On Cyber Warfare

A Chatham House Report

Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke

CHATHAM HOUSE

www.chathamhouse.org.uk

On Cyber Warfare

Paul Cornish, David Livingstone, Dave Clemente
and Claire Yorke

A Chatham House Report

November 2010

CHATHAM HOUSE

www.chathamhouse.org.uk

Chatham House has been the home of the Royal Institute of International Affairs for ninety years. Our mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all.

The Royal Institute of International Affairs
Chatham House
10 St James's Square
London SW1Y 4LE
T: +44 (0) 20 7957 5700
F: + 44 (0) 20 7957 5710
www.chathamhouse.org.uk

Charity Registration No. 208223

ISBN 978 1 86203 243 9

A catalogue record for this title is available from the British Library.

Designed and typeset by SoapBox Communications Limited
www.soapboxcommunications.co.uk

Printed and bound in Great Britain by by Latimer Trend and Co Ltd

The material selected for the printing of this report is Elemental Chlorine Free and has been sourced from well-managed forests. It has been manufactured by an ISO 14001 certified mill under EMAS.

Contents

About the Authors

Dr Paul Cornish is Carrington Professor of International Security and Head of the International Security Programme at Chatham House. His recent publications cover many aspects of contemporary security and defence policy including (as editor) *The Conflict in Iraq, 2003* (Palgrave/Macmillan, 2004); 'The United States and counterinsurgency: "political first, political last, political always"', *International Affairs* (January 2009); 'Technology, strategy and counterterrorism', *International Affairs* (July 2010). He is co-author, with Dr Andrew Dorman, of a series of articles on UK security and defence strategy published in *International Affairs:* 'Blair's wars and Brown's budgets: from Strategic Defence Review to strategic decay in less than a decade' (March 2009); 'National defence in the age of austerity' (July 2009); and 'Breaking the mould: the United Kingdom Strategic Defence Review 2010' (March 2010). Dr Cornish's most recent publication is *Strategy in Austerity: the Security and Defence of the United Kingd*om (Chatham House, October 2010). In the field of cyber security studies he is co-author with David Livingstone and Rex Hughes of *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (Chatham House, March 2009).

David Livingstone is an Associate Fellow on the International Security Programme at Chatham House and the Managing Director of Napier Meridian. His company, established in 2005, provides expertise on business transformation in the national security and resilience domain, with a particular focus on the cyber domain. He was a desk officer in the Directorate of Military Operations in the Ministry of Defence (MoD) for four years in the mid-1990s, when the issue of cyber security (then in the guise of 'Information Warfare') was first identified as an emerging threat. He was a founder member of the Cabinet Office's first official committee addressing the electronic threats to the Critical National Infrastructure. In the MoD appointment he was a staff officer in COBR and worked on a number of other Cabinet Official Committees to do with national security matters. He retired from the Services in 1999. At Chatham House he has written a number of works on cyber security, counter-terrorism, serious organized crime, and other security policy-related subjects. He is a Fellow of the Royal Geographical Society.

Dave Clemente is a Research Assistant with the International Security Programme at Chatham House. He was educated at the Ohio State University, the University of Damascus and the School of Oriental and African Studies. Before coming to Chatham House he worked with the International Institute for Strategic Studies and the Overseas Development Institute. His research covers topics including cyber security policy, US and UK security and defence policy, and stabilization and reconstruction.

Claire Yorke is Manager of the International Security Programme at Chatham House. She was educated at Lancaster University, the University of Exeter and Sciences Po Lille. Following her Masters degree in Middle East Politics she worked for three years as a Parliamentary Researcher in the House of Commons. Her research interests include UK defence and security policy, cyber security, organized crime, post-conflict reconstruction and stabilization.

Acknowledgments

The authors are grateful to colleagues at Chatham House and elsewhere who read and commented upon earlier versions of this report, and to representatives of the UK and other governments who advised on its structure. We have benefited from the advice of experts in the information and telecommunications sector in the United Kingdom and beyond. We are grateful to the Northrop Grumman Corporation for their sponsorship of this project, and especially to Mr Mike Steinmetz for his constructive contributions at all stages of the project. Dr Rex Hughes contributed material to an earlier version of the report.

The views expressed in this document are those of the authors, who accept responsibility for any errors of fact or interpretation.

November 2010 PC, DL, DC, CY

Executive Summary

In recent years, governments and international organizations have become more focused on cyber security and increasingly aware of the urgency connected with it. In the United Kingdom, cyber security featured prominently in the *National Security Strategy* and the *Strategic Security and Defence Review* published in October 2010.

Cyber warfare is arguably at the most serious end of the spectrum of security challenges posed by – and within – cyberspace. Just like the tools of conventional warfare, cyber technology can be used to attack the machinery of state, financial institutions, the national energy and transport infrastructure and public morale. However, while some actions may appear aggressive and warlike, they may not necessarily be intended as acts of war. It is important, therefore, to distinguish between warfare and non-warfare in cyberspace. It is the action and its warlike properties that matter as much as the actor. For example, the cyber actions of terrorist groups, spies and organized criminals can be harmful and appear aggressive but they do not in themselves necessarily constitute acts of cyber warfare.

Cyber warfare could be the archetypal illustration of 'asymmetric warfare' – a struggle in which one opponent might be weak in conventional terms but is clever and agile, while the other is strong but complacent and inflexible. The most distinctive feature of cyber warfare (and cyber security more generally) is the rapidity with which threats can evolve. The pace of change can be so abrupt as to render the action/reaction cycle of traditional strategy out of date before it has begun.

There is a beguiling and dangerous argument that cyber warfare can be preferable as a 'painless' or 'bloodless' form of conflict that still delivers decisive outcomes. Victory and defeat are far from recognizable in cyberspace. These concepts have little traction in a domain where political, ideological, religious, economic and military combatants fight for varying reasons, according to different timescales, and applying their own code of conduct to the fight. This results in a discordant and chaotic sphere of conflict in which it is not yet obvious that a common framework of ethics, norms and values can apply.

Cyber warfare is often discussed in terms of alarming anecdotes which often seem closer to the world of science fiction than public policy. Moving beyond the anecdotal, cyber warfare must, however, be understood in the context of national strategy. This report identifies the essential characteristics of cyber warfare as a strategic phenomenon by describing the actions of cyber attackers and the reactions of defending governments and by analysing the 'ends, ways and means' of cyber warfare. As a result it proposes the following definition:

- Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target.

The most distinctive features of cyber warfare are:

- Cyber warfare can enable actors to achieve their political and strategic goals without the need for armed conflict.
- Cyberspace gives disproportionate power to small and otherwise relatively insignificant actors.
- Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity, at least in the short term.
- In cyberspace the boundaries are blurred between the military and the civilian, and between the physical and the virtual; and power can be exerted by states or non-state actors, or by proxy.

- Cyberspace should be viewed as the 'fifth battlespace', alongside the more traditional arenas of land, air, sea and space. Cyber warfare is best understood as a new but not entirely separate component of this multifaceted conflict environment.
- Warlike actions in cyberspace are more likely to occur in conjunction with other forms of coercion and confrontation. However, the ways and means of cyber warfare remain undeniably distinct from these other modes of conflict.

A number of conclusions can be drawn from this assessment of the evolving challenges in cyberspace:

- The transatlantic relationship is important for a variety of reasons where cyber warfare is concerned. Close cooperation between the United States and the United Kingdom in intelligence and military matters has extended into cyberspace, enabling both states to influence the domain in a way that is difficult, if not impossible, for any other bilateral partnership or alliance to match.
- On both sides of the Atlantic there should nevertheless be a discussion regarding the precise nature of cyber warfare. This discussion should take into account the complexity of cyberspace, the challenges posed to traditional notions of warfare based on attack and defence, and the speed of change in the medium which threatens to overwhelm all but the most technologically competent.
- There is, however, no need to reinvent the wheel and to devise wholly new techniques and procedures related to cyber warfare. Despite the novelty of cyberspace, there are lessons regarding the management of complex problems to be learned from the existing defence environment, wider government and the commercial sector.

Strategy is the servant of politics. While there may be no shortage of politics associated with different acts of cyber warfare around the world, it cannot yet be described as a politically constrained phenomenon in the way that Clausewitz, the nineteenth-century soldier-philosopher and author of *On War*, would understand. This report describes cyberspace as *terra nullius*, currently beyond the reach of mature political discourse. It is precisely the absence of a constraining political framework around cyber warfare that makes cyberspace so attractive as a place in which to pursue aggressively cultural, religious, economic, social and even – paradoxically – political goals.

Cyber warfare should be constrained and validated by politics, ethics, norms and values otherwise the debate can be unbalanced in favour of military and technological responses to emerging threats. In the process, many of the challenges associated with cyber warfare will be clarified and resolved. For its part, politics must also acknowledge the challenges of cyber warfare: its complexities must be extended back into the world of politics, questioning deeply embedded assumptions about the primacy of the state, the authority of government and the role of government agencies and the armed forces as providers of national security.

1. Introduction

> It is impossible that old prejudices and hostilities should longer exist, while such an instrument has been created for the exchange of thought between all the nations of the earth.
>
> *Comment on the transatlantic telegraph cable, 1858*[1]

> Our entire history is connected to space and place, geometry and geography. … the region of combat is most definitely physical. … a new generation is emerging from the digital landscape … Digital technology can be a natural force drawing people into greater world harmony.
>
> *Nicholas Negroponte, 1996*[2]

> I think the Chinese government has been behind many, many attacks – penetrations. 'Attacks' sounds like they're destroying something. They're penetrations; they're unauthorized penetrations. And what they're trying to do is espionage. They're engaged in massive espionage, not only in the U.S. government, in the U.S. private sector as well, but also around the world.
>
> *Richard Clarke, 2008*[3]

Is the global information and communications network good or bad for national security? The first two quotations above typify the optimism and even idealism that has often been associated with the electronic information and communications revolution of the past 150 years or so. In the comment on the transatlantic telegraph cable there is a sense that communication will have a palliative effect on international politics, by reducing prejudice and hostility. Furthermore, it might even be that conflict itself will be consigned to history; a feature of the old 'geographical' world which is to be overtaken by Negroponte's new 'digital' version. The third quotation gives a very different impression, however. Richard Clarke was the principal advisor on counter-terrorism in the US National Security Council under Bill Clinton and initially also under George W. Bush. Elsewhere in this interview, he argues that 'all of our information is being stolen' and that vast sums expended on research and development in key disciplines such as engineering, pharmaceuticals and genetics are effectively being diverted to the benefit of enemies, criminals and the generally unscrupulous. Using language which is becoming increasingly common, in this interview and in subsequent articles Clarke describes nothing less than a crisis (often referred to colourfully as the prospect of a 'cyber Pearl Harbor') in national and international security.

Cyberspace – the global digital communication and information transfer infrastructure – presents a wide range of security challenges for private individuals, commercial enterprises, governments and international organizations. These challenges, usually grouped under the term cyber security, were examined in detail in a March 2009 Chatham House report and need not be re-examined here.[4] Cyber security has risen in the public and media consciousness in recent years, in response to incidents of various sorts and at various levels. It is also the case that governments and international organizations have become steadily more focused on the subject. Policy announcements and spending plans by the governments of Australia, the United Kingdom and the United States, along with many others, all convey a sense of seriousness and urgency concerning cyber security, as does NATO's decision to establish a cyber security centre of excellence in Tallinn, Estonia. But in the past two or three years the

1 'What the Internet cannot do', *Economist*, 19 August 2000.

2 Nicholas Negroponte, *Being Digital* (New York: Vintage Books, 1996), pp. 238, 230.

3 Richard Clarke, 'Seven questions: Richard Clarke on the next cyber Pearl Harbor', *Foreign Policy*, 2 April 2008, http://www.foreignpolicy.com/articles/2008/04/01/seven_questions_richard_clarke_on_the_next_cyber_pearl_harbor, accessed 18 May 2010.

4 Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (Chatham House, March 2009), http://www.chathamhouse.org.uk/research/security/papers/view/-/id/726/.

cyber security debate has acquired an even sharper edge. The techno-idealism of the past 150 years is increasingly being countered by a dark and pessimistic mood of the sort exemplified by Clarke and, worse still, by growing talk of 'cyber war' or 'cyber warfare'. The decision to establish the NATO centre preceded the 'clickskrieg' attack on Estonia in spring 2007, but that attack did most to bring attention to bear on the 'cyber threat domain' described in the March 2009 Chatham House report as 'state-sponsored cyberattacks'.[5]

> "Where the strategic analysis of cyber warfare is concerned, it is as if evidence and inference have been conflated"

This report, published in the aftermath of the UK government's 2010 strategy review in which cyber security figured prominently,[6] is concerned with arguably the most serious end of the spectrum of security challenges posed by – and within – cyberspace: a problem which we describe as 'cyber warfare'. For a variety of reasons, researching this report proved to be more difficult and less predictable than expected, often requiring a return to first principles of security policy analysis. It quickly became apparent that the problem we address here is not only urgent and complex but also, to a surprising extent, still very under-developed.

In the first place, we were struck by the absence of consensus regarding the principal terms of reference. 'Cyber war', although preferred by some commentators, seems to exaggerate the problem, although not ridiculously so. Yet the more cautious 'state-sponsored cyberattacks' is too narrow in that many actors other than states can take part in this activity, whatever it is. Our choice of terms acknowledges Colin Gray's observation that war and warfare have both an 'unchanging nature' and a 'highly variable character': 'We know with a sad certainty that war has a healthy future. What we do not know with confidence are the forms that warfare will take.'[7] Whatever form it takes, we argue throughout this report that cyber warfare (like all warfare) should be constrained and validated by politics: we make frequent reference to Carl von Clausewitz, the early nineteenth-century soldier-philosopher and author of *On War*.[8] We have chosen, however, to use the term 'cyber war*fare*' in order to focus discussion on activities which are 'warlike' but which may or may not be 'war' *per se*. 'Warfare' is a more open-ended term, more useful in exploring an environment that is not only virtual but also largely uncharted. However, some of the activities described here as cyber warfare might well have little to do with war at all, as conventionally understood. In that case, given that it would be conceptually and logically difficult to separate 'war' from 'warfare', there is a case for using another term altogether – 'cyber power', perhaps.

Another difficulty encountered in researching this report was the style and tone of much analysis of cyber warfare, and cyber security more broadly. With some notable and welcome exceptions we found the subject to be discussed largely anecdotally, and often in very vivid and alarmist language. As well as the 'clickskrieg' cyber attacks on Estonia in 2007 and Georgia in 2008, incidents such as Israel's alleged hacking of Syrian air defence computer systems prior to air strikes in 2007, the *Wall Street Journal*'s revelation in 2009 that Iraqi insurgents had discovered how to monitor video feeds from US Predator unmanned aircraft, and in 2010 the 'Stuxnet' attack on Iran do not simply *inform* debate about an important aspect of national and international security; they *are* that debate. Where the strategic analysis of cyber warfare is concerned, it is as if evidence and inference have been conflated. The result is that cyber warfare can be likened

5 Ibid., pp. 3–5.
6 UK Cabinet Office, *National Security Strategy 2010* and *Strategic Defence and Security Review 2010*, http://www.cabinetoffice.gov.uk/, accessed 21 October 2010.
7 Colin Gray, *Another Bloody Century* (Weidenfeld & Nicolson, 2005), p. 24.
8 Carl von Clausewitz, *On War*, ed. and trans M. Howard and P. Paret (Princeton, NJ: Princeton University Press, 1976).

to an archipelago of islands and reefs, each with its own navigational challenge and each moving out of sight from time to time in the dense fog which surrounds everything. It thus becomes impossible to chart the entire archipelago and not even the most astute navigator can be sure where the shallows and hazards are.

To pursue the maritime metaphor without mercy, we found also that too often it was neither the captain nor the navigator in charge (nor even the fleet commander sitting in relative comfort in a national maritime headquarters), but the senior engineer of the vessel: there is a tendency for cyber security – both problem and solution – to be discussed in a highly technological language which is often not accessible and which is increasingly remote from the general security policy debate. It would be absurd to suppose that cyber technology and technologists should have no place in any debate surrounding cyber warfare, but it is clear that cyberspace is an area into which politicians, policy-makers and commentators often fear to venture.

Our final concern was that the vessel we envisaged navigating, albeit rather badly, through the murky cyber archipelago was a warship flying the ensign of a leading maritime state. We found analysis of cyber security and – perhaps not surprisingly – cyber warfare to be driven by a set of assumptions, too often unexposed to criticism: the state has unchallenged primacy in the international system; government has unchallenged authority within the state; and security remains, in the traditional mould, a cycle of action and reaction between aggressors and defenders best understood and managed by the state's armed forces.

In spite of the difficulties we describe, the ambition of this report is to examine cyber warfare in the context of national strategy. A recent report by the House of Commons Public Administration Select Committee (PASC) defines national strategy as 'the capacity we have as a country to devise and sustain a continuing process which can promote our national interest'. We would only add that 'promote' can also imply 'protect'. The PASC report also speaks of a 'renewed need' for a national strategy and laments the fact that in the United Kingdom 'we have simply fallen out of the habit, and have lost the culture of strategy making'.[9] The authors of this report are of the view that if the threats and opportunities associated with cyberspace are to be fully understood and properly managed, then cyber security – and in particular cyber warfare – must become part of the general national security discourse. Not since the advent of nuclear weapons have advanced mathematics and complex physics come quite so close to the rather less precise world of moral values, political choices, foreign policy and national strategy. *On Cyber Warfare* seeks to bridge this gap, to contribute to the development of a national strategic culture by offering an account of cyber warfare that is more than a string of alarming anecdotes and that is accessible to a non-technological and non-military but policy-focused readership.

This report is structured in such a way as to describe and analyse cyber warfare according to a traditional understanding of armed conflict between states, while at the same time demonstrating the limitations of just such an approach. A conventional, narrowly drawn understanding of cyber warfare and its political context is set out in the following 'strawman' definition. This is where most definitions of cyber warfare arrive, based on the anecdotes and generalizations of many years:

> *Cyber warfare is a conflict between states where precise and proportionate force is directed against military and industrial targets for the purposes of political, economic or territorial gain. Cyberspace serves as an adjunct to conflict in the physical domain and therefore shares many of the same characteristics. In cyber warfare weapons are predominantly military, rather than dual-use; adversaries can be identified and deterred; the terrain is predictable; defence is the position of strength; and offensive actions risk vulnerability as one manoeuvres upon the battlefield. Victory and defeat are recognizable in cyber warfare. Since cyber warfare is not a discrete phenomenon and cannot be separated from conflict in the physical domain, it follows that cyber warfare must be guided and constrained by the values and norms of a state and by the prohibitions that apply to conventional warfare.*

9 Public Administration Select Committee, *Who Does UK National Strategy?*, 12 October 2010, http://www.publications.parliament.uk/pa/cm201011/cmselect/cmpubadm/435/43503.htm, p. 3, accessed 18 October 2010.

The aim of this report is to replace this rather crude strawman with a more robust definition after first exploring the nuanced and ambiguous nature of cyber warfare. The next two chapters of the report – 'Action' followed by 'Reaction' – describe, respectively, hostile actions in cyberspace and the defensive reactions of governments. In each chapter we also show where and why a conventional, state-centric, politico-military strategic template is unable to match the challenge posed by cyber warfare: where, in other words, the strawman is least convincing. We then draw these observations together in the form of a 'Reflection' on the continuities and discontinuities of cyber warfare as a problem for national strategy. By this means the report will show which aspects of cyber warfare can be understood using the traditional template and which aspects will require new thinking. We conclude with a broader and more sophisticated definition of cyber warfare and argue that while national strategy must embrace and understand cyber warfare, in the process of doing so national strategy must itself be reviewed and adapted.

2. Action: Threats and Challenges

> Government, the private sector and citizens are under sustained cyber attack today, both from hostile states and criminals.
>
> *UK National Security Strategy, 2010*[10]

Despite growing recognition of the scale and nature of threats emanating from cyberspace, the virtual world remains largely uncharted and little understood. Threats within and from it are disparate, diffuse and disproportionate in the harm they could cause. Moreover, unlike in conventional attacks where the perpetrator is usually physical and identifiable, the attacker in cyberspace can be virtual and anonymous. Differentiating between actors with 'warlike' intentions and those who are merely malicious or criminal and whose actions fall short of 'acts of war' is therefore problematic. Yet distinctions can and should be made to ensure effective and appropriate responses.

Taking a thematic rather than an anecdotal approach, in this chapter we use a conventional analysis of warfare to reveal the characteristics of the cyber variant. What is the source of direct and indirect security threats in and from cyberspace? Who, or what, are the main actors? What is the actor's intent: are his actions motivated by a desire to dominate, gain a political or strategic advantage or cause substantial harm to a state or a population in pursuit of personal financial gain or self-interest? We also seek to identify the challenges which are distinctive and unique to cyber warfare. Is it reasonable to describe all incidents of cyber aggression as 'warlike'? What are the politics which shape an actor's behaviour in cyberspace? How easy is it to distinguish cyber warfare not only from other cyber security challenges but also from other forms of conflict?

Threats

The character of conflict in cyberspace is as diverse as the actors who exploit it, the actions they take and the targets they attack. Cyber targets can be found not only within the state apparatus or the armed forces but also – just as in physical warfare – in the economic, environmental and social domains. The discussion of actions and actors in this chapter is loosely based on the four cyber threat domains identified in the March 2009 Chatham House report: state-sponsored cyber attacks, ideological and political extremism, serious organized crime, and lower-level/individual crime.[11] These domains provide a useful framework, although we will show that the asymmetries of cyberspace enable a range of other actors, and not just states, to use virtual means, in some cases with a psychological dimension, for their own hostile ends. We do not suggest, either, that all hostile actions in cyberspace must fit into one or more of these categories: we could envisage, for example, 'cyber protest' whereby a nuclear facility of some sort is attacked for ecological reasons. In many cases the actions we describe have all the appearance of warlike activity. But often the distinction between what is and what is not warlike is blurred and there are inevitable exceptions to any rule.

Hostile actors in cyberspace can make use of a wide range of techniques. Malicious software (malware), networks of 'botnets' and logic bombs can all be employed to navigate target systems, retrieve sensitive data or overrule command-and-control systems. Yet although the technology and skills

10 UK Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: Cabinet Office, 2010), (London: The Stationery Office, October 2010, Cm 7953), http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy, p. 29, accessed 21 October 2010.

11 Cornish et al., *Cyberspace and the National Security of the United Kingdom*, pp. 3–12.

involved in designing, building, testing and storing these weapons may be complex and advanced, the means by which the weapon is delivered and by which the desired damaging effect is caused may be very basic (if very cunning). One well-known example occurred in 2008 when highly classified US Department of Defense networks were infected by an unknown adversary that 'placed malicious code on USB thumb drives and then dispersed them (in parking lots) near sensitive national security facilities. After a curious finder inserted the drives into computers, the code spread across their networks.'[12] Simple actions of this sort which can nevertheless have a dramatic effect would be described in military terms as an 'asymmetric' attack: asymmetry seems to be characteristic of much hostile action in cyberspace. We begin our analysis of cyber warfare at the level of the direct military threat.

Direct military threats

Cyber technology has clear military applications which can be exploited in conflict situations. Whether through military equipment and weapons systems, satellite and communications networks or intelligence data, armed forces are highly dependent on information and communications technology: 'for the top brass, computer technology is both a blessing and a curse. Bombs are guided by GPS satellites; drones are piloted remotely from across the world; fighter planes and warships are now huge data-processing centres; even the ordinary foot-soldier is being wired up.'[13] In a digital, knowledge-based society this is to be expected. But while technology brings opportunities it can also create vulnerabilities. The People's Republic of China (PRC), in particular, has long recognized the strategic and tactical value of cyberspace. Unable to match the current military superiority of the United States in terms of its military and technical hardware,[14] the PRC has countered this asymmetry by developing its cyber capabilities: 'Chinese military strategists have come to view information dominance as the precursor for overall success in a conflict.'[15]

In order to offset its conventional weakness the PRC is transforming its armed forces 'from a mechanized to an "informationized" force and have stated they intend to use information "as a tool of war [or] as a way to achieve victory without war"'.[16] To date, the PRC's focus has been on 'active defence' in preparation to counter aggression.[17] Questions might be asked about the PRC's perceived methods – principally espionage and network infiltrations (discussed below) – and whether 'active defence' might more accurately be described as 'pre-emptive attack', where such actions may be preparing the ground for a future, more overt act of aggression. Russia has also recognized the importance of cyber capabilities. In both Estonia in 2007 and Georgia in 2008, Russia is alleged to have used cyber technology as part of a 'coordinated and synchronized kinetic and non kinetic campaign'[18] through distributed denial of service (DDOS) attacks which appeared to be orchestrated with military and political operations. While both states deny the actions they are alleged to have committed, the use of cyber capabilities in conjunction with a conventional military campaign seems likely to be a feature of future warfare between states.

Indirect and non-military threats

Just as the targets of physical warfare are the machinery of state, financial institutions, the national energy and transport infrastructure and public morale, so too are they the prime targets in cyber warfare. One of the earliest recorded cyber attacks on national infrastructure occurred during the Cold War, when US President Ronald Reagan approved a SCADA (supervisory control and data acqui-

12 'Pentagon cyber security role expands', *Oxford Analytica: Global Strategic Analysis*, 2 July 2010.

13 'Cyberwar: war in the fifth domain', *The Economist*, 1 July 2010, http://www.economist.com/sites/default/files/images/images-magazine/2010/27/fb/201027fbd001.jpg, accessed 3 November 2010.

14 Analysis of defence equipment expenditure reveals that in 2008 the US spent $125bn compared with just $16bn by China. Twenty-five year projections suggest that China's spending will almost double as a proportion of global defence equipment spending while that of the US will decrease: Steven Bowns and Scott Gebicke, 'From R&D investment to fighting power, 25 years later', *McKinsey on Government* (No. 5, Spring 2010), p. 73.

15 Eleanor Keymer, 'The cyber-war', *Jane's Defence Weekly* (47/39, 29 September 2010), p. 24.

16 Dennis M. Murphy, 'Attack or defend? Leveraging information and balancing risk in cyberspace', *Military Review*, May–June 2010, p. 91.

17 'Tracking *GhostNet*: investigating a *Cyber Espionage* Network', *Information Warfare Monitor*, 29 March 2009, p. 11.

18 Murphy, 'Attack or defend?', p. 95.

sition) attack on the Russian pipeline system in Siberia in 1982. In 2004 Thomas Reed, who had been Reagan's Secretary of the Air Force, described the incident in the following way: 'the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds.'[19] One of the earliest examples of a 'logic bomb',[20] this attack was part of a broader, indirect effort by the US to disrupt the Soviet Union's technological capabilities and military industrial base. In the context of Cold War tensions, the pipeline attack was specifically designed to disrupt the Soviet Union's gas supply and harm the Russian economy and its gas revenues from the West, thus undermining its power.

In a more recent attack, the 'Stuxnet' worm (see Box 1) was infiltrated through the 'back door' of IT systems and used a number of 'zero-day' exploits (previously unknown vulnerabilities) in an attack believed to have been aimed at the industrial control systems at the Bushehr nuclear reactor or the Natanz uranium enrichment plant in Iran – a politically valuable target, particularly given pressures on Iran to halt its uranium enrichment programme.[21] This sophisticated SCADA attack demonstrated the potential of future cyber attacks and cyber warfare. Yet it also revealed its limitations of such attacks, not least the porous borders of cyberspace which led to the infection of thousands of additional computers both in Iran and beyond.[22]

The Russian pipeline and the Stuxnet incidents both reveal the potential of attacks to exploit vulnerabilities in civilian infrastructure and bypass military involvement. If the allegations are accurate, the actors concerned were able to achieve political and strategic effect without the need for armed conflict. The lack of clear attribution and the almost remote and indirect nature of the cyber attacks, which in both instances took time to uncover, made retaliation difficult without the risk of political controversy and, at worst, disproportionate damage.

Box 1: Stuxnet

The identification of the Stuxnet virus may represent the opening of a new chapter in the use of cyberspace to achieve the strategic effect of neutralizing a potent international threat. The origins of the sophisticated virus are not known, nor has the attack been attributed with certainty, but it is highly likely to have been targeted at the Iranian nuclear programme. Although the virus could conceivably have been designed and built by a team of talented software engineers acting independently, more needed to have been done to ensure a 'positive outcome', such as collection of intelligence on industrial control systems, and developing a method of delivery. The resources required to perform these important precursor functions would suggest that the Stuxnet incident reached beyond the capability of an independent group of vigilantes, into a national-level operation.

Disinfecting the control systems from the virus and reaching a level of assurance that they have been completely cleansed will be problematic; it may entail replacement of hardware components and software programs. But even once this repair work has been done, it would only require one 'insider' to re-infect the facility. The Stuxnet incident shows how susceptible critical national infrastructure can be to cyber threats. Without doubt there will be some serious consideration by national security and intelligence agencies around the globe of the implications of a similar attack occurring in the future, launched by any organization that is ill disposed towards its adversary.

19 Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York: Ballantine, 2004), p. 269.

20 'Cyberwar: war in the fifth domain', *The Economist*, 1 July 2010.

21 For more detailed information on the Stuxnet worm see http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

22 'A worm in the centrifuge', *The Economist*, 2 October 2010.

Although attacks upon infrastructure occur in conventional warfare, the implications are very different in cyberspace. As Lord West, former UK Minister for Security, once commented: 'If I went and bombed a power station in France, that would be an act of war [but] if I went on to the net and took out a power station, is that an act of war? One could argue that it was.'[23] These boundaries remain unclear but they pose important questions about the relationship between the civilian and military domains in the context of cyber warfare and the role and involvement of the armed forces in such undertakings.

Terrorism and extremism

As for organized criminals, the asymmetries of cyberspace and its hidden depths can be a valuable resource for non-state actors such as terrorist and extremist organizations. Although there is no conclusive evidence (certainly in the public domain) that groups such as Al-Qaeda have the capabilities or resources yet to launch a major cyber attack, terrorist groups are increasingly web-literate and use the internet and deep web in order to propagate their message and mobilize supporters. The internet has brought disparate groups together and facilitated conflict by enabling militants and extremists to share techniques, spread their message, recruit foot-soldiers and highlight their successes. Moreover, the evolution and democratization of technology have enabled sophisticated but relatively cheap everyday items such as smart phones, online mapping and the internet infrastructure to be used as vital operational components of conflict in conjunction with conventional methods.

The potential applications of communications networks, mobile information systems and intelligent technology in facilitating terrorist attacks were all in evidence during the Mumbai bombings of November 2008 when terrorists (Lashkar-e-Taiba) used GPS systems and 3G smartphones, alongside conventional weapons, to prepare for and carry out attacks on civilian targets. (In this case the technology was used in a relatively rudimentary manner, recording and detailing reconnaissance information on the targets, enabling communication between the perpetrators and providing tactical guidance to the gunmen during the attack.[24])

Cyber espionage

Cyber espionage is one of the most prevalent of cyber activities. Whether used to uncover sensitive government information, steal trade secrets or commercial data or as part of intelligence or reconnaissance work, it fits into the doctrine of using 'information superiority to achieve greater victories at a smaller cost'.[25] As Eleanor Keymer has observed, 'the return on investment for targeting sensitive information can be extremely high compared to the skills and technology required to penetrate the system which are relatively low'.[26]

Although China, unlike Russia, has not yet been linked to attacks connected to conventional military activity, it has employed cyber espionage to great effect to penetrate military, government and industrial targets to gather sensitive information. The Titan Rain attacks in 2007 – one of the most large-scale infiltrations of US and UK government departments, including the US Department of Defense and the UK Foreign and Commonwealth Office[27] – were attributed to China, and had allegedly been under way since 2002.[28] Furthermore, in March 2009 China was linked to 'GhostNet' when it was revealed that a large-scale spying network had attacked a significant number of government departments and strategic targets, including the Tibetan community.[29] In the words of the

23 Jamie Doward, 'Britain fends off flood of foreign cyber-attacks', *The Observer*, 7 March 2010, http://www.guardian.co.uk/technology/2010/mar/07/britain-fends-off-cyber-attacks, accessed 3 November 2010.

24 Timon Singh, 'How social media was used during the Mumbai attacks', *Next Generation Online*, 26 November 2009, http://www.ngonlinenews.com/news/mumbai-attacks-and-social-media/; and Gethin Chamberlain, 'Mumbai gunman convicted of murder', *The Guardian*, 3 May 2010, http://www.guardian.co.uk/world/2010/may/03/mumbai-gunman-convicted-murder. Both accessed 3 November 2010.

25 Wang Pufeng, 'The challenge of information warfare', *China Military Science* (Spring 1995), http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm, accessed 3 November 2010.

26 Keymer, 'The cyber-war', p. 23.

27 Richard Norton-Taylor, 'Titan Rain – how Chinese hackers targeted Whitehall', *Guardian*, 5 September 2007, http://www.guardian.co.uk/technology/2007/sep/04/news.internet, accessed 3 November 2010.

28 Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2010), p. 4.

29 Malcolm Moore, 'China's global cyber-espionage network GhostNet penetrates 103 countries', *The Telegraph*, 29 March 2009, http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html, accessed 20 Oct 2010.

Information Warfare Monitor, the GhostNet affair 'demonstrates the ease by which computer based malware can be used to build a robust, low cost intelligence capability and infect a network of potentially high-value targets'.[30] States are not the only targets: defence companies, commercial companies (such as Google) and NGOs have also been affected by cyber espionage.

However, it would be incorrect to assume that espionage or the infiltration of networks by malign actors constitute cyber warfare in their own right. Espionage is arguably a long-established feature of the physical world – a balanced friction. Its encroachment into cyber networks is therefore, in part, an extension of this tacitly condoned activity. While this may not make it right or any less concerning, cyber espionage may in many ways be a different means to a well-known end, and not necessarily a radically new threat. Nonetheless, as with the nature of this threat, little is known about its current or future potential. What happens, in other words, when this 'balanced friction' in cyberspace is disturbed? In particular, there is growing awareness of the ability of aggressors to use espionage and infiltration to plant 'back doors', Trojan horses and logic bombs which can remain dormant and undetected until time and circumstance require. Once activated, these time bombs would enable an aggressor to rapidly take control of a targeted system before the victim has become aware of either the intruder or the infiltration. These virtual attacks, if coordinated, could unleash significant damage at a designated time, either at a point of political tension or as an accompaniment to conventional warfare.

Economic cyber crime

There is increasing potential for financial institutions to be the target of digital attacks. This normally constitutes cyber crime, described by the UK Home Office as actions 'undertaken by serious organised criminals, who target government, business and the public to obtain money or goods. Their motivation is largely for financial gain, but it can also be to inflict personal harm.'[31] It appears to be organized criminals who are engaged in such attacks on financial institutions and these could not plausibly be described as 'acts of war'. Yet when these attacks are persistent and insidious they could arguably pose a risk to the national balance sheet and be detrimental to industry and society as a whole, consequently affecting the security and stability of a state. According to the UK's National Security Strategy 2010, 'cyber-crime has been estimated to cost as much as $1 trillion per year globally, with untold human cost'.[32]

"These virtual attacks, if coordinated, could unleash significant damage at a designated time, either at a point of political tension or as an accompaniment to conventional warfare"

At what point do such actions become another form of warfare? Or should they remain the preserve and responsibility of financial institutions and their customers? We would argue that given the potential costs to a single nation-state, economic cyber crime should not remain the concern of the financial industry alone and combating it should indeed be incorporated into national strategy, as in the case of the United Kingdom.

A further consideration is that cyber crime provides an environment in which attack techniques can be refined. In the words of Jeffrey Carr, 'cyber crime is the laboratory where the malicious payloads and exploits used in cyber warfare are developed, tested and refined'.[33] This further underlines the interconnectedness of attacks, where actors and agents are not uniform and clear cut but operate within a murky world where it is hard to identify the perpetrators in any given case.

30 'Tracking *GhostNet*', p. 6.
31 UK Home Office, *Cyber Crime Strategy* (London: The Stationery Office, Cm 7842, March 2010), p. 11.
32 UK Cabinet Office, *A Strong Britain in an Age of Uncertainty*, p. 29.
33 Carr, *Inside Cyber Warfare*, p. 5.

Psychological cyber warfare

There can be a psychological dimension to cyber attacks. The infiltration of what are assumed to be secure systems and critical infrastructure highlights national vulnerabilities and weaknesses. This can provoke feelings of insecurity, as evidenced by the Stuxnet worm in Iran and the Titan Rain episodes in the United States and the United Kingdom. Engendering this sense of insecurity could indeed be the attacker's goal, in the same way that the fear of terrorism and its potential harm can have a detrimental and disabling effect almost as great as the terrorist act itself. Indeed, according to Dennis Murphy, 'some observers equated that cyber attack [on Estonia in spring 2007] to an act of war in the Clausewitzian sense, with the intent to create mass social panic'.[34]

Challenges

Actions which take place in cyberspace or on the virtual battlefield may be difficult to identify and therefore to attribute with sufficient accuracy. Although their impact can certainly be felt in the physical realm and in normal life, these attacks take place surreptitiously. Was the attacker a foreign power or a small group of bored youths? Furthermore, the absence of immediate, visible harm and damage can mean that cyber attacks are regarded as somewhat removed from reality, perhaps even as science fiction. In cyber warfare the boundaries are blurred between the military and the civilian, the physical and the virtual, and power can be exerted by states or non-state actors, or by proxy.

Hostile actions short of warfare

Although some actions may appear aggressive and warlike, they may not necessarily be intended as acts of war. In fact, to ensure a rational and proportionate response it can be far from useful to escalate an apparently hostile action to the status of warfare when it might more appropriately be countered at a lower level. This is not to say that hostile actions in cyberspace should not be taken seriously: far from it. But wherever possible distinctions should be drawn between the responses appropriate to different types and levels of cyber action. This should make it more likely that resources will be allocated most effectively and efficiently and it should be possible to reserve valuable political capital for the most serious and harmful of attacks.

The first and most important distinction to be drawn is between those actors whose behaviour in cyberspace can best be described as cyber warfare, and those who, while still constituting a security threat, operate at a separate and lesser level and require a different response. However, there are neither discrete, clearly defined 'camps' of users nor a 'simple hierarchy of threats'.[35] Cyber actors are inherently difficult to categorize and defy rigid definitions, and their activities (and the consequences of their activities) can overlap considerably. If it is important to distinguish between warfare and non-warfare in cyberspace, then it follows that the distinction must be allowed to be mobile and flexible: a challenge for national strategy, perhaps. In other words, it is the action and its warlike properties that matter as much as the actor.

That said, it seems reasonable to suppose that of the four types of threat domain put forward in the March 2009 Chatham House report, two seem most likely to generate acts of cyber warfare: state actors, and terrorist or extremist organizations. Hostile behaviour in these domains will probably require an orchestrated, strategic and warlike response involving government and the security agencies and perhaps also the armed forces and industry. However, the other two domains – organized criminals and individual hackers – principally attack the commercial sector and private individuals for financial gain or for malicious gratification. These threats should be met at the appropriate level – societal, organizational or individual. This is not to say that criminals and lone hackers, or a group of nomadic hackers, could not launch an attack with warlike effects at some point in the future, but at present a large-scale or warlike response to such actions seems dispropor-

34 Murphy, 'Attack or defend?', p. 91.
35 Cornish et al., *Cyberspace and the National Security of the United Kingdom*, p. 3.

tionate. The policy challenge, therefore, is to know what is cyber warfare and what is not, and to ensure that responses are proportionate not just to the hostile action, but also to the actor.

Categories of warfare

Having sought to distinguish between those hostile acts that can be described as warfare and those that cannot, we then find that warfare itself is a difficult and contentious concept. Richard Clarke argues that 'cyber war is a wholly new form of combat, the implications of which we do not yet fully understand'.[36] Yet in many ways cyber warfare differs little from conventional or unconventional forms of warfare. Cyberspace has merely extended the battlefield and should be viewed as the fifth battlespace alongside the more traditional arenas of land, air, sea and space. It distorts our fledgling understanding of cyber warfare to argue that it is a conflict space in its own right. Simply put, cyber warfare is a new but not entirely separate component of a multifaceted conflict environment.

It follows that cyber warfare should generally not be viewed as an independent or stand-alone occurrence. Few of the actions described above would deliver a decisive victory on their own and in any case, as Alex Michael observes: 'what remains unremarked in the popular narrative is a constant ongoing background level of cyber attack as part of a holistic, coordinated programme to achieve the political, economic and social aims of nation states'.[37] Cyber attacks provide force multiplier effects and are just one component of the broader strategic ways and means employed by a state or non-state group. As such, warlike challenges in cyberspace are more likely to occur in conjunction with other methods of coercion and confrontation.

Nevertheless, cyber warfare remains undeniably distinct from these other methods. Unlike diplomacy, military force and economic warfare, it challenges the traditionalist view of the state as the principal actor in the international system and the decisive influence on warfare. Although nation-states have far greater access to the capabilities, resources and budgets needed to carry out substantial and well-directed cyber attacks, and are the most likely to employ cyber ways and means to achieve their ends (and have already recognized its defensive and offensive potential), cyberspace has made it possible for non-state actors, commercial organizations and even individuals to acquire the means and motivation for warlike activity.

Asymmetries in conflict are often exaggerated, with the underdog often supposed to be more cunning and resourceful than he actually is, and more likely to succeed. Yet asymmetric warfare can be extremely potent, and prone to imitation. According to the recently appointed UK Chief of the Defence Staff, the lesson drawn by the opponents of the United States and the United Kingdom from operations in Iraq and Afghanistan is that for 'relatively little cost, unsophisticated opponents with very cheap weaponry' can pose a strategic threat.[38] Much the same can be said for cyberspace. At comparatively low risk, significant damage and disruption can be inflicted on the intended target with little fear of reprisal. As a result, cyberspace gives disproportionate power to small and relatively insignificant actors.

Cyber warfare lends itself especially well to terrorist organizations and extremist groups, which can strike at the heart of society or infrastructure from a remote position and an unidentifiable address. But as Irving Lachow and Courtney Richardson point out, care should be taken not to over-emphasize this threat; while cyberspace may offer strategic value it lacks the impact of physical fear that conventional terrorism employs to maximum effect on a population.[39] Further differences between conventional warfare, cyber warfare and other forms of cyber attack are apparent in terms of the political framework within which such actions are presented (if any) and in terms of intent

36 Richard Clarke, 'War from cyberspace', *The National Interest* (November–December 2009), http://nationalinterest.org/article/war-from-cyberspace-3278, accessed 26 October 2010.

37 Alex Michael, *Cyber Probing: The Politicisation of Virtual Attack* (Shrivenham: UK Defence Academy, September 2010), p. 1.

38 Michael Smith, 'General Sir David Richards calls for new cyber army', *Times Online*, 17 January 2010, http://www.timesonline.co.uk/tol/news/uk/article6991030.ece, accessed 16 October 2010.

39 Irving Lacow and Courtney Richardson, 'Terrorist use of the Internet: the real story', *Joint Force Quarterly* (Issue 45, 2nd Quarter 2007), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA518156, accessed 3 November 2010.

and attribution. As the *Economist* has noted, 'a cyberattack on a power station or an emergency-services call centre could be an act of war or of terrorism, depending on who carries it out and what their motives are'.[40]

> 'Cyberspace is largely an apolitical space. This derives in part from the nature of the environment with its absence of actual people but it also reflects the lack of clarity over the provenance (and seriousness) of threats'

Cyber warfare as an extension of politics

The political dimensions of cyber warfare are underdeveloped yet integral to understanding the threats and challenges that come from cyberspace, and to designing an appropriate response. If we accept Clausewitz's best-known dictum that 'war is not a mere act of policy but a true political instrument, a continuation of political activity by other means',[41] then it follows that the warlike actors within cyberspace are those who seek to use virtual means to achieve political ends. Political antagonisms in the real world, in other words, should be expected to translate into the virtual world. Yet these political antagonisms need not reside exclusively among states and the most sophisticated, politically motivated non-state actors.

Security policy commentators and analysts, and the media, are currently preoccupied, as far as cyber warfare is concerned, with the actions of China and Russia – an interest that is also reflected in this report. It is important, nevertheless, to resist the seductive simplicity of 'attacker versus defender' analogies when contemplating such alleged incidents of cyber warfare. Any supposed antagonisms are, of course, context-dependent and are shaped by the perspective of the analysts and authors concerned and by their audience. More importantly, the blurred boundaries of cyberspace mean that actors may be simultaneously allies and adversaries: allies when faced by a common cyber threat, and adversaries when one of them seeks to defend, protect or advance its own security and interests in cyberspace regardless of, or at the expense of, the other.

The significance of politics should not be overlooked. Cyberspace is largely an apolitical space. This derives in part from the nature of the environment with its absence of actual people but it also reflects the lack of clarity over the provenance (and seriousness) of threats. Although the politicization of cyberspace could facilitate more effective responses and strategies (as will be explored in Chapter 4), careful consideration should be given to the broader implications of a more political approach to cyber warfare. If, for example, cyberspace becomes increasingly politicized and states assert their rights to new, virtual dominions, will cyberspace in turn become a more valuable target and therefore more vulnerable to terrorist attacks and other warlike behaviour? Is that perhaps a risk worth taking?

Cyber intent

In order to understand whether a hostile action in cyberspace is warlike, it is necessary not just to observe the event but also to understand the actor's intent. Warfare, in the Clausewitzian view, is 'an act of force to compel our enemy to do our will'.[42] It follows that the actor's intent or 'will', on either side of the conflict, must be established before it can be stated that what is taking place is an act of war, or something else altogether. Although there are many shades of grey in such an assessment, and although each confrontation should be examined on a case-by-case basis, some guidance on intent and action, cause and effect, can be taken from the analysis of conventional warfare and from an understanding of criminal acts. For example, if a cyber attacker's intent is to seek financial or personal gain through criminal means such as theft, fraud or extortion, the intent should become clear enough and the attack should be seen as a criminal act and dealt with accordingly.

40 'Marching off to cyberwar', *Economist Technology Quarterly*, 6 December 2008.
41 Clausewitz, *On War*, p. 87.
42 Ibid.

But if an attacker has far grander ambitions and aims to cause significant harm to a state or its citizens or disrupt, undermine or disable military or civilian structures/infrastructure, then it would be appropriate to describe such behaviour as something closer to an 'act of war' in the traditional sense. It should be possible to distinguish between actions that may appear aggressive or militarily motivated but that are isolated events, and actual warfare, which would require the mutual and unambiguous recognition of both parties – aggressor and defender – that a state of war exists. The problem of intent poses interesting questions, some of which will be addressed in the final chapter. In particular, what do hostile actors in cyberspace seek to achieve and how can this be determined?

Cyber attribution

One of the main attractions of cyberspace is the shield of anonymity it offers, at least in the short term. Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity. In the case of suspected state-sponsored actions it is difficult to establish beyond any doubt that the order to attack originated in the executive or presidential office, let alone a capital city. Furthermore, the difficulties of attribution allow a degree of plausible deniability. Perpetrators can cover their own tracks and implicate others, particularly when third-party servers and botnets in unrelated countries can be used to originate attacks and provide cover for the actual attacker. Nevertheless, as Carr observes with relation to the attacks on Estonia and Georgia which were, by consensus, attributed to Russia, 'whether or not you accept that some, all, or none of these events occurred with the sanction of the Kremlin, each event has been instrumental in furthering RF [Russian Federation] policy, and the Kremlin has never acted to stop them. Hence the RF benefits.'[43] The attacks on Estonia and Georgia demonstrate how politics, intent and attribution can all fit together in the peculiar environment of cyber warfare, but in a less distinct way than in traditional warfare settings.

Summary

The idea of cyber warfare is deeply rooted in what is already known about conflict and warfare but at the same time it presents new threats and challenges which should be taken into account in national strategy. In addition to the 'known knowns' of cyberspace, its unknown dimensions mean new and innovative threats will certainly emerge; policy will therefore have to be both resilient and adaptable if it is to respond effectively. There are aspects of the cyber warfare challenge which conventional frameworks of analysis cannot expose. However, if governments are prepared to bridge the gap between familiar territory and new ground, conventional frameworks and concepts can be applied intelligently in order to inform understanding about cyber warfare and to guide policy-makers and strategists. Using traditional frameworks of analysis it is possible to establish the character of warfare in cyberspace and its broader military, societal and organizational implications, and to make informed decisions about how to respond and who should lead such a response.

Important questions will remain: what is the mechanism for escalation from an isolated attack to a state of cyber warfare? What will be the implications of cyberspace for the future of conventional and non-conventional conflict? How should we think about cyber warfare in strategic and policy terms? And could cyber technology really make 'bloodless warfare' possible?

43 Carr, *Inside Cyber Warfare*, p. 161.

3. Reaction: Policy and Operations

> Unlike the air, land and sea domains, we lack dominance in cyberspace and could grow increasingly vulnerable if we do not fundamentally change how we view this battle-space.
>
> *General James E. Cartwright*[44]

> The low cost and largely anonymous nature of cyber space makes it an attractive domain for use by those who seek to use cyber space for malicious purposes. These include criminals, terrorists, and states, whether for reasons of espionage, influence or even warfare.
>
> *Cyber Security Strategy of the United Kingdom*[45]

This chapter examines US and UK policy and operations in cyberspace. We focus on the current trajectories of these two countries in using the cyber domain in the pursuit of national security. We also examine other dimensions of conflict such as trade and economic warfare, placing these in the context of cyber-enabled global interconnectivity and interdependence. High levels of online anonymity, and the difficulty in attributing the origins of an attack, allow these particular dimensions of conflict to go relatively ungoverned, and to be exploited for warlike purposes by means other than brute physical force. We assess the domestic and international responses of the United States and the United Kingdom to evolving challenges in cyberspace. In this increasingly complex and murky environment, we propose that some general guidance can flow from existing international frameworks such as those relating to laws of the sea and arms control agreements, though overlaps are sporadic in many areas. Other direction can come through established mechanisms such as civil-military cooperation, public-private partnerships and international alliances or treaties.

Many claims have been made regarding the hazards of cyber security and the growing potential for conflict in cyberspace. This chapter endeavours not to reduce the debate to the level of the anecdote, nor to describe emerging threats in too much technical detail, but to widen the scope of inquiry with regard to the range of issues that should be considered and to the political norms and values that should direct governmental policy and operations. Our intention is to provide a new and more rounded perspective on cyber warfare, making it possible to view the myriad factors in a more granular way without losing sight of their broader significance.

Key actors

The transatlantic relationship is important for a variety of reasons where cyber warfare is concerned. Close cooperation between the United States and the United Kingdom in intelligence and military matters has progressively encompassed cyberspace, enabling both states to extend their reach in a way that is difficult, if not impossible, for any other bilateral partnership or alliance. The US and the UK are widely considered to be at the forefront of innovation for strategic purposes in cyberspace, and are likely to remain in this position for the foreseeable future.

44 The Posture of the United States Strategic Command (USSTRATCOM)', Hearing Before the Strategic Forces Subcommittee of the Committee on Armed Services, House of Representatives, 8 March 2007, http://www.fas.org/irp/congress/2007_hr/stratcom.pdf, accessed 26 October 2010.

45 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (London: The Stationery Office, Cm 7642, June 2009), p. 12.

The United States

The government of the United States is preparing to exploit the cyber domain in support of US national interests, to the extent of conducting defensive and offensive operations in cyberspace. The announcement by the US Secretary of Defense in June 2009 that the US would form a dedicated combatant command for military cyber issues – Cyber Command (Cybercom) – was a strong statement of intent and shows how serious the political and military leadership of the US perceives the threat to be. In November 2010 the Department of Defense announced the new command had reached 'full operational capability'.[46]

From 2010 to 2015, the US government is expected to spend over $50 billion on its cyber defences with a compound annual growth rate (CAGR) of 6.2%.[47] This figure does not, of course, include the sums to be spent by industry and commerce in developing capability against cyber threats to their enterprises.

This expenditure is likely only to increase as the breadth and depth of the challenge become clearer. At present the scale of US military cyberspace usage is vast. There are 15,000 Department of Defense networks with seven million devices (4,000 installations in 88 countries). These systems are being scanned and probed by potential attackers millions of times each day.[48] The cost of cyber attacks is reported to be sizeable and rising. Between October 2008 and April 2009 alone, the Pentagon spent in excess of $100 million recovering from, and repairing, damage caused by cyber attacks as well as network system issues. The Pentagon has only recently begun to track these expenditures and the actual cost could be significantly higher.[49]

According to the first head of Cybercom, General Keith Alexander, who also serves as head of the National Security Agency (NSA), cyberspace is 'a warfighting domain'.[50] During his April 2010 confirmation hearing Alexander assured the US Senate that the US would not militarize cyberspace, and attempted to allay concerns that his new command would lead to overlap with US domestic agencies, although this general point was not developed in the public hearings. These assurances are difficult to confirm since Alexander's answers to a number of key questions including 'what are your priorities for U.S. Cyber Command?' and 'how do you define U.S. Cyber Command missions?' were contained in a classified supplement.[51]

The US Constitution does not allow the military to operate within the boundaries of the United States unless authorized for specific operations by the President; the Department of Homeland Security has responsibility for domestic cyber security. It is one thing to draw a distinction between domestic and foreign spheres of conflict in the physical world, but attempting something similar in cyberspace soon raises significant problems in a global interconnected electronic media infrastructure, and prompts questions as to the validity of concepts such as 'cyber sovereignty'. This blurring is further compounded by the private (and often foreign) ownership of vast swathes of internet infrastructure.

For Cybercom the principal challenge in responding to cyber attacks (including 'acts of war', political extremism and cyber espionage) is the development of an architecture of risk mitigation underpinned by a generally accepted understanding of what actually constitutes cyber war and what price should be paid in preparing for it. Without clear political and legal guidance, understood by all

46 Tim Stevens, 'US Cyber Command achieves "full operational capability," international cyberbullies be warned', 5 November 2010, http://www.engadget.com/2010/11/05/us-cyber-command-achieves-full-operational-capability-interna/, accessed 6 November 2010.

47 'US Federal Cybersecurity Market Forecast 2010-2015, *Market Research Media*, 5 May 2009, http://www.marketresearchmedia.com/2009/05/25/us-federal-cybersecurity-market-forecast-2010-2015', accessed 20 October 2010.

48 William Jackson, 'DOD struggles to define cyber war: efforts hampered by lack of agreement on meaning', *Government Computer News*, 12 May 2010, http://gcn.com/articles/2010/05/12/miller-on-cyberwar-051210.aspx, accessed 4 November 2010.

49 'Pentagon spends big fixing cyber attack damage', *The Independent*, 8 April 2009, http://www.independent.co.uk/news/world/americas/pentagon-spends-big-fixing-cyber-attack-damage-1665728.html, accessed 4 July 2010.

50 Keith Alexander, 'Warfighting in cyberspace', *Joint Forces Quarterly* (Issue 46, 3rd quarter 2007), p. 60, http://www.carlisle.army.mil/DIME/documents/Alexander.pdf, accessed 8 June 2010.

51 United States Senate Armed Services Committee, 'Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command', 15 April 2010, http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf, accessed 10 July 2010.

stakeholders, it will be impossible for certain operations to be undertaken, or in certain circumstances operations might take place but only in the knowledge that legal action could ensue against those commissioning or carrying out the activity should its details arrive in the public domain. Neither of these is a palatable option, and cyber warfare therefore differs significantly from warfare in the physical world where military operations are shaped by relatively clear and well-understood political guidelines and constraints.

This places a responsibility on legislators to provide clarification before critical yet ambiguous situations arise. A difficult discussion therefore needs to begin, probably on both sides of the Atlantic, regarding the nature of cyber warfare and what may be undertaken in its name. 'It is clear there is a lot of cyber espionage where data is being pulled,' commented James Miller, DoD principal deputy undersecretary for policy, 'but we understand that not everything that happens in cyberspace is an act of war.'[52] This acknowledgment is helpful, and the formation of Cybercom shows that the US government is willing to confront and clarify the issue. But many central questions remain, including the role of political leaders in setting values and norms in cyberspace and, of course, in deciding which values and norms should be considered authoritative.

The United Kingdom

The UK government has also made significant changes to its cyber security posture, beginning with the June 2009 release of the first edition of the UK Cyber Security Strategy.[53] The strategy announced the formation of the Office of Cyber Security (OCS) to be located within Cabinet Office, and the Cyber Security Operations Centre (CSOC) to form part of the Government Communications Headquarters (GCHQ). The initial operating budget for OCS for the year to April 2010 was £130,000, while CSOC was not allocated a budget for the fiscal year.[54] Although this figure was low to the point of being miserly, the cyber security budget is set to increase dramatically following the recent publication of the 2010 edition of the UK *National Security Strategy* (NSS) and the *Strategic Defence and Security Review* (SDSR). The NSS ranks 'hostile attacks upon UK cyberspace by other states and large scale cyber crime' as a Tier 1 Priority Risk, along with (in no particular order) international terrorism, large-scale accidents or natural hazards, and an international military crisis between states.[55] The SDSR backs up this high-priority status with a budget commitment of £650 million over the next four years for a new National Cyber Security Programme, which will serve as a unifying force with 'one national programme of activity with supporting strategies in other departments.'[56]

Within the National Cyber Security Programme the defence community will now have an identifiable lead. A new Cyber Operations Group will be formed which will 'bring together existing expertise from across Defence, including the Armed Forces and our science and technology community'.[57] The Programme also acknowledges the need for partnership with the private sector, an essential step if the security of the critical national infrastructure is to be enhanced. These are encouraging developments, but lines of leadership remain unclear. Where will the National Cyber Security Programme be housed and who will lead it? What mandate will the MoD-oriented Cyber Operations Group have to conduct offensive or exploitation operations in cyberspace, and to what extent will it be able to contribute to and facilitate the civilian-sector response?

A doctrinal framework will be essential to the creation and development of a national cyber warfare capability. This process will be complex for both defensive

52 William Jackson, 'DOD struggles to define cyber war: efforts hampered by lack of agreement on meaning', *Government Computer News* (12 May 2010), http://gcn.com/articles/2010/05/12/miller-on-cyberwar-051210.aspx, accessed 18 October 2010.

53 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom.*

54 Baroness Crawley, House of Lords (2009) in answer to Question asked by Baroness Neville-Jones re: 'Office of Cyber Security: Cyber Security Operations Centre' (11 November 2009), http://www.publications.parliament.uk/pa/ld200809/ldhansrd/text/91111w0004.htm, accessed 8 June 2010.

55 UK Cabinet Office, *National Security Strategy* (2010), p. 27.

56 UK Cabinet Office, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (London: The Stationery Office, Cm7948, October 2010), p. 47.

57 UK Cabinet Office, *Strategic Defence and Security Review*, p. 27.

and offensive operations, but some best practice could be drawn from the defence environment, from wider government and from the commercial sector. Despite the novelty of the cyber environment, the essential operating principle will be not to reinvent the wheel by devising wholly new techniques and procedures for cyber warfare. Even though cyber warfare is arguably the most challenging of any of the warfare domains, it would be wasteful to overlook past experience. There are some useful benchmarks for best practice which could be relevant to the cyber domain.

For example, if the development of a national cyber warfare capability could be considered as a discrete programme then there is guidance available for the management of this process. The UK Office for Government Commerce's *Managing Successful Programmes* (MSP) establishes the principles for delivering high-quality public services, including the requirements for achieving value for money, delivery of change, the ability to meet new requirements and conforming to the high standards that the public expects.[58] MSP contains guidance on a series of activities that all contribute to the delivery of capability, such as the need for a properly constituted organization, the establishment of a vision, the need for leadership and identification of the stakeholders who will contribute to achieving the desired effect.

Similarly, the MoD has developed a systems approach to capability development, known as Defence Lines of Development, which complement MSP in a number of respects and which, as a first step, could be adapted and applied to the cyber warfare domain. The approach is known by the acronym TEPID OIL:

- *Training*: the provision of the means to practise, develop and validate, within constraints, the practical application of a common cyber warfare doctrine.
- *Equipment*: the provision of platforms, systems and 'weapons' needed to equip an individual, group or organization.

> "Success will be defined by the ability of all available forces and agencies to train, exercise and operate effectively together in the execution of assigned missions and tasks"

- *Personnel*: the timely provision of sufficient, capable, and motivated personnel to deliver outputs both now and in the future.
- *Information*: the development of capabilities and processes designed to gather and handle data, information and knowledge.
- *Doctrine and concepts*: doctrine is the set of principles by which action is guided; it is authoritative but requires judgment in application. Concepts concern the capabilities that are likely to be needed in the future.
- *Organization*: operational and non-operational relationships.
- *Infrastructure*: the acquisition, development, management and disposal of all fixed and permanent structures in support of the capability.
- *Logistics*: the science of planning and carrying out the operational movement and maintenance of forces.[59]

Interoperability is the theme which connects all these strands of activity. Success will be defined by the ability of all available forces and agencies to train, exercise and operate effectively together in the execution of assigned missions and tasks. The TEPID OIL model set out above can be applied to cyber warfare although some deeper analysis will be necessary in order to clarify the effect required and to ensure that scarce resources are not expended inefficiently.

58 Office of Government Commerce, *Managing Successful Programmes* (London: The Stationery Office, 2007), p. 13.

59 The 11th International Command and Control Research and Technology Symposium, 'Coalition Command and Control in the Networked Era', http://www.dodccrp.org/events/11th_ICCRTS/html/papers/061.pdf, accessed 1 November 2010.

The challenges of conflict in cyberspace

The digital environment is rapidly changing. The US no longer dominates the architecture of the internet in the way it did when the system was conceived. Every year tens of millions of people 'go online' for the first time. With expanding global online access and a growing number of highly connected nodes, internet traffic is increasingly routed around the globe. While this growth is laudable for economic reasons it does bring risks, not least in the opportunities it provides for malicious actors to launch attacks, conceal their identities and shield themselves behind social and governance structures that do not yet fully understand the nature of the internet. The internet is bigger than any state or group of states, and evolves at a pace beyond the scope of control of even the largest and most reactive technology company. It can be put to an ever-widening range of uses and the complexity of cyberspace will only deepen, increasing the potential for friction and conflict. What is being done to meet these challenges, and where are the gaps in policy that cannot be managed by current approaches?

The state: overstretched and out of place?

Several national governments are strengthening their cyber security organizations to conduct defensive and offensive operations, and virtual drawbridges are being raised. The internet is often described as an inherently dangerous place, which is a perspective difficult to dislodge when these warnings emerge into the public domain from a vault of secret knowledge. Traditional notions of warfare, based on attack and defence, are being challenged by the complexity of cyberspace, and the pace of change in the medium threatens to overwhelm all but the most technologically competent. These challenges are like the waves of a storm crashing higher and higher against the walls of the modern state, undermining traditional notions of power and discomfiting those within.

Popular apprehension about the possibility of a 'cyber Pearl Harbor' or a 'cyber 9/11' tempts policy-makers to bolster their national security credentials by adopting a militarized perspective on cyberspace. It becomes politically attractive simply to conflate cyber espionage with cyber war, a step which, by definition, would plunge most countries into an immediate state of conflict (although, because of attribution difficulties, they might not know who their adversaries are or indeed whether and when they have been attacked). This over-reliance on a narrow set of descriptions of interstate behaviour (most notably peace, tension, and war) should be resisted from the outset. The management of cyber warfare requires a clear canvas, unencumbered by the clutter of established international politics and by the modes of activity in the four physical battlespaces (land, sea, air and space). Nevertheless, although cyberspace is an internationalized and interconnected domain that spans government, military, commercial and private stakeholders, there is still a central role for the political dimension of the state in cyberspace, and the values and norms that only the state can provide.

Political engagement

As we have argued above, the character of the cyber environment and the diffuse and opaque nature of the threats emanating from it have the effect of excluding cyberspace from normal political discourse. But cyberspace – and cyber warfare in particular – needs more rather than less politics. The absence of a clear and constraining political framework breaks the Clausewitzian relationship between politics and warfare and unbalances the discourse in favour of military or technological responses. If politics can be introduced then although the resulting norms and values may not be universally agreed or adhered to, the mere fact of debating them will help to assuage current levels of mutual misunderstanding between actors, and may form the basis for sustainable political engagement in cyberspace.

Without an understanding of the cyber environment as a political space it is all too easy to overreact to provocation and to militarize the response. As a result the response can become isolated and non-inclusive, shutting out all but the closest national allies and confined to a select and remote security policy community within the state concerned. At the very least this dynamic will influence (probably adversely) interaction and engagement with other countries and cyber stakeholders. James Lewis

argues that 'for a long time the US focused on unilateral action and no engagement and cooperation, and we appear to have realized that doesn't work in a global network'.[60]

If other countries react by adopting a similarly militarized perspective it could act as an accelerant to the fragmentation of cyberspace, with individual fiefdoms attempting to stake out their respective turf. Ultimately this trend cannot serve the greater good that the internet has promised (at a minimum, it catalyses economic growth for countries with a high usage of electronic media). But all too often anecdotes about cyber attacks are allowed to shape and exaggerate the narrative and to influence the popular understanding of cyber warfare. This happens partly because the anecdotal approach encourages worst-case analysis and dovetails neatly with a military-led perspective, and partly because of a lack of political engagement.

Anecdote is an imprecise and unreliable basis for strategic policy formulation. The coordinated cyber attack on Estonia in 2007 referred to in Chapter 2 is a good example. This event was first announced as a 'cyber war', but analysts have generally concluded that while these DDOS attacks overloaded select government, media and bank web servers, they were not comparable to disabling computers from within and bringing a national grid to the point of collapse.[61] This was not espionage, but nor was it traditional warfare in which the ultimate objective would surely be the surrender of sovereignty to an adversary. When scenarios such as this are deployed to assert that similar fates could befall the US or west European nations, a sense of perspective is needed. While Estonia is well known to be one of the world's most digitally dependent countries, its population (1.3 million) is roughly the same size as that of the city of San Diego, and less than half that of greater Manchester (2.85 million).[62]

Political engagement is also essential for effective international response. During his first public appearance since being confirmed as head of Cybercom, General Alexander pressed for increased international engagement and cooperation on global issues of cyber security: 'When all countries can come up and agree: "This is going to be the way we're going to operate and the way we're going to defend and the way we're going to do this," and we all agree to it, that will go a long way.'[63] While history shows that it is ambitious to expect 'all countries' to agree on anything, the potential of the internet is such that cooperation would be highly beneficial and that it would therefore be worth trying. The insiders' knowledge of military and technical experts gives them a unique and valuable perspective on the problems of cyber warfare.

But on occasions the policy debate can become so specialized that those with insider knowledge can dominate it. This provides one more reason why the cyber warfare debate needs to be more firmly guided by the realm of politics. Expending political capital in order to develop a framework of values, norms and laws that can function at the international level will require a concerted international effort. The internet is not unique in its need for a legitimizing framework, but it will require visionary leaders who are able to recognize the benefits of cooperation in this most pervasive of global commons. To return again to the basic principles set out in *Managing Successful Programmes*: 'Vision is a picture of a better future, [and is] a vital focus and enabler for the buy-in, motivation and activity-alignment of the large community of people involved in any programme.'[64]

Economic cyber warfare

The cyber warfare debate is often one-dimensional, involving countries that might engage in conventional warfare in one way or another. In these cases, cyber warfare is increasingly seen by association merely as a complement to, or even substitute for, such conventional warfare. But there has

60 David Talbot, 'New cyber chief outlines strategy', *Technology Review*, 10 June 2010, http://www.technologyreview.com/printer_friendly_article.aspx?id=25526&channel=Briefings&section=ComputerSecurity, accessed 27 October 2010.

61 John Schwartz, 'When computers attack', *New York Times*, 24 June 2007, http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html?_r=3&adxnnl=1&oref=slogin&pagewanted=print&adxnnlx=1275246125-p54bXxIHZRDBiXPJLEIThg, accessed 8 July 2010.

62 World Bank, World Development Indicators, 'Midyear estimates of the resident population', http://www.google.com/publicdata?ds=wb-wdi&met=sp_pop_totl&idim=country:EST&dl=en&hl=en&q=estonia+population, accessed 4 November 2010.

63 Talbot, 'New Cyber Chief Outlines Strategy'.

64 *Managing Successful Programmes*, p. 41.

always been an economic dimension to warfare, and so it is in cyberspace. Attention should therefore also be given to ways in which the economic dynamics of conflict in cyberspace could shape, direct or constrain the future of warfare. Global financial flows, market stability, trade interdependencies and the sheer cost of fighting can all militate against a government pursuing conventional warfare, particularly through unilateral military action. Regardless of whether damage to financial institutions or other critical infrastructure is caused by either physical or cyber attack, the reputational damage to a country involved in conflict can be severe. Financial investments in that country appear increasingly risky, and higher (and unexpected) risk is anathema to the global financial markets, particularly since 2008. Conversely, if an attack can be attributed with reasonable accuracy then the aggressor's behaviour can also result in far-reaching economic and financial penalties. The threat of these penalties can cause the aggressor to undertake any hostile act covertly.

The economic consequences of engaging in overt cyber warfare could thus be severe, and generally too high for those countries that are not otherwise prepared to engage in conventional war against one another. By extension, if there is reluctance to engage in open conventional warfare, it also seems advisable to refrain from open warfare in cyberspace. But in cyberspace, economics can also expand the opportunities for hostile actions and can even encourage conflict. Economic espionage is one way for a state to hedge its bets in this area, and it is clearly on the rise.[65] This level of conflict could be the shape of things to come, but it seems to fall short of cyber warfare as such. There is no doubt that it is easier and less painful than conventional warfare for the attacker, and the value to be gained is large relative to the resources employed. Cyber warfare and cyber espionage are likely to become increasingly intertwined in the future, slowly subsuming, though never completely replacing, conventional warfare.

Preparing a response

There are valuable parallels to be drawn with other global commons such as space and the high seas, yet the lessons previously learned in these domains do not adequately or fully translate to cyberspace. Existing frameworks can provide only imperfect analogies and partial templates, but none can adequately describe the transactional and relational complexity of cyberspace – a domain that provides a high degree of anonymity and low barriers to entry, and that is becoming integral to modern life. This is a long game, and must be played as such. Patience is a virtue in cyberspace, where attribution of attacks is extremely difficult and the complexity of the landscape is ever-increasing. Although targeted attacks using weapons such as the recent Stuxnet worm (see Box 1) show a glimpse of the future of conflict in cyberspace, even this incident reflected geopolitical tensions in the physical world (between Iran and those countries that wish to delay its nuclear technology). Referring to this immensely complex and well-resourced cyber attack, one analyst said, 'This is what nation states build, if their only other option would be to go to war.'[66]

Agility and attribution

A high degree of agility is needed to prepare for and engage in conflict in cyberspace. Agility in the midst of a chaotic environment is required from military units, but it must also be expected from the policy-makers who must ultimately manage conflict within a political framework. As successive generations of policy-makers enter government, the capability to deal with the complexities of cyberspace will grow. This influx of so-called 'digital natives' is already taking place.

> It is basically not necessary for people to wrack their brains over whether or not information technology will grow strong and unruly today, because it itself is a synthesis of

65 Ellen Messmer, 'Cyber Espionage: A Growing Threat to Business', *PC World*, 21 January 2008, http://www.pcworld.com/businesscenter/article/141474/cyber_espionage_a_growing_threat_to_business.html, accessed 14 October 2010.

66 Richard Spencer, 'Stuxnet virus attack on Iranian nuclear programme: the first strike by computer?', *The Telegraph*, 4 October 2010, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8040656/Stuxnet-virus-attack-on-Iranian-nuclear-programme-the-first-strike-by-computer.html, accessed 8 October 2010.

> other technologies, and its first appearance and every step forward are all a process of blending with other technologies, so that it is part of them, and they are part of it, and this is precisely the most fundamental characteristic of the age of technological integration and globalization.[67]

This technological synthesis creates environments with properties that are markedly different from earlier battlespaces. For example, both state and non-state actors understand that the cyber domain favours offensive action. Static defences are the modern equivalent of a Maginot Line: vulnerable to incessant battering by an unknown opponent and easily circumvented by manoeuvre. In addition, attribution of cyber attacks remains one of the most difficult obstacles to overcome in attempts to make the internet a less chaotic environment. This anonymity challenges the notion of warfare as a relational activity.

Cyber attacks take place at different levels of sophistication and can be driven by a wide variety of political, ideological, economic and even frivolous motives. In this domain, does there still have to be an identifiable opposition, and does the lack of one mean that the attribution threshold for response should be different at the political level, as opposed to the military or technological levels? In other words, what options do policy-makers have when attribution of attacks is less than certain? Perhaps different segments of government need to define attribution differently. The threshold of attribution required for a political response to a cyber attack could be different from that needed for conclusive technological proof of the attacker's identity or origin (an exceedingly rare achievement). In practice this already takes place to a certain extent, though acknowledging that different standards of attribution are acceptable would alleviate the pressure to seek a perfect solution.

Consistency of language

International harmonization of laws, norms and procedures requires consistency of terminology. It is difficult to see, for instance, how a coherent legal framework could result from the current proliferation of cyber terms. The legal department of NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn considers that the 'terminological inconsistency' makes it difficult to pronounce on the legality of 'an incident' and to 'optimize the response in terms of authorities'. As a result, the enforcers of the law are compromised in their efforts to take 'determined action against malicious activities in cyberspace'.[68] It should also be noted that non-Western countries are likely to object to a cyber lexicon whose definitions privilege – or are perceived to privilege – Western notions over non-Western ones. Even if Western nations initiate this process, non-Western nations object to a framework of cyberspace rules (like so many other frameworks from the twentieth century) that originates in the West, thereby complicating the process of finding common ground.[69]

The merits and limitations of existing frameworks

As with the introduction of any new method of warfare, it will take years or even decades before a comprehensive governance regime can be established. One of the major problems involved with the development of a cyber warfare control regime is that there is little consensus among international political or military leaders as to what actually constitutes cyber warfare. When definitions are attempted, they do not often reflect the global nature of cyberspace and thus inhibit the search for stable international consensus. While some states may seek to exploit a lawless battlespace, the current legal

67 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), http://cryptome.org/cuw.htm#Part%20One, accessed 22 October 2010.

68 Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents* (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010), p. 102, http://www.scribd.com/doc/40522828/Book-1, accessed 14 October 2010.

69 Lest potential territorial divides be viewed only in terms of East and West, it is useful to remember that in 1997 French President Jacques Chirac dismissed the internet as an 'Anglo-Saxon network'. Roger Cohen, 'For France, sagging self-image and esprit', *New York Times*, 11 February 1997, http://www.nytimes.com/1997/02/11/world/for-france-sagging-self-image-and-esprit.html, accessed 2 November 2010.

ambiguity or vacuum may actually act as an incentive to cyber attacks. Small states or non-state actors looking to conduct offensive operations outside existing international legal agreements and obligations, or at a low cost of entry, may be induced to fight in cyberspace.[70] As we have suggested, there is also the possibility that unrestricted cyber warfare may undermine long-term confidence in the global internet economy.[71]

Reliance on privately owned infrastructure

Commercialization of the internet in the 1990s greatly expanded what had been a largely government network, so that interconnected public, private and government networks came to form what would become known in the United States as the national information infrastructure (NII). The NII eventually included computer networks, generating equipment, data storage, supporting networks including telephone networks and the internet itself, connections between the network components, private networks and satellite communication. As the network grew, along with increasing dependence on public telecommunications systems and access points, so NII vulnerability increased exponentially. And as the internet continued to evolve so it became ever more apparent to governments both that cyberspace mattered to their national security objectives, and that much of this critical domain was in private hands.

There are dangers in rapid network expansion, including a lack of awareness of potential vulnerabilities that may be created as a consequence. Often this results from a desire to integrate 'islands' into networked systems that are efficient, flexible, cost-effective and remotely accessible. The creation of these inadvertent vulnerabilities and the 'normal accidents' that may result can in part be mitigated by a robust risk management strategy that draws on global best practice. Large multinationals in the private sector have value to add in this area, as their risk registers and processes of standardization between platforms (e.g. in mergers and acquisitions) are becoming increasingly sophisticated.

'As the internet continued to evolve so it became ever more apparent to governments both that cyberspace mattered to their national security objectives, and that much of this critical domain was in private hands'

Public-private partnerships and critical national infrastructure

Governments seek partnerships with private companies in order to protect national interests, but private companies can find that the incentives are often less than attractive. Furthermore, their loyalties are first to their shareholders and boards of directors, rather than to any government. In addition, many have risk registers that will only direct resources to pre-empt a problem if both the potential harm and the likelihood of occurrence are sufficiently compelling to build a case for action. Yet when these companies are categorized by government as part of the critical national infrastructure, expectations of them can only increase. One major weakness in this relationship is the reluctance on both sides to share information: on the private side owing to the risk that commercially sensitive information might reach competitors, and on the government side because of a multitude of issues surrounding national security. The mutual distrust this engenders is counter-productive and corrosive, and mechanisms need to be developed to enable information to be exchanged in an environment that safeguards both sides.

Exhortations by a former US intelligence official to 're-engineer the internet to make attribution, geolocation, intelligence analysis and impact assessment – who did it, from where, why and what was the result – more

70 Charles Miller, 'Kim Jong-il and me: how to build a cyber army to attack the US', presented at DEF CON 2010 Hacking Conference (30 July–1 August 2010), https://www.defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf, accessed 12 September 2010.

71 Clay Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress, 17 October 2003, http://www.fas.org/irp/crs/RL32114.pdf, accessed 7 May 2010, pp. 5, 7, 10.

manageable' reflect a self-centred and nationalist view of a domain that is truly global.[72] Critical internet infrastructure no longer resides entirely within the geographical boundaries of the United States, and is therefore not subject solely to the desires of Washington. The web is an ever-expanding and interdependent 'system of systems', far beyond the ability of any single government to control. It is all too easy to overestimate the political clout of the US, as well as the willingness of allies and trading partners to fall in line with actions that favour, or would be perceived to favour, the West. Aggressive actions by China could change the geo-political calculus of US allies, but reliance solely on the missteps of a perceived opponent is not a sound basis for strategy.

There is also the problem of directing precision force in cyberspace. In 2008, according to the *Washington Post*, an elite US Army cyber team was directed to shut down a joint CIA-Saudi 'honeypot' website that was used by extremists to communicate. The website was allegedly used as an intelligence-gathering tool, but unexpected consequences ensued when the team shut it down. 'The dismantling of the CIA-Saudi site inadvertently disrupted more than 300 servers in Saudi Arabia, Germany and Texas, a former official said. "In order to take down a web site that is up in Country X, because the cyber-world knows no boundaries, you may end up taking out a server that is located in Country Y."'[73] The disturbance that may have been created by this attack resulted from the forced closure of one website: how much more chaos would result from a sophisticated attack on a server farm or a major internet node?

Allies and international agreements

Various experts and political leaders have called for an international accord or treaty on cyber warfare, and the prospects for such a treaty were discussed at the 2010 World Economic Forum in Davos, Switzerland.[74] At that meeting the General Secretary of the International Telecommunications Union (ITU) called for an international accord on cyber war where 'the framework would look like a peace treaty before a war' since he sees the potential for cyber conflicts between two nations growing each year. Industry leaders including Microsoft's chief research and strategy officer, Craig Mundie, expressed a common business fear in calling the internet 'the biggest command and control centre for every bad guy out there'.[75]

Some US officials, however, are concerned at the prospect of a cyber treaty. One State Department official, who asked not to be identified for a 2009 media interview, said that 'they [Russia] want to constrain offence. We needed to be able to criminalize these horrible 50,000 attacks we were getting a day.'[76] This defensive and rather insular mentality does not allow the full scope of the issue to be grasped, however. International treaties and regulations that address conflict in cyberspace are likely to be formed through slow and painful processes, but this politicization of the issue will allow for the gradual coalescence of international norms and values that will have far greater stability than those asserted by any one state.

In June 2010 the US joined a 15-country coalition led by Russia in advocating an arms control approach to cyber warfare.[77] This move appeared to signal that the US was reconsidering its opposition to cyber arms control. General Alexander also endorsed this approach, stating that 'what Russia's put forward is, perhaps, the starting point for international debate'. He added that it was 'something that we should, and probably will, carefully

72 Mike McConnell, 'Mike McConnell on how to win the cyber-war we're losing', *Washington Post*, 28 February 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html, accessed 2 April 2010.

73 Ellen Nakashima, 'Dismantling of Saudi-CIA web site illustrates need for clear cyberwar policies' *Washington Post*, 19 March 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html, accessed 19 April 2010.

74 Rex Hughes, 'A treaty for cyberspace', *International Affairs*, Vol. 86, No. 2 (March 2010), pp. 523–41.

75 Red Orbit, 'Treaty Could Help Prevent Cyber Wars', 1 February 2010, http://www.redorbit.com/news/technology/1816280/treaty_could_help_prevent_cyber_wars/, accessed 8 July 2010.

76 John Markoff and Andrew Kramer, 'US and Russia differ on a treaty for cyberspace', *New York Times*, 27 June 2009, http://www.nytimes.com/2009/06/28/world/28cyber.html, accessed 22 May 2010.

77 The 15-country group of signatories include the UK, US, China, Russia, Belarus, Brazil, France, Germany, Estonia, India, Israel, Italy, Qatar, South Korea, and South Africa. Warwick Ashford, 'US joins UN cyber arms control collaboration', *Computer Weekly*, 20 July 2010, http://www.computerweekly.com/Articles/2010/07/20/242045/US-joins-UN-cyber-arms-control-collaboration.htm, accessed 03 November 2010.

consider'.[78] The shared objective of the arms control approach to cyber warfare would be to prevent a global arms race in cyberspace. However, it will take a lot of work and discussion to reach a shared definition of what constitutes a cyber weapon. And even if this is achieved there are still major hurdles to overcome involving attribution, dual-use weapons and proxy attacks.

NATO is also paying more attention to cyber security threats. Current drafts of the new Strategic Concept prepared by a group of experts chaired by former US Secretary of State Madeleine Albright devote a good deal of attention to cyber security threats, and reportedly consider 'adding cyber warfare to Article 5 of its charter which covers mutual protection of its members'.[79] How this would work in practice is vague and the approach faces many of the same complications as arms control. Estonia appealed to NATO and EU partners for help against Russia, which was suspected of prompting or otherwise turning a blind eye to the 2007 DDOS attacks on Estonian networks. However Estonia's appeal was for technical support, not for the purposes of launching a counter-attack. At what threshold of cyber attack should the Article 5 collective defence measures be invoked, and where should the counter-attack be directed if the aggressor is using zombie computers infected by malware to launch attacks from a third country?

Summary

Before any substantive agreements can be reached on issues such as international cooperation and public-private partnerships, core concepts to do with cyber warfare must be more closely defined, or (as in the case of attribution) a multi-tiered definition approved or tacitly accepted. Once a framework of definitions begins to coalesce, the right questions can be asked in the knowledge that all parties will be working from a (more or less) common understanding. The current politico-military strategic template is unable to cope with the challenges posed by cyber warfare. In the US and UK this condition will be, at best, only mildly improved by the cyber security-related institutional expansion now taking place within government.

New thinking is required in order to assert the role of politics in cyberspace. The cyber warfare discourse must take place uncorrupted by narrow special interests and by inaccessible technical language. National strategy must be willing to be pushed outside its traditional comfort zones in order to cope with rapidly emerging shifts, and political guidance must be confident, knowledgeable and pragmatic about what can be achieved. This brand of politics and strategy must be resolutely determined to avoid the militarization of cyberspace, and agile enough to handle the challenges of this most vibrant and dynamic of environments.

78 'CSIS cybersecurity policy debate series: US cybersecurity policy and the role of US CYBERCOM', transcript from CSIS, 3 June 2010, http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf , pp. 11-12, accessed 30 July 2010.

79 Nick Amies, 'NATO includes threat of cyber attack in new strategic concept document', *Deutsche Welle*, http://www.dw-world.de/dw/article/0,,6072197,00.html, accessed 2 November 2010.

4. Reflection: Strategic Problem and Strategic Solution

Having examined cyber warfare according to a traditional blueprint for strategic analysis – the 'action' of aggressive adversaries versus the 'reaction' of defending governments – we attempt in this chapter to place our assessment of cyber warfare more firmly within the debate on national strategy and security policy. The first task is to be clear what cyber warfare is and why it matters strategically. We have shown that there is both continuity and discontinuity, tradition and novelty in cyber warfare. The first part of this chapter draws together these observations to establish the limits of our knowledge and understanding of cyber warfare as a strategic problem, and to identify where further analysis and reflection would be appropriate. To persist with our earlier maritime metaphor, in cyber warfare the challenge is to identify where navigators can safely use their skills and where there is a need for more work to chart unknown waters. The task of charting these unfamiliar waters can be seen as nothing less than the imposition of a policy framework on cyber warfare, at several levels. But if policy is equivalent to navigation in our metaphor then it is more than merely a framework with which to better understand cyber warfare. In the second part of this chapter we develop the argument that policy, like maritime charting, is too often overlooked as part of the solution to unknown hazards.

Cyber warfare: a strategic problem

The October 2010 Public Administration Select Committee (PASC) report cited in Chapter 1 defined national strategy as 'the capacity we have as a country to devise and sustain a continuing process which can promote our national interest'. It further asserts that strategy is about 'dealing with uncertainty, complexity and the dynamic. It is not a plan or a paper. In modern politics, it is about ensuring that the whole of government identifies and acts effectively upon the national interest.' The select committee also explored the relationship between strategy and policy, insisting that 'strategy is not policy, but is the means of effecting it'. Their report quoted Paul Cornish's suggestion that 'strategy is what gives policy its ways and means, and [military] action its ends'. According to this view, strategy is best understood as lying between policy and activity (military or otherwise), making sense of both.[80]

A similar understanding of strategy can be found in the third edition of the UK National Security Strategy, also published in October 2010: 'A national security strategy, like any strategy, must be a combination of *ends* (what we are seeking to achieve), *ways* (the ways by which we seek to achieve those ends) and *means* (the resources we can devote to achieving the ends).'[81]

The problem is also, it seems, understood in much the same way in the United States: 'US officials acknowledge they cannot solve the cyber security problem simply by applying more human and technological resources. They also need new tactics, techniques and procedures as well as a comprehensive strategy for cyber operations.'[82] Drawing upon observations made in the Chapters 2 and 3, we now use 'ends, ways and means' as a simple

80 Public Administration Select Committee, *Who Does UK National Strategy?*, 12 October 2010, http://www.publications.parliament.uk/pa/cm201011/cmselect/cmpubadm/435/43503.htm, accessed 18 October 2010, pp. 3,7,8.

81 UK Cabinet Office, *A Strong Britain in an Age of Uncertainty*, p.10, para. 0.14 [emphasis in original].

82 'Pentagon cyber security role expands', *Oxford Analytica: Global Strategic Analysis*, 2 July 2010.

template for identifying the most important characteristics of cyber warfare and to ask what these characteristics reveal of its strategic character.

The 'ends' of cyber warfare

There is no consensus of opinion and little received wisdom as to why states (and others) might wish to resort to cyber warfare, when and under what conditions, and indeed why they might choose not to. Cyber warfare, both as an idea and as a set of actions and reactions, is not accompanied by a mature, universally accepted policy, regulatory and normative framework. This is not to say that there is no regulation of cyberspace or views concerning what may or may not take place within it and how it might be exploited. Regulations and even normative restraints can be found at certain levels and in certain niches of the internet – the social networking site Facebook, for example, has rules about which third-party applications may be run on its site and how personal data may be used. It even has its own 'Peace on Facebook' site which seeks to 'play a part in promoting peace by building technology that helps people better understand each other. By enabling people from diverse backgrounds to easily connect and share their ideas, we can decrease world conflict in the short and long term.'[83] But these are sporadic occurrences in the vastness of cyberspace and can scarcely be said to express the settled opinion of the world's internet users. Sadly, perhaps, 'Peace on Facebook' can hardly be seen as the first stirrings of the cyber equivalent of a global arms control and non-proliferation regime. It is of course conceivable that this assessment may change; indeed, this report argues that these isolated efforts at self-regulation not only can but must be replaced by a global effort that is both ambitious in scope and binding in application.

As noted above, at the operational level it can be almost impossible to discern the intent or even the identity of a cyber aggressor, making it very difficult to discuss cyber warfare according to a conventional strategic analysis – as an action by a known party using certain resources in order to achieve specifiable goals. The 'attribution problem' features prominently in any discussion or reporting of cyber warfare:

> Attribution is the key to understanding the motive of an attack and consequently being able to differentiate between a criminal act and warfare in cyberspace and is crucial for co-ordinating national and international responses and determining national policy.[84]

But attribution is not a simple matter. It can be hard to distinguish between different cyber security challenges when cyber warfare, cyber extremism, cyber crime and cyber mischief can all use similar 'tactics, techniques and procedures'. It can be difficult to establish beyond any technical doubt that the government of a state might have been responsible for a cyber attack launched with private computing means from the territory of a second state on the electronic infrastructure of a third – a commodity known as 'plausible deniability', which is in plentiful supply in cyberspace.

Without fast and accurate attribution the identity and intent of the attacker might not be known before an attack has started or even finished. And without such attribution it will be difficult for a defending government to know that its response is both accurately targeted and proportionate to the damage caused. As the *Economist* noted in its comment on the 2010 Stuxnet attack on Iranian nuclear facilities, 'it is rarely clear who is attacking whom. It is hard to tell whether a strike has been successful, or indeed what has happened at all. This, it seems, is what cyber war looks like. Get used to it.'[85] If this is an accurate description of the 'attribution problem', then it marks an important distinction between cyber warfare and warfare as traditionally understood. In the conventional strategic paradigm of state-based defence against enemies (whether other states or even terrorist groups) the prevailing assumption was that the intent (and indeed the identity) would be sufficiently revealed

83 Peace on Facebook: http://peace.facebook.com/, accessed 31 October 2010.
84 Eleanor Keymer, 'The cyber-war', *Jane's Defence Weekly* (47/39, 29 September 2010), p. 22.
85 'The meaning of Stuxnet', *The Economist*, 2 October 2010.

in the act itself. Attribution was not a problem at all, in other words, as it was more or less self-evident who had acted in a warlike manner, and for what reason.

The 'ways' of cyber warfare

What should be expected of cyber warfare as a method for achieving strategic ends, and how ambitious can those ends therefore be? The answer to these questions will depend upon the degree of decisiveness that can be attributed to cyber warfare and where it is placed on a spectrum of strategic methods. The first problem is that there are at least four points where cyber warfare could be placed on such a spectrum. There is one argument, touched on in Chapter 1, that cyber warfare is nothing less than a new and sufficient explanation for 21st-century war in its totality: 'there have even been suggestions that future wars could be waged in cyberspace, displacing conventional military operations altogether'.[86] In the reporting of cyber warfare, and in what passes for scholarly literature on the subject, it is just as common to find references to the possibility of a 'cyber Pearl Harbor' and 'cybergeddon' as it is to find vehement attempts to dismiss such possibilities as scaremongering and worst-case analysis. Our research leads us to a more cautious view of the potential of cyber war but how can we, and a general readership, be confident that we are right and that others – such as Michael Markulec who argues that 'if anything, the severity of the threat has been understated'[87] – are wrong?

The second possibility is that cyber warfare should be understood more as a distinct domain of military operations to be placed on the strategic spectrum alongside land, sea and air operations: 'Much like land, sea and airpower, cyberpower is a weapon of war.'[88] If operations in space are added, then with cyber warfare we arrive at the so-called 'fifth battlespace' idea.[89] Here, the argument would not be that any one of the five 'battlespaces' could be decisive on its own in military operations, but that all must be understood as essential to the whole.

The third option is that this endows cyber warfare with more significance than it deserves and that, rather than being given its own place on the strategic spectrum, it should be seen merely as an ancillary function or 'force multiplier' for the existing four battlespaces, much like radio communications or target surveillance. The fourth, far simpler option would be to consider cyber warfare merely in terms of the 'weapons' it can offer to a wide variety of users, and the effects those weapons might have on societies, governments, businesses and so on. There might even be a fifth option: that cyber warfare should not be placed anywhere on a spectrum of strategic methods because it is fundamentally non-strategic:

> it is easily conceivable that [cyber] attacks may be launched simply to destroy the vital nerves of a society and not for any easily discernible strategic gain, particularly if non-states actors launch them. […] Information warfare may become a kind of nihilistic port or war (*sic*) fuelled simply for its own sake … we may not be able to discern or even determine if there is a strategic rationale behind it beyond the sheer delight of destruction.[90]

'In the reporting of cyber warfare, and in what passes for scholarly literature on the subject, it is just as common to find references to the possibility of a "cyber Pearl Harbor" and "cybergeddon" as it is to find vehement attempts to dismiss such possibilities as scaremongering and worst-case analysis'

86 'Marching off to cyberwar', *The Economist Technology Quarterly*, 6 December 2008.

87 Michael Markulec, 'Defining the network: high-value protection', *Jane's Defence Weekly* (47/39, 29 September 2010), p.18.

88 Murphy, 'Attack or defend?', p. 90.

89 See, for example, Rick Rozoff, *U.S. Cyber Command: Waging War in the World's Fifth Battlespace* (Montreal: Centre for Research on Globalization, 27 May 2010), http://www.globalresearch.ca/index.php?context=va&aid=19360, accessed 31 October 2010.

90 Stephen Blank, 'Web War I: is Europe's first information war a new kind of war?', *Comparative Strategy*, Vol. 30, No. 3 (1 May 2008), p. 240.

None of the above options is implausible. In terms of the challenge for national strategy, this must set cyber warfare apart from other, more conventional discussions of warfare, not because cyber warfare promises something entirely novel or strikingly different, but because it promises everything. 'Quantity', as Stalin is reputed to have said, 'has a quality all of its own'.

What emerges very clearly from the discussion in Chapters 2 and 3 is that, in the parlance of strategic analysis, cyber warfare demonstrates 'offensive dominance'. That is to say, as a strategic method it shows offensive action to be easier, quicker and usually cheaper than defensive action. Cyber warfare could be the archetypal illustration of what has become known as 'asymmetric warfare' – a struggle where one opponent might be weak in conventional terms but is clever and agile, and where the other opponent is strong but complacent and inflexible. The terrorist attacks on the United States in September 2001 are a compelling example of asymmetric warfare: the world's military superpower was attacked by a small group of terrorists using unsophisticated weapons and techniques, with devastating effect. Cyberspace offers opportunities on a similar, if not far greater scale. The annual defence budget of the United States is approximately $700 billion. But according to one cyber security analyst, 'it would take two years and cost less than $50 million a year to prepare a cyberattack that could paralyze the United States', and this effort 'could involve fewer than 600 people working to infect computers'.[91]

Asymmetric cyber warfare need not be the province of individuals or small groups of people, however. As is alleged with regard to China, a state can invest in cyber warfare capabilities in order to offset the conventional military advantages enjoyed by an opponent (i.e. the United States) and in order to attack a critically important part of the opponent's defensive infrastructure (in this case the US military command-and-control organization).[92]

The effect of asymmetric cyber warfare (both low- and high-level) might be difficult to calculate with much accuracy. A cyber attack mounted against a key point or facility is not usually direct (in the conventional sense of a physical attack designed to sabotage or destroy a factory or transport node, for example) but exploits and corrupts information and communication networks in order to bring about the desired effect by indirect means. It is possible that neither attacker nor defender will know the full extent and vulnerability of the network(s) under attack and whether the attack will affect other associated networks.

As well as both low-level and high-level asymmetric cyber warfare, therefore, it is possible to conceive of *accidental* asymmetric cyber warfare where the effect could be beyond the imagination and expectation of both attacker and defender. It is difficult to see how to defend against asymmetric cyber warfare, but it is just as difficult to see how governments could abandon the effort and accept complete vulnerability to the sort of attacks described above. It might be possible to impose export and proliferation controls on key technologies, but given that much 'cyber weaponry' is in the form of software it might be unwise to expect too much of this conventional approach to the problem. Instead, governments might choose to meet the asymmetric security challenge as they have done in the past, when dealing with terrorists and insurgents for example – by responding in similar ways and at similar levels in order to balance the attack/defence equation and remove the asymmetric advantage. Perhaps there is a role, in other words, for government-employed 'counter-hackers' within the intelligence agencies or for a 'Hacktivist Battalion' in the armed services.

It is possible that organizations such as these already exist, behind the traditional veil of secrecy that surrounds the world of signals and electronic intelligence. But if they are to be brought into the mainstream of national strategy the critical factor will be the level at which such capability would be controlled – in the same way that Special Forces, although manoeuvring tactically, are controlled at the highest level of national command. The tasking of these assets will be difficult: the outcome of a whole campaign

91 'Time to wake up to cyber attack threat: experts', *Ottawa Citizen*, 18 June 2010, http://www.ottawacitizen.com/news/Time+wake+cyber+threat+Experts/3170415/story.html, accessed 19 October 2010.

92 'Tracking *GhostNet*', p. 11.

could depend on the result of a tactical (but politically and strategically vital) firefight in a critical part of a critical battlefield. How might an infantry platoon leader, pinned down by accurate conventional artillery fire, call in 'cyber fires' from facilities that are possibly many thousands of miles away, in order to neutralize the weapon-aiming computers of the opposing forces?

Finally, examining the 'ways' of cyber warfare requires a brief consideration of deterrence. Strategy, as already noted, is the use of certain ways and means to achieve certain ends. But strategy need not always be about action. Some 2,500 years ago Sun Tzu argued that 'to win 100 victories in 100 battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.'[93] Strategy can be about preventing the success of an adversary's action or threatening a reaction of a sort which will dissuade the adversary from acting in the first place or, ideally, persuade him to accept defeat. In one way or another deterrence has always been part of strategy and defence, whether in the form of denying success to the adversary by putting in place strong defences or of threatening to punish the adversary with a retaliation of some sort. In cyber warfare, however, deterrence appears to be especially difficult to achieve. The 'attribution problem' discussed earlier, and the general opaqueness of cyberspace, will make it difficult to know what it is that needs to be denied, and who or what should be threatened with a punitive retaliation. Deterrence must be based upon credible assurances that the defender has the capacity to deny and/or to punish; and that capacity must also be communicated to the adversary, who must be identifiable. But, as Richard Clarke asks, 'how does deterrence work in cyber war when our capabilities are secret and our weapons undemonstrated?'[94]

The 'means' of cyber warfare

Cyber warfare must, of course, involve individuals and groups of people. But the 'means' of cyber warfare are best understood as essentially technological: the 'hardware' of communications and information infrastructures and the 'software' with which they are run.[95] This is scarcely surprising: for as long as there has been technology (the application of science and innovation) and strategy (the use of forces and resources to achieve political ends), there has been a relationship of sorts between these two activities.[96] But in at least three respects, the technology of cyber warfare presents a challenge to established thinking about this relationship.

In the view of many analysts and commentators, the most distinctive feature of cyber warfare (and cyber security more generally) is the rapidity with which threats can evolve. According to former CIA director Michael Hayden, as recently as the end of the George W. Bush administration, 'cyber was moving so fast that we were always in danger of building up precedent before we built up policy'.[97] The pace of change can be so abrupt as to render the conventional, action/reaction cycle of strategic evolution out of date before it has begun: it is as if a government operational analyst has been sent to observe the effects in battle of the flintlock musket, only to discover upon arrival that the Maxim gun has been invented.

The rapidity of innovation in cyberspace can tend towards the 'offensive dominance' discussed above which might, in turn, create incentives for a first strike. In terms of classical strategic analysis, therefore, the 'ways' of cyber warfare are such that 'crisis instability' and 'arms race instability' might ensue. The first of these pushes governments to act first in a crisis, probably earlier than might otherwise have been necessary. In these high-pressure circumstances, cyber capabilities might be regarded in the way nuclear weapons were in the early days of thinking about nuclear deterrence, when the stark choice seemed to be to 'use them or lose them'. Arms race instability, on the other hand, will encourage tit-for-tat escalation

93 Sun Tzu, *The Art of War*, trans. S.B. Griffith (Oxford University Press, 1963), p. 77.
94 Clarke, 'War from cyberspace'.
95 The technological characteristics of cyberspace are summarized in Cornish et al., *Cyberspace and the National Security of the United Kingdom*, pp. 1, 5, 13–16.
96 For a discussion of the relationship between technology and aspects of national strategy see Paul Cornish, 'Technology, strategy and counterterrorism', *International Affairs*, Vol. 86, No. 4 (July 2010).
97 Nakashima, 'Dismantling of Saudi-CIA Web site'.

in capability: an arms race in cyberspace. Faced with the very rapid evolution of cyber threats, governments will doubtless wish to draw upon sources of expertise and innovation in order to achieve a speedier response to threat development. With this in mind, they might seek to cooperate with universities and industry. But it will be essential to bear in mind one of the lessons of the nuclear era, that while innovation can address specific vulnerabilities, it can paradoxically make the system as a whole less stable.

> 'We find little evidence of politics and policy, in any consistently recognizable sense, governing behaviour, whether in terms of the proliferation of cyber technology or the aggressive uses to which it is put'

The second distinctive feature of cyber warfare strategic 'means' is that cyber technology exploits normality in a covert, if not invisible way. Conventional military activity has, of course, always exploited normality in that it has made use of land, sea, air and space – mediums with which we are scarcely unfamiliar. What is different is that in conventional strategy these mediums have been exploited in specialized and very well-developed ways, and usually very visibly. A combat aircraft exploits the same principles of flight as a passenger liner. The Royal Navy's new aircraft carriers might have roughly the same displacement as a Panamax cargo ship. And a main battle tank will use its tracks to cross rough terrain just as a large earth mover does. In none of these cases should there be any confusion between what is military (or even merely confrontational) and what is not. The same cannot be said of technology in the cyber domain. Some overlap occurs in that a nuclear submarine or stealth combat aircraft can attack and disappear without a trace, in much the same way as a cyber aggressor. The primary difference is that the expense of these conventional weapons is beyond all but the most developed nations, whereas increasingly powerful and stealthy cyber-weapons are within the reach of non-state actors.

Finally, as a strategic 'means' cyber warfare has been democratized, but in a rather peculiar and hollow manner. Technologies which in the past would have been considered highly specialized have proliferated to become widely available and relatively easily usable. As the *Information Warfare Monitor* has noted:

> cyberspace has empowered individuals and small groups of non-state actors to do many things, including executing sophisticated computer network operations that were previously only the domain of state intelligence agencies. We have entered the era of *do-it-yourself* (DIY) signals intelligence.[98]

What we find most peculiar, however, is not the extent or the pace of the spread of technology but that it is a process of democratization which, in spite of the label, seems oddly apolitical. We find little evidence of politics and policy, in any consistently recognizable sense, governing behaviour, whether in terms of the proliferation of cyber technology or the aggressive uses to which it is put. As noted earlier, Clausewitz's best-known aphorism asserted that 'war is not a mere act of policy but a true political instrument, a continuation of political activity by other means'.[99] But it is not clear that the proliferation and use of cyber technology are seen as politically instrumental, in the Clausewitzian sense.

Cyberspace has developed at very great speed into a global technological commons. But it seems that the values, ideas and norms which should govern human behaviour – particularly, interestingly enough, when a commons is under construction – have not developed at the same pace. This is not to say that values and norms

98 'Tracking GhostNet', *Information Warfare Monitor*, p.47 [emphasis in original].
99 Clausewitz, *On War*, p. 87.

are entirely excluded from cyberspace, as illustrated by the case of Facebook referred to earlier, or the example of Chinese 'human flesh searches' that use the power of crowds to locate and ostracize individuals wanted for punishment for some transgression.[100] But it is important to note that rules and norms have been atomized; they are available as an 'app' or as free software to be configured and used (if desired) by each computer user. We might say that if Clausewitz's ideas are still relevant, then there can be as many interpretations of those ideas as there are users of cyber technology. The problem is both organizational and human. At the organizational level, the *Economist* has argued that

> fifteen years after its first manifestation as a global, unifying network, [the internet] has entered its second phase: it appears to be balkanising, torn apart by three separate, but related forces [governments reasserting their sovereignty, IT companies constructing and controlling their own "digital territories", and network owners introducing differentials in transmission speeds].' It goes on to warn that 'just as it was not preordained that the internet would become one global network where the same rules applied to everyone, everywhere, it is not certain that it will stay that way.[101]

At the human level, the best description of the problem is provided by Anand Giridharadas:

> More people than ever, perhaps, have the opportunity to be makers of culture, even if that means more to choose from and, consequently, fewer standards and blockbusters shared in common. What it means, too, is this paradoxical feeling: that of being more connected than ever, with one-click access to so much of the world's cultural harvest, and yet, with the fragmentation and the constant whirl of these times, of being starved for like-mindedness, synced only with ourselves.[102]

It should be borne in mind that, bleak and disturbing as it is, Giridharadas's vision is of the world of culture. When extended to the world of contest and conflict the prospect of being 'synced only with ourselves' throws up a much more unsettling vision of cyber-anomie and nihilism.

Policy: a strategic framework and a strategic solution

Using a formulation that has become deeply embedded in Western strategic thinking and military doctrine, Clausewitz described a very close, even unbreakable relationship between policy (and politics) and war:

> 'Subordinating the political point of view to the military would be absurd, for it is policy that creates war. Policy is the guiding intelligence and war only the instrument, not vice versa. No other possibility exists, then, than to subordinate the military point of view to the political.'[103]

Some commentators have sensed something like a Clausewitzian logic at work in cyber warfare. Stephen Blank, for example, in his analysis of the 2007 cyber attacks on Estonia, notes that 'these cyberattacks appear to have been strategic in choice of targets and political objectives, part of a larger long-term strategy, and therefore long planned.'[104] Alex Michael goes rather further, arguing that

> the cyber arena has now become far more politicised than traditionally thought. This however does not necessarily imply that all cyber attacks are politically motivated and can be directly associated with government actors; merely that both state and non-state actors around the world are beginning to seize opportunities that cyberspace provides.[105]

100 'China's Cyberposse', *New York Times*, 3 March 2010, http://www.nytimes.com/2010/03/07/magazine/07Human-t.html, accessed 3 November 2010.
101 'A virtual counter-revolution', *The Economist*, 4 September 2010.
102 Anand Giridharadas, 'All together now, to each his own sync', *New York Times*, 17 September 2010, http://www.nytimes.com/2010/09/18/us/18iht-currents.html, accessed 1 November 2010.
103 Clausewitz, *On War*, pp. 87, 605, 607.
104 Blank, 'Web War I', p. 229.
105 Michael, *Cyber Probing*, p. 1.

We are in agreement with a good deal of this analysis but draw a different conclusion. While there may be plenty of *politics* associated with different cyber warfare incidents around the world, we do not see that cyber warfare is a *politically constrained phenomenon* in the Clausewitzian sense. We see cyberspace as *terra nullius*, currently beyond the reach of mature political discourse. In other words, it is precisely the *absence* of a constraining political framework around cyber warfare that makes cyberspace so attractive as a place in which to achieve cultural, religious, strategic, economic, social and even – paradoxically – political goals. Were Clausewitz alive today and commenting upon cyber warfare he might characterize it not as 'a continuation of political intercourse, with the addition of other means'[106] but as 'the insignificance of political intercourse caused by the availability of digital means'.

> "Were Clausewitz alive today and commenting upon cyber warfare he might characterize it not as "a continuation of political intercourse, with the addition of other means" but as "the insignificance of political intercourse caused by the availability of digital means". "

The strategic solution to cyber warfare is in two parts. In the first place, the challenge must be to extend policy and politics into cyberspace in order to govern cyber warfare more closely and according to uniform standards. But if cyber warfare needs to be normalized by politics, politics for its part must acknowledge and adapt to the challenges of cyber warfare. The second task is therefore to extend the complexities of cyber warfare back into the world of politics, reviewing and refreshing many of the assumptions that inform the Clausewitzian, state-centric, government-led approach to warfare. Cyber warfare must, in other words, be transformed by the Clausewitzian framework of analysis, but that framework must also be transformed by cyber warfare.

We see three steps in this process of politicization. The first step is to eschew the current trend of viewing cyber warfare as a disconnected series of more or less alarming anecdotes, with each incident requiring an ad hoc response of some sort. There is a need to examine cyber warfare in the round, to impose some analytical discipline upon it in order to know how best to deal with it.

The second step is to reclaim cyber warfare from the technologists. This is not to say that they should have no part to play in policy and strategy; clearly, technology is essential to the cyber warfare debate, yet it is not sufficient. Cyber warfare must be understood as one of several national strategic challenges – and communicated as such to a largely non-technical audience – if it is to be politicized in the way we recommend.

The final step is for governments to conduct a self-assessment to establish the limits of their own authority and capability in cyber warfare and to know where assistance will be needed, and from whom.

If cyber warfare can be viewed as a mainstream political/strategic problem, it will be possible to resolve many of the difficulties we have discussed in this report. Some of these are structural, others less so. For example, it is hard to judge whether threats in and from cyberspace are understated to the point of complacency, or exaggerated to the point of scaremongering. Such judgment requires a political/strategic rather than a technological frame of reference – a sense of what is vulnerable, what is to be secured, and why.

Similarly, it is widely accepted that the connections and interdependencies within and between ICT networks are highly complex and that this complexity generates vulnerability, perhaps in uncharted areas and in unknown ways. Our March 2009 Chatham House report argued that 'the various illicit uses of cyberspace amount to

106 Clausewitz, *On War*, p. 605.

a system-level challenge to society'. It went on to describe this challenge as

> problematic because society does not act and respond as a coherent system where cyber-security is concerned. Stakeholders remain largely segregated, concerned to maintain security within their narrow ambit. As a result public bodies, commercial enterprises and private individuals can all fail to see that they are affected by another stakeholder's security, or lack of it.[107]

An important step towards meeting a challenge of this breadth and complexity must be, once again, to create a political framework that enables communication and comparison between different sectors of society.

Another difficulty we have observed concerns the asymmetry of cyber warfare. If attempts might be made by adversaries to disrupt national command-and-control systems, which begin with the political leadership, then it is hard to see how governments could do anything other than regard cyber warfare as a political – rather than merely technological – challenge. Attacks on command-and-control systems do not involve the physical destruction of buildings but they are more than the interruption of conversation and the prevention of the transmission of instructions. Command-and-control warfare is intended also to damage the political and moral self-confidence of an adversary: in order to defend successfully against such an assault these qualities must be made as explicit and robust as possible. The politicization of cyber warfare in the Clausewitzian model should also serve to counter the beguiling yet dangerous argument that cyber warfare can be a 'painless' or 'bloodless' form of conflict, yet still decisive and therefore preferable. As Clausewitz observed:

> Kind-hearted people might of course think there was some ingenious way to disarm or defeat an enemy without too much bloodshed, and might imagine that this is the true goal of the art of war. Pleasant as it sounds, it is a fallacy that must be exposed: war is such a dangerous business that the mistakes which come from kindness are the very worst.[108]

Of the many structural challenges associated with cyber warfare, we consider four to be most susceptible to resolution by an effort to politicize cyber warfare: attribution, cooperation, regulation and communication.

As far as attribution is concerned, the difficulty is that the debate has to a large extent been a technological one, in which attribution – if it is to be credible – is expected to meet the highest possible technological standards. The risk here is that the best will be made the enemy of the good and that the attribution of a cyber attack will be put almost beyond the reach of national strategy. This would be a very major drawback, since timely and accurate attribution is essential to the effective and proportionate management of cyber warfare. A more political approach to attribution, however, might accept less exacting standards. Simply by asking who has gained from a cyber attack might make it possible to establish reasonably enough the identity and intent of a cyber attacker. The standard of evidence would be lower than that required by scientific evaluation or by judicial process but could make national strategy more self-confident and might make it possible to seize some of the initiative from the cyber attacker. An element of doubt will thus be introduced into the minds of cyber attackers and their sponsors and it is even conceivable that some self-deterrence will occur as a result.[109]

Cooperation is essential in the management of cyber warfare and impossible without a well-developed political-strategic framework. In the first place, cooperation must be achieved within government, with different departments and agencies all subscribing to a 'common analytical picture' and able to combine their efforts at the right moment and in the right manner in order to meet a cyber threat.[110] Governments must also cooperate

107 Cornish et al., *Cyberspace and the National Security of the United Kingdom*, p. 31.
108 Clausewitz, *On War*, p. 75.
109 For a discussion of the limits of deterrence in cyber warfare see 'Deterrence fails in cyber warfare', *Oxford Analytica: Global Strategic Analysis*, 27 May 2010.
110 Cornish et al., *Cyberspace and the National Security of the United Kingdom*, p. 26.

with a very wide range of non-governmental bodies and agencies. Just as an intra-governmental approach to cyber warfare acknowledges that the MoD, for example, cannot provide all the answers to the problem, so an extra-governmental approach acknowledges that there are areas where government lacks the necessary competence. This is particularly the case with regard to technological innovation and development, where the rapid evolution of cyber technology calls for a close and stable relationship between government, the research and innovation sector and industry. Another level of cooperation is intergovernmental, where industry's contribution is especially important in the development of systems to give early warning (and accurate attribution) of cyber attack. As one official of the Estonian National Cyber Security Council has observed, 'without international co-operation it is impossible to defend your cyberspace'.[111] And all cooperation – whether intra-, extra- or intergovernmental – must be founded upon a comprehensive, comprehensible and above all common political outlook.

Intergovernmental cooperation also makes it possible to contemplate international regulation, the third of the structural challenges we consider here. Will it be possible to overcome the considerable technological difficulties (not least in the field of verification) to develop an arms control regime for cyber warfare that could manage the risks of crisis instability, remove incentives for a cyber first strike and reduce the chances of an arms race in cyberspace? Could there also be something analogous to a non-proliferation regime for cyberspace, in which the availability of certain technologies and ideas is tightly controlled, and the character and intentions of 'end-users' are closely monitored? And might there, finally, be scope for the definition of acts of war in cyberspace and for tighter controls on the use of cyber 'weapons' on humanitarian and other grounds? These are all complex issues, currently under debate in a number of countries and within international organizations such as NATO. It is not for this report to analyse these discussions or to predict their outcome, other than to insist that they are unlikely to result in anything useful if cyber warfare is not seen, in principle, as a phenomenon which should be politically constrained.

Our fourth and final structural challenge concerns language and communication. To a great extent all policy and strategy is about the communication of resolve, intent and capability, to allies and adversaries alike, and ensuring that the language used is clear and unequivocal. Yet cyber warfare seems to have developed its own language, a good deal of which has been mentioned elsewhere in this report: logic bomb; cyber missile; cyber weapon; cyber attack/defence/exploitation/operations; layered defence; cyber threats; cyber mercenaries; cyber test range; and so on. Clearly, much of this language has been borrowed from conventional warfare and adapted to fit. In some cases this language will be appropriate, but not in all. In any case, what do these terms actually mean? Does 'bomb', for example, translate faithfully from aerial munitions to computer software, and is the result worthwhile? More generally, does language of this sort convey a mature and sophisticated understanding of the character, potential and limitations of cyber warfare? Language of this sort is colourful and catchy, but also lazy. It suggests that the problem of cyber warfare has not been considered with sufficient care at the political-strategic level and that, as a result, some cyber warfare events might be classified inappropriately (i.e. in military terms when they might be merely criminal). It also surrenders too much of the initiative to the cyber aggressor, enabling him to articulate his purpose and actions in more ways than the cyber defender can match, narrowing the defender's range of responses and, in spite of the muscularity of his warlike language, making him appear to lack purpose and resolve.

Summary

For cyber warfare to be fully understood it must be analysed systematically and placed within a framework of national strategy. Strategy is concerned with the relationship between ends, ways and means. We have used this template in order to establish what is known and

111 Heli Tiirmaa-Klaar, quoted in Keymer, 'The cyber-war', p. 22.

understood about cyber warfare as a strategic phenomenon. The national strategic framework is more than an explanatory device, however. By placing cyber warfare within a Clausewitzian politico-military model in which warfare is considered to be a phenomenon both constrained and validated by politics, many of the challenges associated with cyber warfare begin to be clarified and resolved. Furthermore, if cyber warfare is to be understood and managed effectively then the Clausewitzian model – with its embedded assumptions about the primacy of the state, the authority of government and the role of the armed forces – must also adapt.

5. Conclusion

> Subordinating the political point of view to the military would be absurd, for it is policy that creates war. Policy is the guiding intelligence and war only the instrument, not vice versa. No other possibility exists, then, than to subordinate the military point of view to the political.
>
> *Clausewitz*[112]

We began this report with a deliberately undernourished strawman description of cyber warfare, its aims and methods and the context in which it takes place. We then proceeded to demonstrate the limitations of such a narrow understanding of the problem. Our purpose was to show that a conventional, state-centric, politico-military strategic template is unequal to the challenge posed by cyber warfare. But having dismantled the strawman we then sought to construct a more muscular and durable definition. We argue throughout this report that cyber warfare must be analysed systematically, rather than presented and interpreted as a series of alarming anecdotes. Cyber warfare is a complex, fast-evolving political and technological phenomenon which can only be understood and managed if placed within a framework of national strategy. National strategy must itself be reviewed and adapted if it is to take proper account of cyber warfare.

Chapter 2 examined hostile actions in cyberspace, including direct and military threats as well as indirect and non-military threats. It took a thematic approach to several well-established strategic problems, all of which have manifestations in cyberspace: interstate conflict, terrorism, extremism, espionage and crime. We examined certain peculiarities of cyber warfare, such as the problem of attributing an attack and of establishing the aggressor's intent. Cyber warfare is made especially complex by the multiplicity of actors in cyberspace and the ease with which they can undertake hostile actions. The scale and nature of these threats are often poorly understood, further complicating the process of addressing them within a coherent national strategy. Moreover, the lack of clarity over the provenance and seriousness of these threats makes cyberspace a curiously chaotic and apolitical environment. To address these problems cyber warfare must be bounded by a political framework in order to constrain activity according to common standards and avoid the fragmentation or 'balkanization' of cyberspace and the increased conflict that would probably result.

Chapter 3 looked at the reaction of governments to these threats, focusing specifically on the policy and operations of the United States and the United Kingdom. Governments in both countries (and indeed others) are expanding their cyber warfare capabilities, yet the politico-military vision that should underpin these policies is often vague, confused and riddled with 'terminological inconsistency'. Confronted with a new and dynamic strategic environment, policy-makers are often left without the necessary skills to navigate the dangerous currents of cyberspace. As a result, the cyber warfare policy and strategy debate can be overpowered by voices which seek to impose either military or technological solutions to the problem. There must, of course, be a military response to the military aspects of cyber warfare, just as technology must play a central part in any effective strategy. But neither the military nor the technological perspective is a substitute for a well-rounded national strategy in which cyber warfare is guided and constrained by political norms and ethical values. In broadening the response to cyber warfare we asked what could be expected of existing mechanisms such as public-private partnerships and international treaties and alliances. We also identified doctrinal and

112 Clausewitz, *On War*, pp. 87, 605, 607.

project management frameworks that might translate into cyberspace in order to avoid unnecessary duplication of effort.

In Chaper 4 we reflected upon the place of cyber warfare in national strategy. We argued that the first step must be to characterize cyber warfare as a strategic problem and activity, and applied the 'ends, ways and means' model of strategic analysis. In order to understand cyber warfare fully at the strategic level, a politico-military framework must be imposed upon it. Our preference is for a Clausewitzian approach in which there is a close, even unbreakable relationship between policy (and politics) and warfare. This approach offers more than merely an explanation of cyber warfare, however. Placing cyber warfare within a Clausewitzian framework – whereby warfare is considered to be a phenomenon that is both constrained and validated by politics – and adapting that framework to meet the challenges of the cyber environment means that many of the problems associated with cyber warfare can start to be clarified and resolved.

Taking in turn each element of our original description of cyber warfare, our new definition differs from the strawman. Instead of *'Cyber warfare is a conflict between states where precise and proportionate force is directed against military and industrial targets for the purposes of political, economic or territorial gain'*, we now argue that**:**

- ***cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target.***

In our original definition, we stated that: '*Cyberspace serves as an adjunct to conflict in the physical domain and therefore shares many of the same characteristics. In cyber warfare weapons are predominantly military, rather than dual-use; adversaries can be identified and deterred; the terrain is predictable; defence is the position of strength; and offensive actions risk vulnerability as one manoeuvres upon the battlefield.*' But it distorts our understanding of cyber warfare to argue that it could be a complete explanation for warfare in the 21st century:

- ***Cyberspace has extended the battlefield and should be viewed as the fifth battlespace alongside the more traditional arenas of land, air, sea and space. Cyber attacks are just one component of the strategic ways and means available to a state or organized non-state group. As such, warlike challenges in cyberspace are more likely to occur in conjunction with other methods of coercion and confrontation. However, the ways and means of cyber warfare remain undeniably distinct from these other methods. The weapons are almost always dual-use, in the sense that they are lines of code and physical hardware that can be modified for other purposes. Problems with attribution mean that adversaries are nearly impossible to identify and therefore deter. The terrain (cyberspace writ large) is constantly shifting and expanding. Offence is the position of strength, as anonymous attackers rarely have to face the consequences of their actions, whereas the static defender must successfully parry every blow.***

Instead of the strawman argument that '*Victory and defeat are recognizable in cyber warfare. Since cyber warfare is not a discrete phenomenon and cannot be separated from conflict in the physical domain, it follows that it must be guided and constrained by the values and norms of a state and by the prohibitions that apply to conventional warfare*', we now argue:

- ***Victory and defeat are far from recognizable in cyberspace, as these concepts have little traction in a domain where political, ideological, religious, economic and military combatants fight for varying reasons according to different timescales. These actors bring their own code of conduct to the fight, resulting in a discordant and chaotic sphere of conflict in which it is not yet obvious that a common framework of ethics, norms and values can apply.***

Cyber warfare is distinct from conventional warfare not because it offers something entirely novel or strikingly

different, but because it offers everything. The crux of the problem, however, is that while there might be plenty of *politics* associated with actual or potential cyber warfare events around the world, we do not see that cyber warfare is a *politically constrained phenomenon* in the Clausewitzian sense. We describe cyberspace as *terra nullius*, currently beyond the reach of mature political discourse. In other words, it is the *absence* of a constraining political framework around cyber warfare that makes cyberspace so attractive as a place in which to achieve cultural, religious, economic, social and even – paradoxically – political goals. We argue that cyber warfare must be bounded by a Clausewitzian framework of analysis, and that framework must also be transformed by cyber warfare. In this way national strategy will adapt to the emerging challenges of cyber warfare, which will in turn be guided by the stabilizing norms and values that national strategy – and only national strategy – can provide.

Cyber Security

Society's increasing dependence on Information and Communications Technology (ICT) infrastructure creates vulnerabilities and opportunities to be exploited by unscrupulous actors. Whether through online financial fraud, the dangers posed by hacking, cyber-attacks or the extensive use of the internet by terrorists and other extremists, the risks to international and national security are increasing.

However, cyber security is not just the concern of governments, commercial enterprises, or individuals. Cyber security is an issue which concerns all of society, particularly as we become ever more dependent on the global information and communications infrastructure.

With this in mind, the International Security Programme at Chatham House is involved in analysing key challenges in the cyber domain, identifying policy responses and establishing a cyber security knowledge base to inform policy-makers, government, industry and wider society.

Current project streams:

- Cyberspace and the National Security of the United Kingdom
- Cyber Warfare: Action, Reaction and Reflection
- Cyber Crime

For further details, please visit www.chathamhouse.org.uk/research/security

Also available:

Cyberspace and the National Security of the United Kingdom: Threats and Responses
Paul Cornish, Rex Hughes and David Livingstone
A Chatham House Report, March 2009

This report provides a general overview of the problem of cyber security. The aim of the report is to inform debate and to make the case for a more coherent, comprehensive and anticipatory policy response, both nationally and internationally.

In every area, society is becoming increasingly dependent upon information and communications technology (ICT). With dependency come exposure and vulnerability to misuse, criminality and even attack. Criminals and extremists are able to take advantage of the same 'global technological commons' upon which society is becoming so dependent. Cyber security has become a fast-moving and complex security challenge, one which requires a coordinated, agile and mutually reinforcing response from all those who benefit from the global ICT infrastructure.

CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org.uk
F: +44 (0)20 7957 5710 www.chathamhouse.org.uk

Charity Registration Number: 208223