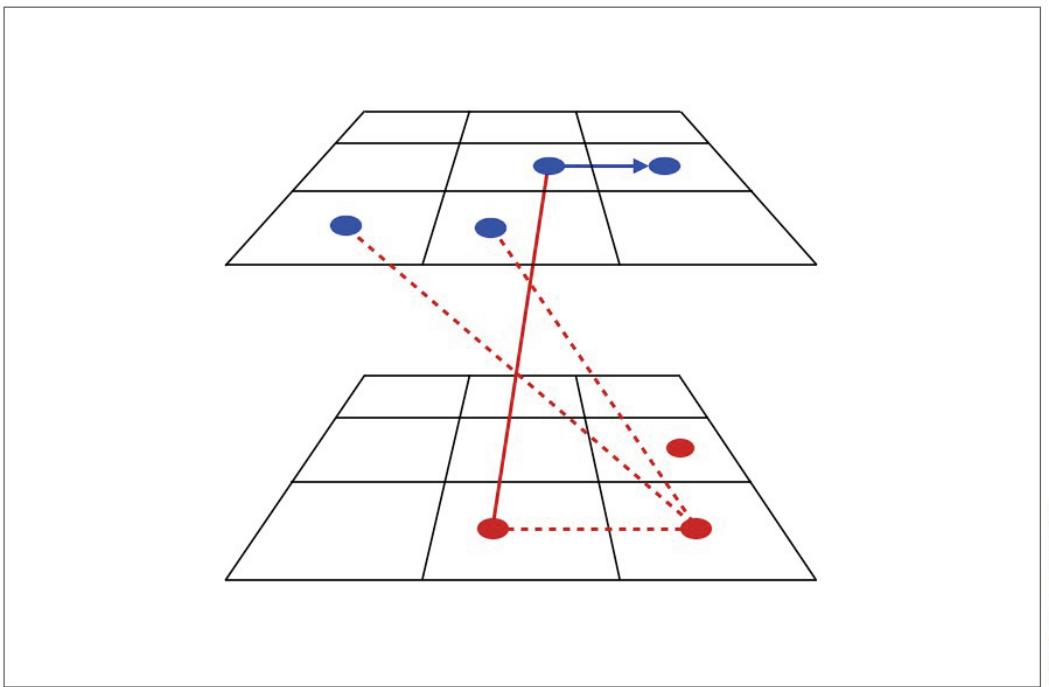
Graphic: © H Tibbs, 2013

United States government versus the Chinese government (alleged)

In short, in this thought experiment, a knowledge era ‘offensive’ is underway. If it is allowed to continue for long enough, the target countries will find that they have lost so much autonomy to the ‘competitor’ country that they are unable to resist a full cultural and economic take-over, which is ultimately accomplished without open hostilities ever being declared, or at least not of a type that would be recognizable as industrial-era conflict.

What lessons emerge from this thought experiment? This is in many ways the most extreme form of pure knowledge era conflict that can currently be imagined. Yet while LOAC is appropriate for industrial-era kinetic conflict, it is largely blind to actions which are hostile in the context of a knowledge economy. An attack can be highly distributed, so that the cumulative seriousness cannot be seen until it is too late. In terms of national security, our collective thinking has not caught up with the possibilities of cyber-era conflict, making us unable to recognize the overall pattern of what is underway or to attribute the right significance to it. National geopolitical strategy can be disguised as normal commercial

activity and, even if this is noticed, it cannot be challenged within the legal systems of target countries. Thus an international-scale offensive could be mounted without it ever being understood as such.



United States government versus the Chinese government (alleged)

These difficulties are somewhat reminiscent of the industrial cartelization strategy pursued by Germany in the years running up to the Second World War. This carefully orchestrated form of economic warfare was effectively invisible because it was positioned in the cognitive blind spot of British Empire industrialists. Until war broke out, and the deliberately engineered shortage of materials became apparent, they were unable to see it as anything but apparently profit-seeking industrial strategy on the part of German industry.¹⁰²

What sort of response should be made to a strategy like this, in the absence of anything that would be regarded as the use of force under international law, or any convincing evidence that one is imminent? Retaliatory kinetic attack would in any case be counterproductive because of the vital importance of mutual economic ties and very high levels of trade. To the extent that this does accurately describe Chinese strategy, possibly the United States and China could decide to wage an ongoing unacknowledged cyber war involving malware that stops short of physical damage. But is retaliation of any kind appropriate? Should the Cyber Game be played as a zero-sum game? The essential problem is that the strategy involves IP

¹⁰² Joseph Borkin and Charles A Welsh, *Germany's Master Plan* (New York: Duell, Sloan & Pearce, 1943)

theft on a grand, indeed global scale. This is real destruction of value for those companies and agencies who have been targeted, as a firm like Dyson is quick to assert.¹⁰³

Is there any other way of looking at this? Possibly the one thought that trumps Western outrage at the idea of information theft is to recall that it can be stolen without being lost, though it may be devalued. It may not be the knowledge itself but how we create it and use it that is important. In this view, the Cyber Game, being ultimately knowledge-based, is genuinely a non-zero game. Among economic players of the Cyber Game, this understanding is gradually turning into an approach that author Don Tapscott calls 'radical openness'. As an illustration, he points out that in October 2012 the pharmaceutical company GlaxoSmithKline took the unprecedented step of releasing all its clinical trials data on the Web. CEO Andrew Witty said the data would be released whether the clinical trial was successful or not. He called the move essential for finding new drugs, and to end suspicion that the company had secrets to hide.¹⁰⁴ In this light, a true knowledge-era strategy may not be stealing information but sharing it, playing the Cyber Game high on the gameboard, as Internet pioneers have been doing all along. Maybe Western democracies should respond to China's alleged actions in the same way. Dare they choose to reframe in this way?

The hypothetical cyber strategy is an example of wéiqí-like play on the Cyber Gameboard, creating a pattern of mutually reinforcing positions across the entire board, including the social power zone. However, in terms of actual Chinese cyber strategy, this is perhaps the point of greatest weakness. Instead of developing true integrative power beyond its diaspora, China appears to be primarily trying to achieve a comparable effect through public relations activity in cell 6 of the Cyber Gameboard. This desire to be seen in a favorable light in itself creates an opening for positive dialogue.

Furthermore, to the extent that China may be following the spirit of wéiqí, what does this say about its ultimate intentions? In wéiqí just fifty-one percent of the board constitutes victory, without requiring Clausewitzian-style destruction of the enemy citadel as in a game of chess. Is there a point at which China will simply stop its alleged strategy, alien though that may be to Western thinking? This prompts an interesting question: what would China lose if it stopped, and conversely, what if anything would the rest of the world gain?

China is far from being one single official line of thought. Different tendencies and outlooks are competing for primacy. To a degree, which aspect of its policy is encouraged, and which constituencies gain influence, will reflect which of their perceptions Western countries choose to act on. The part of China that is on the economic leading edge is very much open to change and adaptation. China's lingering official resentment about the Opium Wars means it can readily present itself as the wronged party and demonize the West. But it could potentially move beyond this, particularly if there is explicit recognition by the West, and specifically by Britain, of the historic injustice. Britain might also add its own thoughtful reflections about the long term burdens of empire. Alternatively, if simply treated as an

¹⁰³ <http://www.telegraph.co.uk/finance/yourbusiness/8936685/Sir-James-Dyson-attacks-China-over-designs-theft.html> accessed 18/02/13

¹⁰⁴ Don Tapscott and Anthony D Williams, *Radical Openness* (TED Conferences (iBook), 2012)

aggressor, Beijing may adopt a hardline position and be less accommodating to Western countries.

Likewise the potential for mutually accepted global rules in relation to cyber conflict may be greater than Western countries imagine if framed in terms of Chinese conceptual thinking. Any such proposals are likely to be much better received if put forward as being aimed at establishing a ‘harmonious global order’ rather than as rules presented as being in conformity with the enlightened Western way, which is increasingly seen as discredited and chaotic by China. China may of course regard itself as *primus inter pares* in any global order, but at least there are indications that it does accept in principle the idea of a multi-polar world.

Russia’s cyber strategy

The Russian view of the Cyber Game is set out in the *Doctrine of Information Security of the Russian Federation* of 2000. Information is seen as having strategic value and as being a key factor for the stability of the state, the regime and influential and leading actors. It is also important in war. According to the Russian Military Doctrine of 2010, information warfare should be used during the initial phase of a conflict against the opponent’s command and control capability, and in the form of a public information campaign during a conflict. Russia sees information warfare capabilities as including computer network operations, electronic warfare, psychological operations, deception campaigns (*maskirovka*), and the deployment of malware, back doors and logic bombs.¹⁰⁵

The cyber attacks against Estonia in 2007, widely believed to have originated in Russia, and the cyber attacks from within Russia that coincided with Russian military action in Georgia in 2008 are consistent with this policy, even though the Russian government has denied any involvement.¹⁰⁶ Interestingly, if they were to have involved the Russian government, the Georgian cyber attacks would be the classic case so far of a ‘strong’ definition of cyber war, which is the use of cyber attacks in conjunction with conventional warfighting, not cyber attacks in isolation.

Russian information security is not seen only in destructive terms, however, as the 2000 Doctrine lists the importance of protecting against ‘information influence of foreign political, economic, military and information structures on development and realization of strategy of the foreign policy of the Russian Federation.’ It also cites the need to ‘ensure formation in a new generation and preservation in the society of necessary moral values, patriotism and civil responsibility for the destiny of the country.’¹⁰⁷ It is instructive to appreciate why this is viewed as legitimate by Russia, and part of the answer goes back to a school of thought that sees Russian society and politics as being founded on the idea of a ‘government of truth’ in contrast to the ‘government of law’ principle in Western democracies. Faith in the ability of a

¹⁰⁵ Roland Heickero ‘Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations’ FOI, Swedish Defence Research Agency, March 2010

<http://www.highseclabs.com/Corporate/foir2970.pdf> accessed 08/03/13

¹⁰⁶ <http://www.economist.com/node/12673385> accessed 30/03/13

¹⁰⁷ ‘Doctrine of Information Security of the Russian Federation’ 9th September 2000, p.26 & p.31

<http://www.dcaf.ch/Chapter-Section/Information-Security-Doctrine-of-the-Russian-Federation> accessed 28/03/13

Russian leader to know the truth is grounded in a belief in the spiritual superiority of Russian culture. Information is then the means whereby the government presents the truth (*pravda*) to the people and *propaganda* (advocacy) for the truth is a legitimate tool. To do this well, the state must be strong but, as Vladimir Putin said in 2000, ‘the stronger the state, the freer the individual’.¹⁰⁸

	Connection Physical data handling domain	Computation Virtual interactivity domain	Cognition Knowledge and meaning domain	
Cooperation Integrative social power (Infopolitik)	7	8	9	<i>Power as positive social reciprocity</i>
Co-option Economic exchange power	4 X	5 X	6	<i>Power as balanced social reciprocity</i>
Coercion Destructive hard power (Realpolitik)	1 X	2 X	3 X	<i>Power as negative social reciprocity</i>

Information hardware Information software Information wetware

Graphic: © H Tibbs, 2013

Russian cyberpower (illustrative)

This stance is not, of course, consistent with the Western concept of ‘Internet freedom’, though it is consistent with industrial-era ‘Westphalian’ sovereignty. But the Cyber Game is both a global and a globalizing game, pushing into post-Westphalian territory, so this issue of the legitimacy of state control of Internet content is a key source of tension, and underlies the ITU versus ICANN struggle for Internet governance. It also needs to be defused if we hope to achieve the upside *N-topia* scenario described later.

In the West the public value of information stems from the right to exchange it freely, regardless of what it is. In Russia the public value of information stems from the power to keep it true. The Western Enlightenment wisdom is that no ruler can be trusted to determine the truth, so the authentic Western cyber perspective should be, as during the Cold War, that vesting truth-telling in the people will ultimately win out over vesting it in a ruler.

¹⁰⁸ Douglas Carman, ‘Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass Media & the Politics of Identity’ *Pacific Rim Law & Policy Journal*, University of Washington School of Law, (Spring 2002) https://digital.lib.washington.edu/dspace-law/bitstream/handle/1773.1/757/16_11PacRimL%26PolyJ339%282002%29.pdf?sequence=1 accessed 05/03/13

For the moment, Russia appears to be biding its time while it builds capability. It does not see itself as necessarily constrained by the same rules that govern Western countries, but it is likely to maintain a cautious stance as long as it still relies on Western cyber infrastructure and until it has built up its own cyber infrastructure.

Civil society cyber players

Civil society cyber players, who span everything from NGOs to open-source software developers, mostly operate in the social power level of the Cyber Gameboard. Possibly the perspective that best reflects their thinking about the Cyber Game is the idea of fluid and open connectedness, or as Geoff Mulgan of NESTA calls it, reviving an old English word, connexity.¹⁰⁹

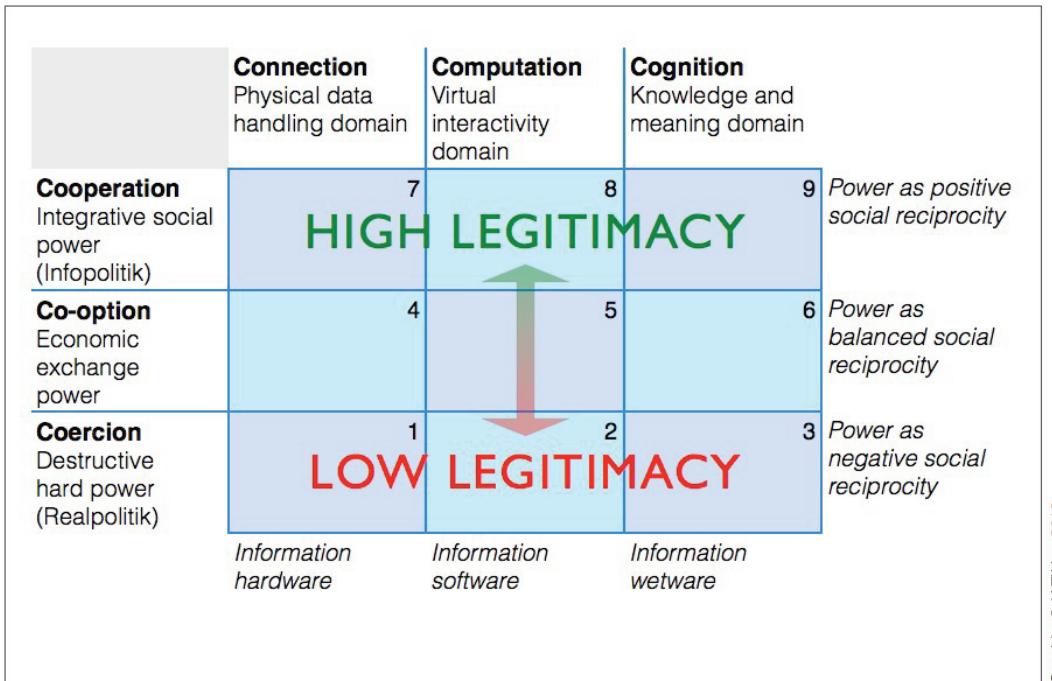
In this view, the rapid growth in global flows of information, travel, transport, and cultural exchange are making obsolete the previously dominant concepts and practices of a world of independent isolated actors. New concepts are emerging for dealings among actors who are no longer neatly bounded, and are subject to complex systemic interlinkages and instantaneous feedbacks. Powerful hierarchies still exist, but the new connectivity is favouring the rise of networks that are able to link concerned individuals directly and foster cooperation, rapid knowledge sharing and adaptation. The flexibility of networks, and their ability to organize quickly around issues and groups in need, is making them far more effective in dealing with complex problems than hierarchies built on the principle of specialized functional activities and layers of coordination and control.

There is an important generational perspective involved here too. In the words of Ben Hammersley, an Internet adviser to UK Prime Minister David Cameron, 'even if we personally are fine with trusting our rulers to decide... [what] we can and cannot see, the Internet collectively is absolutely not fine with it.' This, he says, is a point where the divergence of opinion between 'the networked, techno-literate generations (i.e. those who've grown up using the Internet) and the hierarchical non-literate ones (those who haven't) is most acute'. He goes on, 'For anyone who lives their life on the Internet, it is considered rude when someone denies you access to something. The Internet was built and is still creating itself through a principle of collaboration. If you post something on-line that is restricted access, you are rejecting that collaborative instinct. You should not be surprised that your content is likely to be targeted by hacktivists—on-line activists who use their hacking skills to gain access to the very data that you've tried to lock away.'¹¹⁰

To so-called 'digital natives', the Cyber Gameboard has always been there, and it has its own established and evolving ethic. Those who go against this ethic are seen as lacking legitimacy and credibility.

¹⁰⁹ <http://www.demos.co.uk/files/File/networklogic04mulgan.pdf> accessed 14/02/13

¹¹⁰ Ben Hammersley, *64 Things You Need to Know Now for Then* (London: Hodder & Stoughton, 2012)



Graphic: © H Tibbs, 2013

Legitimacy on the cyber gameboard

Many of the national security players about to enter the hard power level of the Cyber Gameboard must expand their view of the game from militarization to include cooperation, the top level of the gameboard, or they may find that the clash of perspectives provokes a cyber conflict of quite a different sort than they were expecting.

For example, governments in Tunisia, Egypt and Syria have found large international networks of volunteers supporting protester and revolutionary groups on their soil, pushing from outside for regime change and transparency.¹¹¹ Many of these volunteers, digital equivalents of the International Brigades, but who are ‘fighting’ from their own soil, are not fighting because of a perceived kinship with revolutionary groups. They may even lack detailed knowledge of the local political situation. But they do recognize the general appearance of state repression of what they think of as legitimate protest, and are reaching over national borders to provide sophisticated technical assistance to the underdogs simply because they are underdogs. Although no major incident has yet come from this kind of activism, untangling the resulting diplomatic issues could be complex, particularly in scenarios where physical world hard power retaliation was visited on activist networks by the states they were acting against.

Lines become particularly confused when a given packet of information crosses jurisdictional and player-network boundaries several times. For example, data about human rights abuses may be passed from within a regime, through local activist networks, then through international activist networks, and finally to the global media. In a situation like this, actions

¹¹¹ <http://www.aljazeera.com/indepth/opinion/2011/09/201192712428972155.html> accessed 30/03/13

taken early on in the process may be illegal according to local law, but later publication may be clearly legitimate and legal by international standards.

In such instances, the clash of values can be a devastating blow to a regime engaged in an internal struggle. As long as hard power measures taken by regimes to suppress revolutionary movements on their soil stay within their borders the nature of these conflicts will not change much, but as technical support from external third parties becomes an increasingly important part of such struggles, security issues will spread in a complex non-linear fashion. Civil society is a global force but so, potentially, is the counter pressure. Balancing the benefits and risks of civil society activism in international struggles may be a substantial foreign policy issue in future.

Business and the Cyber Game

The business perspective on the Cyber Game is that it is principally a means to make money. Despite the obvious potential, unfamiliarity and the difficulty posed by the information dilemma has made it hard for many businesses to make the transition from pre-existing to information-centric business models. From the heady days of the late 90s, and talk of a new economy based on entirely new principles, to the dotcom crash of the early 2000s, to the more recent convergence of hyperbole and pragmatism, it has taken a great deal of experimenting and theorizing to arrive at viable Internet-native business models and there is no sense that the transformation is complete.

Though forewarned, business was unprepared for the advent of e-commerce in the late 90s, which was based not on mainframe computers but on the World Wide Web, a hyperlinked collection of interactive information resources riding on the Internet. By the mid-2000s the Web had evolved into the so-called Web 2.0, also known as the 'Social Web,' a second generation of web-based communities and services, such as social networking sites and wikis, which aim to facilitate creativity, collaboration and sharing between users. The term Web 2.0 became popular following the first O'Reilly Media Web 2.0 conference in 2004. According to O'Reilly, 'Web 2.0 is the business revolution in the computer industry caused by the move to the Internet as platform, and an attempt to understand the rules for success on that new platform.'

The next development was the 'cloud', the notion of the Internet as a platform for powerful distributed applications. The essence of cloud computing was captured in a 2006 Wired Magazine headline: 'The desktop is dead. Welcome to the Internet cloud, where massive facilities across the globe will store all the data you'll ever use.' In the article following the headline, George Gilder described why this was happening:

'Back in 1993, in a midnight email to me from his office at Sun Microsystems, CTO Eric Schmidt envisioned the future: "When the network becomes as fast as the processor, the computer hollows out and spreads across the network."...In which direction would the profits from that transformation flow? "Not to the companies making the fastest processors

or best operating systems," he [correctly] prophesied, "but to the companies with the best networks and the best search and sort algorithms."¹¹²

The potential of the cloud to deliver full scale applications was realized when Google introduced Gmail, quickly followed by Google Maps, web based applications with rich user interfaces and PC-equivalent interactivity. In a sense this was merely a recapitulation of the client-server model of computing from the 1970s, but with vastly more computers and far faster networks.

The global community of commentators in the blogosphere struggled to interpret what these developments meant for business. Tim O'Reilly, a leading commentator, offered this interpretation: 'Web 2.0 is the network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an 'architecture of participation,' and going beyond the page metaphor of Web 1.0 to deliver rich user experiences.'¹¹³

Many new companies exploited the new features offered by Web 2.0. These included Google (AdSense and Web-based applications), eBay (using reputation), Wikipedia (trusting readers as authors), Flickr and del.icio.us (using tagging instead of taxonomy), BitTorrent (radical decentralization), and Cloudmark (aggregating user decisions).

The Web 2.0 approach is to allow the user to control their own data within a context set by applications that use the Web as a platform. Following from this is the idea that the individual's primary interface with the Web becomes the personal profile, and 'social software' will allow the user to create social networks online and relate to the world and to Web-based applications and services through their profile. As large numbers of users are attracted to these services, the software is able to extract useful information from the aggregate behaviour and choices of all those users. This information then becomes available to the individual user in a way that would not be possible if they, and all the other users, did not participate by registering, establishing their profile and entering the social network.

The latest business development in the Cyber Game is the increasing value of data analytics or data mining and the related idea of 'big data'.¹¹⁴ As the cost of bandwidth and storage drop, and mobile devices proliferate, vast amounts of information about everyone and everything are being generated and captured in real time. Everything that can be digitized will be digitized, and the digitized information will be available everywhere instantly, before, during and after the activities and events it is associated with.

¹¹² George Gilder, The Information Factories' *Wired* vol.14, no.10 (October 2006)

¹¹³ <http://radar.oreilly.com/2005/10/web-20-compact-definition.html> accessed 18/02/13

¹¹⁴

http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation accessed 18/02/13

This exponentially growing flood of data, hence ‘big data’, can be retained indefinitely in a form that can be mined and acted on, and is becoming increasingly valuable as a powerful way to find new business opportunities. The value will increase if this information can be distributed in common formats that allow it to be shared and paired. ‘Information wants to be social’¹¹⁵—it gains in value when it is made available and combined with other information, and when the result is presented in a form that allows action to be taken on it.

A key concept here is ‘informationalizing’, which refers to the addition of dynamic information content, features and functions to a product or service. The resulting increase in value comes not from material changes but from new intangibles, such as choice, variety, responsiveness, intelligence and enhanced services. Often the profitability of the new features exceeds that of the original product or service. The more dynamic information capability a product has, the more it mobilizes information and the more it is likely to evolve beyond the usage patterns and scope of the original product or service.¹¹⁶

One consequence of the flood of data is that business players are compiling substantial dossiers on individuals. The ability to deliver precisely targeted advertising is the major revenue stream of many, if not most, large dotcom companies. Programmes from Google or Facebook compile information from a wide variety of sources, enrich it with ‘clickstream’ resources from ‘Like’ buttons, searches, partner sites and more detailed psychographics and biographies. When the Obama campaign used these techniques to mobilize support during the US presidential race, big data began to translate into big political power. This points to a potential convergence of business and state cyberpower resources that could have significant implications for civil liberties.

The energy and effort business players are pouring into understanding the economic dimension of the Cyber Game is enabling them to build very considerable know-how in using digital information to create economic value. Although they are lagging on the cyber security front, they are definitely the leading player in creating direct value from the global information infrastructure. If governments are to have any hope of regulating this concentration of know-how, they have a long way to catch up.

Criminal players and the Cyber Game

The value created by business Cyber Game players is, of course, subject to rising costs imposed by a class of cyber players directly opposed to the public interest, the organized crime groups. They use a mirror-image of cyber-business methods to create sophisticated online sales platforms for stolen information and malware, and it is big ‘business’.¹¹⁷ The selling price of a previously unknown vulnerability or remote zero-day exploit for the

¹¹⁵ <http://www.socialsquare.dk/2012/06/03/information-wants-to-be-social/> accessed 14/02/13

¹¹⁶ Thomas Redman, *Data Driven* (Boston: Harvard Business School Publishing, 2008)

¹¹⁷ Chris Grier et al., ‘Manufacturing Compromise: The Emergence of Exploit-as-a-Service’ *The Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS)*, (October 2012) http://www.imchris.org/research/grier_ccs2012.pdf accessed 26/02/13

Macintosh OS, for example, is reported to be \$200,000.¹¹⁸ And in a 2011 study, the cyber security firm Symantec estimated global cyber crime was running at \$114 billion annually.¹¹⁹

The existence of very large botnets under criminal control also gives criminal cyber players immense computing power. A botnet is formed when malware penetrates and links a large group of computers, allowing them to be remotely controlled to act in a coordinated fashion for malicious purposes, usually without the owners' knowledge. Each compromised computer is called a bot or a 'zombie'. Botnets can be used to send malware or spam, or to launch attacks. BredoLab, reported to be the largest botnet so far discovered and partially dismantled in 2010 by Dutch law enforcement, consisted of 30 million zombie computers, capable of sending 3.6 billion spam messages a day.

Just as business often creates environmental pollution and leaves the government to pay for cleaning it up, so business is leaving much of the cost of cyber insecurity to others. Considering the paltry investment in countering cyber crime by the government, it might be wise to look to the main beneficiaries of cyber commerce to carry more of the costs of its cyber-security; instead a new industry is springing up to sell cyber security to government.

Public perspectives on the Cyber Game

As cyber players, the public range from passive bystanders to a few so-called 'super-empowered individuals' who are empowered by digital information technology. In general though, most people would be well-advised to pay more attention to what is happening on the Cyber Gameboard around them, or they will find they are the subjects of collateral damage.

People know that business models based on amassing personal data are not entirely benign. Facebook users of all ages are frequently irritated by the cavalier way it changes privacy settings without warning, and the uncertainty about what is happening to their personal information. But the implicit deal with Facebook is that if you are intrepid enough to trust it with your personal data, it will sell your resulting 'social graph' in exchange for connecting you with your friends.

If government and business begin to join forces in online profiling, so that, for example, Internet service providers' traffic logs are merged with databases such as credit card transactions into a single integrated picture of a person's life, at some point a 'threshold of transparency' will be crossed. Past this threshold, individuals will feel their lives represent an open book to the government and private enterprise. The threshold of transparency will vary from individual to individual, with responses ranging from a generic 'Facebook is compiling data about me' to a literal paranoia about being watched because, after all, it actually is true that mobile phones are evolving into more and more effective surveillance platforms.

The threshold will quickly be approached if industry persuades government departments to amass big data on citizens without appropriate safeguards. When mandating large-scale databases, governments should be wary of using their powers to compel citizen compliance

¹¹⁸ From commentary submitted to the Inquiry by Smari McCarthy

¹¹⁹ http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 accessed 18/02/13

with schemes that could put safety and privacy at risk. However attractive the economic opportunities may look, government's task is also to protect citizens, not merely to facilitate the plans of private enterprise. This appears to explain why, for example, the latest plans to introduce an integrated electronic health record in the UK¹²⁰ have drawn strong objections from both computer experts and health professionals.¹²¹ If the benefits of big data are to be realised in the area of public services provision, governments must be able to distinguish between well-designed and poorly thought-out schemes, which means freedom from conflict of interest and a balance of know-how between public sector and private sector cyber players in the economic power level of the Cyber Gameboard.

On these issues, EU and US data protection philosophies diverge sharply. In the EU, the nascent 'right to be forgotten' suggests that users have an inherent right to ask institutions and companies to purge their records, based on the principle that the individual owns the data companies hold about them. In the US, information about individuals is regarded as the property of the organization that obtained it, and there is no parallel right. This may have substantial long-term implications for the interoperability of EU and US ventures, perhaps resulting in delayed treaty harmonization, as has been the case for copyright and patent differences between EU and US approaches.

Another public concern is the impact of the Cyber Game on employment. Advanced information-processing algorithms plus the continued march of Moore's Law may be about to displace many old jobs,¹²² but the view of business economists is that the useful output of the algorithms can be expected to replace the old jobs with new ones. Where and what these jobs will be is glossed over, as no one knows. But if algorithms have now reached the level of performance where they disproportionately erode professional jobs, then the hollowing out of the middle class will accelerate. The question for government cyber players is whether this itself is a cyber security risk.

Kim Dotcom versus the US government

The information dilemma described earlier has the potential to be a source of conflict, involving the interests of civil society, business and state in complex combinations that have not been well understood to date. This is illustrated by the case of Kim Dotcom, formerly Kim Schmitz, a German national living in New Zealand, whose company Megaupload was taken down on 20th January 2012 in a law enforcement operation initiated by the US government. Megaupload.com was a free online storage space, a warehouse in the cloud with 50 million users a day at its peak and annual revenues of \$175m. The US Department of Justice maintained that the site was used for illegal file sharing, particularly of videos and music, and had Dotcom arrested for copyright infringement among other charges.¹²³

¹²⁰ <http://www.telegraph.co.uk/news/politics/9804402/Privacy-fears-as-Jeremy-Hunt-orders-health-records-to-be-shared-throughout-NHS.html> accessed 18/02/13

¹²¹ <http://www.lightbluetouchpaper.org/2013/01/16/privacy-considered-harmful/> accessed 18/02/13

¹²² <http://singularityhub.com/2012/11/12/1-million-robots-to-replace-1-million-human-jobs-at-foxconn-first-robots-have-arrived/> accessed 30/03/13

¹²³ Charles Graeber, 'Kim Dotcom' *Wired* vol.20, no.11 (November 2012), 158-161 & 192-200.

Businesses selling content that either is or can be digitized, such as the music industry and newspapers, are strongly affected by the information dilemma. The information 'wants to be free' but the content industry wants it to be expensive. The problem is that accessing this content for free by computer has become easier than purchasing and consuming it in its traditional form.

One response to this dilemma is to accept that content will become free and devise alternative business models. As Internet commentator Chris Anderson put it in his blog, 'Unlike simply selling what we make, *free* requires creative thinking about how to make money *around* what we make.'¹²⁴

Commercial music content first became free thanks to innovations such as Napster, the free music file sharing service that operated between 1999 and 2001, and other peer-to-peer file sharing software. The underlying idea seems to have been that if online content is going to become free anyway, this tendency might as well be actively harnessed to make the information free and accessible for use and re-use by everyone, since this would be a social good.

If information content is free, commercial opportunities for content do not disappear. Instead they transform. Although some musicians, such as Radiohead, found Napster useful as a form of promotion, the established music business fought it vigorously in the courts, leading to its bankruptcy and closure in 2002. Meanwhile, Apple made use of exactly the same information technology principles to reinvent the music business legally.

Incumbent content firms faced by the information dilemma can either choose to fight back or innovate. Taking legal action is not exactly good publicity, and consumers understandably prefer the convenience of digital access. Innovation is likely to involve a fusion of new business model and new technology, as Apple demonstrated with iTunes and the iPod, which made paying for digital content as easy as free access, and integrated it into a very desirable consumption device. Interestingly, despite grumbling from the music industry, both music companies and artists make more money from each iTunes sale than they do from a retail store music CD sale.¹²⁵ By mid-2012 in the US, Apple had 64 percent of the digital music market and 29 percent of all retail music sales.¹²⁶

When newspapers first moved online they voluntarily provided free access which, along with a loss of advertising to the web, gradually undermined their traditional business. Towards the end of his life, Steve Jobs was instrumental in persuading *The New York Times* to charge for subscriptions on the iPad, reportedly berating them for having given away the paper free online for too long¹²⁷. Jobs has been vindicated once again, as *The New York Times* is now one

¹²⁴ http://www.longtail.com/the_long_tail/2007/11/free-is-more-co.html accessed 14/02/13

¹²⁵ <http://www.cultofmac.com/38097/infographic-most-artists-earn-more-revenue-through-itunes-than-at-retail/> accessed 14/02/13

¹²⁶ <https://www.npd.com/wps/portal/npd/us/news/press-releases/itunes-continues-to-dominate-music-retailing-but-nearly-60-percent-of-itunes-music-buyers-also-use-pandora/>!ut/p/c5/04_SB8K8xLLM9MSSzPy8xBz9CP0os3g3b1NTS98QY0MDbydTA08vSzcnV38LQ0dTc_1I_ShznPI-ZvoF2YGKAMP77Ro/! accessed 14/02/13

¹²⁷ Walter Isaacson, *Steve Jobs* (New York: Simon & Schuster, 2011)

of the most successful online newspapers, with rapidly rising subscription sales estimated to be \$91m and 12 percent of all subscription sales this year.¹²⁸

	Connection Physical data handling domain	Computation Virtual interactivity domain	Cognition Knowledge and meaning domain	
Cooperation Integrative social power (Infopolitik)	7	8	O	9 <i>Power as positive social reciprocity</i>
Co-option Economic exchange power	4	O	O	6 <i>Power as balanced social reciprocity</i>
Coercion Destructive hard power (Realpolitik)	X	X		3 <i>Power as negative social reciprocity</i>
	<i>Information hardware</i>	<i>Information software</i>	<i>Information wetware</i>	

Graphic: © H Tibbs, 2013

United States government versus Kim Dotcom

Although companies themselves may be reluctant to take legal action, the US government does seem willing to defend legacy industries, allegedly due to high level lobbying.¹²⁹ The heavy-handed takedown action against Kim Dotcom in New Zealand (which may yet prove legally and reputationally problematic for the US government) and the US federal prosecution of Internet innovator Aaron Swartz are cases in point. This had a tragic outcome in the case of Swartz, who committed suicide,¹³⁰ but in the case of Dotcom it has simply triggered a new and more resistant round of evolution that further intensifies the information dilemma. He openly describes the goal of his new online business, Mega,¹³¹ in these terms: ‘...within the next five years, I want to encrypt half of the Internet. Just reestablish a balance between a person—an individual—and the state. Because right now, we are living very close to this vision of George Orwell and I think it’s not the right way. It’s the wrong path that the government is on, thinking that they can spy on everybody’.¹³²

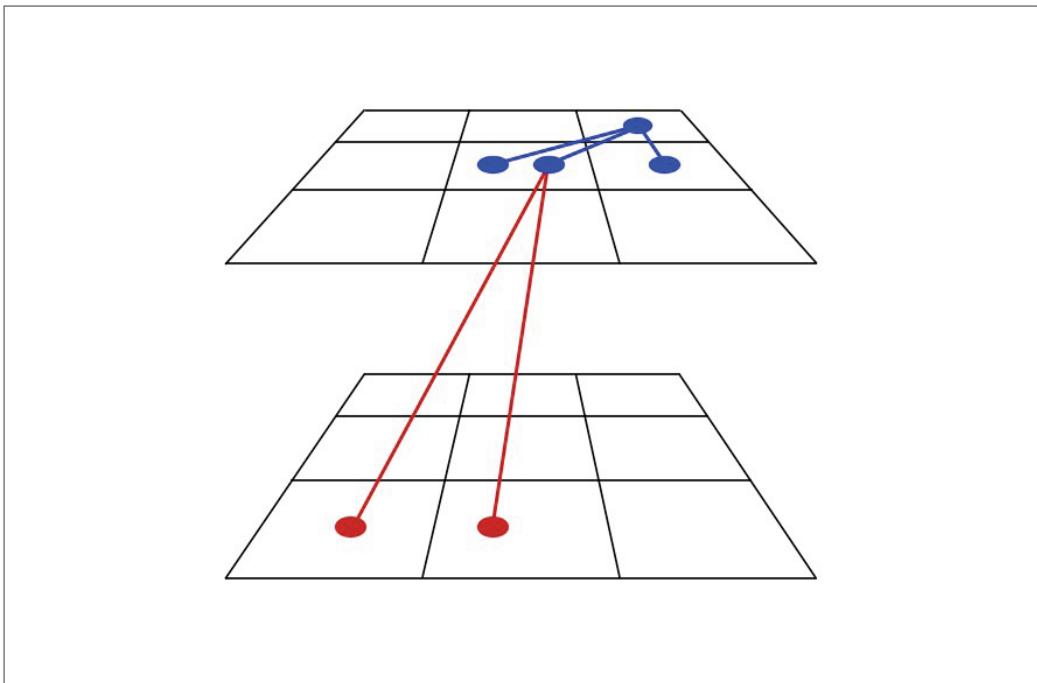
¹²⁸ <http://go.bloomberg.com/tech-blog/2012-12-20-the-new-york-times-paywall-is-working-better-than-anyone-had-guessed/> accessed 14/02/13

¹²⁹ <http://rt.com/usa/news/kim-dotcom-interview-mega-673/> accessed 14/02/13

¹³⁰ http://www.huffingtonpost.com/2013/02/05/aaron-swartz-memorial-darrell-issa_n_2619872.html accessed 14/02/13

¹³¹ <https://mega.co.nz/#privacycompany> accessed 14/02/13

¹³² <http://rt.com/usa/news/kim-dotcom-interview-mega-673/> accessed 14/02/13



Graphic: © H Tibbs, 2013

United States government versus Kim Dotcom

Dotcom is playing the Cyber Game at two levels, the economic and the social power level. Enabling people to share information is a social power play that gives him a high degree of cyber legitimacy, even though the means of providing the service is a commercial company. The US government is seen to have lower cyber legitimacy because it is using hard power to act against a social power resource. In this round of Cyber Game play Dotcom 'wins' and the US government 'loses'. Seen in terms of the Cyber Gameboard, this US Cyber Game play makes little strategic sense, particularly as there is a distinct risk it may lose in the courts against Kim Dotcom. If the US government is going to ally itself with US commercial Cyber Game players, it would do better to choose ones like Apple, which has very successfully managed to resolve the information dilemma for digital content and as a result has high cyber legitimacy.

Scenarios for the future of the Cyber Game

The Cyber Gameboard is not a static arena of interaction. The gameplay it supports is of course highly dynamic, but over longer time periods the gameboard itself as well as the play on it will also be subject to deep crosscutting currents of change and development. These are important for strategy as they will tend to shape and condition the game as time goes on, and influence strategic aims.

A number of change drivers have already been discussed, mainly related to the consequences of new information dynamics. They are central to the future of the Cyber Game, but are not of course the only future-shaping factors at work.

This section briefly discusses four additional potentials for change that are not a direct function of information dynamics. These include the redesign of Internet technology, the changing nature of future conflict and the future of the state. Overarching all these is the possibility that the entire global system may be on the threshold of discontinuous change, either a general collapse or a jump to a new pattern of organization. In addition, since this whole system outcome is at least partly related to continued information abundance, the way the Cyber Game is played could affect or even determine the overall fate of the global system.

The various change drivers are mainly described in terms of existing trends projected forwards. The future is not bound to follow existing trends, though it often does. But even when technology-driven trends consistently point to a more promising future, events may derail expected progress and these possible alternative outcomes can be captured as contrasting scenarios. At the end of this section, therefore, alternative future paths for the Cyber Game and the wider world context are framed in terms of scenarios.

Future Internet redesign

A good deal of the current concerns around cyber security are the result of the near-absence of security features in the original design of the Internet. It was originally built to facilitate communication in the closed communities of the military and academia, where people knew each other and could be trusted. In the 1970s, when the Internet was being developed, the encryption capability that could have made the Internet secure was still classified, and was only declassified in 1997 by President Clinton, long after the Internet's intrinsically insecure design had become entrenched. Public access to encryption allowed Internet commerce to explode, as Clinton intended, but it could only patch over the underlying problems.

Several efforts are now underway to address this problem at a fundamental level. The US government's Defense Advanced Research Projects Agency (DARPA) is funding a number of such efforts, some involving the original developers of the Internet, to redesign it from the ground up. The goal of DARPA's Clean Slate Design of Resilient, Adaptive, Secure Hosts (CRASH) project is to design 'new computer systems that are highly resistant to cyber-attack, can adapt after a successful attack to continue rendering useful services, learn from previous attacks how to guard against and cope with future attacks, and can repair themselves after

attacks have succeeded.¹³³ Peter Neumann, an 80-year old computer scientist at SRI International, is leading the CRASH effort and another, Mission-Oriented Resilient Clouds (MRC). The idea is to rethink everything from the silicon wafers to the applications, with potential solutions ranging from applications that continually change to elude attackers, to tagged architecture, in which each component of an application is encrypted to ensure its integrity.¹³⁴

In the same vein, Robert Kahn, the other co-inventor of the TCP/IP protocol, has proposed a Digital Object (DO) architecture which would identify all information flowing across the Internet by packaging it into 'digital objects' which allow easy identification of the type of data they contain, but not the actual data. Digital objects would have unique and persistent identifiers, which would specify such things as the nature and function of the data, how it should be handled and who should have access to it. One advantage of this proposal is that it could be incorporated into the existing Internet.¹³⁵

There are numerous Internet redesign initiatives, including the US National Science Foundation (NSF) funded Future Internet Architecture Project (FIA), its predecessor Future Internet Design (FIND), and the Global Environment for Network Innovations (GENI); the Named Data Networking (NDN) project of the University of California, Los Angeles (UCLA); the European Union's Future Internet Assembly (FIA) collaboration which combines 150 Internet research sub-projects; Japan's New Generation Network (NWGN) project, various projects sponsored by China's Ministry of Science and Technology;¹³⁶ and The Republic of Korea's Future Internet Project, among others.

The breadth of this basic research means that over time it is almost bound to lead to fundamental improvements in Internet security. This means that much of the cyber security problem that exists now may well be transient and, within 10 to 15 years, be just a bad memory. While it lasts, however, it is presenting serious problems which, if not handled skilfully, could leave a damaging aftermath.

From a national security perspective there are clear motives for wanting a more secure information infrastructure. One is the sheer uncertainty of knowing if critical information systems are compromised, particularly if pre-positioned malware is not used unless a real-world conflict erupts. Most military equipment now relies on on-board computers and network connections. At the moment of operational use, continuing cyberspace insecurity may mean that equipment does not function as and when expected. This will add enormously to the fog and friction of any incident, and may lead to unintended escalation in

¹³³ [http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_\(CRASH\).aspx](http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_(CRASH).aspx) accessed 18/02/13

¹³⁴ <http://www.nytimes.com/2012/10/30/science/rethinking-the-computer-at-80.html?pagewanted=all> accessed 18/02/13

¹³⁵ Robert E Kahn, 'The Role of Architecture in Internet Defense', *Chapter XII, America's Cyber Future, Volume II, Center for a New American Security*, 2011

http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf accessed 14/02/13

¹³⁶ Jianli Pan et al., 'A Survey of the Research on Future Internet Architectures', *IEEE Communications Magazine* vol.49, no.7 (July 2011) <http://www.cse.wustl.edu/~jain/papers/ftp/internet.pdf> accessed 14/02/13

a panicked effort to get something, or anything, to work. This could well overcome any strategic prudence that might otherwise be operating.

There are also some motives for resisting a fundamentally more secure Internet, mostly relating to intelligence operations. Whether an assurance that key equipment will work outweighs the loss of convenient surveillance is a question that defence organizations will need to address, though when the wider economic advantages are included in the calculus the advantages of secure information look persuasive. Some would argue that this is a non-issue as technological development is always an endless game of technical leapfrog, which would include the race between encryption and decryption. Nevertheless, individual technologies do mature and stabilize, locking in¹³⁷ around the outcomes of exactly this type of decision.

If the Internet and the information infrastructure in general do become substantially secure, and at the same time are architected to allow access for intelligence agencies, this does raise important ethical issues related to the right to privacy. Since, at this point, a secure Internet would almost certainly lock in for the long run, it is vital that the civil liberties and state accountability issues are addressed and built in before redesign is taken over by a 'just because we can' mentality.

The wildcard in this is the future of encryption; either encryption remains effective by always being a step ahead of all but the best-resourced players (the NSAs and GCHQs of the world) or conceivably some combination of Moore's Law and say quantum computing might tip the balance decisively in favour of either unbreakable ciphers or the cracking of every cipher. Either case would have severe consequences and, for example, the latter would be a disaster for all online economic transactions. If it came at a point when essentially all personal communication was online, it could transform social dynamics, though if it happened to the generation who have grown up with Facebook, perhaps they would be well-prepared for this outcome! Nevertheless, at least in terms of the prospect for quantum computing tipping cryptography into a terminal condition, this currently appears unlikely.¹³⁸

In short, the intrinsic security weakness of existing information architectures cannot be expected to last indefinitely. Either the Internet will be hardened and encryption will remain strong, which on balance in the wider picture would seem the best outcome, or the Internet itself may be progressively dismembered—Balkanized into islands—in search of security.

The future of human conflict

Although much of the Global Cyber Game will be about positioning for competitive advantage, some destructive cyber conflict is to be expected. Rather than immediately trying to think what form this might take, however, it is instructive to think about the future of human conflict in general, as it helps to put more speculative thinking into perspective.

¹³⁷ W. Brian Arthur, *The Nature of Technology* (London: Penguin Books Ltd., 2009)

¹³⁸ Ross Anderson and Robert Brady, 'Why quantum computing is hard—and quantum cryptography is not provably secure' *Quantum Physics* 7351 (Jan 2013) <http://arxiv.org/abs/1301.7351> accessed 26/02/13

It is at first surprising to learn that, despite the popular impression of increasing violence, war and violent deaths have actually been decreasing over time. According to evidence quoted by Harvard Professor Steven Pinker, violence in human society is in long run decline. According to the UCDP/PRI Armed Conflict Database, worldwide battle deaths in the first decade of the 21st century were 0.5 per 100,000 a year, which is lower than the homicide rate in the world's least violent countries. In absolute numbers, annual battle deaths have fallen by 90 percent from half a million per year in the late 1940s to 30,000 per year in the early 2000s. During this period interstate war shrank to vanishing point, and the greatest source of deaths was civil war. Even civil wars have become less lethal. In 1950 the average armed conflict of any kind killed 33,000 people, by 2007 it killed less than 1,000. Among the wealthy countries in the developed world the purely statistical risk of civil war is essentially zero.

If the long run decline and the recent statistics are taken as a guide to the probability of conflict over the next few decades, a not unreasonable assumption, then the most likely form of conflict is now civil war in countries with governments referred to as anocracies, neither fully democratic nor fully autocratic.¹³⁹

Income polarization is rising within wealthy countries, as a side effect of globalization, and is hollowing out the middle class. Commentators and researchers have noted this effect particularly in the US.¹⁴⁰ Whether this rising polarization could raise the risk of civil war in wealthy countries is questionable, as long as their governments remain effective. This itself will be a function of how well they adapt to the evolving information environment. If they fail, and a combination of financial, economic and environmental crises threaten the ability of governments to maintain the quality of life, then internal conflict is entirely possible.

One way of thinking about this possibility is that the economic impact of global F-space (the transnational 'flow-space' of global social and economic flows as described in the next section) on states that must govern locally in the 'space of places' is to sharply heighten income polarization in their home geography. The front line of potential conflict is not between nations but between social groups who benefit from the global economy of F-space, and those who do not. Either this disparity will be addressed or, if it develops too far, it will become a serious political issue, possibly in many countries at once, with populations splitting into two factions, either resisting or supporting civil society-led reform movements. Successful reform might be the result of crowd-sourced social redesign spanning many societies globally, along the lines of a more effective Occupy movement. If reform is denied, the anger of the 'indignados' might be expressed in the form of cyber attacks on the 'ground stations' of F-space, such as the wealthy financial districts of major cities.

In short, while globalization has been helping to reduce interstate conflict, it has simultaneously been stoking possible intrastate conflict. This would imply that any cyber conflict is less likely to be between states as such, and more likely to be between the winners and losers of globalization, even though the statistics suggest that the overall probability is

¹³⁹ Steven Pinker, *The Better Angels of Our Nature* (London: Penguin, 2011)

¹⁴⁰ <http://www.pewsocialtrends.org/2012/08/22/the-lost-decade-of-the-middle-class/> accessed 18/02/13

low. Nevertheless the trendline of declining conflict is not smooth, and an upsurge is possible.



Photograph: © H Tibbs, 2011

A meeting of the 'indignados' movement in Bilbao in May 2011

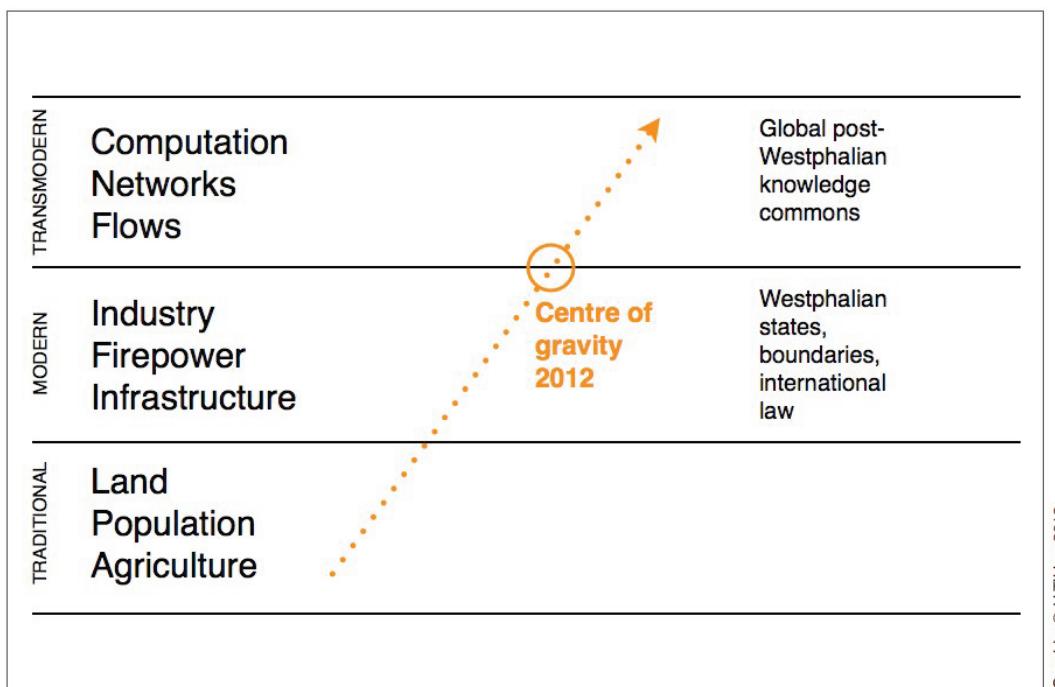
Nations become post-Westphalian

The industrial-era form of the nation state is referred to as Westphalian, after the Peace of Westphalia in 1648 after the Thirty Years War. This established the principle that states are the only international players and have a monopoly on force within their mutually recognized borders. States in the Westphalian system are independent and may not intervene in the domestic affairs of another state, either for reasons of self-interest or by appeal to any higher principle, as no higher power than state sovereignty is recognized. The domestic and international spheres are separated, and coexistence between states is regulated by diplomacy and treaties that form international law. Power is thus decentralized, and the use of force is not prohibited: occupation is considered a legitimate means of acquiring territory.

In a formal sense, the UN Charter in 1945 marked a move beyond the Treaties of Westphalia, because although it is strictly a treaty between signatory states, it regulates the use of force between states and, with the concept of human rights, introduced the idea that states are accountable to international norms for their domestic actions. This shift became decisive with UN Resolution 1244 on Kosovo in 1999 which, by declaring the Yugoslav government's authority invalid and sanctioning military intervention, redefined the sovereign character of the nation state.

In a less formal sense, the Westphalian system has been slowly dissolving for some time. This is particularly evident in the greater range and much larger number of players operating

internationally, including transnational companies, global media organizations, NGOs, and at the coercive end of the spectrum, international terrorist groups such as Al Qaeda. The freedoms and tools these organizations and networks employ are very similar to the tools used by transnational business for globalizing operations and, in many cases, they run ahead of state use of the same tools. Westphalian erosion is also clear from the growing constraints on state unaccountability, and on state freedom to use armed force. This pressure towards accountability is coming from many directions, ranging from NGO pressure to media coverage. Populations too are no longer static and ethnically homogenous, they are very large, highly mobile internationally, mixing ethnically, and the webs of social and business interactions are complex and global.



Graphic: © H Tibbs, 2013

The post-Westphalian transition

Life is no longer simple for the state. Once one of a few privileged players enjoying relative isolation, the state is now crowded together with very large numbers of other types of players in a high pressure environment in which geography is not a buffer. The state still has a special level of some resources, such as military power, but in the multiplayer information saturated environment these resources may prove less useful than before.

States are at different stages of development in their exposure to, recognition and acceptance of the evolution beyond Westphalianism. Some countries, for example China and Russia, are still keen to assert full Westphalian independence. Other countries, notably those of the EU, are already enmeshed in a deeply post-Westphalian situation. If the driving forces towards post-Westphalianism are such things as the increased migration, communications,

and trade that form part of rising global connectivity, then all states are on a conveyor belt to post-Westphalianism, but some will arrive sooner than others.

Possible global system discontinuity

The global socio-economic system has been experiencing a growth surge for over 200 years from a condition of low interconnectedness, low complexity, low technology, low throughput, low population, and low interdependence to high values of all those factors. This growth surge is the result of the scientific and industrial revolutions, and the spreading culture of modernity, which together have lifted global population from less than half a billion to over 7 billion people in under 300 years. A key measure of this change is complexity.

The global system has an 'evolutionary direction' towards greater complexity. This complexity delivers greater capability up to a threshold at which the structure of the existing system cannot handle the level of throughputs and intercommunication, and where marginal returns start falling.¹⁴¹ At this point, in order to continue developing, it must either transform to a qualitatively different state of organization from which it can continue to deliver increased capability or, if this fails, it will fall back to a lower level of complexity and capability. Falling back would be somewhat like a disorderly return to a previous time period.

What is not plausible is that the system will simply continue on its existing trajectory of increasing complexity supported by the existing pattern of organization. This is essentially why the current structure of the global system has frequently been described as unsustainable. To use the analogy of the board game snakes and ladders, the principal scenarios now are a very big snake or a very big ladder.

The jump to a qualitatively new level of organization is highly unlikely to be accomplished by conscious deliberate design from within the existing system structure, because present human knowledge and human agency operating within today's system are not up to the challenge.

A new structure is much more likely to emerge spontaneously as a consequence of the developing potentialities of the system as a whole. This is most plausibly going to involve massively parallel responses among large numbers of highly connected individuals, simultaneously generating many networked solutions to today's issues.

The quality of global connectedness, its openness and transparency, and the freedom it allows to innovate collaboratively and without fear, and to critique the existing system, will be a critical resource for enabling the system transformation that is now needed. Many other existing and emerging attributes would also be involved, but without the full functioning of global connectedness the potential of the whole system to make a transformational jump will be impeded or prevented.

A cyber scenario framework

The possible future changes described here, taken together with the earlier discussion and the history of cyber security to date, allow a simple scenario framework for the Cyber Game to

¹⁴¹ Joseph Tainter, *The Collapse of Complex Societies* (Cambridge: Cambridge University Press, 1990)

be assembled. The aim is to capture the extremes of where the game could end up. This spans three slightly overlapping periods, running from the past into the future:

- *The first period, running from approximately 1990 to 2010, is referred to here as the '**Free Lunch**' when states and hackers were essentially free to explore and exploit cyber possibilities on the Internet without any real expectation of detection, let alone reprisals. This meant that they did not have to fully resolve questions of doctrine, and were still operating in an experimental mode. The World Wide Web appeared and online commerce burst into life. Effective surveillance was possible because targets were naive about Internet vulnerabilities, and state and hacker capability. Defences were weak or non-existent, and while most activity was fairly random, a few well-organized, clear-sighted players were able to make substantial positioning gains.*
- *The second period, from approximately 2010 to 2020, is referred to here as '**Rising Alarm**'. The problem of cyber insecurity is now severe, but denial is still widespread, and the response of many organizations is disorganized and largely ineffective. The risk is high, because much of the global economy now depends on the Internet. State intelligence agencies are making effective use of cyber capabilities, but are beginning to encounter various forms of blowback. National military organizations are developing doctrine, and threaten to militarize cyberspace at the expense of economic and social development. Debate about ethical concerns is heating up, including issues such as privacy and surveillance, and robotic weapons. The long run implications are still not well understood as the experience base is limited, but a succession of limited cyber conflicts help to clarify thinking.*

The third period, from 2020 onwards, progressively splits into two different primary future possibilities, in which the best potentials of global information abundance are either won or lost. The big watershed is the likely global system 'bifurcation' from 2020 onwards, in which the overall system either transforms to a new state of organization, or regresses.¹⁴² This development affects everything, and is closely interwoven with the Cyber Game. The information revolution is entangled in most aspects of global change, frequently as a catalyst, and is an enabler of some of the more far-reaching potential solutions, so cyber change and global change tend to go hand in hand. Cyber-catalysed scenarios of global change are therefore an appropriate way to understand the various futures that both shape the Cyber Game and are shaped by it.

- *In the upside scenario, '**N-topia**', the world as a whole goes through the final 'deployment' stage of the information revolution and this turns out to be exactly the transformation needed to address most of the major global issues that looked intractable at the start of the 21st century. As a key part of enabling this, all the critical cyber issues are well managed. The global information infrastructure is re-architected and is now far more secure. The level of cyber exploits drops to a minimal level, and cyber security has become a matter of routine skills. Most online criminal activity is locked out by the new Internet architecture. As a result the Internet remains globally open and, following several rounds of negotiation, governance is shared*

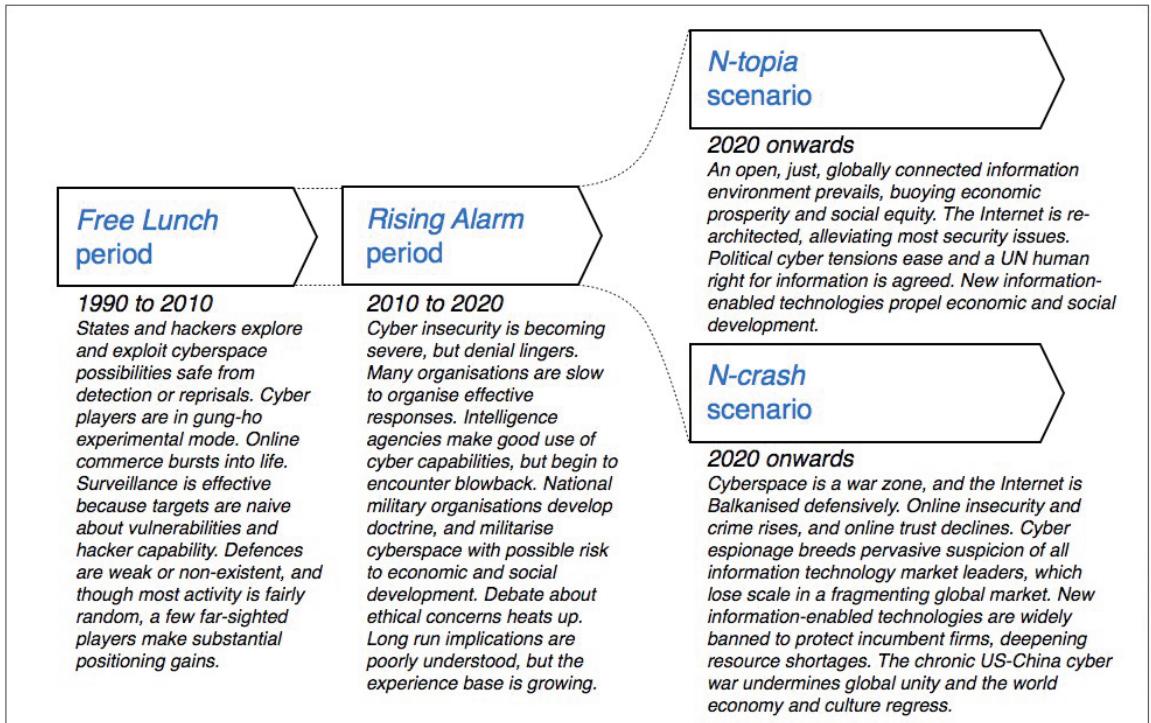
¹⁴² The conjectural timing for this is taken from Scenario 1 of *Limits to Growth*. Donella Meadows et al, *Limits to Growth: The 30-Year Update*. (London: Earthscan, 2004) p.169

internationally and is made democratically accountable. New algorithmic approaches to resource allocation are introduced in response to the technologies of abundance such as 3D printing. These displace market fundamentalism and economic disparities decline both within countries and between them. Privacy and state surveillance issues are addressed by a new UN Human Right for Information. What could have been serious emerging threats, involving nanotechnology and biotechnology, are managed effectively in the newly secure information environment. Reassured by the success of the architectural reforms and the new economic system, the US, China and Russia move far from their positions a decade or two earlier, and many of the old abuses now appear pointless.

- *In the downside scenario, 'N-crash', things do not go so well. The existing Internet architecture persists because there are too many alternative solutions and no consensus. The level of cyber crime rises to levels that act as a significant drag on economic activity. A massive but botched cyber offensive against online criminal organizations leaves the participating states looking weak and emboldens the criminals. Continued cyber attacks and espionage by the US undermine US market dominance in information products, and many countries and consumers who feel threatened by the US turn to Chinese manufacturers and Russian software providers. All the former information technology market leaders suffer because they lose critical scale as the global market fragments, and the pace of technological development slows. US total domestic online surveillance creates a repressive model that undermines much of its previous moral authority. Iran surprises everyone by creating an effective national intranet that proves robust to outside intrusion, and sells it to many states that feel threatened by the oppressive climate of online espionage. This further Balkanization undermines already faltering economic growth and trade. The technologies of abundance are made illegal in many countries to protect old resource-intensive industries, which heightens resource shortages and the rising environmental problems in many parts of the world. The chronic cyber war between the US and China spills over into cyber attacks on resource supply lines which splits the world into separate spheres of economic influence and greatly weakens the US.*

The message of these simplified scenarios is that the Global Cyber Game could have widely different outcomes over a 10 to 20 year period into the future. The aim of this report is not primarily to create cyber-security scenarios but to assess possible strategies for playing the game with reference to what we value culturally.¹⁴³ By depicting the upside and downside extremes, these scenarios aim to show the stakes for which the game is being played. Many players will be focused on winning short term advantage in the Cyber Game. But no player can cash out, and the longer run stakes are so high that all strategies must ultimately be evaluated against the contribution they make to the bigger outcome. The Cyber Game is both a game of tactical advantage and a contest for the future of humanity, and this means lifting the game to a higher level of thinking than has been typical in the geopolitics of the past.

¹⁴³ Scenarios can be used simply to explore different combinations of uncertainties, or can depict preferred (normative) or aversive futures, as here. Because the future remains persistently unknowable, both approaches are ultimately based on subjective judgments.



Graphic: © H Tibbs, 2013

Cyber Game scenarios

How the Cyber Game relates to cyberspace

The Cyber Gameboard is closely related to cyberspace, but rather than existing *in* cyberspace, it would be more accurate to think of it as being on the *surface* of cyberspace. This can be understood by looking more closely at the meaning of cyber and cyberspace.

The terms cyber and cyberspace are typically used in a fairly ambiguous way, and the words themselves need some clarification. In normal usage, according to the Oxford dictionary, 'cyber' is an adjective that means 'relating to the culture of computer and information technology.' Until recently the more popular word for this was *online*. The word cyber is a shortened version of cybernetics, the study of regulatory systems, which comes from the Greek word κυβερνητικός meaning *good at steering*.¹⁴⁴

Cyberspace is a noun that means, according to the Oxford dictionary, 'the notional environment in which communication over computer networks occurs.' In defence circles, the word cyber is sometimes also used as a noun to mean either cyberspace or more generally the Internet or the net.

The idea of cyberspace

The notion of cyberspace originally came into use almost as a joke. The term was first used in the early 1980s by cyberpunk science fiction author William Gibson, who later said, '...it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.'¹⁴⁵

John Perry Barlow, who founded the Electronic Frontier Foundation in 1990, famously said, perhaps somewhat tongue-in-cheek, 'cyberspace is where you are when you're on the telephone.' He also wrote in 1990 that 'the ambiguophobes' would soon want to define the conceptual map of cyberspace 'with punitive over-precision.'¹⁴⁶ And in 1994 Wolfgang Staehle, an artist and early online innovator, said of cyberspace, 'I don't know, if I try to define it today, I laugh about it tomorrow. It's developing so fast.'¹⁴⁷

In the years since, cyberspace has been adopted unquestioningly as a real thing and this presents a problem, at least for strategic analysis and operational purposes. The problem centers on the idea that the evocative but vague notion of cyberspace must first be precisely defined to make it operationally usable, just as John Perry Barlow anticipated.

The search for a perfect definition of cyberspace mesmerizes the Western mind. It does not trouble the Russian or Chinese mind. Part of the problem is linguistic. In English, cyberspace clearly implies the existence of a space or place that can be treated much like any other space. But cyberspace has no middle or inside, nowhere that can be entered. The border of cyberspace is cyberspace. Its interior is non-existent, somewhat like the inside of a Klein

¹⁴⁴ Henry Liddell & Robert Scott, *A Greek-English Lexicon* (Oxford: Clarendon Press, 1940)

¹⁴⁵ William Gibson: *No Maps for These Territories*, directed by Mark Neale, UK: Docurama, 2000.

¹⁴⁶ http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/crime_and_puzzlement_1.html accessed 14/02/13

¹⁴⁷ <http://www.lacan.com/frameVIII15.htm> accessed 14/02/13

bottle¹⁴⁸ (which is, approximately, a three dimensional version of the Möbius Strip). It could be said that cyberspace is a manifold of high-dimensionality with no ‘inside.’¹⁴⁹ It is all surface, all boundary. A simple analogy would be with a sheet of fishing net, which has no ‘inside’. Each node of the Internet, each connected computer, sits on the boundary of cyberspace, accessible from outside the network by virtue of its physical existence, giving entry not to an inside but to an interactive networked medium.

So cyberspace is not a space in the sense that it can be entered, occupied or conquered. It is not even the same thing as virtual space, although an infinite number of virtual spaces can be created, thanks to interfaces that simulate 3D environments. It would be less misleading to call cyberspace ‘electronic space’ or ‘computational space’ as that conveys the idea of networked computational power rather than a space similar to air or sea. It might be helpful to bring cyberspace down to earth by calling it ‘C-space’ to suggest computational space, while still keeping the link to cyberspace.

The concept of C-space is difficult to pin down because it is not a physical thing, or at least it is only partly physical. It is a dynamic field-like phenomenon generated by the entire networked computational environment, including all the user inputs and outputs, the software, the processing, and the hardware that directly hosts these functions. The best analogy is the brain, with its physical structure, its neural activity, and its resulting mental phenomena all contributing to a sense of mental space. C-space is, in effect, the global brain with its physical infrastructures, computational processing, and resulting intangible cognitive augmentation effects.

Any serious intent to act directly ‘in’ C-space (other than just disrupting it) would involve something equivalent to electronic psychology. Perhaps in the future it may be possible to work with ‘thought-like’ cognitive phenomena that arise literally within C-space itself and, thereby, influence human psychological responses.¹⁵⁰ For the moment, however, this prospect lies largely in the realm of science fiction.

In practical terms, thinking of C-space primarily as a boundary or surface yields a number of useful insights. Because C-space is not a place it cannot be entered by any physical object or person, therefore all users, and all physical objects acted on through C-space, are on the outside surface of the boundary. The boundary itself can be regarded as the interface between human consciousness and the ‘cognitive augmentation field’ of C-space. For the most part this interface is at the meeting point between an individual human awareness and the sensory affordances¹⁵¹ of a computational device (e.g. the screen and keyboard).

This means that the frontier of C-space is everywhere online individuals are. An organization may operate in C-space, but networked individuals must always act as its avatars, so to speak. In many cases, these individuals do not need to use their real-world identities. Indeed, the

¹⁴⁸ http://www.kleinbottle.com/whats_a_klein_bottle.htm accessed 14/02/13 & <http://plus.maths.org/content/imaging-maths-inside-klein-bottle> accessed 14/02/13

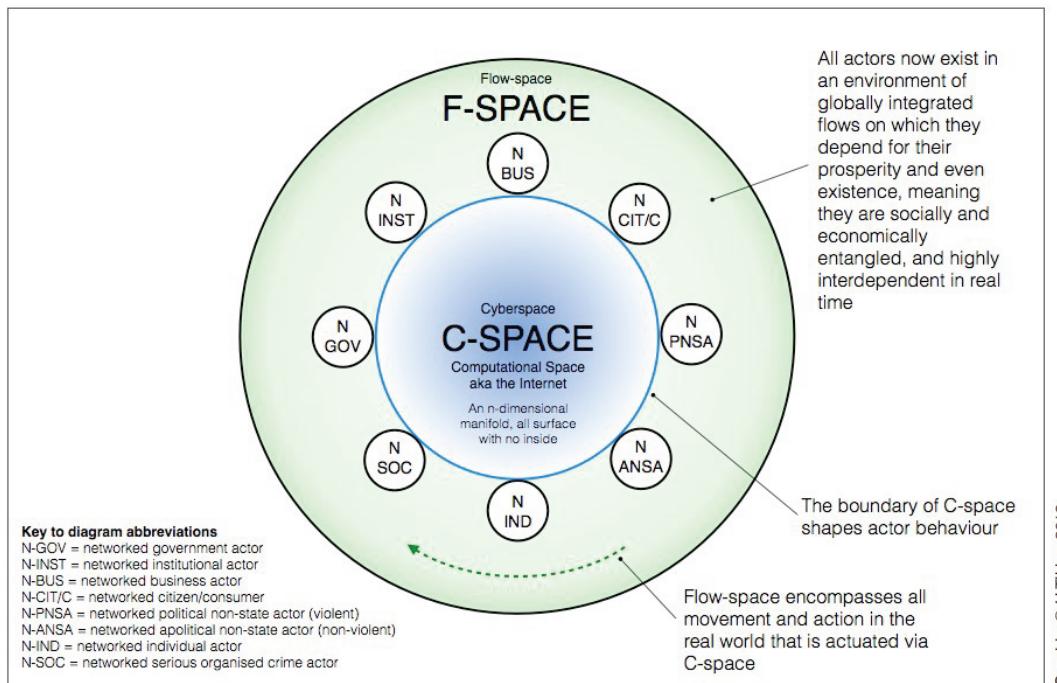
¹⁴⁹ From commentary submitted to the Inquiry by Smari McCarthy

¹⁵⁰ Ben Cerveny, *The Luminous Bath* <http://liftconference.com/videos/ben-cerveny> accessed 14/02/13

¹⁵¹ James J. Gibson, *The Ecological Approach to Visual Perception* (New Jersey: Lawrence Erlbaum Associates, Inc., Publishers, 1986), p.127

activist movement Anonymous demonstrates that an entire network of online actors can operate without any reference to their real-world identities.¹⁵²

All connected citizens of all countries live on the frontier, and they directly face the citizens of all other countries as individuals across the no-human's-land of C-space. This brings all global cultures into direct contact, and makes online culture shock a likely source of friction if not conflict (e.g. the Danish cartoons episode¹⁵³). At the same time, over the longer run it should tend to bring all cultures into much greater comfort with each other.



Graphic: © H Tibbs, 2013

C-space and F-space

The limitations of C-space as a new domain or environment

It is very tempting to imagine that C-space is fully analogous to familiar operational spaces such as air and sea, as they appear to provide a ready-made model for security thinking. In the native English-speaking (and Francophone) world, much emerging thinking about cyber security rests on the idea that a new military domain or environment¹⁵⁴ called cyberspace has come into being, and that it needs to be made secure for the state, commerce, and citizens—with preparation even being made for military operations 'in' cyberspace.

Unfortunately the cultural and operational limits of this perspective are likely to lead to the risk of being strategically blindsided by players such as Russia and China, as well as leading to incomplete operational doctrine.

¹⁵² http://canopycanopycanopy.com/15/our_weirdness_is_free accessed 30/03/13

¹⁵³ http://en.wikipedia.org/wiki/Jyllands-Posten_Muhammad_cartoons_controversy accessed 14/02/13

¹⁵⁴ MoD Operational Doctrine manual, 'Campaigning - Joint Doctrine Publication 01' MoD DCDC, 2nd Edition, December 2008

One way of categorizing state cyber actors would be in terms of those who want to play according to the rules as far as they can discern them, those who simply make use of whatever information potential is available, and those who make use of whatever information technology potential is available. The Russians think of Western countries as 'rule-based' players, but do not regard themselves as being limited by the same rules. The rule-based players tend to want clear definitions as a basis for codifying the rules, while the more opportunistic players simply take action and may gain an unforeseen advantage.

It would be more constructive, therefore, to shift from thinking about trying to do things 'in' C-space, which strictly speaking remains an illusion, to thinking instead about the comprehensive control of effects produced via C-space. This is both a more accurate interpretation of the technical reality and more closely focused on fundamental operational objectives.

A growing feature of our highly networked world is that more and more effects achieved in physical space are actuated via C-space, that is to say a growing number of actions in physical space are dependent on and determined by information flowing through C-space. Increasingly, flows of information through C-space are directly determining physical flows and actions in real space, to the extent that this is giving rise to a new hybrid space that can be called flow-space (abbreviated here to F-space), after the 'space of flows' concept originally articulated by sociologist Manuel Castells.¹⁵⁵ If there is a new operating domain or environment, a good case can be made that it is F-space, not C-space.

The distinction between C-space and F-space brings useful insights to the Cyber Game which, at the risk of introducing additional new terms, are worth exploring.

The anatomy of F-space

An increasing number of Internet nodes are mobile, and their movements and actions in real space are partly or completely determined by information flowing to them from C-space. These mobile nodes range from individuals in the street with smartphones, to container ships on the high seas, to stock-picking robots in warehouses.¹⁵⁶ All actors now exist in an environment of globally integrated flows on which they depend for their prosperity and even existence, meaning they are socially and economically entangled, and highly interdependent in real time. F-space is this dynamic aspect of physical space, encompassing all movement and action in the real world that is actuated via C-space.

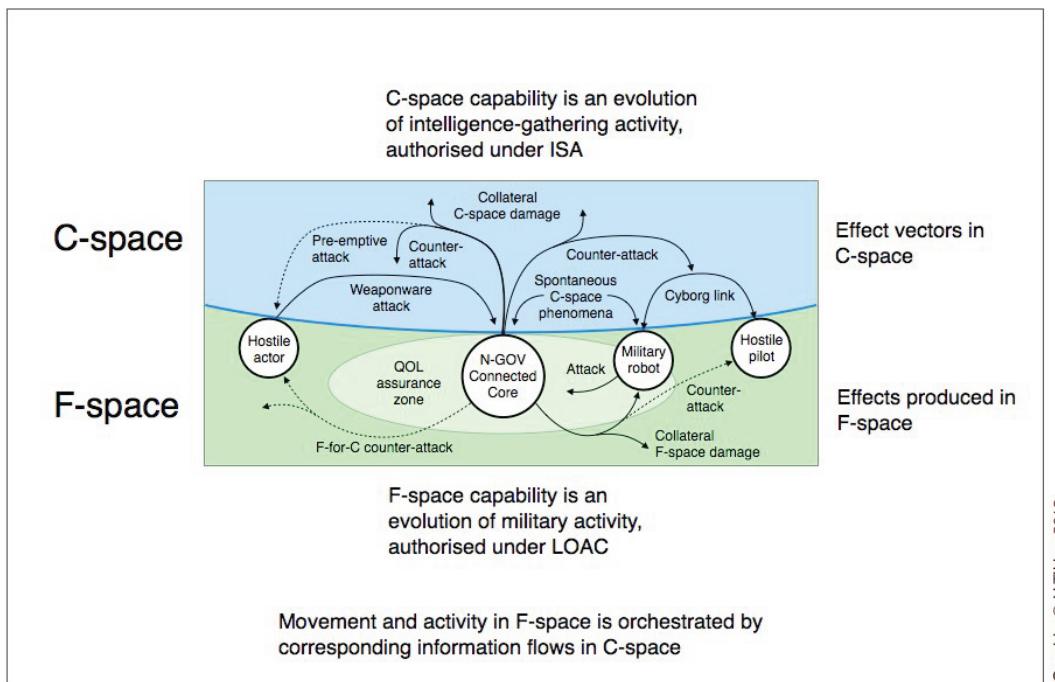
Movement in F-space is a blend of movements and actions determined in the ordinary way by direct contact with the physical world, in combination with movements determined by a flow of information from C-space, which may range from sensor data, map information, routing instructions, customer orders, to social contact coordinates. In the future it will be increasingly important to be able fluidly and elegantly to coordinate complex interacting combinations that include people, cyborgs,¹⁵⁷ remotely piloted aircraft, semi-autonomous

¹⁵⁵ Manuel Castells, *Communication Power* (Oxford: Oxford University Press, 2011)

¹⁵⁶ <http://www.forbes.com/sites/markpmills/2012/03/23/amazons-kiva-robot-acquisition-is-bullish-for-both-amazon-and-american-jobs/> accessed 14/02/13

¹⁵⁷ A cyborg, short for 'cybernetic organism', is a being with both organic and cybernetic parts

robots,¹⁵⁸ transport equipment, and even moveable parts of buildings. This capability will be a hallmark of efficient operations, from the factory floor to public entertainment spectaculars.



Graphic: © H Tibbs, 2013

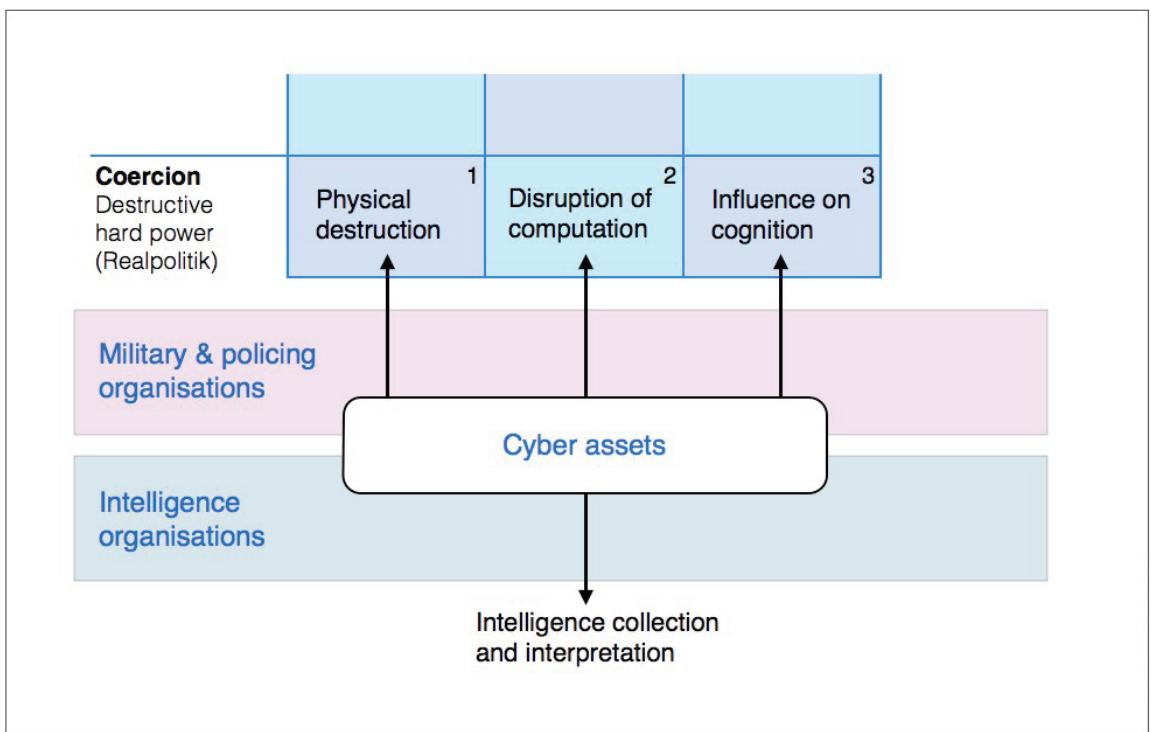
Parallel operations in C-space and F-space

This is also relevant to military manoeuvres in that network connectivity is already pervasive for all aspects of military equipment, platforms and personnel, and manoeuvres are increasingly coordinated by data-flows through C-space (in this case, not necessarily the public Internet). This networked warfighting is known as Network Centric Warfare (NCW), and it is likely to evolve towards sophisticated F-space capability (rather than C-space capability) as a critical new factor that will help determine the conduct and outcome of operations. F-space capability will involve C-space skills, but the primary focus of military cyber expertise will be support for seamless orchestration of 'sense and shoot' activity in F-space. The future battlefield looks set to contain huge numbers of mobile nodes, including thousands of robots of all sizes, drones, soldiers with robotic exoskeletons, smart-dust sensors, conventional aircraft, and walking vehicles. The highly specialized knowledge and skills required to do this well make it likely that the 'flow-space' function will need to become an operational component of military operations.

Military expertise in F-space operations as authorized under the international Law of Armed Conflict (LOAC) will need support in C-space that is likely to be fielded by future incarnations of today's electronic intelligence gathering agencies. These C-space activities could include intelligence-gathering, surveillance, infiltration of remote computers, exfiltration and

¹⁵⁸ <http://www.theengineer.co.uk/sectors/automotive/news/robots-to-organise-themselves-like-a-swarm-of-insects/1012101.article> accessed 14/02/13

manipulation of data, and C-space interdiction. In the United Kingdom these would need to be authorized under the 1994 Intelligence Services Act (ISA).¹⁵⁹ In fact many aspects of what are currently being thought of as cyber warfare capabilities may well sit more logically with an evolution of the intelligence gathering function than with military capability.



Cyber interdiction roles, option 1

Graphic: © H Tibbs, 2013

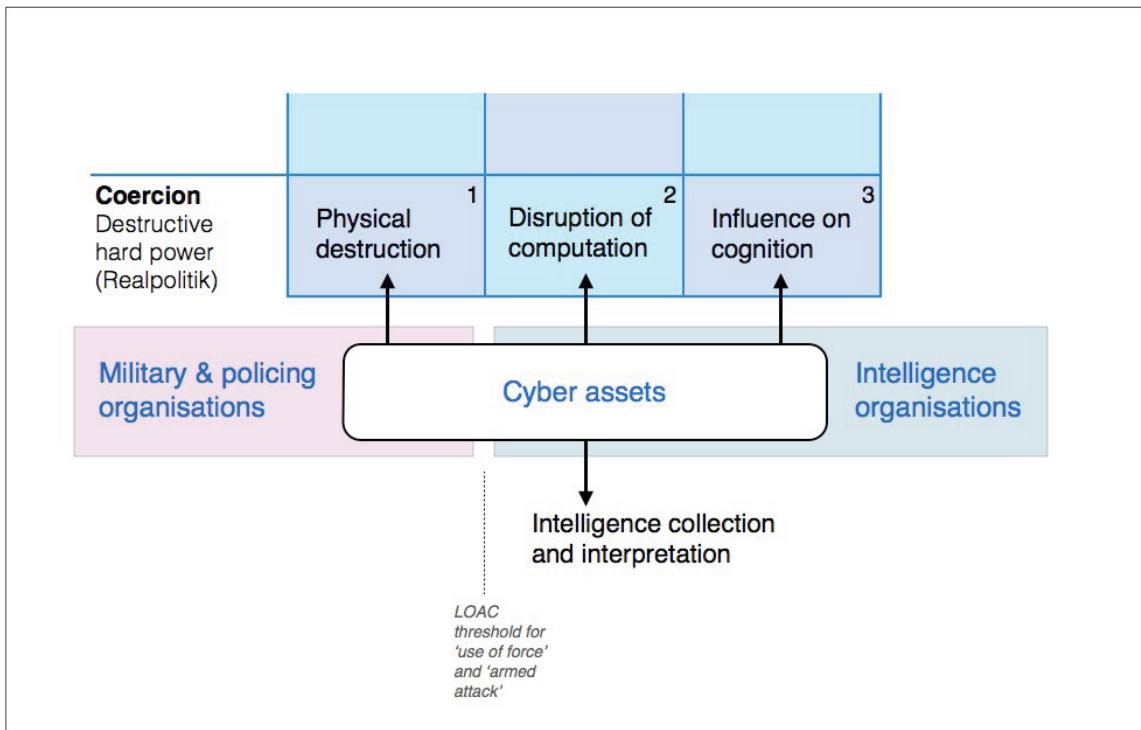
In future the degree of F-space competence is likely to determine the success of operations, both civilian and military, in physical space. Any application of military hard power will seek effects in F-space, because this is where hard power dominance is achieved, and this will require a secure C-space. Whether the actuating information flowing through C-space can (from a technical point of view), or will (from a political point of view), be made secure is an uncertainty that is discussed later.

To achieve effective F-space operations, attention will need to focus on the boundary between C-space and F-space. The C-space surface itself can be dissected into a number of operationally important layers, on both C-space and F-space sides of the boundary. On the C-space side there is a 'C-space stack' running from the physical network and its connected computers, through the information flow, the local processing, to the user interface. The boundary itself is the meeting point between the user interface and the user's consciousness. On the F-space side, an 'F-space stack' runs through user consciousness, user orientation, user decision, to user action. This corresponds to the well-known OODA loop of John Boyd,¹⁶⁰ and emphasizes both the 'soft power' effects on the flesh and blood or 'meatspace' side of the

¹⁵⁹ <http://www.legislation.gov.uk/ukpga/1994/13/contents> accessed 07/03/13

¹⁶⁰ Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Boston: Little Brown & Co., 2002)

Internet surface, and the need for all interfaces to be designed in a way that optimizes the flow-space actor's OODA loop.



Cyber interdiction roles, option 2

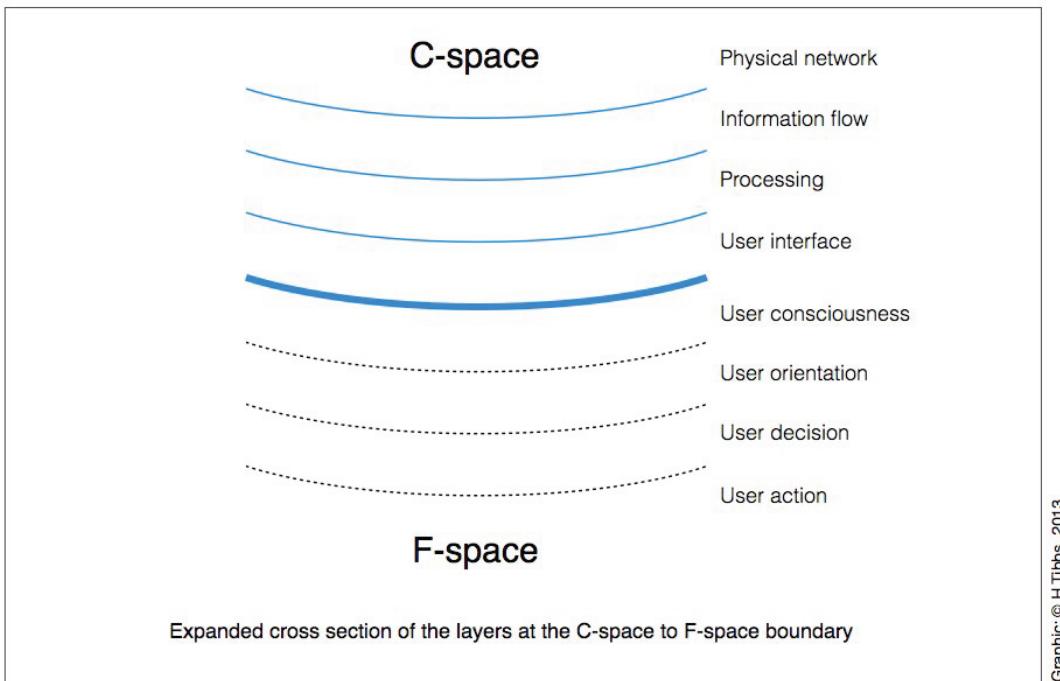
Graphic: © H Tibbs, 2013

The Cyber Gameboard can be thought of as symbolically representing the C-space surface, the boundary between C-space and F-space, viewed from F-space. The gameboard categorizes types of cyberpower, and in so doing it represents C-space capabilities and effects in F-space. In a sense, the C-space 'side' of the surface is the networked medium that conveys various combinations of power and information from cell to cell, resulting in effects that are either caused or suffered on the F-space side of the surface.

Flow-centric warfare

More than 50 percent of the global population is now urban, and city life is overwhelmingly dependent on continuous flows of information, energy, goods and people from around the globe. These flows are now crucial for human life-support. They are driven by economic activity that is enabled and coordinated through C-space, and the business of keeping them going now dominates government, market, and civil society interactions worldwide.

In a fully globalized knowledge society, a key function of the state and source of legitimacy will be to maintain and improve the quality of life of its citizens. Global flows are as much a contributor to quality of life as economic growth and, if anything, at a time of flattening economic growth, uninterrupted global flows are a greater priority for governments than economic growth because they are a survival issue.



Graphic: © H Tibbs, 2013

The boundary of C-space and F-space

As long as C-space remains vulnerable, global flows in F-space are an obvious target for cyber attack via C-space. This opens up the prospect of flow-centric warfare (FCW) which would be aimed at disrupting extended global flow networks, thereby directly and rapidly threatening urban functioning in a target nation. In contrast to the existing cyber security focus on critical national infrastructure (CNI), FCW shifts the focus of attention from national nodes to the flows between international nodes. This shift is attractive for a potential attacker, as the flows have more modes of vulnerability than the nodes and, since the advent of just in time supply chains, the levels of static inventory at nodes have been greatly reduced.

The key national security concerns in global F-space are therefore not so much about protecting geographic territory, and CNI within geographic territory, as about protecting the globally extended F-space dependencies of the nation. Being flows, as opposed to static assets, this will require complex dynamic mapping and considerable cooperation from commercial organizations.

Many of the firms involved will have a global perspective and interests, and the high level of cross-dependence within the system of flows will complicate the clear identification of national interest. Consequently, FCW may require federated defence arrangements, not a go-it-alone national defence posture.

In a scenario of worsening impacts from climate change, FCW could conceivably be waged amid conditions of growing global crisis, intensifying already acute environmental, humanitarian, food, and energy problems. Finally, although very little of the existing materiel of defence is likely to be useful for FCW, the appropriate capability would be equally suited

for dealing with the impacts of serious environmental disruption. This might include, for example, the ability to deploy distributed power systems when centralized systems have been disabled.

F-space weapon development

In any future when C-space becomes more secure, the focus of action in cyber conflict is likely to shift to the superior orchestration of operations in F-space. Until now, the notion of a cyber weapon has primarily meant malware for disruption via C-space, but in a future world where C-space is secure, accomplished deployment of F-space weapons will provide the operational edge. This implies that the future meaning of cyber weapons would shift to autonomous and semi-autonomous systems such as drones, operating in F-space.

A drone is a ‘mechatronic’ device (a combination of mechanics and electronics), and it might seem a stretch to regard it as a cyber weapon. But even if drones simply look like advanced radio controlled model aircraft, the capabilities of current and future drones are very much a function of the computation and communication power of C-space.

Up to now, drones themselves have been vulnerable to malware. In 2011, US military drones were reported to be infected by a virus that proved difficult to remove. At one point the US Air Force was reportedly reduced to following instructions on the Kaspersky Labs website to help them debug drones at Creech Air Force Base.¹⁶¹ The video feed from drones has been intercepted using off-the-shelf software, as happened in Iraq,¹⁶² and it is possible that a drone compromised by malware could be remotely hijacked and turned against its operators.

But in a future where C-space is secure, or at least the part of C-space that provides the link, F-space weapons (drones, and robots in general when used for projecting coercive power) would quickly become the main focus of the military aspect of the Cyber Game.

Under these circumstances, the future technological development of drones can be foreseen relatively easily. They will continue to get smaller, following the current trend, to the point where they resemble insects¹⁶³ and, for surveillance purposes, will be deliberately designed to do so. Some will even be so small that they are below the level of resolution of the human eye, that is, effectively invisible.

In use, drones are already tending to become remote assassination weapons, and they are likely to become even more precisely deadly. This development is starting to raise serious ethical questions¹⁶⁴ which are only going to get more intense as drones get smaller. Imagine a future scenario similar to the discovery of Osama bin Laden’s house in Abbottabad. A mosquito-sized drone could be sent in to verify his identity by sampling his DNA, followed later by a wasp-like drone equipped to administer a lethal injection, much easier than

¹⁶¹ <http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/> accessed 14/02/13

¹⁶² <http://www.wired.com/dangerroom/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/> accessed 14/02/13

¹⁶³ <http://www.snopes.com/photos/technology/insectdrone.asp> accessed 14/02/13

¹⁶⁴ http://www.huffingtonpost.com/2013/02/07/armed-drone-debate_n_2639565.html accessed 14/02/13

deploying stealth helicopters without knowing for sure if OBL was in the house.¹⁶⁵ Now imagine a future in which this technology has become widespread. Who then would want to be the leader of any hierarchical organization that uses coercive power? If information abundance gives networks an advantage over hierarchies already, this will only make the advantage decisive, or serve to drive strategy more strongly away from using coercive power and towards the top right corner of the Cyber Gameboard.

Even in future scenarios where C-space is not secure, the development of drones and robots will no doubt still continue, but the complexities and uncertainties in the resulting Cyber Game will be greater.

Ethical complexities, for example, are increasing as robots and computerized systems in general become more autonomous. Automated decision making by robots will not eliminate responsibility but will shift it from a concurrent or real-time act to an asynchronous act that happens when the decision software is written. This is because there is ultimately a human will behind the design of all machine systems, and responsibility can be traced back to that will.

War, for example, can be understood as a 'dynamic contention of opposed wills'.¹⁶⁶ A war continues as long as the human wills are opposed and stops when one or other gives up. Any weapon used, even a fully automated system, should be expected to respond to this underlying change of will, and if it does not it will be problematic as a weapon system, as is evident in the case of land mines. More capable automated weapons that do not give up, such as fully autonomous battle robots, would quickly become a serious problem and are very likely to be banned if the problem presents itself dramatically enough. Isaac Asimov's 'Three Laws of Robotics' may yet become actual laws.¹⁶⁷

This is relevant to the Cyber Game because the distinction between robots and malware is increasingly likely to be blurred, meaning that the same ethical principles will apply. For instance, malware designed to operate autonomously and asynchronously would raise the same need for responsiveness to the changing will of its creators, assuming they were thinking far enough ahead. And if they were not, this could become a source of conflict in itself.

¹⁶⁵ The narrative as depicted in the film *Zero Dark Thirty* <http://www.imdb.com/title/tt1790885/> accessed 14/02/13

¹⁶⁶ Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge (USA): Harvard University Press, 2001)

¹⁶⁷ <http://online.wsj.com/article/SB10001424052702304363104577390473311236692.html> accessed 30/03/13

National strategic priorities for the Cyber Game

At the time of writing, no generally effective way exists to kill somebody using the Internet. Although there may be a few individuals who have a special vulnerability to cyber attack, such as people wearing heart pacemakers which are insecure, in general very few lives could be predictably ended by pure cyber attack. Although there is a significant potential for economic damage and systems disruption, at the current time the online environment empowers a very large class of cooperations, but allows only a narrow range of options for conflict. Pre-existing systemic risks in supply chains, financial markets and energy grids are vulnerable to a wide range of systemic pressures, from pandemic flu through to ordinary software errors producing cascade failures. These risks are real and serious, but when placed against the more general risk framework from armed conflict including asymmetric warfare, it is not immediately apparent that cyber is a stand-out risk.

One reason is that pure cyber attack is one of the less effective forms of cyber gameplay. Networked digital computers are enormously powerful tools for collaboration, but lack many fundamental properties required to apply hard power with coercive intent. Unlike aircraft, their direct application as a form of warfare is non-obvious. However, their capabilities are extraordinarily well suited to two other forms of cyber gameplay: cyber espionage and cyber sabotage. The loose, over-general use of the term 'cyber war' obscures this useful distinction.

Cyber espionage constitutes the vast majority of the current coercive use of cyber. Societies, governments and organizations use computers to manage and organize their information. This information has value to opponents, and the more value an organization is generating using computers to organize and store information, the more value is at risk if that organization's competitors obtain and misuse it. The simple alteration of intent from 'organize our information' to 'misapply the organized information' is well-suited to what computers can be made to do. Most cyber weapons are nothing of the kind; they are simply 'cyber lockpicks' which enable illicit access to an otherwise protected information source. The desire to categorize all hostile activity from states on the Internet as 'cyberwar' using 'cyberweapons' comes from an over extension of once useful metaphors. Cyber espionage with cyber lockpicks sounds a lot less impressive.

However, consider how useful Internet search is for researchers. The ability to access much of the world's information in a few clicks helps academics find references, helps ordinary people make decisions, helps scientists collaborate to solve problems. The equivalent power in the hands of hostile intelligence services, with unfettered access to the supposedly private files of individuals, business and government is certainly not a minor threat. Although the coercion involved here is non-violent, the sheer scale and ease of illicit access to confidential information possible using cyber espionage is breathtaking. Over time it could be extremely damaging, although in most cases few lives are immediately at risk.

Many computer systems have uses beyond managing and storing information. SCADA controls (an acronym for 'supervisory control and data acquisition') and avionics systems control large, complex machinery, often in safety-critical situations, ranging from power generation to communications grids and aircraft engines. Once cyber lock picking has

granted access to a computer which is part of a control system, cyber sabotage becomes possible, but if all it contains is record storage, little can be achieved. In the vast majority of computer systems, the maximum possible damage would be to erase invoicing and inventory records. Disruptive, but hardly a weapon of war in most instances.

But how much damage can cyber-sabotage do, given a more attractive target? The answer is highly dependent on the nature of the systems being infiltrated. Systems with good separation between SCADA process control systems or banking trade triggers and the general Internet are hard to access. Once access is obtained, however, cyber sabotage can in theory do damage up to the full operational capacity of the system and more. Planes could fall from the sky or be used as improvised guided missiles. Power grids can destroy a very substantial subset of the assets on the grid, if manual overrides are not exercised in time. Cyber sabotage at this scale is technically possible, and at the upper end certainly fades into territory which justifies the use of the term cyber war.

However, only vulnerable systems can be compromised by cyber sabotage. Military computer systems are extensively hardened and aim to be resistant to even the most determined attackers. The state of the art in security is sufficient to defend even extremely valuable assets from attack. So why is so much of the civilian asset base left vulnerable to cyber espionage and cyber sabotage, up to and including destruction in cyber war?

The answer is simple: security is expensive, and without regulation to create a level playing field, companies can derive commercial advantage from putting minimally secure systems into the field, rather than footing the bill for providing high level security for customers who, on the whole, do not appreciate it. Simple market failure has left many critical systems under secured in a way which is already being exploited on a vast scale in international cyber incursions.

The speed with which these systemic flaws in the installed equipment base can be closed is critical to any nation's ability to return cyber to being a moderate espionage threat, rather than an urgent risk to national infrastructure. Computers are not inherently secure or insecure, they are as we program them. The limits of cyber sabotage are set by the vulnerabilities of non-military systems. If computers are generally made secure in proportion to the value of the assets they control, the possibility for a sudden asymmetric surprise attack with devastating consequences will largely be removed.

Making the transition to a situation where exposure to cyber espionage and cyber sabotage is low enough to be at a similar level to other common risks is possible. Security, if done at scale, is not expensive. The common router hardware which every household with broadband uses to provide a Wi-Fi signal can either be secure or insecure depending on how the software is configured. But industry has deployed several rounds of weak encryption, resulting in a decade of system compromises. Older hardware running insecure protocols is still everywhere. The situation is even worse in desktop operating systems, where vendors distribute software with known security bugs because they bear no legal liability for distributing insecure software. Even after exploits are discovered, vendors continue to sell

compromised software without any penalties even though their irresponsible actions are, in total, a threat to critical national infrastructure.

Treating software as if its quality is important is risk free. It will not trigger any conflicts, and has few unforeseen consequences except perhaps a general rise in the cost and quality of software. Government action in this area is likely to be resisted by industry, but welcomed by consumers. Reliable software serves all of our needs, and operating system software companies have made enough profit over the past 20 years to be well able to afford the costs associated with comprehensively better security engineering.

At present, US companies supply most of the major computer operating systems. Unilateral action by other governments on software security might improve any home grown production, but is unlikely to be effective in pressuring large US vendors to produce more secure systems. For EU countries it may require a more patient approach, working at the European scale, to encourage a different culture in software engineering by imposing European standards on commercial software quality.

Lowering the ability of our Cyber Game competitors to use our own systems against us is the primary tool we have in limiting their effectiveness in cyber espionage and cyber sabotage. It may require strategic efforts which amount to an industrial policy dedicated to secure software engineering to close the vulnerabilities, but it can be done. Secure systems can be created and deployed, and creating the right system of incentives to migrate secure software engineering techniques into consumer devices is possible. The same is doubly true of the systems which manage critical national infrastructure. At this level we are entirely responsible for our own national vulnerability.

Network centric warfare

What then, accounts for the high level of military concern about cyber warfare? Part of the answer is the vulnerability of US-style Network Centric Warfare (NCW). This concept stresses the construction of a parallel digital environment which tracks and maps all physical and information assets in a conflict. The idealized vision is a transparent battlespace in which sensor feeds from platforms as diverse as satellites and sensors mounted on individual soldiers are woven into a comprehensive overview of the conflict. Battle commanders are then, ideally, freed from the 'fog of war' which has been the historic norm and can make effective, rational decisions based on accurate, timely data. It is easy to understand the attraction of such a capability, however difficult the technical challenges are of implementing such a system.

Unfortunately, in a NCW environment, many real world phenomena like camouflage have direct digital counterparts. A piece of software which infiltrates an NCW grid could simply hide, say, tanks or ships by silently discarding the primary sensor data rather than displaying them as a threat on the commander's battle display. For all practical purposes, until sighted by a person on the ground who issues some kind of overriding alert, the vehicles are now effectively invisible to the battle's commanders. At the point where a discrepancy is spotted between the real world and the transparent battlespace presented by the NCW software, all

assumptions are now back to manual testing and commanders are worse than blind; they cannot trust the evidence of their own electronic eyes.

An example is the ‘Suter’ airborne network attack system developed by BAE Systems. Rather than jamming radar signals, Suter hacks into them. According to news reports, this enables ‘operators to invade enemy communications and computer networks, particularly those associated with integrated air defence systems, while preventing enemy operators from understanding or counteracting the exact nature of the invasion....Suter operators can then act as replacement managers to control enemy radars....By steering the enemy sensors away from friendly aircraft, Suter operators can figuratively put blinders on the enemy operators. Consequently, friendly aircraft don’t even have to be stealthy because enemy sensors can’t scan to find them, like eyes that can focus but can’t rotate.¹⁶⁸

Much military concern about cyber risk therefore legitimately comes from the potential to completely disrupt and betray NCW. The benefits of NCW are gained at the cost of a catastrophic new kind of battlefield risk, compromise of command-and-control software.

Unfortunately this concern reflects only a small part of the overall Cyber Game, and fails to address the clear and present danger to the civilian Internet, both from espionage and sabotage, but also from retaliation for state cyber attack. The ongoing cyber sabotage conflict between the United States and Iran demonstrates that Internet commerce provides a soft target for retaliation. From a national strategy point of view, closing this vulnerability means, in part, taking steps to improve security as described above. But in order to do this, the state must confront another instance of the information dilemma, this time in the area of privacy and surveillance.

Privacy and the information dilemma

The information dilemma shows up in many guises, and it is so emblematic of problems in security that a 2007 UK Royal Academy of Engineering report on technological challenges to privacy had the title ‘Dilemmas of Privacy and Surveillance’.

In terms of security, the information dilemma shows most clearly when privacy is involved. Individuals would like their information to be private, and keep it from the public domain unless they choose to put it there. The state, in the interests of national security, would like to waive privacy provisions, ostensibly to detect and prevent crime and terrorism. Once again, the information dilemma shows up: the owners of information would like it to be private, but the state would like it to be accessible.

Before the Internet, phone tapping legislation required a court warrant to be issued for tapping each specific landline phone number. The technology of the Internet and the general lack of encryption now makes blanket surveillance of all Internet traffic possible, but makes applying for warrants impractical. In the United States, the legal impediments to warrantless interception of even domestic communications have now been substantially removed.¹⁶⁹

¹⁶⁸ <http://www.airforce-technology.com/features/feature1669> accessed 30/03/13

¹⁶⁹ Susan Landau, *Surveillance or Security?* (Cambridge (USA): The MIT Press, 2011)

While the technical plausibility of blanket surveillance has been questioned,¹⁷⁰ the high profile resignation of CIA Director David Petraeus in November 2012, following Internet surveillance by the FBI, did dramatically demonstrate the existence and possible consequences of unconstrained access to this type of capability.¹⁷¹

What is an appropriate balance between privacy and surveillance? Privacy is considered to be a basic human right in Article 12 of the United Nations Universal Declaration of Human Rights, in the Fourth Amendment of the US Constitution, and in Article 8 of the European Convention on Human Rights, and it has a long history of protection in law. Individuals value privacy as a shield from crime, persecution, and unlawful coercion, and against intrusion into personal and intimate life. Not only is it an important individual right, but it is also an important public good, essential for democracy. Privacy allows for freedom of conscience and diversity of thought and, flowing from these, freedom of speech and association, which are essential for democratic participation.¹⁷² These are important properties that are at least as important as national security concerns, indeed these properties are exactly what national security exists to protect. This dilemma resembles that of antiterrorism: the risk of overreacting and inadvertently taking on the very qualities one is trying to fight, instead of resisting by refusing to be terrorized, as the Queen did when she reportedly declined to reinforce Buckingham Palace for President George W Bush's visit. How then can the privacy-surveillance version of the information dilemma be resolved?

Curiously, for someone discredited in the Iran-contra scandal, one way of doing this was described by John Poindexter in March 2002, when he put forward the 'Total Information Awareness' programme to merge existing government databases and scan commercial transactions and private communications to detect terrorist plots. He proposed that the software would 'anonymize' the data, so that information could only be linked to an individual through a court order and generate an audit log, which would keep a record of who had used the system for what.¹⁷³ The programme proved controversial and was shut down the following year. However, in the years since, the US National Security Agency (NSA) has developed a very similar capability but without the accountability or oversight Poindexter proposed. Wired magazine reported that in 2011 in the Utah desert, the NSA began construction on what will be the world's most powerful data collection centre, using supercomputers to monitor, decrypt, analyse and store every phone call, email, text message, online search, or other electronic communication originating in or transiting US networks, plus anything else that can be intercepted around the world.¹⁷⁴

¹⁷⁰ <http://www.technologyreview.com/view/508571/is-the-us-government-really-a-spy-machine/> accessed 14/02/13

¹⁷¹ <http://www.nytimes.com/2012/11/14/us/david-petraeus-case-raises-concerns-about-americans-privacy.html> accessed 14/02/13

¹⁷² Priscilla Regan, *Legislating privacy: Technology, social values, and public policy* (Chapel Hill: The University of North Carolina Press, 1995)

¹⁷³ http://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html?_r=0 accessed 14/02/13

¹⁷⁴ James Bamford, 'The Black Box: Inside America's Massive New Surveillance Centre' *Wired* vol.20, no.4 (April 2012), p.78-84 & p.122-124

This is the Big Brother scenario that Kim Dotcom, and many civil libertarians, are opposed to. One alternative to this, essentially using the same safety provisions proposed by Poindexter, would be similar to what the UK Royal Academy of Engineering called the 'Little Sisters' scenario.¹⁷⁵ In this vision of the future, personal data is encrypted and held in partial form by many separate organizations including government departments (the Little Sisters¹⁷⁶), depending on the information they need for the service or function that they perform, and can only be brought together into a single picture and linked with the person's identity by official and accountable authorization. In the Little Sisters scenario the information dilemma is resolved by making it difficult and expensive to breach privacy (because the information is encrypted and dispersed), while simultaneously allowing the state to access private information but making it fully accountable.

The Little Sisters approach makes use of the distinction between authentication and identification, which is increasingly important for protecting personal identity in the current information environment. Authentication is a process that simply confirms that a person has a certain qualifying attribute without revealing their identity, their age for example, while identification discloses who a person is. It is often, and unnecessarily, assumed that identification is needed when authentication would be enough, and this distinction deserves to be more widely applied.

The Little Sisters scenario, in a sense, protects us from ourselves. Most of us are now carrying the camera- and microphone-equipped communication devices that allow central surveillance to be so effective, and the Little Sisters scenario would help prevent the central amassing and misuse of this 'souveillance' (surveillance from below) information.

Unfortunately, the Little Sisters scenario will only apply in countries with an effective balance of powers, not in countries where a single centre of power dominates. Nonetheless, if enough countries were to subscribe to the Little Sisters approach, most telecommunications equipment sold in the world market could be designed by default to meet these legal requirements, with an audit function that is permanently enabled, which would help to spread this type of protection. This would be in marked contrast to the current situation, in which the telecommunications equipment being sold around the world actually facilitates unaccountable surveillance.¹⁷⁷

The state would like to retain its prerogative to undertake espionage, but when much of the information is obtained from the Internet, it cannot do this without placing its own civilian population under surveillance, because the Internet obscures the key Westphalian distinction between domestic and international. This contravenes domestic legislation in democratic countries, but not the provisions of international law, which permit espionage. Methods for accountability for domestic surveillance do exist, but they are very difficult to assert in a global telecommunications marketplace. The only way round this dilemma in the longer term

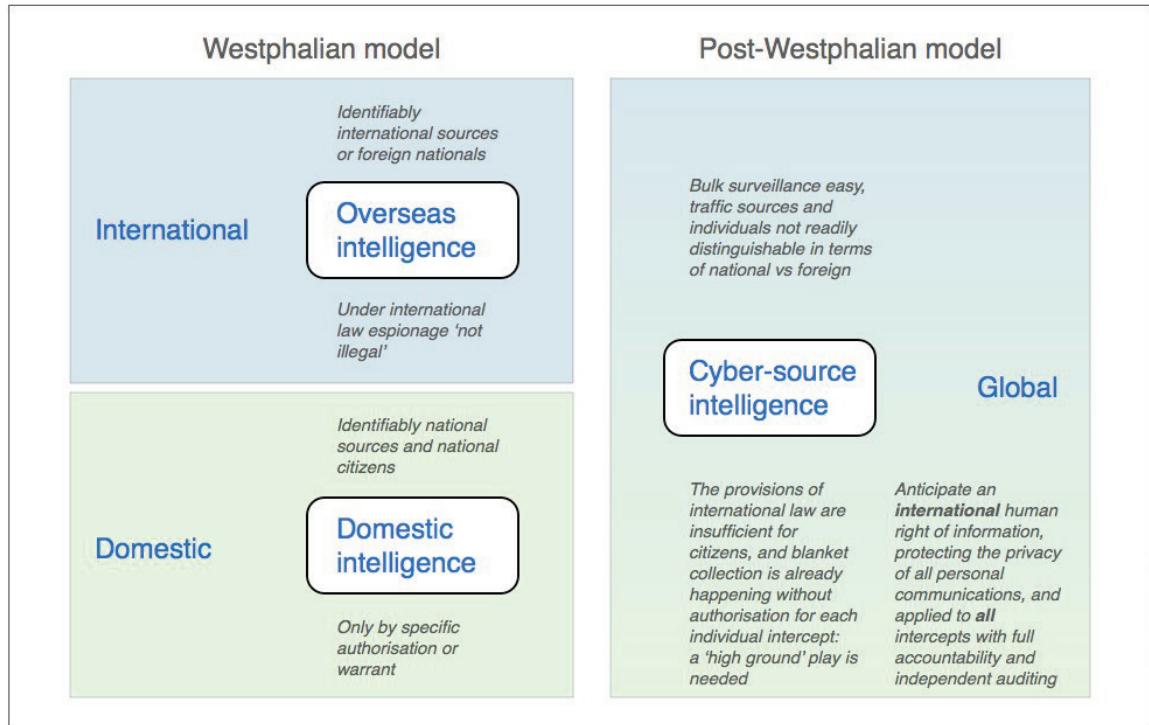
¹⁷⁵

http://www.cl.cam.ac.uk/research/dtg/www/publications/public/ah12/dilemmas_of_privacy_and_surveillance_report.pdf accessed 14/02/13

¹⁷⁶ Manuel Castells, *The Power of Identity* (Oxford: Wiley-Blackwell, 2010)

¹⁷⁷ Susan Landau, *Surveillance or Security?* (Cambridge (USA): The MIT Press, 2011)

is for democratic states to introduce legislation to regulate all Internet interception that is as tough as their domestic protections are now. If the world is moving towards the *N-topia* scenario, this is a plausible outcome, as in this scenario there is likely to be a UN Right of Information which would mandate such standards internationally.



Past and future cyber intelligence roles

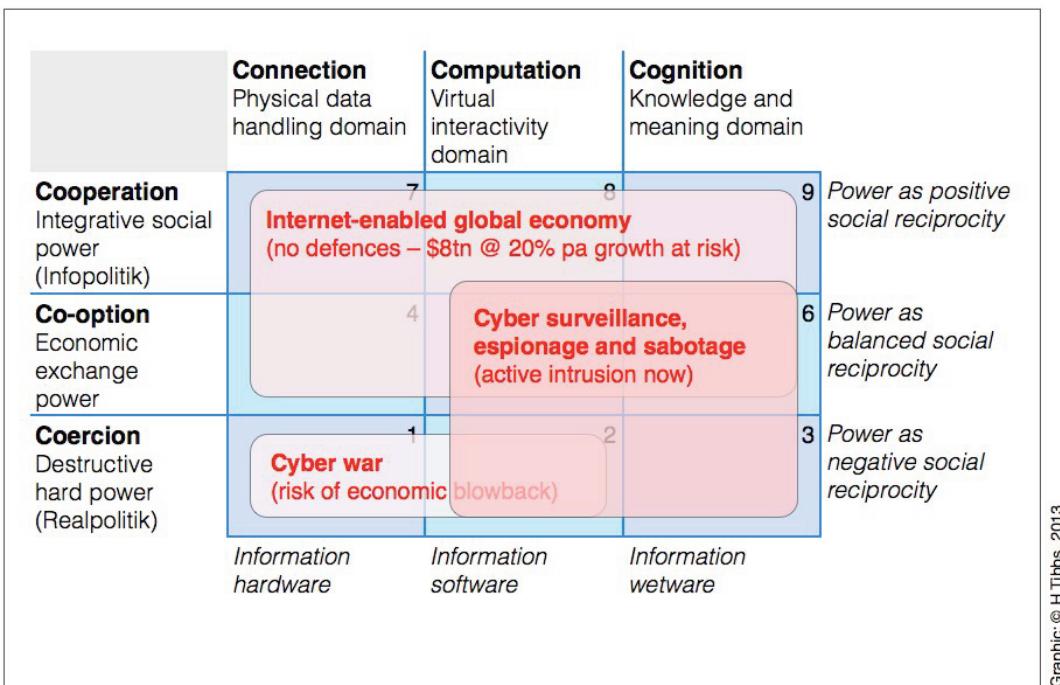
Meanwhile, this issue is likely to pose mounting internal tensions for democratic states. One possible Cyber Game play to defuse this tension would be for democratic states unilaterally to give up Internet surveillance. This would confer very high international cyber legitimacy on any state doing it, but what would be the cost of losing the surveillance?

An age-old version of the information dilemma relates to intelligence gathering. Any use of intelligence information risks exposing the source, and shutting off further information. For example, Osama bin Laden stopped using his satellite phone in 1998 after its presumed use to target a cruise missile attack on his training camps, narrowly missing him.¹⁷⁸ This dilemma gives intelligence organizations a distinctly different culture from action oriented defence organizations. It also lies behind controversial proposals for secret courts in the UK, as the government would like to present evidence obtained secretly, and fears that if this evidence is presented in open court it will cause the secret methods or sources to become ineffective or unwilling.¹⁷⁹ To the extent that it applies to digital interception, this calculus frames the Cyber Game too narrowly. It risks undermining trust in the government and creating

¹⁷⁸ <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/21/AR2005122101994.html> accessed 14/02/13

¹⁷⁹ <http://www.guardian.co.uk/law/2012/sep/25/secret-courts-the-essential-guide> accessed 14/02/13

sympathy for the defendants, a point made to Andrew Tyrie MP, chairman of the all-party group on rendition, by two retired US generals who warned that forfeiting values in the face of danger drives ‘undecideds into the arms of the enemy’.¹⁸⁰



Graphic: © H Tibbs, 2013

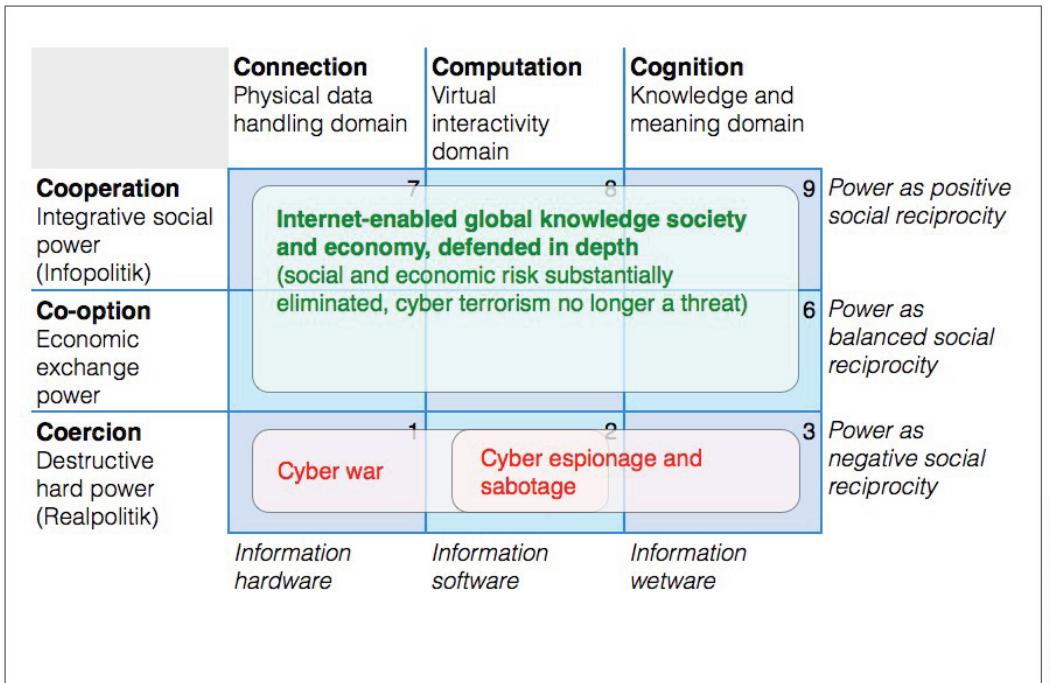
Threat and risk footprint of cyber conflict

The intelligence dilemma also applies to the public at large. State surveillance is most effective for information gathering when there is very little of it. As everyone becomes aware, through news stories, that all their communications are under surveillance, they will simply stop saying anything that is of any interest to law enforcement or espionage agencies. As Internet security expert Dan Kaminsky said after the Petraeus affair, ‘...everything is logged. The reality is if you don’t want something to show up on the front page of The New York Times, then don’t say it.’¹⁸¹ If this advice is widely adopted, blanket surveillance will have rendered itself largely useless. Except, that is, as a tool of repression. The clear lesson being, don’t do it if you don’t want to become a repressive state.

If the choice for democratic states is between a future defensible public Internet and the loss of continued Internet surveillance, the decision should be easy. Domestic surveillance capability is inimical to Internet security, and hence to the enormous economic growth and social development potential that it promises. It is also ultimately self-defeating and contrary to the values of democratic states.

¹⁸⁰ <http://www.telegraph.co.uk/news/politics/9829914/Secret-court-hearings-will-do-more-harm-than-good-Tory-MP-says.html> accessed 14/02/13

¹⁸¹ <http://www.nytimes.com/2012/11/17/technology/trying-to-keep-your-e-mails-secret-when-the-cia-chief-couldnt.html?pagewanted=all> accessed 18/02/13



Graphic: © H Tibbs, 2013

A future secure Internet would refocus the Cyber Game

A future secure Internet would shift the Cyber Game from a condition where the future of the global knowledge society and economy is at risk from active threats, to one where it is substantially protected and able to flourish. The use of cyberpower by states that involved deception, espionage and sabotage would then focus back on the hard power level of the Cyber Gameboard, with a largely military-on-military focus.

If at the same time military NCW systems became secure enough, hard power plays on the Cyber Gameboard would increasingly tend to involve F-space cyber weaponry, as described earlier. However, this is the future world of the *N-topia* scenario, in which case the level of violent conflict would be continuing to follow its long run downward trend, and hopefully there would be few if any F-space wars.

Alternatively if democratic states continue to leave the Internet at risk, with little to gain but surveillance capability of self-cancelling value, the world will be following a path towards the *N-crash* scenario. In this future, ultimately the only available defensive cyber options for states will be to Balkanize the Internet, thereby undermining a substantial part of humanity's hope for the future.

To a significant degree, the choice between the world of *N-topia* and *N-crash* lies in the hands of states and the way they decide to play the Global Cyber Game.

For states there are fundamentally two ways of playing. They can play from a Westphalian perspective, as if it is a zero-sum game with absolute winners and losers, which will emphasize adversarial geopolitics. Alternatively they can adopt a post-Westphalian, pro-

knowledge economy perspective, as if it is a non-zero game with an expanding pie for all, which will emphasize global cooperation. The adversarial mode will be the easiest for state players to adopt, as it tends to be their default mode of operation, but it carries much greater risks of absolute loss of global development potential. The cooperative mode has a far greater pay-off socially and economically, but it goes against the grain of traditional geopolitics and will require far-sighted leadership and strong will on the part of state actors.

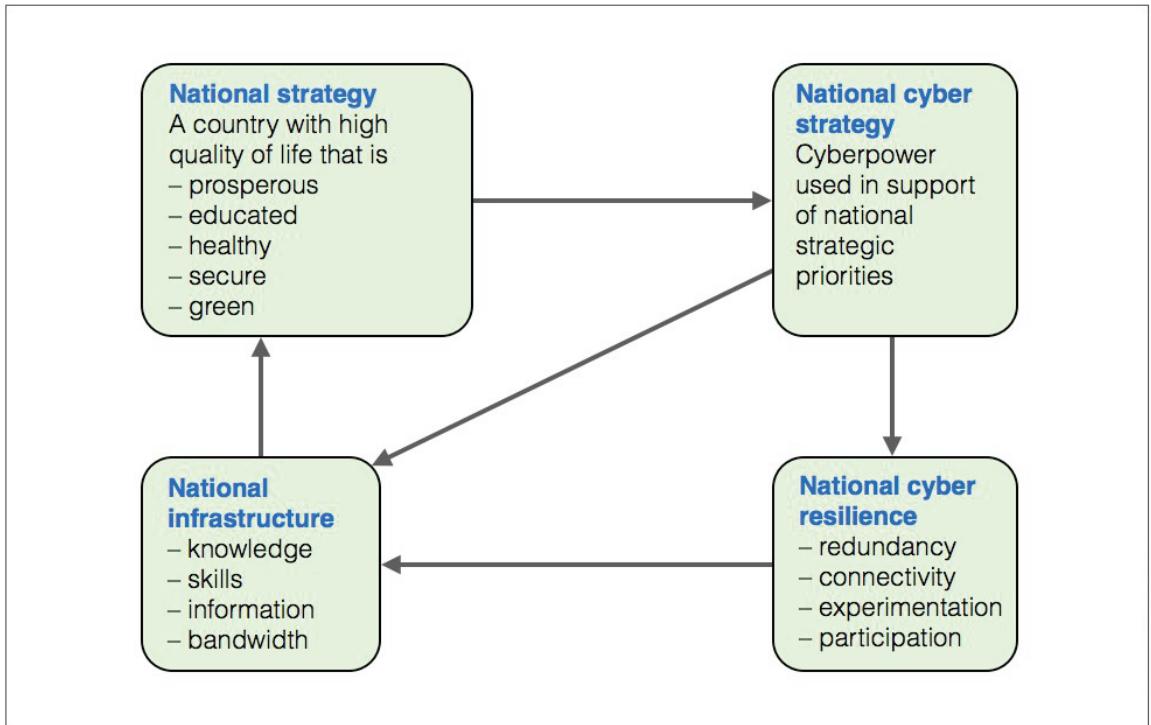
Adversarial
*play that risks the integrity of
the global knowledge commons*
or
Cooperative
*play that aims to keep the global
knowledge commons intact*

Graphic: © H Tibbs, 2013

The Cyber Game: two possible modes of play

Strategic responsibility for national cyber resilience

If state actors are to play the Cyber Game with the type of comprehensive strategic perspective being advocated here, they will need to bring responsibility for cyber strategy together into one organizational unit. In many states responsibility for what may be called 'national cyber resilience' functions is currently fragmented among several defence, intelligence, policing, economic and social welfare organizations, as it is in the UK. To ensure the state acts as a strategically coherent Cyber Game player, a single coordinating unit with topsight responsibility for cyber strategy needs to be created. At its top level, this unit would align Cyber Game play with national strategy, at its middle level it would set strategy for cyber infrastructure resilience, and at an operational level it would set strategy for the cyber interdiction functions of law enforcement and the military.

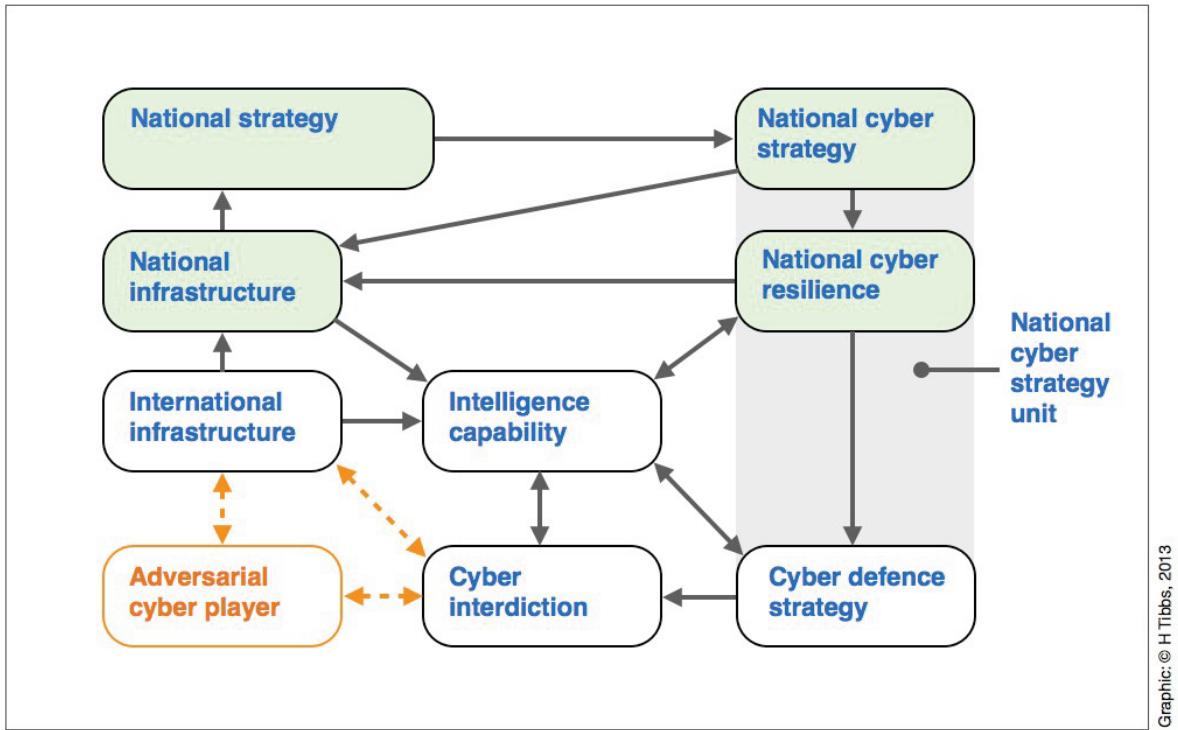


Graphic: © H Tibbs, 2013

National cyber strategy

Ideally, such a unit would work to maintain national Cyber Game play in a cooperative rather than an adversarial mode, continually looking for opportunities to maximize integrative power at the top level of the Cyber Gameboard. It would be very conscious of the dangers of adopting an adversarial mode of play, one that would view the gameboard merely as an arena for potential conflict and seeing only threats arising at the hard power level. By keeping the wider strategic perspective of the whole gameboard in view, it would particularly try to avoid hard power interdiction moves against genuine social power players. At the highest level of thinking, such a unit would see its ultimate global responsibility as being to keep the global knowledge commons intact, to encourage all possible steps to increase the overall defensibility of the Internet, and to resist any tendency towards Balkanization of the public Internet.

The overall stance being recommended here amounts to strategic stewardship of the Global Cyber Game, aiming to sustain both national quality of life and the development and defence of a global knowledge society. The next section offers a summary set of recommendations for playing the Cyber Game that correspond with this outlook which, if adopted by a majority of states, should ensure the world enjoys a prosperous future cyber peace.



National cyber resilience

Graphic: © H Tibbs, 2013

Recommendations: How to play the Cyber Game

The following summary recommendations for playing the Global Cyber Game correspond with the strategic objective of maximum global advantage described above. They are written with state players particularly in mind, but most apply equally for all players, if only as a matter of enlightened self-interest.

Take the Global Cyber Game seriously

Everyone who uses a networked computer is part of the Cyber Game, and the game is getting potentially dangerous. Most players, individuals and organizations, are unprepared for the severity and speed of possible future developments.

Use a comprehensive gameboard

Map your understanding of the Global Cyber Game onto a fully comprehensive cyber power framework that can incorporate the social, economic and military aspects of power, plus the technological, social and psychological/cognitive aspects of information. This report proposes a framework, the Cyber Gameboard, that has these characteristics.

Think in terms of the whole gameboard

When making policy and strategy, include the whole gameboard in your thinking, don't inadvertently see the game only from the perspective of one part of the board. Policy and strategy should be holistic with respect to all dimensions of the gameboard.

Bring everyone onto the gameboard

All players, and government players particularly, should encourage other players to see the Cyber Game in comprehensive terms, that is to use the same Cyber Gameboard. This will create a shared cyber taxonomy and language, help ensure against strategic misjudgments, and make it easier to identify common ground.

Keep to the high ground

Hold in mind that the global knowledge commons is a shared human heritage and that it needs to be enhanced and protected. Defending the present and future information value it represents is an implicit responsibility of national cyber strategy. No tactical Cyber Game plays should violate this principle.

Faites vos jeux: open or closed cyber play?

The central ideological decision of the Cyber Game is whether to play as if freedom of information content is a public good in itself, or whether extensive control of information content is necessary for public safety. The Western democratic wisdom, and the basis of open society, is that freedom of content ultimately wins out because it creates more public value. This is the acid test: will Western democracies stay true to that principle as the Cyber Game unfolds?

Assume transparency

During the present 'Rising Alarm' scenario period, information transparency is likely to be a persistent reality. All strategy and policy should be made as if it will become public

knowledge. As long as policy and strategy have been formulated from the big picture perspective of the whole board, it should have high legitimacy when seen in public.

Don't proliferate gameboard risk

The transparency principle also applies to military malware, and indeed to all malware, which should be built as if it will escape into the wild and proliferate, and the design should guarantee it will be harmless when this happens. Governments shouldn't develop cyber weapons or encourage malware markets that will increase risk for all players through proliferation. No players should develop malware that directly or indirectly impairs or endangers the functioning of the entire information infrastructure (the 'high ground' principle).

Be aware Moore's Law is gaining over Clausewitz

The informationalization of weapons is reducing the size and increasing the precision of the bang for the buck. Weapons of all types, in C-space and F-space, are tending towards remote individualized destruction or disablement of hardware, software, information, persons, and minds. This is the shape of total information war. There is no distant frontline. All nodes are potential targets. Who is now fighting who and why?

Don't rely on pre-emptive attack

An openly held doctrine of pre-emptive attack, for example as advanced by President Bush after 9/11, has multiple weaknesses. It requires unattainably reliable intelligence; it leaves decision-makers susceptible to disinformation from interested parties; and it encourages all who fear they may be targets to use extreme secrecy, and to use rather than hold weapons.¹⁸² For all these reasons it is a destabilizing and inadvisable move in the Cyber Game. An unconditional 'no first strike' doctrine, as declared by China and India in relation to nuclear weapons, is preferable because it increases stability through the use of integrative power.

Develop non-provocative defence

When destructive power is used for deterrence it leads to inherently unstable arms races.¹⁸³ Cyber deterrence will simply have this effect faster, because the Cyber Game runs at a higher clock rate than industrial-era geopolitics. The challenge in cyber deterrence, while acknowledging problematic issues such as attribution, is to rediscover the principle of 'non-provocative defence' developed in Europe in the late stages of the Cold War.¹⁸⁴ The key question for cyber strategists and technologists is: how can cyber defence and deterrence be designed in a way that it demonstrably poses no threat of pre-emptive attack?

Avoid excessive secrecy

Cyber Game players need to be fast and flexibly networked. Governments do have some things that legitimately need to be secret, but the current extent of secrecy is an impediment to playing the Cyber Game effectively, just as it was in the much slower-paced Cold War.¹⁸⁵

¹⁸² Richard Rumelt, *Good Strategy, Bad Strategy* (London: Profile Books, 2011)

¹⁸³ Kenneth E. Boulding, *Three Faces of Power* (Newbury Park: SAGE Publications Inc., 1989)

¹⁸⁴ Geoffrey Wiseman, *Concepts of Non-Provocative Defence* (New York: PALGRAVE, 2002)

¹⁸⁵ Daniel Patrick Moynihan, *Secrecy* (New Haven: Yale University Press, 1999)

Apply the legitimacy test

Legitimacy is the ultimate currency of cyberpower in the Cyber Game. A general rule of legitimacy can be applied on the Cyber Gameboard: the closer a cyber gameplay is to cells 7, 8 & 9, the more legitimacy it will have. In other words, don't take down a social power player using coercive power if you want to preserve legitimacy.

Keep resolving the information dilemma

The information dilemma—information wants to be public, information wants to be private – will keep manifesting in many guises in the Cyber Game, and it must consistently be resolved in a way that avoids becoming locked into one of the extremes of the dilemma.

Assess information value

Develop the discipline of assessing information value, to gauge whether any given cyber move will increase it or destroy it in any gameboard cell. To paraphrase President Clinton, it's the information, stupid!

Go post-Westphalian, but be kind to the Westphaliosaurus

Recognize that the information revolution is transcending many Westphalian assumptions, and find ways to make the transition without losing coherence. Play the Cyber Game as a post-Westphalian, but remember that not everyone has got there yet.

Reset internal boundaries

The boundary between domestic and international affairs, the key demarcation line for Westphalian states, has no intrinsic existence in C-space, and is far more ambiguous in a post-Westphalian world. This means that national cyber security functions need to be organized so that the domestic-international distinction is not an obstruction. States typically treat citizens and foreigners differently in terms of information rights. Recognizing that full human rights will eventually be granted to everyone in a post-Westphalian world, and in the *N-topia* scenario, the 'high ground' resolution is for each country to grant everyone whichever set of local information rights gives the greatest protection, either those of citizens or foreigners.

Create a cyber strategy unit

In many countries, responsibility for national cyber resilience functions is currently fragmented among several defence, intelligence, policing and other organizations. To make a nation a coherent Cyber Game player, a single coordinating unit with topsight responsibility for cyber strategy should be created.

Distinguish C-space and F-space

National cyber security operational responsibilities should be divided between C-space and F-space. C-space operations should be allocated to the intelligence community. F-space operations should be allocated to the military. This move anticipates two future developments: that the centre of gravity of all military operations will move into F-space; and the (scenario-dependent) re-architecting and hardening of C-space.

Protect F-space and geographic space

National defence is traditionally concerned with defending the geographic territory of the nation. But national economic dependence on F-space is global in extent. National defence therefore needs to extend into F-space globally, but this move should be framed strategically in terms of mutually protecting the global F-space commons, because from a Westphalian perspective it is otherwise likely to appear threatening.

Let robots play by cyber rules

The rapidly expanding deployment of autonomous and semi-autonomous F-space (robotic) weapons and platforms presents a fresh challenge for defence doctrine. The conceptual development of C-space and F-space as parallel modes of cyber operation allows robotic weapons to be treated as part of the Cyber Game. F-space weapons are Cyber Game players too.

Conclusion

When the Internet first appeared, the cultural bias of Western countries was to see it as a wonderful and welcome innovation. The fact that it created security problems somewhat took them by surprise and they have been reluctant to respond.

In contrast, states such as Russia and China saw the Internet as a potential threat from the outset, and looked at the problem in the round from their perspective. They formulated strategy and began to move pre-emptively, which has allowed them to take the initiative and to some extent define the Cyber Game.

As a result, cyberspace is now justifiably seen by Western countries as a new and potentially serious avenue of international attack, which must logically be militarized to protect the nation.

Treating cyberspace as a new military domain or environment is a pragmatic and robust response to a new type of threat, but what if it inadvertently exposes us to more risk than it removes? What if, perversely, information operates counter-intuitively in the military arena like the shock wave in early supersonic flight, which unexpectedly reversed the effect of familiar aircraft control surfaces with initially disastrous results?

Cyber realpolitik starts with the usual military logic of peacetime, that is, by preparing for potential threats. The problem is that this causes escalatory pressure at the best of times, let alone in a technologically hyper-charged context. The realpolitik of cyberpower makes what seem reasonable underlying assumptions. Is it not realistic to take geopolitical conflict as an inevitable part of the human condition, and to see cyberpower as a new capability tossed into an age-old mix?

But what if information abundance is so deeply transformative that it is changing not only the old game between nations but the global gameboard itself? In this case, we need a different approach, one that seeks to fully appreciate the new game and gameboard before making recommendations for national security.

The ability of national governments to understand and tame the Global Cyber Game, before it takes on an unwelcome life of its own, may be the crucial test for the effectiveness and even legitimacy of the nation state in the information age.

The means of doing this is to establish a set of principles grounded in the root characteristics of information and power. These principles can then form design criteria for the development of cyber policy and strategy.

This approach is similar to the current effort to devise international norms for cyber conflict, with the difference that these are primarily based in international law.¹⁸⁶ The approach suggested here starts as close as possible to the root of the challenge, and then uses more triangulating factors to arrive at a more broadly cast set of principles for cyber security. The factors considered should include the range of cultural perspectives, such as the Russian and

¹⁸⁶ e.g. Prof. M. Schmidt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013)

Chinese outlooks and the information-based asymmetric approaches they are pursuing, with the hope that the insights generated can anticipate developments and facilitate coalition-building. They would also provide a basis for constructive input to any proposed norms.

Principles relating to freedom of expression will not be welcomed by Russia and China, for whom ideas are regarded as threats. On the other hand, what China sees as benign Internet surveillance is regarded as intellectual property theft by Western countries. A clash of values is to be expected as a result of the cultural collision, or possibly convergence, produced by the Internet. If viewed from a static perspective based on a historical assessment of national values, the clash will be seen as inevitable and unavoidable. On the other hand, the global system may be seen as following an evolutionary trajectory. In this case the cultural gap can be seen more in terms of time rather than geography, and as gradually closing, pointing to a way for Western countries to engage, for example, the leading edge of Chinese thinking.

Another important principle is that governments should avoid defending the information infrastructure in a way that puts the whole at risk. This principle would mean forgoing some lesser tactical advantages for the sake of the strategic gain of protecting the whole, and making up the difference with alternative tactics.

Similarly, it is likely that an online arms race would threaten the integrity of the Internet either directly or indirectly, as described earlier, and a strong case can be made that the Internet itself is simply not robust enough to be a medium of war. This cannot be proved definitively, but it is amply indicated by the balance of risks. Protection of the Internet as a whole is therefore probably not compatible with the development of offensive online weapons, which in any case do not provide any absolute advantage. Such a principle would mean that online defence and offence would need to be clearly distinguished. This may take some technical ingenuity, plus longer term design changes. Expressing this principle differently, states may wish to play geopolitical chess or *wéiqí*, but it does not make sense for them to destroy the gameboard.

In short, the period of the Internet ‘Free Lunch’ for state actors is over. It is no longer possible to project hard power through a soft power medium without widespread blowback. The tough message for governments is that they must consciously accept a loss of some cyber options they have enjoyed during the free lunch period, in order to maximize future social and economic value. Acting to make the global information infrastructure as secure as possible will reduce the scope for certain online activities including cyber surveillance and sabotage. This adjustment in priorities will open the way for entirely feasible technical design changes to the Internet that will make it enduringly robust and secure.

The information revolution was brought into being by open policies and societies, and expresses their values of open information exchange. But critics of open society in China point out that the social and economic chaos of Western societies means that closure and information control is essential. The open societies themselves falter in their conviction and resolve because they too fear the apparently growing chaos. This is why they have previously allowed terrorism to undermine their dedication to principle, so setting a shaky background for the advent of cyber competition.

Yet the Cyber Game cannot be won without a return to principle and conviction, and the open societies cannot now create a convincing cyber narrative that involves closure and negation of the individual. The closed societies will try to operate without such a narrative, but the more they adopt the networked forms of operation the more this will undermine them. It is through the heart of apparent chaos that the new narrative must be found.

Much as in biological systems, a new geo-systemic position must be found close to the boundary between chaos and order, just on the side of order. If this position can be found effectively through the expansion of the global knowledge commons, it will mute the criticisms of the closed societies, who will despite themselves find it attractive because it will solve what they know are the shortcomings of their own approach, and it will temper the worst excursions into chaos by the open societies. This may ultimately result in discovery of a form of economy and society that will resolve the still relevant ideological standoff between capitalism and socialism, charting a future middle way.

We need to identify the high ground in the Cyber Game. We need to be clearer about the central values of the global knowledge commons, and how these relate to Western democratic values. In practice Western governments have not yet discovered how to create a link between their values and the operative principles of the knowledge commons. This accounts for the Western failure to articulate a coherent position on freedom of information content in the struggle over Internet governance.

It is vitally important that Western governments acknowledge any failure to live up to their values when it comes to the Cyber Game. They are in danger of giving away the family silver without even realizing it. They must stake out a position that affirms their core values, relates them clearly to the Cyber Game and the knowledge commons, and uses them to orient cyber policy and strategy. This will clarify the differences in their positions vis-à-vis Russia and China, and will help guide constructive diplomacy.

George Kennan argued for a similar stance in his ‘Long Telegram’ during the Cold War. ‘We must formulate and put forward for other nations a much more positive and constructive picture of [the] sort of world we would like to see than we have put forward in [the] past....Finally we must have courage and self-confidence to cling to our own methods and conceptions of human society. After all, the greatest danger that can befall us in coping with this problem of Soviet communism, is that we shall allow ourselves to become like those with whom we are coping.’¹⁸⁷

The overarching perspective being advanced here is that, in the information age, the integrity of the Internet as a whole is crucial for international development, prosperity and stability. In any future in which the full potential of the Internet is realized, the protection of the integrity of the entire Internet will also have been internationally recognized as a primary responsibility shared by all governments.

In that future, all governments, acting in their own enlightened self-interest, will see the structural and functional integrity of the Internet as a key part of their national strategy. This

¹⁸⁷ <http://www.gwu.edu/~nsarchiv/coldwar/documents/episode-1/kennan.htm> accessed 18/02/13

will be understood as not only the best way to achieve economic prosperity, but also as a general pre-condition for national security. It will also be seen to help ensure international stability and as opening the way to the most promising possible future(s) for the human race as a whole.

Bibliography

- Arquilla, John & Ronfeldt, David. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: Rand Corporation, 1997.
- Arthur, W. Brian. *The Nature of Technology*. London: Penguin Books Ltd., 2009.
- Bateson, Gregory. *Mind and Nature, A Necessary Unity*. New York: Bantam, 1988.
- Benkler, Yochai. *The Wealth of Networks*. New Haven: Yale University Press, 2006.
- Bobbitt, Philip. *The Shield of Achilles*. London: Anchor, 2003.
- Borkin, Joseph and Welsh, Charles A. *Germany's Master Plan*. New York: Duell, Sloan & Pearce, 1943.
- Boulding, Kenneth E. *Three Faces of Power*. Newbury Park: SAGE Publications Inc., 1989.
- Brand, Stewart. *The Media Lab: Inventing the Future at MIT*. New York: Viking Penguin, 1987.
- Castells, Manuel. *The Power of Identity*. Oxford: Wiley-Blackwell, 2010.
- Castells, Manuel. *Communication Power*. Oxford: Oxford University Press, 2011.
- Clausewitz, Karl von. *On War (The Book of War)*. New York: Random House Inc., 2000. (p.249 onwards)
- Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. Boston: Little Brown & Co., 2002.
- Davis, Stan. *Lessons from the Future*. Oxford: Capstone Publishing Ltd., 2001.
- Gaffney, Frank. *War Footing*. Annapolis: Naval Institute Press, 2005.
- Gibson, James J. *The Ecological Approach to Visual Perception*. New Jersey: Lawrence Erlbaum Associates Inc. Publishers, 1986.
- Hammersley, Ben. *64 Things You Need to Know Now for Then*. London: Hodder & Stoughton, 2012.
- Isaacson, Walter. *Steve Jobs*. New York: Simon & Schuster, 2011.
- Landau, Susan. *Surveillance or Security?*. Cambridge (USA): The MIT Press, 2011.
- Liddell, Henry & Scott, Robert. *A Greek-English Lexicon*. Oxford: Clarendon Press (Oxford University Press), 1940.
- Lloyd, Seth. *Programming the Universe: A Quantum Computer Scientist takes on the Cosmos*. London: Vintage, 2007.
- Luttwak, Edward N. *Strategy: The Logic of War and Peace*. Cambridge (USA): Harvard University Press, 2001.
- Martin, Roger. *The Opposable Mind: Winning Through Integrative Thinking*. Boston: Harvard Business School Press, 2009.
- Moynihan, Daniel Patrick. *Secrecy*. New Haven: Yale University Press, 1999.
- Naughton, John. *A Brief History of the Future*. London: Phoenix Paperbacks, 2000.
- Nye, Joseph. *The Future of Power*. New York: Public Affairs, 2011.
- Perez, Carlota. *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*. Cheltenham: Edward Elgar Publishers, 2003.
- Pinker, Steven. *The Better Angels of Our Nature: The Decline of Violence in our History and its Causes*. London: Penguin, 2011.
- Redman, Thomas. *Data Driven: Profiting from your most Important Business Aspect*. Boston: Harvard Business School Publishing, 2008.

- Regan, Priscilla .M. *Legislating privacy: Technology, social values, and public policy*. Chapel Hill: The University of North Carolina Press, 1995.
- Rumelt, Richard. *Good Strategy, Bad Strategy*. London: Profile Books, 2011.
- Sahlins, Marshall. *Stone Age Economics*. Abingdon: Routledge, 2011.
- Sanger, David. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Random House, 2012.
- Schmidt, Prof. M. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.
- Tainter, Joseph. *The Collapse of Complex Societies*. Cambridge: Cambridge University Press, 1990.
- Tapscott, Don & Williams, Anthony D. *Radical Openness: Four Unexpected Principles for Success*. TED Conferences (iBook), 2012.
- Toffler, Alvin. *War and Anti-War*. London: Warner Books, 1994.
- Wiseman, Geoffrey. *Concepts of Non-Provocative Defence*. New York: PALGRAVE, 2002.

Journal Articles

- Anderson, Ross. & Brady, Robert. 'Why quantum computing is hard—and quantum cryptography is not provably secure' *Quantum Physics* 7351 (Jan 2013) <http://arxiv.org/pdf/1301.7351v1.pdf> accessed 26/02/13
- Bamford, James. 'The Black Box: Inside America's Massive New Surveillance Centre' *Wired* vol.20, no.4 (April 2012), 78-84 & 122-124.
- Carman, Douglas. 'Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass Media & the Politics of Identity' *Pacific Rim Law & Policy Journal, University of Washington School of Law*, (Spring 2002) https://digital.lib.washington.edu/dspace-law/bitstream/handle/1773.1/757/16_11PacRimL%26PolyJ339%282002%29.pdf?sequence=1 accessed 05/03/13
- Gilder, George. 'The Information Factories' *Wired* vol.14, no.10 (October 2006) http://www.wired.com/wired/archive/14.10/cloudware.html?pg=1&topic=cloudware&topic_set=1
- Graeber, Charles. 'Kim Dotcom' *Wired* vol.20, no.11 (November 2012), 158-161 & 192-200.
- Grier, Chris., Ballard, L., Caballero, J., Chachra, N., Dietrich, C.J., Levchenko, K., Mavrommatis, P., McCoy, D., Nappa, A., Pitsillidis, A., Provos, N., Rafique, M.Z., Rajab, M.A., Rossow, C., Thomas, K., Paxson, V., Savage, S. & Voelker, G.M. 'Manufacturing Compromise: The Emergence of Exploit-as-a-Service' *The Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS)*, (October 2012) http://www.imchris.org/research/grier_ccs2012.pdf accessed 26/02/13
- Klimberg, Alexander. 'The Whole of Nation in Cyberpower' *Georgetown Journal of International Affairs* (Special issue, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity, 2011), pp.171-179
- Noya, Javier. 'The Symbolic Power of Nations' (Translation from Spanish) *Elcano Royal Institute Working Papers* vol.2005, no.35 (2005) <http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=13678> accessed 12/03/13 (Also in *Place Branding and Public Diplomacy*, 1 January 2006, vol.2, 53–67)
- Pan, Jianli., Paul, Subbarthi., & Jain, Raj. 'A Survey of the Research on Future Internet Architectures', *IEEE Communications Magazine* vol.49, no.7 (July 2011)

<http://www.cse.wustl.edu/~jain/papers/ftp/internet.pdf> accessed 14/02/13

Tibbs, Hardin. 'Changing Cultural Values and the Transition to Sustainability' *Journal of Futures Studies* vol.15, no.3 (March 2011), 13-32.

Tibbs, Hardin. 1998 'Sustainability' *Deeper News publications (Global Business Network)* vol.10, no.1 (January 1999)

Tong, David. 'The Unquantum Quantum' *Scientific American* vol.307, (December 2012)

Reports, Papers & Manuals

Albright, David., Walrond, C., Stricker, A. & Avagyan, R. 'Analysis of IAEA Iran Safeguards Report' *Institute for Science and International Security (ISIS)*, 30th Aug 2012 http://isis-online.org/uploads/isis-reports/documents/ISIS_Analysis_IAEA_Report_30Aug2012.pdf accessed 14/02/13

'Campaigning - Joint Doctrine Publication 01' *MoD Development, Concepts and Doctrine Centre*, (2nd Edition), December 2008

http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CDUQFjAB&url=http%3A%2F%2Fwww.da.mod.uk%2Fcolleges%2Fjscsc%2Fcourses%2FRAFJD%2FCourses%2F20090219JDP_01.pdf&ei=aPI5UajFC6ve7Aa1pICgCA&usg=AFQjCNGm7NVRK-wOUUpYI5QBVTNoC7yjgQ&bvm=bv.43287494,d.ZGU accessed 08/03/13

'Dilemmas of Privacy and Surveillance' *The Royal Academy of Engineering*, March 2007, http://www.cl.cam.ac.uk/research/dtg/www/publications/public/ah12/dilemmas_of_privacy_and_surveillance_report.pdf accessed 14/02/13

'Foresight Future Identities- Executive Summary' *The Government Office for Science*, London, 2013 <http://www.bis.gov.uk/assets/foresight/docs/identity/13-524-future-identities-changing-identities-summary.pdf> accessed 08/03/13

Hallion, Richard P. 'Precision guided munitions and the new era of warfare' *APSC Paper Number 53*, Air Power Studies Centre, Fairburn, 1995 <http://www.fas.org/man/dod-101/sys/smarts/docs/paper53.htm> accessed 30/03/13

Heickero, Roland 'Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations' *FOI, Swedish Defence Research Agency, Division of Defence Analysis*, Stockholm, March 2010 <http://www.highseclabs.com/Corporate/foir2970.pdf> accessed 08/03/13

'Science as an Open Enterprise' -The Royal Society Science Policy Center report 02/12, *The Royal Society*, London, June 2012.

http://royalsociety.org/uploadedFiles/Royal_Society_Content/policy/projects/sape/2012-06-20-SAOE.pdf accessed 14/02/13

'The Shell Global Scenarios to 2025- The future business environment: trends, trade-offs and choices' *Shell International Limited (SIL)*, 2005 <http://www.static.shell.com/content/dam/shell/static/aboutshell/downloads/our-strategy/shell-global-scenarios/exsum-23052005.pdf> accessed 08/03/13

Media

BBC News Technology. 'Flame malware makers send "suicide" code' 8th June 2012 <http://www.bbc.co.uk/news/technology-18365844> accessed 14/02/13

Bowcott, Owen & Cobain, Ian. 'Secret Courts: The Essential Guide' *The Guardian*, 25th Sept 2012 <http://www.guardian.co.uk/law/2012/sep/25/secret-courts-the-essential-guide> accessed 14/02/13

Carter, Zach. 'Aaron Swartz Memorial on Capitol Hill Draws Darrell Issa, Elizabeth Warren' *Huff Post Politics USA*, 2nd May 2012 http://www.huffingtonpost.com/2013/02/05/aaron-swartz-memorial-darrell-issa_n_2619872.html accessed 14/02/13

Chivers, Tom. 'MOD 'How to stop leaks' Document is Leaked' *The Telegraph*, 5th Oct 2009 <http://www.telegraph.co.uk/news/uknews/defence/6261756/MoD-how-to-stop-leaks-document-is-leaked.html> accessed 18/02/13

Collins, Nick. 'Sir James Dyson Attacks China over Designs "theft"' *The Telegraph*, 6th Dec 2012 <http://www.telegraph.co.uk/finance/yourbusiness/8936685/Sir-James-Dyson-attacks-China-over-designs-theft.html> accessed 18/02/13

Finn, Peter. 'FBI is Increasing Pressure on Suspects in Stuxnet Inquiry' *The Washington Post*, 26th Jan 2013 http://www.washingtonpost.com/world/national-security/fbi-is-increasing-pressure-on-suspects-in-stuxnet-inquiry/2013/01/26/f475095e-6733-11e2-93e1-475791032daf_story.html accessed 18/02/13

Gross, Michael. 'World War 3.0' *Vanity Fair*, May 2012 <http://www.vanityfair.com/culture/2012/05/internet-regulation-war-sopa-pipa-defcon-hacking> accessed 14/02/13

Harris, Shane. 'Giving in to the Surveillance State' *The New York Times*, 22nd Aug 2012 http://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html?_r=0 accessed 14/02/13

Johnson, Wesley. 'Secret Court Hearings "will do more harm than good"' *The Telegraph*, 28th Jan 2013 <http://www.telegraph.co.uk/news/politics/9829914/Secret-court-hearings-will-do-more-harm-than-good-Tory-MP-says.html> accessed 14/02/13

Kessler, Glenn. 'File the Bin Laden Phone Leak Under "Urban Myths"' *Washington Post*, 22nd Dec 2005 <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/21/AR2005122101994.html> accessed 14/02/13

Kusisto, Laura. 'Putting the Tech in Metrotech' *The Wall Street Journal*, 7th May 2012 <http://online.wsj.com/article/SB10001424052702304363104577390473311236692.html> accessed 30/03/13

Lee, Dave. 'Flame: Massive Cyber-attack Discovered, researchers say' *BBC News Technology*, 28th May 2012 http://www.bbc.co.uk/news/technology-18238326#_jmp0 accessed 14/02/13

Markoff, John. 'Killing the Computer to Save It' *The New York Times*, 29 Oct 2012 <http://www.nytimes.com/2012/10/30/science/rethinking-the-computer-at-80.html?pagewanted=all> accessed 18/02/13

Nakashima, Ellen. 'U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say' *The Washington Post*, 19th June 2012 http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html accessed 14/02/13

Obama, Barack. 'Taking the Cyberattack Threat Seriously' *The Wall Street Journal*, 19th July 2012 http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?KEY_WORDS=Obama+cybersecurity accessed 14/02/13

Pavel, Tal. 'Report: Iran seeks support to censor Internet, disconnect from global network' *Haaretz*, 20th Apr 2012 <http://www.haaretz.com/news/middle-east/report-iran-seeks-support-to-censor-internet-disconnect-from-global-network-1.425602> accessed 14/02/13

Perlroth, Nicole. 'Hackers in China Attacked The Times for last 4 Months' *The New York Times*,

30th Jan 2013 <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&r=0> accessed 18/02/13

Perlroth, Nicole. 'Trying to keep your Emails Secret when the CIA Chief Couldn't' *The New York Times*, 16th November 2012 <http://www.nytimes.com/2012/11/17/technology/trying-to-keep-your-e-mails-secret-when-the-cia-chief-couldnt.html?pagewanted=all&r=0> accessed 18/02/13

Perlroth, Nicole & Hardy, Quentin. 'Bank Hacking was the Work of Iranians, Officials Say' *The New York Times*, 8th Jan 2013 <http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?r=2&> accessed 18/02/13

Ross, Tim. 'Privacy Fears as Jeremy Hunt order Health Records to be Shared Throughout NHS' *The Telegraph*, 15th Jan 2013 <http://www.telegraph.co.uk/news/politics/9804402/Privacy-fears-as-Jeremy-Hunt-orders-health-records-to-be-shared-throughout-NHS.html> accessed 18/02/13

RT. 'Kim Dotcom wants to encrypt half of the internet to end government surveillance' 25th Jan 2013 <http://rt.com/usa/news/kim-dotcom-interview-mega-673/> accessed 14/02/13

Sanger, David E. 'Obama Order Sped up Waves of Cyberattacks Against Iran' *The New York Times*, 1st June 2012 <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?r=1&pagewanted=all> accessed 14/02/13

Shane, Scott. 'Online Privacy Issue Is Also in Play in Petraeus Scandal' *The New York Times*, 13th Nov 2012 <http://www.nytimes.com/2012/11/14/us/david-petraeus-case-raises-concerns-about-americans-privacy.html> accessed 14/02/13

Siobhan Gorman & Julian E. Barnes, 'Cyber Combat: Act of War' *The Wall Street Journal*, 30th May 2011
<http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>
accessed 14/02/13

The Economist - Technology Quarterly. 'Marching off to Cyberwar' Q4, 4th Dec 2008
<http://www.economist.com/node/12673385> accessed 30/03/13

The Economist. 'The Printed World' 12 February 2011, p.75.

Wood, David. 'Armed Drone Debate Should Focus On Killing, Not The Weapon, Military Experts Suggest' *Huff Post*, 7th Feb 2013 http://www.huffingtonpost.com/2013/02/07/armed-drone-debate_n_2639565.html accessed 14/02/13

Internet Sources

Anderson, Chris. 'Free is More Complicated than you Think' *Wired Blog*, 4th Nov 2007
http://www.longtail.com/the_long_tail/2007/11/free-is-more-co.html accessed 14/02/13

Anderson, Ross. 'Privacy Considered Harmful?' *Light Blue Touchpaper*, 16th Jan 2013
<http://www.lightbluetouchpaper.org/2013/01/16/privacy-considered-harmful/> accessed 18/02/13

Aron, Jacob. 'The Cyberweapon that could take down the Internet' *NewScientist - Tech News* (11th February 2011) <http://www.newscientist.com/article/dn20113-the-cyberweapon-that-could-take-down-the-internet.html> accessed 18/02/13

Barlow, John Perry. 'Crime and Puzzlement'
http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/crime_and_puzzlement_1.htm
I accessed 14/02/13

Briscoe, B., Odlyzko, A. & Tilly, B. 'Metcalfe's Law is Wrong' *IEEE Spectrum*, July 2006

- <http://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong/0> accessed 28/03/13
- Brownlee, John. 'Infographic: Most Artists Earn More Revenue Through iTunes than at Retail' *Cult of Mac*, 14th April 2010 <http://www.cultofmac.com/38097/infographic-most-artists-earn-more-revenue-through-itunes-than-at-retail/> accessed 14/02/13
- Cerveny, Ben. 'The Luminous Bath' 8th Feb 2007 <http://liftconference.com/videos/ben-cerveny> or <http://blip.tv/lift/ben-cerveny-the-luminous-bath-lift07-en-2584070> accessed 14/02/13
- Cisco. 'Global - 2016 Forecast Highlights'
http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html accessed 14/02/13
- Cleevely, David & Matthew. 'The n Bells' *Blog*, 19th Feb 2012
<http://www.thenbells.com/2012/02/font-face-font-family-cambriap.html> accessed 14/02/13
- Coleman, Gabriella. 'Our Weirdness is Free' *triplecanopy* 15, 13th Jan 2012
http://canopycanopycanopy.com/15/our_weirdness_is_free accessed 30/03/13
- Corera, Gordon. 'MI5 fighting "Astonishing" level of Cyber Attacks' *BBC - News*, 25th June 2012
<http://www.bbc.co.uk/news/uk-18586681> accessed 07/03/13
- DARPA. 'Clean Slate Design on Resilient, Adaptive, Clean Hosts (CRASH)'
[http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_\(CRASH\).aspx](http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_(CRASH).aspx) accessed 8/02/13
- Dean, David., DiGrande, Sebastian., Field, Dominic., Lundmark, Andreas., O'Day, James., Pineda, John. & Zwilrenberg, Paul. 'The Internet Economy in the G-20' *bcg.perspectives*, 19th March 2012
https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/ accessed 14/02/13
- 'Doctrine of Information Security of the Russian Federation' 9th September 2000
<http://www.dcaf.ch/Chapter-Section/Information-Security-Doctrine-of-the-Russian-Federation> accessed 28/03/13
- Friedl, Steve. 'An Illustrated Guide to the Kaminsky DNS Vulnerability' *Steve Friedl's Unixwiz.net Tech Tips*, 7th Aug 2008 <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html> accessed 30/03/13
- Gasparre, Richard B. 'The Israeli "E-tack" on Syria - Part II' *airforce-technology.com*, 11th March 2008 <http://www.airforce-technology.com/features/feature1669> accessed 30/03/13
- Grosse, Eric. 'Security Warnings for Suspected State-Sponsored Attacks' *Google Online Security Blog*, 5th June 2012 <http://googleonlinesecurity.blogspot.co.uk/2012/06/security-warnings-for-suspected-state.html> accessed 14/02/13
- Hill, David J. '1 Million Robots to replace 1 Million Human Jobs at Foxconn? First Robots Have Arrived.' *Singularity Hub*, 11th Dec 2012 <http://singularityhub.com/2012/11/12/1-million-robots-to-replace-1-million-human-jobs-at-foxconn-first-robots-have-arrived/> accessed 30/03/13
- Huawei. 'BT and Huawei Seal 1st Century Network Contract' Dec 2005
<http://www.huawei.com/uk/about-huawei/newsroom/press-release/hw-088555-news.htm> accessed 18/02/13
- Internet Movie DataBase. 'Zero Dark Thirty' <http://www.imdb.com/title/tt1790885/> accessed 14/02/13

James, Malcolm. 'Blackhole Exploit Kit used in Conjunction with Spam Emails' *All Spammed Up*, 17th July 2012 <http://www.allspammedup.com/2012/07/blackhole-exploit-kit-used-in-conjunction-with-spam-emails/> accessed 14/02/13

Kahn, Robert E. 'The Role of Architecture in Internet Defense' *Chapter XII, America's Cyber Future, Volume II, Center for a New American Security*, 2011
http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf
accessed 14/02/13

Kaspersky Lab. 'Kaspersky Lab Discovers 'Gauss' – A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts' 9th Aug 2012
http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts
accessed 14/02/13

Kaspersky, Eugene. 'What Wired is not Telling You - a Response to Noah Shachtman's Article in Wired magazine' *Kaspersky Online Blog*, 25th July 2012
<http://eugene.kaspersky.com/2012/07/25/what-wired-is-not-telling-you-a-response-to-noah-shachtmans-article-in-wired-magazine/> accessed 19/03/13

Kok, Jan de., Vroonhof, Paul., Verhoeven, Wim., Ton Kwaak, Niek Timmermans., Florieke Westhof, Jacqueline Snijders. 'Do SMEs Create More and Better Jobs?' *EIM*, Nov 2011
http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/supporting-documents/2012/do-smes-create-more-and-better-jobs_en.pdf
accessed 18/02/13

Lee, Edmund. 'The New York Times Paywall is Working Better than Anyone had Guessed' *TechBlog*, 20th Dec 2012 <http://go.bloomberg.com/tech-blog/2012-12-20-the-new-york-times-paywall-is-working-better-than-anyone-had-guessed/> accessed 14/02/13

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., Byers, AH. 'Big data: The next frontier for innovation, competition, and productivity' *McKinsey Global Institute*, May 2011
http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation accessed 18/02/13

McKinsey Global Institute. 'Internet Matters: The net's sweeping impact on growth, jobs and prosperity' May 2011
http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Internet%20matters%20-%20Nets%20sweeping%20impact/MGI_internet_matters_full_report.ashx (Page 25) accessed 12/09/11

MEGA <https://mega.co.nz/#privacycompany> accessed 14/02/13

Microsoft TechNet. 'Common Types of Network Attacks' 2013
<http://technet.microsoft.com/en-us/library/cc959354.aspx> accessed 14/02/13

Mills, Mark P. 'Amazon's Kiva Robot Acquisition is Bullish for Both Amazon and American Jobs' *Forbes - News*, March 2012 <http://www.forbes.com/sites/markpmills/2012/03/23/amazons-kiva-robot-acquisition-is-bullish-for-both-amazon-and-american-jobs/> accessed 14/02/13

Mikkelsen, Barbara & David. 'Insect Spy Drone' *Snopes*, 14th Aug 2012
<http://www.snopes.com/photos/technology/insectdrone.asp> accessed 14/02/13

Mulgan, Geoff. 'Connexity revisited' *DEMOS*
<http://www.demos.co.uk/files/File/networklogic04mulgan.pdf> accessed 14/02/13

Muncaster, Phil. 'Symantec: Don't blame us for New York Times hack' *The Register*, 1st Feb
http://www.theregister.co.uk/2013/02/01/symantec_responds_nyt_apt/ accessed 18/02/13

Namestnikov ,Yury. 'Kaspersky Security Bulletin, Statistics 2011'
http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011#8 accessed 14/02/13

NPD. 'iTunes Continues to Dominate Music Retailing, but nearly 60 Percent of iTunes Music Buyers also Use Pandora' 18th Sept 2012
https://www.npd.com/wps/portal,npd/us/news/press-releases/itunes-continues-to-dominate-music-retailing-but-nearly-60-percent-of-itunes-music-buyers-also-use-pandora!/ut/p/c5/04_SB8K8xLLM9MSSzPy8xBz9CP0os3g3b1NTS98QY0MDbydTA08vSzcnV38LQ0dTc_1I_ShznPI-ZvoF2YGKAMP77Ro!/ accessed 14/02/13

O'Reilly, Tim. 'Web 2.0: Compact Definition?' O'Reilly, 1st Oct 2005
<http://radar.oreilly.com/2005/10/web-20-compact-definition.html> accessed 18/02/13

OECD. 'The economic impact of shutting down Internet and mobile phone services in Egypt' 4th Feb 2011
<http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm> accessed 14/02/13

Pélissié du Rausas, Matthieu., Manyika, James., Hazan, Eric., Bughin, Jacques., Chui, Michael., & Said, Rémi.'Internet matters: The Net's sweeping impact on growth, jobs, and prosperity' *McKinsey Global Institute*, May 2011
http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/internet_matters accessed 14/02/13

PEW Research. 'The Lost Decade of the Middle Class' Aug 2012
<http://www.pewsocialtrends.org/2012/08/22/the-lost-decade-of-the-middle-class/> accessed 18/02/13

Ragan, Steve. 'Germany Admits to Existence of Cyberwarfare Unit' *Security Week*, 8th June 2012 <http://www.securityweek.com/germany-admits-existence-cyberwarfare-unit> accessed 14/02/13

Redman, Thomas C. 'Integrate Data into Products, or Get Left Behind' *Harvard Business Review Blog Network*, 28th June 2012
http://blogs.hbr.org/cs/2012/06/integrate_data_in_products_or_get.html

Reisinger, Don. 'Is the US Government Really a Spy Machine?' *MIT Technology Review - News*, 10th Dec 2012 <http://www.technologyreview.com/view/508571/is-the-us-government-really-a-spy-machine/> accessed 14/02/13

Ross Anderson et al., 'Measuring the Cost of Cyber Crime' *WEIS Workshop on the Economics of Information Security*, 25/26th June 2012
http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf accessed 14/02/13

Schubarth, Cromwell. 'Tech Shift Turns up the Heat on Cisco Systems' *Business Journal - News*, 9th Nov 2012 <http://www.bizjournals.com/sanjose/print-edition/2012/11/09/tech-shift-turns-up-the-heat-on-cisco.html?page=all> accessed 18/02/13

Security - News. 'Huawei Proposes Australian Cyber Security Test Centre', (25th Oct 2012)
<http://www.securitymagazine.com/articles/83669-huawei-proposes-australian-cyber-security-test-center> accessed 18/02/13

Shachtman, Noah. 'Exclusive: Computer Virus Hits U.S. Drone Fleet' *Wired - News*, 7th Oct 2011 <http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/> accessed 14/02/13

Shachtman, Noah. 'Insurgents Intercept Drone Video in King-Size Security Breach' *Wired - News*, 17th Dec 2009 <http://www.wired.com/dangerroom/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/> accessed 14/02/13

Shachtman, Noah. 'Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals' *Wired - News*,

23rd July 2012 http://www.wired.com/dangerroom/2012/07/ff_kaspersky/all/ accessed 19/03/13

Shachtman, Noah. 'Syria Has Just Been Taken Offline' *Wired - News*, 29th Nov 2012
<http://www.wired.com/dangerroom/2012/11/syria-offline/all/> accessed 30/03/13

Simonite, Tom. 'Welcome to the Malware Industrial Complex' *MIT Technology Review - News*, 13th Feb 2013 http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/?utm_campaign=newsletters&utm_source=newsletter-daily-all&utm_medium=email&utm_content=20130213 accessed 18/02/13

Simonite, Tom. 'Stuxnet Tricks Copied by Computer Criminals' *MIT Technology Review - News*, 19th Sept 2012 <http://www.technologyreview.com/news/429173/stuxnet-tricks-copied-by-computer-criminals/> accessed 18/02/13

Simonite, Tom. 'The Antivirus Era is Over' *MIT Technology Review - News*, 11th June 2012
<http://www.technologyreview.com/news/428166/the-antivirus-era-is-over/> accessed 18/02/13

Sonderlev Christensen, Martin. 'Information Wants to be Social' *Social Square*, 3rd June 2012
<http://www.socialsquare.dk/2012/06/03/information-wants-to-be-social/> accessed 14/02/13

Staehle, Wolfgang & Avgikos, Jan. 'The Thing' <http://www.lacan.com/frameVIII15.htm> accessed 14/02/13

Symantec. 'Internet Security Threat Report, Volume 17' April 2012
<http://www.symantec.com/threatreport/> accessed 14/02/13

Symantec. 'Norton Security Calculates Cost of Global Cybercrime' 7th Sept 2011
http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 accessed 18/02/13

The Engineer - News. 'Robots to Organise themselves like a Swarm of Insects' March 2012
<http://www.theengineer.co.uk/sectors/automotive/news/robots-to-organise-themselves-like-a-swarm-of-insects/1012101.article> accessed 14/02/13

The George Washington University Archives, Cold War Documents
<http://www.gwu.edu/~nsarchiv/coldwar/documents/episode-1/kennan.htm> accessed 18/02/13

The national archives. 'Intelligence Services Act (UK)'
<http://www.legislation.gov.uk/ukpga/1994/13/contents> accessed 07/03/13

Thomas, Timothy L. 'Information Security Thinking: A Comparison of US, Russian, & Chinese Concepts' *Foreign Military Studies Office*, July 2001
http://fmso.leavenworth.army.mil/documents/infosecu.htm#_ftnref15 accessed 18/02/13

U.S. Department of Defense. 'DOD Announces First U.S. Cyber Command and First U.S. CYBERCOM Commander' 21st May 2010
<http://www.defense.gov/releases/release.aspx?releaseid=13551> accessed 18/02/13

U.S. Department of the Treasury Press Centre. 'Treasury Designates Iranian Ministry of Intelligence and Security for Human Rights Abuses and Support for Terrorism' 16th Feb 2012
<http://www.treasury.gov/press-center/press-releases/Pages/tg1424.aspx> accessed 14/02/13

United Nations Rule of Law. 'Non-Governmental Organisations'
http://www.unrol.org/article.aspx?article_id=23 accessed 30/03/13

Vulnerability Notes Database. 'Vulnerability Note VU#800113' Homeland Security, 8th July 2008 <http://www.kb.cert.org/vuls/id/800113> accessed 30/03/13

Walker, Matt. 'Huawei, ZTE hold upper hand in vendor financing wars' *Ovum*, 14th March 2012 <http://ovum.com/2012/03/14/huawei-zte-hold-upper-hand-in-vendor-financing-wars/>

accessed 18/02/13

'What is a Klein Bottle?' http://www.kleinbottle.com/whats_a_klein_bottle.htm & <http://plus.maths.org/content/imaging-maths-inside-klein-bottle> accessed 14/02/13

Wikipedia. 'Flame (malware)' 28th Jan 2013 [http://en.wikipedia.org/wiki/Flame_\(malware\)](http://en.wikipedia.org/wiki/Flame_(malware)) accessed 14/02/13

Wikipedia. 'Jyllands-Posten Muhammad cartoons controversy'
http://en.wikipedia.org/wiki/Jyllands-Posten_Muhammad_cartoons_controversy accessed 14/02/13

Wikipedia. 'Search Engine Optimization' 29th March 2013
http://en.wikipedia.org/wiki/Search_engine_optimization accessed 30/03/13

Williams, Christopher. 'Chinese Firm Hlts Back at Cyberspy Claims' *Security*, 12th June 2009
http://www.theregister.co.uk/2009/06/12/cybersecurity_huawei/print.html accessed 18/02/13

York, Jillian C. 'Hacktivism for Syria' *Aljazeera*, 29th Sept 2011
<http://www.aljazeera.com/indepth/opinion/2011/09/201192712428972155.html> accessed 30/03/13

Presentations, Conferences, Workshops & Projects

2012 Workshop on Cyber Security and Global Affairs and Global Security Forum, Polytechnic University of Catalonia, Barcelona, Spain, 19th-21st June 2012.

Harvard-MIT-University of Toronto Cyber Norms Workshop 2.0, Cambridge/Boston, USA, 11th-14th September 2012.

Multinational Experiment 7, (MNE-7), a US-managed two-year multinational and interagency Concept Development and Experimentation effort, 2011-2012.

The School of International Futures, a conference at Wilton Park on the theme of Strategic Foresight, Wilton Park, West Sussex, 13th-17th August 2012.

Films

William Gibson: No Maps for These Territories. Directed by Mark Neale. UK: Docurama, 2000.

ISBN 978-1-905962-99-0

ISBN 978-1-905962-99-0

serco  Media +
Graphics

Serco Media & Graphics SN6 8LA 54702 20130430
sercomedia@da.mod.uk 01793 785450/788666



www.da.mod.uk