palgrave pivot

CYBER-WAR

The Anatomy of the Global Security Threat

Julian Richards

Cyber-War

DOI: 10.1057/9781137399625.0001

Also by Julian Richards

THE ART AND SCIENCE OF INTELLIGENCE ANALYSIS

A GUIDE TO NATIONAL SECURITY: THREATS, RESPONSES AND STRATEGIES

DOI: 10.1057/97811373996625.0001

palgrave pivot

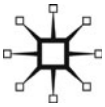
Cyber-War: The Anatomy of the Global Security Threat

Julian Richards

Co-Director, Centre for Security and Intelligence Studies, University of Buckingham, UK

palgrave
macmillan

DOI: 10.1057/9781137399625.0001



Softcover reprint of the hardcover 1st edition 2014 978-1-137-39961-8

First published 2014 by
PALGRAVE MACMILLAN

Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Palgrave Macmillan in the US is a division of St Martin's Press LLC, 175 Fifth Avenue, New York, NY 10010.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

Palgrave® and Macmillan® are registered trademarks in the United States, the United Kingdom, Europe and other countries.

ISBN: 978–1–137–39962–5 PDF

ISBN: 978–1–349–48584–0

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

A catalog record for this book is available from the Library of Congress.

www.palgrave.com/pivot

DOI: 10.1057/9781137399625

For my family

DOI: 10.1057/9781137399625.0001

Contents

DOI: 10.1057/9781137399625.0001

Preface

The accelerating rise of information and computer technology through the end of the twentieth century and into the beginning of the twenty-first century defies all superlatives. The first commercially available web browser – Netscape – only became available in 1994, and yet just 20 years later, the size, complexity and penetration of the internet and networked technologies into our daily lives has been astonishing.

With all technological revolutions, there is usually a dark side to accompany the new opportunities and positive stories. It is also the case that one of the first uses to which new technological innovations are put to use is in the military sphere. This is as true of information and computer technology as it has been of previous military revolutions, from the use of bows and arrows to the use of firearms. Particularly since the end of the Cold War, the notion of network-centric warfare and a new expression of information operations has pervaded discussion and research in defence.

There are, however, two problems with analysis of these developments. The first is that cyber technologies are an inherently technical realm, by definition. This means that considering the political, social and cultural implications of the cyber revolution has been somewhat hampered by the intense technical complexities of the subject. To make the technical and non-technical constituencies talk to, and understand, each other on this subject has sometimes proved difficult. The second problem is that much of the

DOI: 10.1057/9781137399625.0002

debate on the potential threat of cyber warfare has been imbued with the language of science fiction, rather than scientific fact.

There is a strong need, therefore, to cut through some of the myth and hyperbole surrounding the cyber debate, and to do so in terms that both technical and non-technical audiences can comprehend and appreciate in equal measure. I hope this book can make some contribution to advancing understanding and promoting informed debate in this field.

DOI: 10.1057/9781137399625.0002

1

Introduction: The Cyber Landscape

Abstract: *The opening chapter introduces the key debates in the sometimes confused realm of cyber security and cyber warfare. It identifies that a normative narrative is developing that the threat of major cyber warfare is a real and present danger. At the same time, a number of scholars cast doubt on the level and likelihood of the threat, not least because of legal ambiguities over what constitutes an act of war. Debate is complicated by the heavy involvement of military, security and commercial actors in the discussion. An argument is presented that, while cyber-related threats are present in and around modern warfare, the more catastrophic risks of attack may be unlikely at the present time.*

Richards, Julian. *Cyber-War: The Anatomy of the Global Security Threat*. Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399625.0003.

In November 2011, an event occurred in the normally peaceful location of Springfield, Illinois, which soon caused a considerable stir in the world's media. The story was triggered by the failure of a pump at a public water plant, which caused a number of homes in the Springfield area to find themselves without mains water. On investigation, the pump was found to have had a fault in which it had been turning itself off and on again inexplicably, eventually failing. Analysis of the fault traced the problem back to five months previously when evidence was discovered of traffic between a Russian internet protocol (IP) address and the Illinois plant's Supervisory Control and Data Acquisition (SCADA) system – essentially the plant's control network, which can be accessed in certain circumstances over the internet to effect remote controls. The fault in the pump seemed to have developed after this initially unidentified connection over the internet from Russia.

The story gained legs when a security commentator, Joe Weiss, who works for a commercial organisation advising utility companies in the US on how to protect themselves from cyber security threats, mentioned in a blog article that the FBI and Department for Homeland Security (DHS) had been investigating the incident and viewed it as a suspicious cyber attack emanating from Russia.

This was enough for media outlets across the world to pick up the story and present it as one of the first verified examples of cyber techniques being used to attack and disable civilian utility networks. Some of the less circumspect news organisations were unequivocal in their analysis. This was clearly an attack by "Russian cyber criminals", and represented a worrying precedent. When a DHS spokesman said there was no apparent threat to the integrity of public utilities or to public safety, an anonymous online hacker disagreed and claimed to have hacked into the SCADA network of a second public utility in South Houston, Texas.[1]

The problem with the story, as was reported reasonably widely a few weeks later, albeit with slightly less attention, was that its whole premise turned out to be erroneous. A contractor at the Illinois plant in question, Jim Mimlitz, revealed that he had watched the hacking story unfold with incredulity. He explained that the origin of the original online traffic from Russia to the water plant's network was himself. While holidaying in Russia, Mimlitz had been asked to check something at the plant and had done so over an internet connection, inadvertently causing the fault.[2]

DOI: 10.1057/9781137399625.0003

The mystery was solved, but the incident, and more importantly the way in which it had been reported, said a great deal about the way in which potentially destructive cyber attacks are conceptualised and articulated in Western national security discourse.

A couple of years prior to the Illinois incident, the President of the United States, Barack Obama, had delivered an address at the White House on the question of "securing our nation's infrastructure". He painted a bleak picture about the cyber security threats that were emerging, and the need to establish a sound strategy to mitigate them. One of the particularly interesting assertions he made, on which the cyber security expert Kenneth Geers picked up, was that cyber attackers "have plunged entire cities into darkness".[3] This was a bold statement: not only did cyber attackers have the capability to probe and interfere with public utilities, but they had actually carried out attacks which had affected entire cities. This is important because it means the threat is not just theoretical or apocryphal, as many of the critics of the cyber security debate would argue, but is proven and present with us today, if the president is to be believed. If we were to adopt a constructivist security perspective on this situation, we could say that President Obama's words were a classic securitizing "speech act"[4] that elevated a particular threat to a higher plane and thus justified extraordinary national security expenditure and action.

Again, however, further analysis reveals that the claims are based on less-than-solid foundations. It appears that the specific episodes to which President Obama referred had occurred in Brazil in the state of Espirito Santo in 2007 and in Rio de Janeiro in 2005. Here, widespread urban electricity failures had been blamed by many media outlets on cyber attackers hacking into Brazilian utility networks. A few months after President Obama's address, in November 2009, Brazil experienced a further wave of power blackouts in a number of urban centres, and these were also blamed on hackers. By coincidence, these latest problems had occurred just a few days after a CBS *60 Minutes* television report had been aired in the US, which had made the connection between the Brazilian power outages and cyber attackers, citing unnamed sources.[5] However, it is reported that the Brazilian energy ministry chief of staff, José Coimbra, had claimed that investigations had pinpointed the earlier outages as being due to short circuits on certain high-voltage lines in the Sao Paulo area. Meanwhile, the then director of Homeland Security Information and Security in Brazil, Mandarino, revealed that there had

DOI: 10.1057/9781137399625.0003

indeed been cyber intrusions into the energy company's networks in 2005 from criminals making an attempt at extortion. The attack had caused a minor loss of data from an administrative computer and had been quickly resolved. There was widespread debate in the Brazilian government which had come to the conclusion that the two incidents were not connected, and that the power outages could not have been caused by cyber attacks.[6]

The Illinois story had broken about a year after the effects of the Stuxnet attacks in Iran had been revealed (which is discussed later). Stuxnet has been described by many analysts as the first real military-grade cyber weapon worthy of the name.[7] These stories illustrate a number of important facets of the debates around cyber security and cyber warfare in the second decade of the twenty-first century. Firstly, there is clearly a high degree of anxiety and discomfort about the possibility of major cyber attacks on critical infrastructure and the level of effect they could have on civilian populations. Such attacks are considered to be the weapons and techniques that would be used in a full-scale cyber war, or substantial cyber terrorist attack. This anxiety appears to be causing a tendency to leap on incidents before full analysis has been made, and to herald them as examples of destructive cyber capability being put into action. The commentators making these connections and assertions vary from media outlets to cyber security industry "experts", and sometimes all the way up to political leaders at the highest level of influence.

At the same time, it is clear that the veracity of the claims and the scoping of these threats are, at the time of writing, subject to a high degree of ambiguity and confusion. Incidents which are heralded as attacks are often found to be either not attacks at all or to have so much doubt and obscurity around them as to be highly dubious affairs about which very little can be said with any certainty.

These are the issues at the heart of the debate on cyber war which this book aims to explore. It does so by identifying and unravelling two spectra at the heart of the contemporary narrative on cyber war. First is the spectrum of cyber threats in which the potential of cyber war is found. This is important as "cyber" has become something of an all-pervasive term which can be applied to almost any human endeavour. Outside of the security-threat environment we might now talk about cyber bullying, cyber romance, cybernetics, and a mysterious realm called cyber space, to name but a few. The origins of the "cyber" label can be traced to ancient Greek. One of the first writers to use the term extensively was

DOI: 10.1057/9781137399625.0003

Norman Wiener, whose 1948 book *Cybernetics* explored the potential connection between animals and machines.[8] In the security sphere, much as it is semantically possible to have a "war" on just about anything (obesity, drugs, cancer) so can all threats have a potentially cyber dimension to them, now that we live in an inexorably networked world. Thus, cyber security means security against a range of threats including crime, espionage, vandalism, activism, and terrorism, as well as actual war and warfare-related activities.

Cyber war is very much at the extreme end of the cyber security-threat environment, much as is the case with traditional war and conflict. One of the key questions about cyber security is how we prioritise the range of threats, in the traditional risk-assessment sense of calculating both likelihood and impact. It may be the case, for example, that an act of war using cyber mechanisms is unlikely, and would not be very damaging if it were to happen. (Indeed, as I will discuss, it could even be seen as strangely virtuous in some circumstances.) At the same time, cyber crime such as online fraud or credit card skimming is probably a much more immediate and serious threat at the present time. Perhaps we should not be worrying so much about cities going dark and planes falling out of the sky, and direct more of our attention at fairly low-level and routine online fraud. For these reasons, this book will consider the question of cyber war very much within the wider context of cyber threats and cyber security across the spectrum.

The second key spectrum in the cyber war debate is that covering the range of views about how much of a threat cyber war really is, and how damaging it could be. This book will aim to uncover and discuss the range of views being put forward, and the relevant merits of each. At one end of the spectrum are the Cassandrist doom-mongers, who will say that the threat of cyber war is not only very real but is happening today, whether it is in the shape of electricity or water plants being disrupted, or computer worms knocking out nuclear weapons facilities. In 1993, Arquilla and Ronfeldt warned us that cyber war was coming.[9] Just over 15 years later, a former director of the National Security Agency (NSA), Mike McConnell, told us that it had arrived, and we were losing.[10]

At the other end of the spectrum there is a range of critical commentators who cast doubt over such assertions. These cover a breadth of views, from those who say that activities that could reasonably be called cyber war will never be seen (as Thomas Rid argues[11]) to those who do not necessarily rule it out completely in the future but claim

DOI: 10.1057/9781137399625.0003

that it has not arrived yet (such as George Lucas Jr.[12]). The reasons for such analysts taking critical views will vary from those noting, as do the opening paragraphs of this book, that there is some degree of hyperbole over recent events that have been equated with cyber war and we need to be more careful about ascribing such a label to these events; to those who frame their critique in terms of a conspiracy theory, suggesting that the military–industrial complex has good reason to exaggerate the threat of cyber war since it will lead to a number of very lucrative defence contracts and the chance to exercise dominant power over weaker nations.

The author is not a great advocate of conspiracy theories, but this book will take something of a critical view about the threat of cyber war. I will suggest that, while we cannot rule out the possibility of cyber war in the future – since it is impossible to predict the future and the march of technology makes it even more so – there has to be a great deal of doubt about labelling any attacks we have seen hitherto as acts of war. Unfounded anxiety or even intellectual curiosity about the possibilities of cyber war should not be allowed to drive the political agenda in this area.

Of course, all of this depends partly on how we define cyber war. This is another task that this book will aim to tackle. There are various ways to approach the question. Again, the cyber term is quite pervasive, like a sort of virus itself. At one level, the cyber realm has merely offered new technological expressions for existing elements of warfare, as it has for other threat dimensions such as crime and espionage. The sixth century BC statements of Sun Tzu about the importance of activities "other than war", and particularly his statement that "all warfare is based on deception",[13] suggest that techniques such as denial and deception, psychological operations and propaganda have been central to warfare for a very long time. New cyber capabilities merely extend the opportunities and techniques for practising such techniques against an enemy. The manner in which the Israeli military purportedly altered the output from Syrian air defence equipment in their 2007 raid on the Dayr-Ez Zor nuclear reactor[14] is perhaps a modern example of the sorts of deception operations seen in the past, such as Operation Fortitude in the Second World War. Similarly, the Russian cyber attacks against Georgia prior to invasion of the country in 2008 could be seen as modern iterations of both sabotage and psychological operations that would have presaged and accompanied many military actions in history.

DOI: 10.1057/9781137399625.0003

So, cyber capabilities can accompany, enable and enhance existing activities that together constitute acts of war and conflict, but can they actually be used to directly commit acts of war themselves? This, of course, depends on definitions. The first reference point is probably Article 2(4) of the United Nations (UN) charter, which stipulates that nations should refrain from the threat or use of force against other sovereign nations. However, Article 51 provides a loophole in which nations are given the right of individual or collective self-defence in the face of armed attack. The question is how we define "force", and whether this could be said to apply to the sorts of cyber attacks we have seen so far. As Waxman points out, the United States and its allies have generally considered force and self-defence under the UN charter to apply to military attacks or armed violence.[15] Thus, a missile attack against an Iranian nuclear facility would be an act of force and would allow the Iranians to use violent force in response (unless, of course, it could be argued that the original attack was in self-defence). But the Stuxnet attacks, which did not actually kill or injure anyone or cause significant damage to property, could not be classified in these terms.

These factors mean that there are important lacunae in international treaties and laws at present which cause ambiguity over both defensive and offensive cyber activities. NATO is one of the organisations that has grappled with this dilemma in recent years, particularly after one of its members, Estonia, came under a sustained and highly disruptive cyber attack in the midst of a dispute with Russia during 2007. The US has urged the alliance to consider cyber attacks on member states as akin to military attacks, necessitating collective response upto and including military action.[16] Meanwhile, the former NATO Deputy Assistant Secretary General, Jamie Shea, sees it as a "powerful political signal", that NATO should consider cyber attacks as "just as unacceptable as an attack by tanks or aircraft".[17] These are, of course, tricky statements to make, since they could be seen as necessitating a military response by a NATO member were there to be another attack like that on Estonia (which, like Stuxnet, did not actually cause any death or physical destruction). This could in turn ratchet up international diplomatic temperatures.

These areas of ambiguity relate to a range of legal and ethical issues about the evolving cyber capability in many nations. Questions of what constitutes military force, and what would be a reasonable act of self-defence, are, in a sense, just the beginning of the story. There are also questions of what would be permissible or indeed ethical under

DOI: 10.1057/9781137399625.0003

international laws and norms in such areas as pre-emptive and defensive cyber attack operations, or espionage. As with other areas of international law and regulation around military capabilities such as nuclear, chemical and biological weapons, there is something of a deadly embrace in this area for nations to disentangle. Nowhere is this question more complex than in the US. Here, a very high level of network dependency both in civil and military spheres means that the US is extraordinarily anxious about its vulnerability to cyber attack. In this way, strength suddenly becomes a great weakness in the face of unconventional and asymmetric war, particularly when faced with an adversary who offers much less network vulnerability, such as North Korea or China. This almost certainly drives the slightly panicky responses to attacks with which we opened this book.

There is therefore a strong impetus for the US to press hard for international treaties, obligations and "rules of the road" in the emerging domain of cyber warfare. At the very least, this could allow the US to respond with force were such recognised international treaties transgressed. At the same time, however, there are two problems. Firstly, international treaties are not always observed in equal measure. As Clarke and Knake point out, the Nuclear Non-Proliferation Treaty (NPT) and other conventions on weapons of mass destruction did not prevent a number of signatories from continuing to develop and proliferate such technologies.[18] (Others merely refused to sign.) So for the US or any of its allies to sign and observe such treaties could merely mean they tied their own hands behind their backs while others forged merrily ahead. Secondly, the US and its allies wish to develop and retain large and effective cyber capabilities themselves and to be able to do unto others as they would have done unto them, whether that is in the shape of espionage or preventative cyber attacks. We do not yet know who unleashed the Stuxnet malware on the Iranians, for example, and we may never know, but it would not be beyond the bounds of possibility to consider that it might have been Israel, with or without the help of the US. In this sense, the liberal and unregulated nature of the cyber warfare domain is not necessarily an entirely bad thing for such nations.

All of the examples of possible cyber attack we have mentioned so far involve state-on-state conflicts and disputes. Of course, when we consider the possibility of cyber terrorism in the contemporary era, we are generally referring to sub-state groups such as Al Qaeda and its various regional affiliates. There has been much debate around whether the

DOI: 10.1057/9781137399625.0003

likes of Al Qaeda will attempt to co-opt cyber attack into their arsenal. It is certainly the case that individuals with highly developed information technology (IT) skills have been seen working for such terrorist organisations. The case of Younis Tsouli is an indicative one. Tsouli was a young computer expert who presented himself to Al Qaeda in password-protected jihadist forums in the early stages of the Iraq war. In the ensuing months, he became a critical webmaster for Al Qaeda, ensuring they could stay one step ahead of Western intelligence agencies in posting videos and messages extolling the cause of Al Qaeda in Iraq on the internet.[19]

At the same time, Tsouli's story supports the views of another sceptic in the cyber war debate, James Lewis, who points out that terrorist organisations such as Al Qaeda have so far shown interest in information technology only from the point of view of propaganda, radicalisation and recruitment, and fund-raising. They have not really shown much interest in using the internet as a direct weapon to inflict physical or psychological damage on their targets.[20] Indeed, many recent terrorist outrages by groups affiliated to Al Qaeda have stuck to tried-and-tested conventional methods of bombing and shooting. It may be the case that there are two reasons why Al Qaeda and similar terrorist organisations may not undertake destructive cyber attacks on infrastructure in the foreseeable future. Firstly, the effects of cyber attacks are often less visible and terrifying than the effects of explosions and killings using conventional ordinance. (Use of unconventional weapons such as chemical or biological weapons may be more attractive.) Terrorists are in the game of conducting symbolic acts of extreme violence to terrorise and influence audiences. A cyber attack which, as Lewis notes, might not even be noticed as being an attack[21] is hardly terrifying in quite the same way. Secondly, a major cyber attack on a national infrastructure that was large enough to cause serious disruption and damage, and large enough to be noticed and understood by its intended audience, is a difficult thing to do. It requires considerable resources and expertise, and is becoming harder to conduct with each passing day as cyber security on networks improves. It may be the case that only well-resourced states with large numbers of personnel dedicated to cyber operations are able to undertake such attacks. This means we are in the realm of state-on-state war rather than terrorism or other types of threat, when we consider major cyber attacks. Cyber terrorism may remain, at least for the moment, in the area of information warfare and psychological operations.

DOI: 10.1057/9781137399625.0003

In the failure of the Illinois water plant with which we opened this chapter, we saw how anxiety over the possibility of a cyber attack against infrastructure quickly caused the finger to be pointed at Russia (in this case at "cyber criminals" rather than necessarily at the state). Russia has often been invoked by the West as one of the key bogeymen in the rise of strategic cyber threats, as has China. This has happened very much at the level of high diplomacy, reiterating the importance of securitizing speech acts by key officials. During the same year as the Illinois water plant incident, despite reluctance by some officials to openly point the finger of blame at Russia and China, a former UK security minister and adviser to the Prime Minister, Baroness Neville-Jones, said that the Russian and Chinese governments were "certainly" at the forefront of a wave of cyber attacks and infiltrations on British governmental networks.[22] In March 2013, President Obama's national security adviser, Tom Donilon, was much more specific and robust in his condemnation of an "unprecedented wave" of cyber attacks on US official and private networks sponsored by the Chinese government, and issued a warning that a failure to address such attacks were becoming a point of major diplomatic difficulty between the US and China.[23] The statement came a month after the publication of a report by the cyber security consultancy, Mandiant, which claimed to have identified a specific building in Shanghai, owned by the People's Liberation Army (PLA), from which a massive wave of cyber attack and espionage primarily directed at the West was being directed on a daily basis.[24]

Many of the cyber warfare alarmists have made a doctrinal link between the 1999 publication *Unrestricted Warfare*, written by two senior PLA colonels,[25] and the clear work being undertaken in the Chinese military to build a large and effective cyber operations capability. This is sometimes interpreted by senior military officials to mean that China is preparing for a future cyber war with the US. Clarke and Knake present the logical thesis, emphasised by the asymmetric doctrine of *Unrestricted Warfare*, that a mismatch in conventional military capabilities between China/Russia and the US, which will take a long time to fill, could be mitigated by the use of cyber attack techniques against the highly networked and sophisticated US military.[26] The conventional gap could also be filled more quickly (as could the general gap in infrastructural development) if the likes of China were able to steal the latest intellectual property using cyber espionage rather than go through the laborious process of having to develop it themselves. Here again we see the

DOI: 10.1057/9781137399625.0003

particular anxiety in the US that its technological dominance could, in the wrong situation, become its greatest Achilles heel.

For its part, China has so far responded angrily to the repeated suggestions that it is behind a major wave of cyber attack and espionage on the West. It argues that, given the technical difficulties of pinpointing who is behind any particular cyber attack, and the ease with which attackers can obscure their origins (the "attribution problem" to which we will return later), the West's repeated and increasingly vociferous accusations against China are part of a lingering "Cold War mentality". This narrative, claim Chinese media sources, ties in with confrontation with China over Taiwan, strategic considerations generally in the Pacific region, and US economic protectionism over the rise of the Chinese economy and the penetration of the US market by Chinese companies such as Huawei and ZTE.[27]

The questions of which state players are involved in cyber warfare, present or future, and what this means for international diplomacy are explored further in Chapter 4. While much of the debate in this area is characterised in "new Cold War" terminology, there is also important state-centric cyber activity being undertaken in a number of other confrontations and conflicts, in the Middle East, the Korean peninsula and a number of other locations. In this way, we can again see that cyber activity is an adjunct to other political, diplomatic and indeed military activity.

One of the aims of this book is to present a big-picture analysis of the issues revolving around cyber threat and cyber war. This should be useful not only for those closely involved with cyber security and cyber operations, but for a much wider range of observers and analysts involved with understanding and commenting on contemporary security threats and policy formation. In many ways, this task is an extraordinarily difficult one in the cyber realm, and more so than might be the case in some other threat areas. One of the reasons for this is that conceptualising the cyber threat encompasses a wide spectrum of issues; from understanding modern conflict and security at the strategic level to understanding a set of intensely technical and specialised issues, the detail of which is often beyond the easy grasp of many outside of a small minority of technicians. This also means that a proper conceptualisation of the real threat is sometimes difficult to define and articulate. For those from a non-technical background, how does one explain what Stuxnet is exactly, and what is its potential power and destructive

DOI: 10.1057/9781137399625.0003

capability? This complicates the debate, and also carries a strategic risk. The risk is that debate and decision-making can be led, if not hijacked, by those with a deep technical understanding of the issues. This includes commercial IT consultancies and organisations who themselves have a financial interest in suggesting that the threat is sufficiently large and immediate and that their cyber security products and expertise must be purchased without delay. Again, the author is not hinting at some sort of grand conspiracy in which we are all being duped by the IT companies. But it is the case with debate on cyber security that – unusually within security studies – a great deal of the analysis and discourse originates from commercial organisations with a role in selling solutions to the problem. There is a strong need for objective and careful analysis of this very complex and fast-evolving area. Many of the cyber security companies themselves absolutely understand this need, and many have provided admirably well-researched and objective assessments of the situation. I hope that this book will contribute to that understanding in this very complex area.

Notes

1 *Daily Mail* (21 November 2011) "'Russian' Hackers Seize Control of US Public Water System by Remotely Destroying Pump".
2 *State Journal Register*, Springfield, Illinois (2 December 2011) "Vacationing Contractor Talks about 'Cyber Attack' that Wasn't".
3 K. Geers (2011) *Strategic Cyber Security* (Tallinn: CCD COE), p. 13.
4 B. Buzan, O. Waever and J. De Wilde (1998) *Security: A New Framework for Analysis* (London: Lynne Riener), pp. 25–6.
5 M. Mylrea (15 November 2009) "Brazil's Next Battlefield: Cyberspace", *Foreign Policy Journal*, http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/, data accessed 18 November 2013.
6 M. Soares (12 June 2010) "WikiLeaked Cable Says 2009 Brazilian Blackout Wasn't Hackers, Either", *Wired*, http://www.wired.com/threatlevel/2010/12/brazil-blackout/, date accessed 10 November 2013.
7 See for example R. Langner (2011) "Stuxnet: Dissecting a Cyberwarfare Weapon", *IEEE Security and Privacy* 9/3, 49–51.
8 A. Hodges (1992) *Alan Turing: The Enigma* (London: Vintage), p. 403.
9 J. Arquilla and D. Ronfeldt (1993) "Cyberwar Is Coming!", *Comparative Strategy* 12/2, 141–65.

DOI: 10.1057/9781137399625.0003

10 M. McConnell (28 February 2010) "How to Win the Cyber-War We're Losing", *The Washington Post.*
11 T. Rid (2013) *Cyber War Will Not Take Place* (London: Hurst and Co).
12 George Lucas, "Permissable, Preventative Cyber War", Presentation at the Oxford Institute for Ethics, Law and Armed Conflict, Oxford, 23 November 2011.
13 S.B. Griffith (1971) *Sun Tzu: The Art of War* (Oxford: Oxford University Press).
14 R.A. Clarke and R.K. Knake (2010) *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins), p. 5.
15 M.C. Waxman (2011) "Cyber-Attacks and the Use of Force", *The Yale Journal of International Law* 36, 427–8.
16 NATO (20 September 2011) '*NATO Chronicles: Fighting the Invisible Enemy*', NATO Channel TV.
17 NATO, *NATO Chronicles.*
18 Clarke and Knake, *Cyber War*, p. 222.
19 J. Richards (2010) *The Art and Science of Intelligence Analysis* (Oxford: Oxford University Press), pp. 60–1.
20 J.A. Lewis (2012) *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. (Washington DC: Center for Strategic and International Studies (CSIS)), p. 8.
21 Lewis, *Assessing the Risks.*
22 K. Rawlinson (1 November 2011) "China and Russia Accused of Orchestrating Cyber Attacks", *The Independent.*
23 J. Swaine and R. Sanchez (11 March 2013) "China Must Stop 'Unprecedented Wave of Cyber Attacks', Says Obama Administration", *The Telegraph.*
24 Mandiant (2013) *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria VA: Mandiant).
25 Q. Liang and X. Wang (1999) *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House).
26 Clarke and Knake, *Cyber War*, p. 53.
27 M. Macdonald (8 October 2012) "China Slams 'Cold War Mentality' in US report", *International Herald Tribune.*

DOI: 10.1057/9781137399625.0003

2
Cyber and the Changing Nature of Conflict

Abstract: *This chapter examines the debates around the changing nature of conflict, and the manner in which the cyber element has been presented as a new revolution in military affairs. The analysis notes how conflict has evolved and mutated under processes of globalisation, particularly since the end of the Cold War, whereby asymmetric tactics and strategies are increasingly the norm. Cyber methodologies have the potential to represent the archetypal modern asymmetric technique, especially when wielded against a highly networked nation and military such as those of the US. The conclusion is that cyber has both offered modern ways of conducting old activities (such as information operations) and, at the same time, offered the potential for wholly new ways of conducting warfare in the future.*

Richards, Julian. *Cyber-War: The Anatomy of the Global Security Threat*. Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399625.0004.

DOI: 10.1057/9781137399625.0004

We noted in the previous chapter how military strategists and analysts, especially in the US, have thought about potential future conflicts with the likes of China or North Korea by thinking about how relative network and cyber capabilities and vulnerabilities between the two sides in the conflict could be a decisive factor. Clarke and Knake interpret Liang and Wang's 1999 publication *Unrestricted Warfare* as "a blueprint for how weaker countries can outmanoeuvre status quo powers using weapons and tactics that fall outside the traditional military spectrum".[1] In the menu of available tactics, cyber attack against the highly networked infrastructures of status quo powers looms large. Here, then, it is suggested that we have a modern manifestation of "activities other than war", to which the cyber realm has offered potentially devastating new possibilities. (As Sun Tzu is reputed to have said, it is better to conquer the enemy without fighting.)

Whether Liang and Wang's book really does constitute an official military doctrine is a highly moot point, but the debate does highlight the manner in which notions of asymmetric warfare have increasingly permeated thinking and discussion about conflict in the post–Cold War era. These issues are challenging traditional notions of not only the nature of armed conflict on the battlefield, but, to a certain extent, of the significance and strength of the traditional Westphalian nation-state and its ability to control power and offer security within national borders. In this context, there has been much debate and analysis about the changing nature of conflict in the modern era, and the cyber dimension is becoming a very important part of this debate.

A recent major study of the future character of conflict by the UK Ministry of Defence's (MOD) Development Concepts and Doctrine Centre (DCDC) noted how contemporary conflicts were "transcending our conventional understanding of what equates to irregular and regular military activity".[2] The "conflict paradigm" was shifting, and Western powers need to adapt their military postures accordingly if they were not to lose advantage significantly on the battlefield.[3]

The thinking grows out of experience of major post–Cold War conflicts in which Western powers have been involved, such as those in the Balkans, Iraq and Afghanistan, not to mention smaller engagements such as that in Somalia in 1993. To a certain extent, the West has been surprised that it would be involved in such conflicts at all following the collapse of the Soviet Union, since that event could reasonably have been predicted to have negated the need for major Clausewitzian armies

DOI: 10.1057/9781137399625.0004

facing one another on the battlefield. Ripsman and Paul noted the theory at this time that a greater interconnectedness in the post–Cold War world would radically reduce the instance of state-on-state conflicts in favour of low-intensity and internal conflicts.[4] The subsequent experience through the 1990s and into the twenty-first century has shown that the US and its Western allies remain, from time to time, engaged on the battlefield in largely traditional war-fighting form.[5]

The way in which such post–Cold War conflicts have been described has often centred around notions of "complexity". Adversaries seem to become spread across a spectrum, from state, to state-sponsored, to non-state groupings. Conventional (military) and unconventional threats (involving such issues as environmental and demographic stress) start to blur together, as do the range of threats, including proliferated WMDs, cyber, and "other novel and irregular threats".[6] Mackinlay describes an increasingly "crowded" battle-space, in which militaries find themselves rubbing shoulders with NGOs and private security companies, not to mention irregular insurgents and guerrilla forces, many of whom become increasingly indistinguishable from the general population.[7]

The picture may be a familiar one in the context of Iraq and Afghanistan after 2001, but much of the discussion about the contemporary changes to conflict date back to the concept of a Revolution in Military Affairs (RMA) that accompanied an earlier campaign in Iraq, in 1991. Here, for the first time, ultra high-tech military equipment could both deliver to the living room exciting pictures of ordinance hitting targets through 24-hour news channels, and also restrict casualties (at least on the coalition side) to historically miniscule proportions. In the 1991 Gulf campaign it is estimated that the Coalition forces suffered 240 battle deaths, of which 148 were US service men and women.[8] This compares to more than 47,000 US battle deaths during the nine years of the Vietnam conflict,[9] and represents an extraordinary change in the dangers of waging war over just 20 years of military development. It was clear that post–Cold War conflicts would be very different affairs: increasingly mechanised and surgical.

In addition to the essentially asymmetric character of such conflicts (in the sense that the US and its allies have access to much more technologically advanced equipment and munitions than their adversaries), an essential element of the new RMA is the dimension of information and network capability. Precision-guided weaponry and increasingly unmanned technology require a high level of real-time network capability

DOI: 10.1057/9781137399625.0004

on the battlefield to control and direct the equipment from behind the battle-lines. They also need to extract information from the field in terms of geolocational data and imagery, which allow rapid and near-real-time intelligence gathering and targeting in the tactical environment. Nider was among many proclaiming the arrival of "network-centric warfare" in such conflicts, in which "total information dominance" was proving to be one of the key factors.[10] In much more critical terms, Gregory outlined the dangers of such network-centric asymmetric conflicts in turning violent conflict into "a simulacrum of a video game",[11] characterised by network operators thousands of miles away from the battlefield directing lethal drone strikes through their computer terminals. Aside from the ethical issues of such separation of virtual representation from reality, there are the very real tactical issues about the consequences of near-real-time intelligence being wrong, as it can sometimes be.[12]

Much as there have been pivotal changes in society and technology which have affected the development of conflict in the past, many are seeing the effect of the Information Revolution that has unfolded since the latter part of the twentieth century as being part-and-parcel of the new RMA. Some have suggested that the possibilities presented for network-centric warfare are as significant a change to conflict as Napoleon's *levée en masse* at the end of the eighteenth century,[13] which ushered in the classic Clausewitzian era of warfare. While technology started to have a major impact on conflict in the First and Second World Wars, in terms of new radio communications technology and weapons systems such as aircraft, submarines, armoured vehicles and ballistics, the extraordinarily high casualty rates of both conflicts amongst military personnel attest to the fact that most of the fighting was still being done on the battlefield between opposing national armies, much as Napolean and his adversaries had been doing a century earlier.[14]

Information and computer technology (ICT), it is argued, is a technological revolution of fundamentally wider implications for conflict than those earlier technological advancements in the machinery of war. Much as the world of business has transformed with the advent of ICT, whereby speed and flexibility of action based on information advantage have become much more significant than traditional notions of developing and manufacturing products on industrialised production lines, so advanced militaries have realised that traditional wars of attrition can be adapted and sidestepped with speed of thought and action enabled by information dominance in and around the battle-space.[15] In a sense,

DOI: 10.1057/9781137399625.0004

this is the natural development – writ large – of events in history such as the Battle of Tannenberg in August 1914, in which the German army outflanked the Russian army and scored a decisive victory by intercepting unencrypted radio messages about troop deployments.[16]

Here, information dominance allowed a victory that was both swift and involved far fewer casualties than most of the battles that followed in the conflict. Today, network-centric warfare means using highly advanced networked military capabilities to achieve information dominance over the enemy by gathering and acting upon accurate intelligence in near-real time, to allow both rapid and highly targeted operations and to outflank disrupt or deceive before the battle can even take place. The conflict in Iraq in 1991 appeared to deliver on many of the promises of this new network-centric warfare, by demonstrating almost total information dominance over the enemy and thus conducting a campaign that was swift, comprehensive and involved far fewer battlefield casualties than had been the case in such conflicts previously. Twenty years later, the Deputy Secretary of Defense in the US, William Lynn Jr. III, noted that "information technology enables almost everything the US military does: logistical support and global command and control of forces, real-time provision of intelligence, and remote operations".[17]

For those protagonists on the wrong side of the asymmetric equation, however, having to face highly dominant and network-centric capabilities means there are two options, if they are to attempt to level the playing field. Firstly, such protagonists may wish to try to obtain such capabilities themselves. This means that technology such as the latest unmanned aerial vehicles (UAVs) and cybernetic technology become the key targets of contemporary industrial espionage. The blueprints for the latest UAV may be just as important now as were the details of the Manhattan Project in the early stages of the Cold War. Much of this key information will be sitting on the computer networks of departments of defence, and of the commercial contractors with whom they are increasingly working on developing the technologies. These become prime targets for cyber attack and cyber espionage.

Secondly, from a tactical point of view, we have already noted a slightly paradoxical anxiety in the West that accompanies information dominance. One's greatest strength could become one's greatest weakness if exploited successfully by the enemy. This means that highly network-dependent systems and capabilities could rapidly become useless lumps of metal if their command-and-control systems were neutralised

DOI: 10.1057/9781137399625.0004

or disrupted. Even worse, such systems could be turned against their owners if control networks could be hijacked. Much as is the case with panicky reports about utility infrastructures being attacked, there are occasional reports about instances in which network-centric capabilities may have been disrupted or compromised in the battle-space. The classic example is the as-yet unverified story that Hezbollah managed to hack into the control system of an Israeli unmanned "Shoval" drone in 2012, causing Israeli forces to shoot it down before it could be stolen or deployed against them.[18] As is the case with all such cyber-related stories, this has to be taken with extreme caution, even though it is being reported by many as fact. With that said, it is clear that adversaries finding themselves at the wrong end of the surveillance and targeting capabilities of such advanced technologies will have a strong interest in disrupting such technologies, and, indeed, in stealing the capability for themselves.

Such cyber attacks and counter-attacks on the command-and-control systems of advanced technologies, and indeed cyber espionage that aims to steal such technologies and capabilities, are a component of "information warfare". In the late 1990s, the former director of the US Department of Defense (DoD) Information System Security program, Robert Ayers, outlined his notion of information warfare and what this meant for the transformations in contemporary conflict.[19] Focusing on the way in which cyber capabilities could be used for espionage, disruption, and possibly to effect real-world physical damage to systems and infrastructure, the picture painted was very similar to that of the contemporary battlefield in an insurgency such as that in Afghanistan. With cyber attacks, the identity and location of the attacker is usually unclear, and it may often be the case that the attacker is not a formal member of an opposing army but a civilian. In short, the attacker does not wear a uniform. In terms of rules of engagement, there are none. With traditional warfare, the Geneva Conventions and other instruments of international law and regulation have determined what is and is not acceptable, and what does and does not constitute an attack. None of this applies to the cyber realm, where the definitions of cyber warfare have not yet been established, let alone the rules and regulations which should govern its practice.

On the question of where the battle-space is situated, it could be argued that potential cyber warfare demonstrates another parallel with the changing nature of contemporary conflict, specifically in relation

DOI: 10.1057/9781137399625.0004

to modern terrorism. This is the second option for adversaries finding themselves on the wrong side of the information dominance equation. In discussing the evolution of modern terrorism, David Rapoport's much-examined historical analysis notes how the aftermath of the First World War led to the rise of anti-colonial rebel movements in many territories that remained as mandates or direct colonial possessions.[20] What characterised many of these movements is that they felt compelled to use what we would now describe as guerrilla tactics, since they were faced with a much more powerful and well-equipped adversary in the shape of the colonial power. Hit-and-run attacks, and a propensity to hide weapons and attackers amongst the civilian population were key elements of the strategy. This period is the one in which the difficulty of defining a "terrorist" became most troublesome: the colonial authorities viewed such rebels who "played dirty" and did not obey the rules of traditional conflict as terrorists. For their supporters, however, such people were liberationists. Ultimately, the semantics do not really matter. The point is that such developments marked the confluence between asymmetric conflict and "terrorism" as a strategy.

In the contemporary world there is an argument that the very asymmetric nature of modern conflicts, in which one of the protagonists has an extraordinary degree of technological dominance, may be inadvertently fuelling the evolution of contemporary terrorism. The blueprint is perhaps the Mujahideen's resistance to the massive and very well-equipped Soviet invasion of Afghanistan in 1979. Like the Viet Cong in Vietnam a few years before, the Mujahideen demonstrated how asymmetric techniques, such as the use of guerrilla tactics and advantageous use of difficult terrains, could level the playing field with the mightiest and most technologically advanced adversary. In turn, rebel movements such as Al Qaeda have decided that another way to hit such adversaries is to take the conflict away from the battle-space altogether, and into other domains, such as civilian settings in the adversary's home country. In the face of unexpected and difficult-to-spot shock tactics in such domains, governments might find themselves under pressure from their civilian constituents, who are bearing the brunt of terrorist attacks. As the former UK Chief of Defence Staff, General Sir David Richards, observed, hi-tech weapons platforms that were characteristic of the Cold War era, such as aircraft carriers and nuclear submarines, are useless in the face of insurgent and terrorist foes armed with cheaply made, improvised explosive devices (IEDs) and Kalashnikov rifles.[21]

DOI: 10.1057/9781137399625.0004

Such experiences of contemporary terrorism feed into notions of how cyber warfare could evolve in the future. Again, the particular experience of modern terrorism in the US, including the fact of having suffered the single most shocking and destructive terrorist act in history, has probably influenced much of the debate. Notions of catastrophic asymmetric cyber attacks against civilian settings, plunging cities into darkness and causing planes to drop from the sky, may be born from an experience of terrorist attacks in civilian settings. At the same time, such anxiety may have deeper historical roots. Use of the term "digital Pearl Harbor" to describe a large cyber attack that, like the Japanese attack on the US Navy in 1941 which shocked a slumbering and complacent superpower into action, reflects a view held by many analysts in the US who believe that a major cyber attack on critical national infrastructure would be the only thing that would make the country wake up to the size and seriousness of the threat. Ayers describes a major exercise held at the US DoD in Spring 1995 (interestingly more than six years before the 9/11 attacks) called "Global 95", in which the possibility of a major cyber attack on US infrastructure was simulated to consider the potential implications.[22] His conclusion from the exercise was that the US government had no discernible strategy for how to span the gap between the public and private sectors in the task of protecting critical national infrastructure from major cyber attack.[23] Some years later, Clarke and Knake warn that the Obama administration is still beset with dangerous policy inertia on this same issue.[24]

What we see here is that, rather like the crowded and complex battlespace that has come to define at least some modern counter-insurgency conflicts, the manner in which cyber attacks could become a part of modern conflict is characterised by a complex overlapping of boundaries, actors and activities. The differences between traditional combatants and insurgents, terrorists or indeed members of the public, become extremely blurred and difficult to delineate in the cyber realm.

We have already discussed how NATO has grappled with these issues in defining its new Strategic Concept for a post–Cold War world. The new doctrine emerged from the NATO Lisbon Summit in November 2010. Described as NATO's "roadmap for the next ten years", the declaration reaffirmed the alliance's commitment to work together for collective Euro-Atlantic defence "in a changing world, against new threats, with new capabilities and new partners".[25] The Strategic Concept reaffirms the three core NATO objectives of collective defence, crisis management

DOI: 10.1057/9781137399625.0004

and cooperative security. While recognising the continued need for "conventional" military capabilities and risk-assessments (within which the nuclear deterrent is retained, for example), it also recognises the emergence of new security threats, in which cyber threats sit alongside those from terrorism, the proliferation of WMDs and environmental hazards. It is interesting how somewhat normative language is used about the cyber threat. The Strategic Concept notes that cyber attacks can now "reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability". Among others, "foreign militaries and intelligence services" can purportedly be the authors of such attacks.[26] This latter may point to a near-certainty in Western governments, as we have discussed already that actors such as the PLA in China are behind a large proportion of the attacks that have been seen on their networks. The logic of the new NATO Strategic Concept may be sound, but, arguably, the somewhat definitive nature of its language may be premature.

Nevertheless, if the changes in society wrought by the information revolution at the end of the twentieth century are leading to a concomitant change in military conflict, whether we describe that as network-centric warfare, information warfare, or cyber war, how is it to be characterised? One mechanism that could be used is to step back slightly and think about the notion of "power", which is central to conflict in terms of power-projection and balancing. The originator of the notion of "soft" power, Joseph Nye, has considered this question. The first thing to note is Nye's assertion that cyber power is different from and offers new possibilities over and above traditional notions of having information advantage in conflict,[27] the basic essence of which goes all the way back to Sun Tzu and probably to the birth of human conflict. The first conception of significance here is the characterisation of "domains" in military capability and conflict. The former US Deputy Secretary of Defense, William J. Lynn III, was among many in describing cyberspace as the new "5th domain" alongside land, sea, air and space. The Pentagon's formal recognition of this new domain has led to the creation of Cyber Command, to sit alongside various regional military commands.[28]

Of course, cyberspace is fundamentally different in important respects from those other domains. In addition to its virtual rather than physical nature, it demonstrates an ability to capitalise on new technological developments with unprecedented rapidity and geographical reach. Developing dominance or effectiveness in physical realms is beyond most sub-state actors, and, indeed, beyond most state actors at present

DOI: 10.1057/9781137399625.0004

in the face of the US's power hegemony. (As we have seen, this may lead to a strategy of guerrilla warfare and "terrorism" by sub-state actors; and industrial-scale espionage for aspiring strong state actors.) With cyber power, however, access to the right technical capability can enable rapid, cheap and highly effective deployment against dominant powers.[29] In a sense, it is potentially the archetypal asymmetric tool for modern conflict.

In this way, the ephemeral nature of cyberspace means that notions of cyber war may be fundamentally different from traditional notions of conflict, and thus require a completely different frame of reference. We have already noted how the "cyber" prefix is somewhat pervasive and viral, and tends to span all areas of activity in a way that defies categorisation. This leads us to a notion of cyber warfare as comprising a set of different activities that apply in different ways to conflict in different situations. One way to look at it might be to break it down into three categories.

First is the category of Information Warfare. I would argue that this activity is actually a continuation of activities with long histories in human endeavour and conflict. Since the birth of time, information has been used in conflict both defensively (in the sense of gathering accurate intelligence on an adversary that can allow for counter-strategies) and offensively (in the sense of actively deceiving, disrupting or outflanking an enemy). These sorts of activities have been described in the past as a variety of things, including information operations, psychological operations or denial and deception operations. In all of these cases, information is central and new cyber technologies merely allow new mechanisms for extracting, propagating and manipulating information around the context of a conflict.

The second category is that of cyber attacks and operations which *enable* physical conflict on the ground. Again, this is essentially a component of some of the traditional element of information warfare with longer histories, dating back at least to the advent of new communications technologies and their use in war at the beginning of the twentieth century. Disruptive operations such as the jamming of the German *Knickebein* radar signals, or the activities of the "Ferret" aircraft in South-East Asia during the Second World War,[30] are essentially early corollaries of such events as the purported jamming of the Syrian air defences by the Israelis prior to their raid on a nuclear facility in 2007, or the apparent activities of the Russian military in information shaping and denial

DOI: 10.1057/9781137399625.0004

directed at the Georgian military and government prior to the conflict in 2008 (more on these incidents in the next chapter). With the greatly enhanced network centricity of modern militaries, cyber operations in these areas may encompass a much greater range of possibilities.

The final category is that of cyber attacks and operations which have an actual physical effect on the ground which could be described as an act of war. Here, I would argue, we may be into the realm of possibility rather than fact at this stage, since it is difficult to pinpoint any cyber attack so far that has caused actual death or destruction on the ground. Various scenarios can be imagined: the hacking into a control system for a fighter jet which causes it to crash, the disruptive hacking of a utility plant which causes it to fail in a physically destructive way, or the disruption of civilian transport or utilities which leads to death and destruction in the shape of traffic accidents, or even the breakdown of organised society. At the more dramatic end of this spectrum, critics such as Thomas Rid are certain that no such cyber attack has happened, nor is it likely to in the future.[31]

Note that, in this last category, there is a range of possibilities of destructive cyber attack that could take place both in the military realm (e.g an attack within the battle-space on a weapon system that affected the outcome of the conflict) and in the civilian sphere. As discussed, this reflects the modern asymmetric nature of conflict in which civilian spaces are sometimes made part of the battle-space with the intention of influencing the strategy of one of the state protagonists in the conflict. Nye uses a slightly different model to describe the range of possibilities of modern cyber war by delineating physical and virtual components of cyber power.[32] This fits with his conception of hard and soft power in the wider context. Thus, the Stuxnet attack on the SCADA network at the Natanz nuclear facility was a "physical" or "hard" cyber attack, since it had a physical effect in the real world. Information operations to sway public opinion would be a "soft" form of cyber operations. Similarly, the network itself could be the victim of both virtual and physical attacks. A denial of service attack on a military network would be an example of the former, while the bombing of communications networks or nodes would be a physical attack with the aim of affecting the information network of an adversary.

We can derive from this discussion a number of points. Firstly, we can only determine whether and how cyber war is a fundamentally

DOI: 10.1057/9781137399625.0004

new and revolutionary element of conflict, if we can define what it is. An initial analysis of cyber war seems to suggest that it is actually a number of different activities working in concert with one another. Some of these have long histories and doctrines, and it is the case that information technology is merely offering new ways of doing old things in the military realm. At the same time, there is no doubt that the rise of network centricity in modern militaries, accelerating through the end of the twentieth century, is effecting a big change in conflict in ways that could reasonably be described as revolutionary. This is happening in different ways. Firstly, the essentially uneven spread of these technologies and capabilities across state and sub-state actors in conflict is leading to an asymmetry which, in turn, is feeding into the waging of asymmetric conflict. There is a complex paradox here. Total information dominance by advanced militaries may be prompting asymmetric responses by adversaries, and one of those responses may be to target the very technology that is causing the asymmetry in the first place. In this way, cyber attacks could be a very attractive new weapon for conflict actors on the wrong side of the asymmetric equation, given the speed and simplicity of deploying such weapons, and the manner in which the network centricity of the dominant powers could become their greatest weakness, if targeted effectively. Thus, there are elements of cyber war which are certainly new, and which promise to continue to change modern conflict in very significant ways.

Notes

1 Clarke and Knake, *Cyber War*, p. 50.
2 MOD, DCDC (2010) *The Future Character of Conflict* (Bicester: DSDA Operations Centre), p. 1.
3 MOD, *The Future Character.*
4 N.M Ripsman and T.V. Paul (2010) *Globalization and the National Security State* (Oxford: Oxford University Press), p. 29.
5 Ripsman and Paul, *Globalization*, p. 55.
6 MOD, *The Future Character*, p. 6.
7 J. Mackinlay (2001) "Intervening in Conflict: The Policy Issues", *Conflict, Security and Development* 7/1, 175.
8 Imperial War Museum, http://www.iwm.org.uk/server/show/ConWebDoc.2480, date accessed 27 June 2011.

DOI: 10.1057/9781137399625.0004

9 A. Leland and M-J. Oboroceanu (2010) *American War and Military Operations Casualties: Lists and Statistics* (Washington DC: Congressional Research Service), p. 3.
10 S. Nider (21 May 2003) "Transformative Military Plan Vindicated in Iraq", *The Hill*, http://www.dlc.org/ndol_cif23c-2.html?kaid=85&subid=65&contentid=252695, date accessed 18 November 2013.
11 D. Gregory (2010) "War and Peace", *Transactions of the Institute of British Geographers* 35, 176.
12 W.G. Chapman (1996) *Organizational Concepts for the "Sensor-to-Shooter" World: The Impact of Real-Time Information on Air-Power Targeting* (School of Advanced Airpower Studies, Alabama), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA349387, date accessed 18 November 2013.
13 A.K. Cebrowski and J.J. Garstka (1998) "Network-Centric Warfare: Its Origin and Future", US Naval Institute, *Proceedings Magazine* 124/1/1.
14 At the same time, it is recognised that civilian casualties arising from these two conflicts were enormous also.
15 Cebtrowski and Gratska, "Network-Centric Warfare".
16 D. Kahn (2001) "An Historical Theory of Intelligence", *Intelligence and National Security* 16/3, 82
17 W.J. Lynn III (2010) "Defending a New Domain: The Pentagon's Cyerstrategy", *Foreign Affairs* 89/5, 98.
18 R. Silverstein (11 May 2013) "Advanced Israeli Drone Hijacked by Iran or Hezbollah, then Destroyed by Israel", *Tikun-Olam*, http://www.richardsilverstein.com/2013/05/11/advanced-israeli-drone-hijacked-by-unknown-hostile-party-then-destroyed-by-israel/, date accessed 18 November 2013.
19 R. Ayers (1999) "The New Threat: Information Warfare", *The RUSI Journal* 144/5: 23–7.
20 D. Rapoport (2002) "The Four Waves of Rebel Terror and September 11", *Anthropoetics* 8/1.
21 R. Norton-Taylor (18 January 2010) "UK Military Chiefs Clash Over Future Defence Strategy", *The Guardian*
22 Ayers, "The New Threat", p. 25.
23 Ayers, "The New Threat", p. 27.
24 Clarke and Knake, *Cyber War*, p. 261.
25 NATO (2010) *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, Adopted by Heads of State and Government in Lisbon: Active Engagement, Modern Defence*, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf, date accessed 16 September 2011.
26 NATO, *Strategic Concept*.

DOI: 10.1057/9781137399625.0004

27 Joseph S. Nye Jr. (2010) *Cyber Power* (Harvard Kennedy School: Belfer Center for Science and International Affairs), p. 3.
28 Lynn, "Defending a New Domain", p. 101.
29 Nye, *Cyber Power*, p. 4.
30 R.J Aldrich (2010) *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: HarperPress), p. 110.
31 Rid, *Cyber War Will Not Take Place*, p. 174.
32 Nye, *Cyber Power*, p. 5.

DOI: 10.1057/9781137399625.0004

3
Has Cyber War Happened?

Abstract: *One of the key questions in the debates around the likelihood and seriousness of the cyber warfare threat is whether any of the attacks we have seen in recent years constitute solid examples of cyber warfare. In this chapter, a number of much-analysed and discussed instances of conflict involving a cyber element are reviewed, from the 1980s to the present day. In this analysis, doubt is cast over whether any of these attacks really constitute acts of war in the traditional sense of the term. At the same time, the argument is reiterated that cyber activities in and around warfare and other conflicts are becoming increasingly present and increasingly significant. What the future holds in this area, it is argued, defies classification.*

Richards, Julian. *Cyber-War: The Anatomy of the Global Security Threat*. Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399625.0005.

DOI: 10.1057/9781137399625.0005

As we have seen, the question of whether anything that could equate to cyber war has yet been seen depends in large part on how we define the concept. In the last chapter I introduced a three-tiered framework for considering the notion of cyber war. First are elements that could be described as information operations, being conducted in and around a conflict. Second are activities that could be described as tactical-enabling activities associated with a conflict, that help one of the protagonists either defensively or offensively. Third are cyber-enabled attacks which have a direct destructive outcome in the real world.

In this chapter, I will look at a number of incidents that have been reported in varying degrees as being examples of modern cyber war, and consider them in the context of the above framework. I do not propose that these examples form a definitive list, but are merely some of the indicative episodes. Before examining these examples, it is worth recapping on some of the legal questions and definitions around the concept of war and armed force. I would argue that it is important to reprise these issues at this stage because cyber war is – and is not – something new in the context of the history of conflict. In some ways it offers unique new possibilities, while in others it is merely a continuation of activities that have been undertaken for a very long time.

Here, the main framework for analysis is the international Law of Armed Conflict (LOAC), as derived from a number of international treaties and conventions which govern both the acceptable conditions in which war can be undertaken (*jus ad bellum*) and the humanitarian and other conventions and norms which should govern its conduct (*jus in bello*). Of course, when we discuss international law and its applicability to states and actors within states, there is a flaw in the sense that the Vienna Convention on the Law of Treaties of 1969, whereby UN member states agreed to abide by international treaties and conventions by passing relevant aspects into their own domestic legislation, is not universally followed. There are a number of notable countries who have signed the Vienna Convention but not yet fully ratified it, including some interesting examples such as the US and Iran.[1] However, this is not the place to go into detail about the question of the applicability of international law, and for this analysis we will merely use its existing framework as a point of reference for considering potential acts of cyber warfare and their legal and political consequences.

Within the range of treaties and agreements, the Hague Conventions of 1907 and the various Geneva Conventions of 1949 loom large.

DOI: 10.1057/9781137399625.0005

Generally, analysts and commentators tend to focus on the elements of the UN charter which deal with the use of force and with conflict, and especially Article 2(4) which prohibits the "threat or use of force"; chapter VII which deals with "threats to peace" and "breaches of peace"; and Article 51 which allows for acts of self-defence in the face of force. We will return to this framework of international law and agreement, but for now it is worth stating that the collection of treaties which together broadly constitute international LOAC comprise three core principles: acts of war must be undertaken for reasons of military necessity; they must consider basic principles of humanity; and war must be conducted within a framework of chivalry between combatants.

In our first category of acts of cyber war are located those activities which, I am arguing, constitute modern iterations of "information operations". Here, a small cautionary note needs to be added regarding definitions. My intention is to consider this category in terms of a fairly broad spectrum of information-related activities. The term information operations is considered advisable here, if Schmitt is correct in his analysis that "information warfare" should really only be used to refer to specific combat-related information attacks on military infrastructure and communications, and not to more general operations which could happen in peacetime as much as during war.[2] Information warfare, in its more restricted definition, would include notions such as "netwar" and "network-centric warfare", which emerged as concepts particularly around the time of the Gulf conflict of 1991, and referred to combat operations in which information and network dominance and attack were operationally central. (These are more suited to our second category of acts that could be considered to be consistent with cyber war.) Within the broader category of information operations, however, which has a much longer history and has only recently evolved into cyber dimensions, there are a number of very interesting examples of how modern cyber warfare may be developing.

There are a number of recent instances in which cyber information operations have become important in and around traditional conflicts on the ground. The 2008 war between Russia and Georgia, which I will examine more closely below in the second category of cyber warfare activities, contained important elements of cyber-enabled information operations. Two slightly different examples, on which I will concentrate here, are the activities of Israel and Hezbollah in the Middle East, and

DOI: 10.1057/9781137399625.0005

the activities of the Syrian Electronic Army within the context of the civil war in Syria.

The case of Israel and Hezbollah is an interesting one in terms of the frameworks and categories we have presented so far. For a start, from the perspective of international law, Hezbollah is not a state actor as such (even if it receives some state patronage) and so cannot be directly party to UN conventions on *jus ad bellum* or *jus in bello*, as is the case with any number of sub-state insurgent or terrorist actors. (It may choose to observe such conventions, however, for reasons of establishing political legitimacy.) As we highlighted in the discussion on the ways in which conflict is changing in the twenty-first century, this is a wider issue that goes beyond the cyber dimension. Secondly, Israel and Hezbollah are not at war in the sense of a formally declared physical conflict (aside from a couple of episodes in history where this has been the case, most notably in 2006), but have mostly been engaged in a low-level war of words and attrition. Within this context, cyber-enabled information operations have played an important role.

In the long-running dispute between Israel and Hezbollah, narratives and information are critically important. Both sides wish to disseminate messages about the legitimacy of their cause and the justifications for their actions, weaving into the story narratives about land, history and security. Cyberspace has become an important field in which the battle of ideas can be played, and has been the place for attacks against each other's information channels, using such techniques as distributed denial of service (DDoS), defacement of websites, and even video games[3] and fully fledged television channels such as *Al-Manar*. As technology develops and changes, the information battle-space changes in tandem and becomes more complex in the sense that the boundaries between those activities carried out by militaries and governments and those carried out by skilled civilians and sympathisers become distinctly blurred.

In the context of more specific military activities and engagements, information becomes crucial. The conflict between Israel and Hezbollah is one that occasionally erupts into real conflict on the ground. One of the most significant recent events was the brief "July war" of 2006, in which Israel retaliated for the capture of some of its soldiers by Hezbollah by conducting a brief invasion of southern Lebanon to engage Hezbollah directly on the battlefield. The military significance of the conflict was relatively small since it did not redraw the map of the region nor lead to any significant shifting in wider political outcomes. The symbolic

DOI: 10.1057/9781137399625.0005

elements of the conflict and its outcome, however, tell a different story. As Saad, Baran and Varin noted, "in 2006, psychological impact was as significant as physical destruction".[4] Many of the messages that came out of the conflict were to do with the asymmetric nature of the situation in the region: the mighty Israel should have been able to wipe out the relatively small Hezbollah forces in southern Lebanon, but appeared to be unable to do so. Hezbollah managed to hang on and score some psychological victories, even if, as Israel claimed, its military capabilities were severely denuded in the process and it achieved very little. These were the narratives that both sides were trying to disseminate to the watching international communities.

The ongoing cyber conflict has manifested itself in a variety of ways. These have included carefully managed web dissemination, particularly of graphic images and stories during the 2006 conflict, to demonstrate the perfidy and savagery of either side. Malware, DDoS attacks and general hacking defacements of websites – both official and civil – by both sides has been a growing and important feature of the struggle. Israel has also taken more physical measures to interfere with the communications channels of Hezbollah, such as disrupting satellite signals in southern Lebanon allowing access to the web.[5] We have also seen more military-oriented cyber attacks – if they are to be verified – such as Hezbollah's alleged "hijacking" of an Israeli drone in 2012, described in the previous chapter. All of these actions comprise a complex combination of information operations and information warfare.

In the same region, the Arab uprisings that commenced in 2011 have had a variety of complex outcomes and effects, many of which are still in their very early stages at the time of writing. In Syria, a bitter civil war has seen a battle of ideas and information similar to that between Israel and Hezbollah, but in this case the battle is between the sitting government's version of events and that of the various rebel forces with whom it is battling. For students of politics and international relations, the manner in which the state news agency, the Syrian Arab News Agency (SANA), reports the situation in the country has been fascinating. One of the most notable elements of SANA's narrative has been its persistent attempts to characterise the uprising as terrorism and all the rebel forces arrayed against it as terrorists. In non-Syrian media, the same people are usually referred to as rebels or insurgents (although the Syrian picture is an extremely complex one and includes Al-Qaeda affiliated groups such as Jamiat Al-Nusrat, for whom the West also uses the term "terrorist").

DOI: 10.1057/9781137399625.0005

The battle of ideas and rhetoric with observers outside of the country has increasingly incorporated a significant element of cyber information operations. One of the key actors in this strand of the conflict has been an organisation calling itself the Syrian Electronic Army (SEA). This shadowy organisation, dubbed in the Western media as "Assad's cyber warriors", has undertaken hacks and attacks on the websites of major Western news organisations and on the social networking site Twitter. In the case of the latter, the SEA managed to hijack an account and spread a false rumour that President Obama had been killed in an explosion, causing multiple billions of dollars to be briefly wiped off stock markets until the story could be quashed.[6] At the same time, individuals supportive of the uprising against Assad have been waging their own cyber battle, uploading blogs and information to the web about the brutal activities of the Syrian military, much as Hezbollah is keen to do with the Israeli military's activities. It is not clear where any of these activists, on either side of the battle, are located, nor who is directing their activities. It is almost certainly the case that many of them are merely internet-savvy individuals with an axe to grind. What is certain is that all of their narratives and counter-narratives are contributing to the thickness of the fog of war, especially over such issues as the use of chemical weapons in the conflict.

These activities are classic information operations designed to sway the opinion of observers either to or from the official government narrative. As the conflict is being scrutinised so closely in the international community and could lead to punitive intervention, as has happened elsewhere in the region in recent times, the importance of the battle of narratives is extremely significant. With the SEA in particular, however, this battle has been much more active, international and indeed offensive than has been the case with similar conflicts before, and the enabling element of cyber capabilities and technologies appears to be a central factor in this regard. It is also the case that the degree of official government patronage and direction of the SEA is far from clear, and many of the protagonists may be just sympathetic individuals located in diverse parts of the global Syrian diaspora. The story of Syria has yet to be told since the conflict is still very much underway at the time of writing, but it is clear that the story will include a significant cyber dimension.

In the second category of incidents which could be described as cyber war are those which demonstrate a tactical-enabling facility relating to real conflict on the ground. Unlike information operations equating

DOI: 10.1057/9781137399625.0005

largely to propaganda and psychological operations, this is the area in which information warfare in its "netwar" iteration is more central. One of the most pertinent examples of such an incident would appear to be the manner in which Israel used cyber operations to facilitate an air-raid on the Dayr az-Zawr nuclear reactor in Syria in September 2007. Citing US intelligence sources, Fulghum, Wall and Butler claim that the raid was preceded by a combination of kinetic and cyber bombardment of an air defence facility on the Turkish border, which allowed Israeli jets to enter Syrian airspace unnoticed and carry out their raid on the reactor. The jamming of the air defence system purportedly included a combination of air-to-ground and computer-to-computer electronic attack on the relevant systems.[7] The audacity of the raid and its stunning success excited many observers, especially when before-and-after satellite pictures were released of the newly constructed facility being left as a shattered shell. Clarke and Knake ascribe high significance to this event in the discourse on cyber warfare, opening their 2010 book with a detailed and florid description of it. "Cyber warriors around the world ... were not surprised", they explain. "'This was how war would be fought in the information age, this was Cyber War."[8]

It is also tempting to look at an episode that happened almost a year later as another example of a conflict enabled tactically by cyber attack. The conflict in question is the brief but violent skirmish between Russia and Georgia that took place for a few days during August 2008. The conflict has generated much interest in the broader realm of politics and international relations, with some noting that it is one of the first examples of classic state-on-state conflict in the post–Cold War era.[9] It is also a conflict in which many observers have noted the significant – if not exactly decisive – cyber activity in and around the conflict.[10] In many ways the incident straddles our first two categories of cyber war, since it involved both information-shaping operations in terms of a battle of narratives for outside observers and direct tactical information warfare.

In the case of the former, a well-planned and coordinated information campaign strove to present the Russian incursion as a peacekeeping operation designed to protect ethnic Russians in South Ossetia from Georgian attack. President Saakishvili of Georgia, meanwhile, spent a great deal of time being interviewed and making statements for international media bemoaning unwarranted Russian aggression towards a smaller former member of the Soviet Union. In response, a wave of DDoS attacks using botnets and hacking attacks targeted key Georgian

DOI: 10.1057/9781137399625.0005

government websites and internet access points, restricting the Georgian government's ability to relay its messages to the outside world. On the tactical front, both kinetic strikes against information nodes and DDoS attacks on internet-based communications were effective in disrupting and delaying tactical military communications on both sides.[11]

Interestingly, while it is clear that many of the DDoS attacks on Georgia originated from servers in Russia, it also appears to be the case that many originated elsewhere. Very similar to the case of the SEA in Syria, therefore, a great deal of ambiguity still exists over how far official Russian government or military actors were directly responsible for the cyber attacks on Georgia, beyond possibly tacit support or encouragement.

This leads to mention of another incident involving Russia and its former Soviet neighbours, which has been subject to a great deal of scrutiny and debate in the context of cyber war. The incident in question is the wave of cyber attacks that the Estonian government suffered in the Spring of 2007 when a decision to move a historically significant statue of a Russian soldier in the city of Tallinn led to an outcry among the vocal ethnic Russian population in the small Baltic state. The moving of the statue caused some disturbance on the streets of Tallinn, but also led to a very considerable wave of cyber attacks against the websites of Estonian government ministries, banks and political parties. DDoS attacks against one bank in particular were estimated to have incurred losses of $1 million, and to have caused all credit card transactions and ATM withdrawals to be suspended for several days.[12] The Estonian government saw the incident as a very serious example of aggression from their Russian neighbour, and there was much debate on whether the attacks merited invoking NATO's Article V of collective defence. The incident probably did much to ensure that the new NATO Strategic Concept unveiled at the Lisbon Summit in 2010 included a substantial treatment of the potential seriousness of cyber attacks to member states.[13]

In the final analysis, the Estonia episode was a curious one for those predicting cyber war in that it was more of an act of rioting and activism than of war, in Thomas Rid's analysis, more of a cyber blockade than an attack.[14] This brings us to the third and ostensibly most serious of our categories of acts potentially constituting cyber war: namely those acts that cause actual death or destruction.

In some analyses, modern cyber war of a destructive nature is considered to have started rather early in the process, and indeed deep in the latter stages of the Cold War, before widely networked computers and

DOI: 10.1057/9781137399625.0005

the internet had really been established. The specific incident to which we are referring here is the sabotage of a trans-continental pipeline in Russia, purportedly engineered by the CIA in the early 1980s, which allegedly generated the largest non-nuclear explosion the world has seen to date.[15] The method of attack was interesting. It is suggested that a piece of malware was introduced by the CIA into the software controlling the valves at both ends of sections of the pipeline when they were in manufacture in a third country (in this case, in Canada). Once the Russians had bought and installed the equipment, it was designed to catastrophically fail at a certain point in the future.[16] This it purportedly did, in spectacular fashion, in the late summer of 1982.

The logic and plausibility of the operation are both sound, in that we know the CIA did make efforts to supply the Soviet Union with defective technology, to thwart their industrial progress, under a programme officially approved by President Reagan and revealed in 1982. A former US Air Force secretary who served in Reagan's National Security Council, Thomas C. Reed, describes these operations including the Siberian pipeline explosion in his book, published some years later.[17] However, there are grounds to be sceptical about the event, and certainly about whether – if it occurred at all – it was the result of a successful cyber attack or just an industrial accident. The Soviet Union suffered a number of such accidents, especially in its pipelines crossing the environmentally very extreme terrain of Siberia. Rid points out that a former KGB official who was based in the area of the alleged incident at the time has suggested that Thomas Reed could have mistaken the explosion for an event earlier in the same year on a pipeline in the region, which was caused by sections of pipe shifting in the semi-frozen tundra.[18]

On balance, the clear evidence for this case is not solid, especially in the light of the manner in which infrastructural events are often claimed to be cyber attacks, when they prove not to be. The availability of accurate news in a very closed society, as was the Soviet Union at the time, means that accurate contemporaneous reporting was not available. Leaving aside these problems, however, if the attack did happen in the way that has been alleged, then it would have fitted into our third category of cyber war activities, namely an attack that causes actual physical destruction in the real world (and could have killed people had they been in the wrong place at the time). From the perspective of the law, it could also be argued that this attack would have been in the category of sabotage, with some question as to whether it could have been claimed

DOI: 10.1057/9781137399625.0005

as an attack of military necessity. (Had the pipeline been crucial to the supply of offensive Soviet military forces, for example, then such a claim could be made.) Under LOAC, activities such as sabotage and espionage are not generally considered to be acts of war, although scale and degree of destructiveness must surely bring this into question in some cases.

If the pipeline attack happened in the way described, then the mode of delivery of the cyber attack may be very similar in essence to a later and much better-known attack, namely the Stuxnet attack on Iran's nuclear facility at Natanz. A great deal of analysis and commentary has been undertaken on this incident, which was discovered by the Iranians in 2010. Indeed, it is probably the most closely examined and discussed potential example of cyber warfare to date, and probably the only one potentially worthy of the name.

The story is now well known, but it is worth briefly recapping the details here. In 2010, the Stuxnet worm was found to have infected at least 60,000 computers worldwide. It was found to be an example of a "fire and forget" piece of malware which affects a very specific element of the control systems on Siemens systems, such as those used to operate centrifuges for enriching uranium at the highly secretive Natanz plant in Iran. While the worm was considered to be a very cleverly constructed example of a virus which was able to hide itself within machine code, for the most part if would have caused very little disruption to its unwitting hosts and defensive controls could quickly be put in place once it was discovered. In Natanz, however, the specific configuration of the uranium enrichment centrifuges lent itself perfectly to the full disruptive capability of the worm and it worked away in the background to eventually cause a large number of the centrifuges to fail. It is assumed that any alleged programme to develop weapons-grade uranium at the plant was subsequently set back seriously by the attack.[19]

One of the very interesting aspects of the Stuxnet worm is that it caused its biggest effect – in the Natanz plant – on a system that is scrupulously "air-gapped", that is, not connected to outside networks electronically. This means that the worm would have to be introduced physically into the plant's control system, either through a USB stick inserted into one of the computers (by an authorised member of staff or by an intruder) or, as we are led to believe was the case with the Siberian pipeline, introduced as a nascent feature of the Siemens computers purchased by the Iranians some time before the equipment was shipped out and installed in the plant. There is also a theory that a worker at the plant could have

DOI: 10.1057/9781137399625.0005

taken an office laptop home and used it to connect to the internet, inadvertently picking up the virus and then reintroducing it into the Natanz system when he returned to work.[20]

However it occurred, we can be much more certain that this attack actually happened, and the specific example of the malware in question has been closely examined subsequently by companies such as Symantec (who declared it to be unlike anything they had seen before).[21] In terms of categorisation, there have been some fairly superlative claims made about the Stuxnet worm and its significance. The German cybersecurity expert Ralph Langner was bold in his analysis, for example. Stuxnet represented "a turning point in the history of cyber security", and was "the first cyberwarfare weapon ever", he claimed.[22] Farwell and Rohozinski concurred by suggesting that the discovery of the attack means that, for cyber war, "the future is now".[23] Similar examples of malware, such as the "Flame" and "Duqu" viruses, have been noted subsequently and are believed to be later iterations of Stuxnet-type worms with ever-increasing destructive capabilities.

The reason Langner attributed such significance to the Stuxnet attack was that it had crossed a threshold from merely espionage or sabotage of information to causing physical damage in the real world:[24] it enabled an "attack" of physical force in the traditional sense of the term. In terms of our categorisation of attacks, this again falls into the third category, namely a cyber attack that aims to cause real physical damage and disruption rather than just enabling other operations. Interestingly, the attack happens in a context that is not one in which two or more states are at declared war, as such, leaving aside the fact that we do not know who actually launched the attack and whether the Iranian nuclear plant was indeed the prime intended target. (It is probably reasonable to assume it was given the effect that was wrought there.)

At the same time, caution is needed, if only to point out that this attack probably had much less physical destructive power and capability than is sometimes suggested. If the story is to be believed, the attack did cause the centrifuges to malfunction in a way that caused them physical damage. But we can assume that there was little or no widespread risk to people or property: there were no enormous explosions or collapsing of buildings. It is also a matter of conjecture as to how much damage and disruption to Iran's long-term aim of creating weapons-grade uranium was actually achieved by the attack. From a military perspective, it is interesting to compare the modality and

DOI: 10.1057/9781137399625.0005

utility of this attack with the 2007 Israeli attack on the Syrian nuclear facility, which used cyber capabilities to enable a much more destructive kinetic attack.

It is not claimed that all of the incidents described above constitute a definitive list of potential acts of cyber war, but merely some of the more publicised and analysed incidents to date. It is also the case that events will develop and unfold rapidly much as information technology is developing apace, and new possibilities for cyber war will be constantly emerging. Interestingly, many of the incidents above have been examined not for the specific damage that they caused but for the future potential that they demonstrated: almost as if these incidents represent dry runs for the watching cyber warriors. As Herzog said of the 2007 attacks in Estonia, while the effects of the attacks were more akin to a bad riot than to a military attack, they "served as a wake-up call to the world, as it became clear that potentially autonomous transnational networks – like unhappy pro-Kremlin 'hacktivists' – could avenge their grievances by digitally targeting and nearly crippling the critical infrastructure of technically sophisticated nation-states".[25] Here again we can see the anxiety about the paradoxical implications of a high degree of network connectivity in a society: Estonia is one of the most highly networked societies on earth, and this proved to be its very weakness in the 2007 incident. If the websites of government ministries and banks were the target here, who can say that attacks on more vital infrastructure could not be the target of the hackers tomorrow?

I have tried to frame the above incidents within a three-tiered categorisation comprising information operations, tactical-enabling operations, and attacks causing real-world death or destruction. In answering the question we have posed ourselves as to whether cyber war has yet happened, the results of this analysis are mixed. It is worth returning again to the legal debate over what constitutes an act of war. The UN charter uses the term "force", stipulating in Article 2(4) that it is prohibited. Western nations have generally taken this to mean traditional armed force rather than other types of coercion such as political or economic force, pointing out that both the preamble to the UN Charter and Article 44 talk more specifically about armed force and armed forces respectively. In 1974, the UN General Assembly further reiterated the principles of Article 2(4) by defining aggression in classically Westphalian terms, namely the "use of armed force by a state against the sovereignty, territorial integrity or political independence of another state".[26]

DOI: 10.1057/9781137399625.0005

Under this rubric, a cyber attack can only really be considered an act of war if it causes real-world death or destruction, and indeed is undertaken by one state against another. Similarly, a state could only take forceful retaliatory action if the above criteria were satisfied. As Farwell and Rohozinski point out, the Stuxnet attack could be claimed to be one on a militarily appropriate target (if, as is assumed, the Iranians are attempting to produce weapons-grade uranium at Natanz) and could even be characterised as a legitimate act of self-defence for states such as Israel, who may feel there is a valid and high-level military threat from Iran's development of a nuclear missile capability.[27] At the same time, the attack did not cause any death (as far as we know) or even widespread damage, and thus perhaps falls more into the category of sabotage rather than war. Acts of sabotage, espionage or other activities in the information operations category cannot really be said to be acts of war under the existing international LOAC.

Similarly, cyber acts are problematic when considered in the light of international LOAC in that many of them have probably involved non-state and non-military actors, with or without some degree of state patronage or support. In this sense, many of the attacks we have seen hitherto are perhaps better classified as cyber terrorism, activism or even vandalism rather than cyber war. With that said, this may be a problem as much for the nature of international law as for a question of how to deal with cyber attacks. The post-Westphalian world in which we live is one in which security threats have changed and mutated away from traditional categorisations and regulations.

We can conclude from this analysis that cyber attacks that have caused death or destruction, and thus could properly be classified as acts of war, have not yet happened at the time of writing, as far as we know. Importantly, however, it is clear that cyber activities are becoming an important part of the overall military strategy. This is particularly the case in terms of information operations before and during conflicts, and enabling information warfare activities in which communications infrastructures vital to the prosecution of a conflict are being attacked using both cyber and kinetic means. It is also my assessment that we cannot rule out truly destructive attacks undertaken through cyber means in the future, given the speed at which information technology is developing. The relatively low-level outcome of episodes such as those in Georgia, Estonia or Iran, for example, merely serve to show what might be possible on a much grander scale in the future. At the same time, we are not at that stage of development just yet and may not be for some time to come.

DOI: 10.1057/9781137399625.0005

Notes

1 Of course, I am not suggesting that a failure to ratify the Vienna Convention means that states ignore all aspects of international law, and, indeed, will often appeal to its provisions in negotiations within the UN.
2 M.N. Schmitt (1999) *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework* (Wright-Patterson AFB, OH: US Air Force, Institute for Information Technology), p. 7.
3 CNN (16 August 2007), "Hezbollah Video Game; War with Israel", http://edition.cnn.com/2007/WORLD/meast/08/16/hezbollah.game.reut/, date accessed 18 November 2013.
4 S. Saad, S. B. Bazan and C. Varin (2011) "Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a New Strategic Battlefield", *Proceedings of the WebSci conference 2011, Koblenz*, p. 2, http://journal.webscience.org/526/, date accessed 18 November 2013.
5 Saad, Bazan and Varin, "Asymmetric Cyber-warfare", p. 3.
6 L. Harding and C. Arthur (30 April 2013) "Syrian Electronic Army: Assad's Cyber Warriors", *The Guardian.*
7 D. A. Fulghum, R. Wall and A. Butler (2007) "Cyber Combat's First Shot: Attack on Syria Shows Israel Is Master of the High-Tech Battle", *Aviation Week and Space Technology* 167/21, 28.
8 Clarke and Knake, *Cyber War*, p. 6.
9 See for example: K.M. Campbell (2002) "Globalization's First War?", *The Washington Quarterly* 25/1, 5–14.
10 R.J. Deibert, R. Rohozinski and M. Crete-Nishihata (2012) "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War", *Security Dialogue* 43/1, 4.
11 Deibert, Rohozinski and Crete-Nishihata, "Cyclones in Cyberspace", p. 9.
12 S. Herzog (2011) 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', *Journal of Strategic Security* 4/2, 51–2.
13 See J. Richards (2012) *A Guide to National Security: Threats, Responses and Strategies* (Oxford: Oxford University Press), p. 158.
14 Rid, *Cyber War will Not Take Place*, p. 7.
15 Clarke and Knake, *Cyber War*, p. 93.
16 Clarke and Knake, *Cyber War*, p. 93.
17 D.E. Hoffman (27 February 2004) "CIA slipped bugs to Soviets", *The Washington Post.*
18 T. Rid (2012) "Cyber War will Not Take Place", *Journal of Strategic Studies* 35/1, 10–11.
19 For a good account of the Stuxnet attack, see J.P. Farwell and R. Rohozinski (2011) "Stuxnet and the Future of Cyber War", *Global Politics and Strategy* 53/1, 23–40.

DOI: 10.1057/9781137399625.0005

20 G.R. Lucas Jr. (2013) "Privacy, Anonymity, and Cyber Security", VU University Amsterdam: *Amsterdam Law Forum*, p. 107.
21 Farwell and Rohozinski, "Stuxnet", p. 23.
22 R. Langner (2011) "Stuxnet: Dissecting a Cyber Warfare Weapon", *IEEE Security and Privacy* 9/3, 50.
23 Farwell and Rohozinski, "Stuxnet", p. 23.
24 Langner, "Stuxnet", p. 50.
25 Herzog, "Revisiting the Estonian Cyber Attacks", p. 56.
26 M.N. Schmitt (1999) *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework* (Wright-Patterson AFB, OH: US Air Force, Institute for Information and Technology).
27 Farwell and Rohozinski, "Stuxnet", p. 33.

DOI: 10.1057/9781137399625.0005

4

A New Cold War? Russia, China, the US and Cyber War

Abstract: *At the state level, one of the key narratives within the contemporary cyber warfare debate is that China and, to a lesser extent, Russia are actively developing offensive cyber capabilities for use against the West. The suggestion is – particularly in the US – that military-grade cyber capabilities are being developed for use in a major future conflict. China, in particular, has reacted angrily to these allegations and suggested that the West is stuck in a "Cold War mentality". This chapter unpacks the notion of such a mentality, reviewing similar debates during the Cold War. The conclusion is that China's protestations should not be dismissed out of hand, and that they may argue for a greater inclusion of critical and alternative analysis in Western strategic thinking.*

Richards, Julian. *Cyber-War: The Anatomy of the Global Security Threat*. Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399625.0006.

In its 20 April 2013 edition, the London-based *Economist* magazine published a letter by He Rulong, a spokesperson for the Chinese Embassy, entitled "Cyberspace and the state". The latter took issue with a report in an earlier edition of the magazine in which China had been heavily criticized for its restrictive regulation of the internet and for launching "state-sponsored cyber attacks". In fairly robust terms, Rulong wrote that these accusations were "untrue, unfair and unacceptable". He pointed out that China was as much a victim of cyber attack as a perpetrator of it, yet Western reporting failed to present the picture in this way.[1]

The Embassy spokesperson's letter was part of a wider Chinese diplomatic push against vilification of the Chinese state for being behind a massive wave of cyber espionage and attack on other countries. China has also been accused of using state-backed telecommunications infrastructure companies such as Huawei and ZTE to install Trojan horse vulnerabilities into Western networks, which could be used at a later date for penetration and compromise of the networks. In October 2012, the US's Congressional Intelligence Committee formally made such an accusation and urged the US government and companies to shun such Chinese firms.[2] Meanwhile, in the UK, Huawei has established a small Cyber Security Evaluation Centre in which it works closely with the UK government to evaluate new network infrastructure products and attempts to reassure the government and private corporations over cyber security fears. The centre is conveniently located a short distance from the Government Communications Headquarters (GCHQ), in which is housed the UK's Cyber Security Operations Centre (CSOC), and which has allegedly supplied some former staff members for the Huawei facility.[3]

At one level, the issue is a technical one concerning the application of appropriate cyber security measures, both in spotting and disrupting attacks and in accrediting new network equipment for installation in critical parts of the national telecommunications infrastructure. The issue is sufficiently controversial, however, that it is also being elevated to the realm of high politics and diplomacy. At the 18th Communist Party Congress in Beijing in 2012, the Commerce Minister, Chen Diming, poured scorn on the accusations of state-sponsored seeding of US and other networks through companies such as Huawei and accused the US of adopting a "Cold War mentality".[4]

We saw in the first chapter how countries such as the US and the UK have pointed the finger – with varying degrees of directness – towards

DOI: 10.1057/9781137399625.0006

both Russia and China as being the key state architects of organised cyber attack against other countries. One of the key analytical questions at present within the study of cyber security is the question of how far such accusations are justified, and what they mean for future cyber security policy and regulation.

There is no doubt that a normative narrative is developing in the bulk of writing about cyber security and cyber warfare, much of which is being written in the US, which suggests that China in particular is hell-bent on large-scale cyber attack and espionage and will inevitably use it in a conflict with the US at some stage in the future. On the question of Russia, Clarke and Knake share a view held by many analysts that the post–Cold War development of intelligence capabilities in Russia and the growing "Putinisation" of the state in recent years has meant that large-scale cyber attacks of the likes seen in Estonia and Georgia simply could not have been carried out without central government patronage and direction.[5] Indeed, Clarke and Knake go a little further than many in suggesting that the Estonia and Georgia episodes were a fairly restrained dry-run for the Russian state, and that they are "probably saving their best cyber weapons for when they really need them, in a conflict in which NATO and the United States are involved".[6]

A military perspective on the rise of China has also led many observers in the US to consider that conflict is inevitable in the future. The official Chinese narrative attempts to counter this view by asserting that its rise will be a peaceful one. Zheng Bijian, for example, claims that China is attempting to develop and rise in ways that will differ from traditional realist notions of power competition and hegemony. He suggests that China will "transcend ideological differences to strive for peace, development, and cooperation with all countries of the world".[7]

Yet, many in the West are not convinced by this narrative. The US naval commander James Kraska, for example, wrote in 2010 that a gradual erosion of US maritime dominance in the face of China's naval development, in which cyber capability is an important component that helps to balance-out some of the other physical shortfalls in physical capability, would mean that the US would lose a maritime confrontation in the Pacific arena by 2015.[8] Similarly, a former US Air Force chief of information operations, Barrington Barrett, echoed a prediction made by many that a conflict between the US and China over Taiwan would be "inevitable" by 2015 at the latest.[9] Thankfully, such a confrontation has not yet materialised at the time of writing and is unlikely to do so within the

DOI: 10.1057/9781137399625.0006

predicted timeframe, although it is fair to say that recent years have been characterised by naval confrontations between China and neighbouring countries such as Japan and the Philippines over disputed territories in the Pacific region.

The opening paragraph of Barrett's analysis of potential conflict in the South China Sea encapsulates the normative thesis that is currently at large:

> *Through political and economic dealings, China is attempting to establish itself as the new Asian superpower. Its stated goal is to recreate the bipolar political society that existed, at its height, throughout the 1970s and 1980s with itself as the Communist alternative to the United States.*[10]

The argument is that the US has enjoyed a hegemonic political, economic and indeed military position since the end of the Cold War, and that any reduction in that position is bound to lead to violent power confrontations in certain places at certain times. From a military perspective, cyber capabilities allow China to compensate for a gap in physical military capability and use more asymmetric strategies to level the battlefield. In the meantime, industrial-scale cyber espionage will allow China to more quickly close the gap than might otherwise have been the case.

The supposed threat from state actors such as Russia and China in the military realm therefore has a number of dimensions to it. First is the suggestion that network infrastructures can be built with secret "trapdoors" installed for future use in the event of a major cyber conflict. When the time comes to do so, the attackers could literally turn off the lights. For the likes of China, whose ICT industries are growing quickly to become major world competitors, such an approach would be, on paper, a real possibility. Second is the suggestion that massive cyber espionage is being undertaken, targeted particularly at sensitive military capabilities, so that emerging state actors can close the expensive and lengthy research and development gaps that exist between them and the likes of the US. Finally, there is a suggestion that, were physical conflict to break out between Russia or China, and the US or indeed any of its allies, cyber warfare techniques could be used in an asymmetric fashion to neutralise physical military superiority. The whole picture is therefore one that entails both current and future dimensions.

In the case of Russia, Anderson notes that a lack of investment in technological capabilities since the end of the Cold War has meant that

DOI: 10.1057/9781137399625.0006

the intelligence apparatus – which, if anything, has increased rather than diminished since the turn of the century – has tended to rely heavily on traditional Human Intelligence (Humint) activities.[11] At the same time, there is no doubt that investment is being made in the extensive Signals Intelligence (Sigint) facilities such as that in Lourdes, Cuba, to upgrade capabilities with a cyber component.[12] In echoes of the Cuban missile crisis in the 1960s, this could become diplomatically difficult for the US in the wrong circumstances. It is also the case that Humint techniques can complement cyber attack capabilities in very effective ways. Remember that Stuxnet was probably introduced into the Iranian computers physically at some stage, rather than through hacking over a network. Break-ins or the subversion of insiders can allow the introduction of malware into systems through removable media, or, indeed, the stealing of passwords and other crucial information that can allow attackers to more easily hack into systems.

While Anderson pulls no punches over the neo-Chekist nature of Putin's Russia, and points out that general hostility towards NATO and the West defines much of its foreign policy in such areas as partnerships with other countries, Giles suggests that much of the language emanating from Russia about the threat of cyber attack has been more defensive than offensive and tends to stress the central importance of information assurance rather than attack.[13] It may be that, to a certain extent, Russia is worried about technical deficiencies as much from the point of view of the vulnerability of its own networks as for the opportunities to attack those of others. I will return to this point below in the context of interstate communications and perceptions.

As we have seen, notably in the case of the Syrian Electronic Army (SEA), one of the difficulties with cyber warfare planning and analysis is the ability to confidently make connections between cyber attacks and state actors. This is the "attribution problem" that currently bedevils international diplomacy and discussion on countering cyber attack, not to mention local planning for attack mitigation and response. Returning to Russia, it is worth noting that one of the earliest recognised mass data exfiltration attacks on a US military network occurred in 1999, and became known by the subsequent FBI investigation as "Moonlight Maze". While the authorship of the attack has never been firmly established, it was clear that the daily attacks seemed to cease outside of Russian business hours.[14] It is therefore perhaps wise not to be too naive about Russia's defensive-centric language around cyber policy.

DOI: 10.1057/9781137399625.0006

Similar logic has been used to suggest official Chinese authorship of attacks. In Chapter 1 I mentioned the recent report by the cyber security company Mandiant, which claimed to establish a direct link between a shadowy Shanghai-based hacking group called APT1 (Advanced Persistent Threats, on which more is discussed in the next chapter) and the Chinese PLA's Unit 61398, which equates to the 2nd Bureau of the PLA General Staff's 3rd Department, believed to be the Chinese military's central office for cyber network operations (CNO).[15] The report suggested, in very robust terms, that the PLA is engaged in massive and wide-reaching theft of intellectual property from the West, both from government networks and those of private corporations. In the wake of the report, Rand Corporation's cyber security expert Martin Libicki picked up on analysis that suggests that much hacking originating from China conforms to patterns of Chinese office hours, and seems to happen mostly during the week rather than at weekends.[16] Thus, the belief that APT1, also known as the "Comment Crew", is a private group of hackers along the lines of Lulzsec or Anonymous may need further scrutiny: it may be that they are a front for a government department, or are private individuals but officially contracted to carry out state business.

As mentioned earlier, however, China argues that problems of attribution mean that it is very difficult to point fingers at specific authors of attacks. For a start, network-savvy hackers can route traffic through multiple pathways and make attacks appear to emanate from almost anywhere in the world. There has been some interesting analysis recently by the cyber security company Akamai on the origins of global hacking attacks. Up until the beginning of 2013, China was allegedly the number one source of cyber attack traffic, at 34 percent of the total globally. The US was third with 8.3 percent, and most other countries were in small single figures. In the second quarter of 2013, however, Indonesia has risen to become the single largest source of attack traffic, at 38 percent of the total, pushing China into second place, with 33 percent. The US is down to being the source of 6.9 percent of attack traffic (third place) and Russia languishes some way behind at just 1.7 percent of the global total.[17]

These figures both do and do not reveal interesting features of the global picture. Firstly, Chinese servers have clearly been a very dominant source of cyber attacks, dwarfing the role of most other countries other than China's near neighbour, Indonesia. At the same time, these raw figures say nothing about the nature of those attacks: who their authors

DOI: 10.1057/9781137399625.0006

were (and specifically whether they were state or non-state actors), or whether a lot of the attacks could not have been spoofed to appear to come from China when they actually originated elsewhere. This might explain the Indonesia factor, which is certainly curious. Indonesia is an emerging country but is not a big state player on the international stage, and has not, hitherto, shown any signs of aggressively pursuing particular commercial or ideological agendas. It is thought to have a relatively underdeveloped intelligence capability, and would not be generally considered to be a key player in the technological world of cyber capabilities. All of this may mean that its networks are being used as a convenient staging ground for attacks originating elsewhere, in order to confuse the picture. It may be that the particular configuration of Indonesia's networks is such that it is a good place through which to pass international attack traffic, and to spoof its origins. Of course, this might mean that the finger could be pointed back at Indonesia's large neighbour to its north, but it could equally mean that any number of other attackers were involved from numerous different parts of the globe. It could also, of course, mean that Indonesia itself is indeed emerging as a major player in the world of cyber attack.

As we have seen, the US is becoming increasingly robust in its accusations against Chinese cyber attack, particularly in the realm of cyber espionage. The chairman of the Congressional Intelligence Committee, Mike Rogers, has described the degree of theft of intellectual property by China as historically unprecedented and "intolerable".[18] Beijing, meanwhile, has reacted angrily to the accusations and said that there is lacking proof to show that they are the hidden hand behind the attacks.

We have noted that the phrase "Cold War mentality" is often used by Chinese officials to refer to the diplomatic difficulties, yet what does this mean exactly? Hirshberg has presented an interesting analysis of the way in which US attitudes towards China, both public and official, changed through the period of the Cold War and through its end. Through the bulk of the period, Hirshberg argues that an "American patriotic schema" formed the basis for US attitudes towards other countries such as China, in which the self was equated with high-level values such as democracy, freedom and righteousness. Communist countries were generally seen to be the antithesis of American society, in which there was oppression and a lack of freedom, and this made them fundamentally "bad". In this respect, China was linked with attitudes towards the Soviet Union more generally and seen as a communist puppet of Moscow.[19] Intriguingly,

DOI: 10.1057/9781137399625.0006

attitudes towards China seemed to improve through the 1980s as the country opened up and there was an increasing amount of diplomatic contact between it and the West (triggered by Nixon's landmark visit to China in 1972) until the Tiananmen massacre in 1989, which reaffirmed a belief in the West that China was essentially an oppressive country.[20]

The suggestion is that attitudes are formed on the basis of grand ideological conceptions. The Cold War was conceptualised by many as a fundamental confrontation of ideas and belief-systems: a free, open, prosperous and tolerant capitalist West against a centralised, oppressive, miserable and intolerant Communism. The two could not come together as they were fundamentally opposed to one another, a yin and yang, hence the frozen stand-off. When the actual Cold War with the Soviet Union ended with the latter's collapse in 1991, some scholars noted that ideological differences were mutating into subtly different factors but that fundamental differences between identities and belief-systems were seen to remain. In his highly controversial "clash of civilizations" thesis presented in 1993, for example, the American academic Samuel Huntington wrote that "underlying differences between China and the United States have reasserted themselves in areas such as human rights, trade and weapons proliferation".[21]

Chinese officials and scholars such as Bijian like to stress that international relations should not be seen in such ideological terms alone, and to do so perpetuates the Cold War mentality that we should be shedding by now.[22] Certainly, China pursues a different ideological outlook from the West and there are important differences between them in certain areas of policy and society, but this does not mean that the two systems cannot co-exist in a fundamentally co-operative and peaceful world, Bijian argues.

From the point of view of potential military confrontation between the US and China, there are two issues in play. First is the question of realist politics, and whether, as is suggested in many of the normative accounts of the situation, China's main objective is to attain superpower status alongside that of the US. This is seen as something of a zero-sum game by many, in the sense that the rise of Chinese power will inevitably mean the reduction and dangerous weakening of US power as it moves from being a hegemon to being a player in a bipolar or multipolar world. This is the essence of the security dilemma[23] which characterised the Cold War confrontation between the US and the Soviet Union, and led to a massive proliferation of military capability on both sides. Such

DOI: 10.1057/9781137399625.0006

a preoccupation with power relationships and balancing leads to a concentration of attention on the relative military capabilities of each, since it is assumed that at the point on the graph where China's rising power meets the declining line of US power and threatens to overtake it, some sort of violent military confrontation is more than likely. This, in turn, leads to analysis of relative military symmetries and the way in which cyber capabilities can be used to complement or balance-out capabilities and level playing fields.

Second is the question of perception and misperception of intentions between states, and the security problems that can be generated as a result. As the political scientist Robert Jervis noted, misjudgements of states' intentions and the hostility of their words and actions can lead to very serious consequences. Jervis used the two World Wars in the twentieth century as a framework for how such misjudgements can lead to conflict. The Second World War was arguably triggered by an underestimation of states' willingness to fight in the face of aggression. (In this model, deterrence can be potentially very significant.) The First World War, on the other hand, was caused by an overestimation of states' hostile intents when their differences might have been bridgeable.[24] Jervis was writing during the latter stages of the Cold War and considering the misjudgements that could lead to a disastrous Third World War, but his thoughts remain prescient today, particularly in the sense of needing to avoid the First World War or "spiral" model.

Indeed, the analysis of the Cold War, both during and subsequently, led to a shifting pattern of ideas on what had actually happened and how the long, frozen conflict had come about. Hopkins' recent discussion of the historiography suggests that there is a dearth of analysis about China during the Cold War period, while much of the writing perhaps understandably focuses on the US–Soviet confrontation.[25] In this analysis, the original view that the Cold War was triggered by aggressive communist expansionism in the immediate aftermath of the Second World War was increasingly critiqued by a set of revisionists from the 1960s onwards (such as Williams, Fleming and Horowitz), who suggested that it was in fact American expansionism that engendered a paranoia in the Soviet Union and encouraged their scramble for power parity.[26] Later post-revisionist perspectives emerged in the 1970s and 1980s, suggesting that a combination of misperceptions, politics and deliberate obfuscation in some cases contributed to the Cold War impasse. As one of the proponents of post-revisionism John Lewis Gaddis noted "a variety of

DOI: 10.1057/9781137399625.0006

preconceptions, shaped by personality, ideology, political pressures, even ignorance and irrationality" all played a major contribution to foreign policy formation on both sides.[27]

A good modern example of how these issues may still be relevant with regard to Russia and its intentions is provided by Giles in his analysis of the Russian Federation's Information Security Doctrine of 2000. This document talks about the threat from "certain countries" and their information warfare capabilities, which could have a "dangerous effect on other countries' information systems", including disrupting information and telecommunications systems and gaining unauthorised access to data.[28] The language in this section of the Russian doctrine closely reflects that of the US military's "Electronic Warfare" document, last updated in 2012, which talks of the need to use information operations to "influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries".[29] The similarity in language may be coincidental or it could reflect the fact that Russia senses a serious cyber threat from the likes of the US and consequently feels it needs to develop its own cyber warfare capabilities.

Whatever the truth, it is clear that foreign policy perceptions of another state's intentions can often be seriously flawed. In the intelligence realm, much has been written about the dangers of fixed mindsets and how these have contributed to a succession of intelligence failures and strategic shocks throughout history. Much renewed analysis of these issues was triggered in the early twenty-first century in the wake of the 9/11 terrorist attacks in the US, and the 2003 invasion of Iraq which turned out to be based on faulty intelligence assessments of the Iraqi regime's stocks of weapons of mass destruction (WMD). These mistakes in Western intelligence communities led to much discussion of the need to avoid fixed "analytical mindsets" about targets and threats, and to develop what Roger George called "alternative analysis" techniques, namely methods for considering alternative scenarios which challenge established analytical assumptions about states or other intelligence targets.[30]

I would argue that there is a danger currently of a normative view developing in the West of the cyber warfare threat from China and, to a lesser extent, from Russia, which is not being subjected to sufficient levels of critique and challenge. This may be because much of the writing and commentary on the threat is being conducted by current and former government and military personnel who may be at risk of seeing

DOI: 10.1057/9781137399625.0006

the world in very particular ways. At the very least, alternative scenarios which consider strategic politics more extensively could probably do with more of an airing in the analysis than is currently the case.

One of the features of much of the writing about cyber warfare currently is a tendency to develop lurid scenarios about a potential future cyber attack on the US of a scale equivalent to a Third World War. Many of these scenarios tiptoe unashamedly around the line separating academic analysis from popular fiction. A good example is presented in Clarke and Knake's recent analysis of the threat of cyber war.[31] A scenario is presented in which the reader is invited to "imagine a day in the near future" in which one is the assistant to the President for Homeland Security in the US. A scenario is then described of a multi-faceted and rapidly escalating cyber attack on the US, hitting both military and civilian infrastructure targets. Within a short space of time, civil airliners are crashing into each other and dropping from the sky because the air traffic control system has failed. Power blackouts have hit 157 major metropolitan centres at rush hour time, causing panic and confusion. Subway trains have crashed and freight trains have derailed catastrophically. "Poison gas clouds" are drifting towards major urban centres. Major looting and the general breakdown of society unfolds as stores run out of supplies and the ATM system fails. To end the day, you are invited by the Pentagon's Cyber Command to authorise a counter-strike on either Moscow or Beijing, since one of the two is assessed to be behind the attacks (although they are not certain which).

A similar catastrophic scenario is described by Barrett, but this time in the context of a military confrontation between the US and China over Taiwan. Barrett recalls two military scenarios that have been presented by McClain and Gertz,[32] in which a major Chinese military exercise simulating an invasion of Taiwan is suddenly put into effect, rather like the manner in which Egypt fooled Israel in the Yom Kippur war of 1973. The attacks involve a combination of physical attack and massively disabling cyber attacks that cripple Taiwan over a very short space of time and ensure a rapid Chinese victory. Barrett suggests, however, that McClain's scenario neglects the need to simultaneously neutralise US counter-action in the region in the face of an invasion of Taiwan. (Gertz receives plaudits for thinking of this factor, by suggesting that the Chinese might want to block the Panama Canal and thus frustrate US efforts to move forces into the region quickly.) To achieve neutralisation of the US counter-offensive, Barrett suggests that China might

DOI: 10.1057/9781137399625.0006

pre-emptively attack US military bases across the Pacific region with ballistic missiles, including in Japan, while simultaneously conducting large-scale cyber attacks on the US mainland to pressure the US public into rejecting their government's involvement in a war in a distant land in which they might want no part. There is even suggestion of a nuclear device being exploded over Taiwan to cause a catastrophic energy surge to its power networks.

All of these scenarios are interesting think-pieces which explore the nuts and bolts of both attack and defence in a contemporary war with a major cyber component. It is recognised that the authors are not suggesting any of these scenarios may actually happen, but are merely providing food for thought for policymakers in thinking about real and potential risks and how to mitigate them. These issues of policy will be explored in the next chapter. At the same time, I would argue that the strategic logic of such scenarios is highly dubious. For China or Russia to launch a crippling attack on the US and its allies which caused multiple civilian casualties on the US mainland and involved use of ballistic missiles and even nuclear devices would be tantamount to starting a Third World War which could rapidly lead to the end of civilization: in short, to mutually assured destruction, as was the fear during the Cold War. Such scenarios appear to make little strategic sense for the likes of China, and, I would argue, this is a somewhat neglected element of current debate on this issue at present. It may be that some of Roger George's alternative analysis techniques, such as Devil's Advocacy or Red Teaming, badly need to be exercised around such discourse in the military and intelligence communities. On this issue, it could be argued that Chinese officials and analysts may be at least partly correct when they accuse Western commentators of being stuck in a Cold War mentality when considering the cyber war debate at the present time.

Notes

1 H. Rulong (20 April 2013) 'Letters: Cyberspace and the State', *The Economist*, p. 14.

2 K. Hille and P. Taylor (24 April 2013) "Huawei 'Not Interested in US Any More' after repeated Denials for Market Access", *CNN,* http://edition.cnn.com/2013/04/24/business/huawei-not-interested-us/index.html, date accessed 18 November 2013.

DOI: 10.1057/9781137399625.0006

3 *Economist* (4 August 2012), "The Company that Spooked the World", http://www.economist.com/node/21559929, date accessed 18 November 2013.
4 V. Mangin and C. Freeman (10 November 2012) "Chinese Official Accuses Washington of 'Cold War' Mentality", *The Telegraph.*
5 Clarke and Knake, *Cyber War*, pp. 20–1.
6 Clarke and Knake, *Cyber War*, p. 21.
7 Z. Bijian (2005) "China's 'Peaceful Rise' to Great Power Status", *Foreign Affairs* 84/5, 22.
8 J. Kraska (2010) "How the United States Lost the Naval War of 2015", *Orbis* 54/1, 35–45.
9 B.M. Barrett Jr. (2005) "Information Warfare: China's Response to US Technological Advantages", *International Journal of Intelligence and Counterintelligence* 18, 682–706.
10 Barrett, "Information Warfare", p. 682.
11 J. Anderson (2007) "The HUMINT Offensive from Putin's Chekist State", *International Journal of Intelligence and Counterintelligence* 20, 267.
12 Anderson, "The HUMINT Offensive", p. 273.
13 K. Giles (2011) *Information Troops – A Russian Cyber Command?* In C. Czosseck, E. Tyugu and T. Wingfield (eds) *Proceedings of the 3rd International Conference on Cyber Conflict* (Tallinn: CCD COE), p. 47.
14 Giles, *Information Troops*, p. 55.
15 Mandiant. *APT1*, p. 3.
16 Cited in Foxnews (25 February 2013) "Chinese Hackers Seen as Increasingly Professional, Experts Say", http://www.foxnews.com/tech/2013/02/25/chinese-hackers-seen-as-increasingly-professional-experts-say/, date accessed 18 November 2013.
17 Akamai, cited at C. Albanesius (16 October 2013) "Indonesia Tops China as Cyber Attack Capital", *PC Mag.com*, http://www.pcmag.com/article2/0,2817,2425836,00.asp, date accessed 18 November 2013.
18 J. Smith (4 October 2011) "Rogers: US Must Confront 'Intolerable' Chinese Espionage", *National Journal*, http://www.nationaljournal.com/njonline/rogers-u-s-must-confront-intolerable-chinese-cyberespionage-20111004, date accessed 10 November 2013.
19 M.S. Hirshberg (1993) "Consistency and Change in American Perceptions of China", *Political Behavior* 15/3, 250–1.
20 Hirshberg, "Consistency and Change", p. 249.
21 S.P. Huntington (1993) "The Clash of Civilizations?", *Foreign Affairs* 72/3, 34.
22 Bijian, "China's 'Peaceful Rise' ", p. 22.
23 R. Jervis (1978) "Cooperation under the Security Dilemma", *World Politics* 30/2, 169.
24 R. Jervis (1988) "War and Misperception", *The Journal of Interdisciplinary History* 18/4, 685.

DOI: 10.1057/9781137399625.0006

25 M.F. Hopkins (2007) "Continuing Debate and New Approaches in Cold War History", *The Historical Journal* 50/4, 913.
26 Hopkins, "Continuing Debate", p. 915.
27 J.L. Gaddis (1972) *The United States and the Origins of the Cold War, 1941–1947* (New York: Columbia University Press), p. 360.
28 Giles, *Information Troops*, p. 47.
29 Joint Chiefs of Staff (2012) *Electronic Warfare*. Joint Publication 3–13.1, I–14.
30 See R.Z. George (2004) "Fixing the Problem of Analytical Mindsets: Alternative Analysis", *International Journal of Intelligence and Counterintelligence* 17, 385–404.
31 Clarke and Knake, *Cyber War*, pp. 64–8.
32 Barrett, "Information Warfare", pp. 697–702. See A. McClain (2001) "Will China Attack Taiwan? What China-Watchers Should Be Looking For", *Defense Intelligence Journal (China)* 10/1 and B. Gertz (2000) *The China Threat: How the People's Republic Targets America* (Washington DC: Regnery Publishing).

DOI: 10.1057/9781137399625.0006

5

Responses to the Threat: National Cyber Security Planning

Abstract: *In this chapter, the question is asked as to how states are approaching their counter-threat strategies in the contemporary era. A particular area of complexity is indentified in the manner in which the threat of cyber attack in its various iterations spans both public and private sectors. This leads to a particular complex set of questions for government policymakers. A fear of government intrusion into privacy further complicates the matter. Many analysts have tried to approach the policy question by analogising with previous threats. The nuclear threat in the twentieth century has often formed the basis of analysis in Western circles, although many have argued that cyber weapons are perhaps more akin to chemical or biological, than to nuclear weapons.*

Richards, Julian. *Cyber-War: The Anatomy of the Global Security Threat*. Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399625.0007.

The peculiar complexity and mutability of the emerging cyber-threat picture becomes particularly pertinent for state governments when they consider what sorts of counter-threat policies need to be put in place. We have established that, unlike the case for some other threat factors, conceptualising, prioritising and countering the cyber-threat is far from a straightforward process. This is certainly true within the military context in the sense that there is debate and disagreement, as we have seen, about what would actually constitute an act of war in a cyber context, and whether such acts have yet happened or are likely to do so in the future. At the same time, the military threat aspect of cyber security is but part of a much wider spectrum of cyber-threat vectors, encompassing crime, espionage, activism and sabotage. Before considering cyber-threat policies, it is important to establish where on this spectrum the threat of cyber warfare sits, and how it is to be prioritised in national planning.

Some interesting analysis has been conducted in recent years on how cyber threats are being verbalised and securitised in national and international discourse. Myriam Dunn Cavelty suggests that the process of securitisation has inevitably meant a move towards the more extreme end of the cyber-threat spectrum, and increasing talk of cyber warfare as one of the most important elements of the cyber threat, especially in the US.[1] Lawson sees a more specific transition to talk of cyber warfare threats from 2007 onwards, when the attacks against Estonia happened.[2] While there is much debate about the true seriousness of these attacks in terms of the real-world effect on the ground, much of the language both in and outside of Estonia was military in nature. The speaker of the Estonian parliament at the time likened the effect of the attacks to that of a nuclear strike.[3] While many other observers would not go as far as this, there was a widely held view in military circles that the attacks had shown the potential of widespread and organised attack on a country's electronic infrastructure.

One of the more vocal critics of the cyber war thesis James Lewis has suggested that the Bush administration's *National Strategy to Secure Cyberspace* of 2003 contained within it an imbalanced view of the cyber-threat spectrum. In particular, he suggests that the perceived vulnerability of key elements of national infrastructure to catastrophic cyber attack, such as the utilities, finance, transport and manufacturing sectors, was greatly exaggerated in the strategy. He argues that the same was the case

DOI: 10.1057/9781137399625.0007

with the potential societal effects of a cyber attack, and the probability that terrorists would be able to achieve a catastrophic attack.[4]

Another interesting example in the Western world of official approaches to the cyber threat is that of the UK, on which I have written elsewhere.[5] With the establishment of a new National Security Council at the top of the government in 2010, the Cameron-Clegg administration attempted to bring more rigour into decision-making on the most important national security issues. This included conducting a comprehensive security risk assessment exercise (the National Security Risk Assessment) which delivered a three-tiered prioritisation of security threats to the UK, and which formed the basis of the National Security Strategy and Strategic Defence and Security Review. On the cyber front, a Cyber Security Strategy was published in 2011 to sit alongside a blizzard of other security strategies and documents appearing at the time.

Within the UK's National Security Risks, the cyber threat is situated in the topmost tier of threats and is articulated as a threat of "hostile attacks upon UK cyberspace by other states and large-scale cyber crime".[6] The National Security Strategy (NSS) recognises the complex interplay of threats, encompassing crime, espionage, terrorism and cyber war, while recognising that these have to be set against the economic benefits to be had from being a world leader in information and communications technology.[7] The articulation of the potential military threat is clear. The NSS notes that "attacks in cyberspace can have a potentially devastating real-world effect"; the Stuxnet episode represented "an example of the realities of the dangers of our inter-connected world".[8] If the language here is more that of potential threat in the future rather than today, the current reality certainly involves cyber attacks against official networks. Speaking at the time of the NSS's publication, the minister for defence at the time, Dr Liam Fox, noted that the Ministry of Defence had blocked and investigated "more than 1000 potentially serious cyber attacks" during 2010.[9] The attacks had taken a variety of forms, from denial-of-service attempts to penetration and data exfiltration attempts.

As well as being intertwined with other types of threat, such as those from espionage, crime and activism, the threat of cyber warfare also includes a peculiar difficulty for governments in considering how best to respond. This is partly a result of the way in which information technology has developed under globalisation, and comprises the fact that many of the referent objects of the threat, namely elements of the critical national infrastructure, are not owned or managed by the government

DOI: 10.1057/9781137399625.0007

itself but by private corporations. This is another way in which cyber warfare could be very different from other types of traditional conflict. This factor applies not only to civilian networks that could be targeted as an element of asymmetric attack to put pressure on a government, but also to the military's own networks and systems, many of which are now designed, installed, managed and operated by private-sector contractors.

Defence and security are traditionally public goods. This was the logic in Max Weber's consideration in the early twentieth century that a strong state is characterised by a monopoly on the use of force by the state itself in delivering security.[10] In the post-modern, post-Westphalian world, however, many of the state's monopolies on institutions and processes are starting to change: witness the emergence of the private military and security industries, for example, which have grown to such an extent that, argues Singer, the US would not have been able to conduct the 2003 war in Iraq without the involvement of private military contractors.[11]

However, Lewis argues that private companies are notoriously bad at filling gaps in the need for public goods.[12] An example of the effect of this is the UK government's attempts to pass a new Data Communications Bill in recent years, which would compel communications service providers to store and make available on request data pertaining to public communications using a range of internet-based services. The bill is deemed necessary because the government does not control or have access to this data, yet the communications companies have no commercial need to keep much of it, and would only do so if it was mandated by law.

The new bill has not yet been passed through parliament as it has fallen foul of civil liberties concerns over mass surveillance by the state. This is a particularly difficult issue and it illustrates one of the difficulties in forming cyber security policy at the present time. Specifically, government has to work in tandem with private corporations in both adequately conceptualising the threat to networks and agreeing on appropriate counter-threat strategies. (I will return to this issue later.)

Within this process, there are a number of complex issues. One is the commercial sensitivity over threat reporting. Many corporations are not keen to publicise that they have been attacked or compromised, as this could lead to a confidence issue that could be beneficial for competitors. This means that accurate data on cyber attack trends and methodologies can be patchy. There is also the issue of cost in delivering cyber security, and whether the government should pay for it. Furthermore, in countries

DOI: 10.1057/9781137399625.0007

such as the US, there are intellectual difficulties over the government interfering with business and applying excessive regulation. The "small state" principle becomes difficult when the state needs to work with the private sector in essentially regulating and monitoring the infrastructure. As Clarke and Knake noted, President Obama declared in a 2008 speech that the US's cyber infrastructure was "a strategic asset".[13] However, official US government strategy in cyber security has tended to restrict itself to protecting government networks. Under the previous Bush administration, the Comprehensive National Cybersecurity Initiative (CNCI) focused primarily on the protection of public sector networks.[14] It appears that the Obama administration has taken the same line. When pressed on the issue in 2009, the President said that the government "will not dictate security standards for private companies".[15]

It is therefore the case that the two official organisations in the US primarily responsible for cyber security strategy when it comes to major strategic cyber threats, namely the Pentagon's Cyber Command and the Department for Homeland Security (DHS), can only really have purview over government networks. It is not clear who would be responsible for other networks that are nevertheless critical to the US economy and stability, such as the financial, telecommunications, utilities or transport networks, in terms of establishing standards for protection and attack mitigation, and paying for the measures needed. There are also issues over influencing commercial policy over companies and corporations which may be seen to be a "back-door" threat to infrastructure (such as Huawei, as discussed earlier). Finally, as we have seen in the case of the Data Communications Bill in the UK, there are sometimes issues over public perceptions of the need for privacy, and the ways in which governments might be seen to transgress this right through the monitoring and shaping of communications networks. These are sometimes difficult issues for corporations, partly because they are themselves part of the public consciousness, but also because practices seen by sections of the public to be negative could be considered to be commercially deleterious for individual companies in a competitive marketplace.

The public/private axis is, in a sense, just one of the complicating factors in cyber-threat conceptualisation and mitigation. We have seen how countries such as China have criticized the West for slipping into a Cold War mentality when approaching the question of cyber threats. Part of this, as we have discussed, is the tendency to see international relations as a sort of zero-sum game of ideology in which Western democracies

DOI: 10.1057/9781137399625.0007

are locked in a fight to the death with other less democratic political systems. The other manner in which Cold War thinking may be poisoning the well of thinking about counter-threat strategies is in the manner in which many have likened the threat of cyber war to that of nuclear war during the twentieth century.

In some ways, as Joseph Nye remarks, the fact that we are in the very early stages of thinking about the possibilities of cyber warfare and its effects allows us to draw parallels with the middle of the twentieth century when the new technology of nuclear weapons was unleashed on the world and states began to think about how they could mitigate and confront the threat.[16] Nye concludes that, while the two threats are very different in crucial ways, there is much that could be learnt in terms of the way in which states get to grips with the new technology and consider issues such as international co-operation, deterrence and civil–military relations. Clarke and Knake concur with this view, noting that the early period of the nuclearised Cold War involved a number of crises and confrontations – some of them extremely dangerous – which eventually led to a balanced system of mutual deterrence and strategy.[17]

However, as Nye also notes, there are fundamental differences between the threat of nuclear war and that of cyber war. For a start, a nuclear attack is "unambiguous"[18]: it is difficult to conceal that it has happened or who is responsible. Cyber attacks on the other hand can work away behind the scenes and not even be noticed for long periods. When they do come to the surface, as Stuxnet did in the Natanz plant in 2010, it is usually impossible to determine the author of the attack or their motives. Second, many would agree that cyber attacks are not yet at the stage where they could be considered an existential threat to human society on the scale of nuclear war. Whether that will always be the case is a matter of conjecture, but for the time being it could reasonably be argued that even a serious disruption to essential infrastructures would not have the same destructive effect on a state as a nuclear attack. After all, infrastructures sometimes break down by accident anyway. This, in turn, should tell us something about strategies to adopt in the areas of deterrence and counter-attack.

Thomas Rid argues that comparisons with the Cold War and the nuclear threat are "almost always flawed, unhelpful, and technically misguided".[19] Nevertheless, many analysts have applied twentieth-century thinking to consider how Mutually Assured Destruction could be adapted to a notion of Mutually Assured Disruption,[20] or how cyber

DOI: 10.1057/9781137399625.0007

weapons could be Weapons of Mass Disruption.[21] Again, there are difficulties with equating these concepts across the two technologies, similar to those mentioned above. The principle of nuclear deterrence involved a rapid counter-strike capability against the adversary, and a second strike capability to ensure that the defending state was not completely destroyed in the first round of attack. (This is the logic of the Continuous at Sea Deterrence (CASD), for example, which forms the basis of the UK's nuclear deterrent capability.) A counter-strike capability could be developed in a cyber context and, as Young argues in what he identifies as a useful comparison with nuclear strategy, this would need to be rapid to the point of near-simultaneity, since the launch and delivery of a cyber attack over a network can happen almost literally at the speed of light.[22]

In this way, developing a credible cyber attack capability over and above merely putting in place defensive cyber security measures, and ensuring that the world is aware of your plans, could be argued to pose some sort of deterrent effect against would-be aggressors.[23] This may be why such offensive capabilities are explicitly described by Western nations in their defence and cyber security strategies. Interestingly, it might also be why some states and organisations such as NATO will occasionally talk about linking kinetic responses to cyber attacks, namely threatening to respond with physical force in addition to cyber attack in some of the more serious scenarios.

However, there is clearly a fundamental problem with the notion of counter-strike in a cyber context, and that is the difficulty of attributing authors to attacks. It is all very well announcing that a serious cyber attack could be answered with a missile attack or even a nuclear response, but this is pointless if a state cannot identify with absolute certainty who had launched the cyber attack against them.[24] There are several dimensions to this problem. First, as we have discussed in the context of accusations against China, whether all or even some of the supposedly state-sponsored cyber attacks against Western nations are being authored by the likes of the PLA is difficult to establish with absolute certainty at the present time, and to make such accusations can risk serious diplomatic rifts, not to mention international crises.

Second is the question of who the attackers are in terms of personnel. In this area, there is a useful parallel that can be drawn with modern counter-insurgencies. In conflicts such as those more recently in Iraq and Afghanistan, the West and its allies have struggled with the notion of who is a combatant and who is a non-combatant in the battlefield, since

DOI: 10.1057/9781137399625.0007

insurgents do not wear uniforms and tend to hide amongst the civilian population. They are also uninterested in international agreements such as the Geneva Conventions, while their uniformed army foes cannot afford to be so, as the recent prosecution in the UK of a marine convicted of murdering a Taliban prisoner in Afghanistan attests.[25]

In the cyber context, there is often uncertainty about whether a cyber attack has been launched by a military or government employee sitting in an official building, or by sympathetic or franchised civilian hackers, or even, indeed, by an independent civilian who is mounting the attack for some personal motivation such as notoriety or displaying technical prowess. The case of APT1 or the Comment Crew in China is a good example, since it is unclear whether this group is an independent civilian group of hackers with some connection with the Chinese government, or is indeed the Chinese military masquerading under a civilian persona. A similar ambiguity swirls around the Syrian Electronic Army. In the context of independent civilians with less identifiable motivations, shadowy groups such as Lulzsec or Anonymous are interesting. Here, the case of the British teenager Ryan Cleary, aka "Viral", is an indicative one. Cleary and four other independent hackers formed the core of the Lulzsec group, which was eventually broken up when one of their number, Hector Monsegur (aka "Sabu"), turned informant for the FBI. Cleary and his British counterpart Jake Davis (aka "Topiary") were the classic troubled-teenager-in-a-bedroom hackers. When Cleary called up his army of botnets ("zombie" computers unwittingly co-opted to carry out malware and DDoS attacks) to attack the CIA's website and cause it to crash briefly in 2011, Davis announced the success on Twitter, adding that the attack had been "for the lulz". Both Cleary and Davis were arrested in 2011, the former in the bedroom of his inconspicuous suburban home which he had not left for the previous six months.[26]

At the state level, there is clearly a belief in Western analysis of cyber war that states such as Russia and China are able to call upon armies of "patriotic hackers" or "netizens" to do their bidding, given the perceived ideological and totalitarian nature of those societies. Taking up the notion of Mao Tse-Tung's theory of a "People's War", Barrett makes reference to an idea amongst unspecified US intelligence analysts that China may issue laptops to the populace in the event of a future cyber war so that they can lead the battle in a sort of "take-home war".[27] Similarly, in the case of Russia, Giles notes how the cyber attack activities that accompanied conflicts and unrest in Estonia, Georgia and Kyrgyzstan appeared

DOI: 10.1057/9781137399625.0007

to be the work of sympathetic Russian citizens who may have had – or indeed needed – little more than encouragement from the Russian state.[28] A "nudge in the right direction" might be enough, leading to a private/official nexus that is similar to the case of the Russian Business Network's pre-eminent role in cyber crime.

A belief in armies of patriotic hackers may be another unfortunate outcome of an overly definitive Cold War mentality, and of a fixed mindset about non-democratic regimes, although the basic point about there being a blurring of boundaries between civil and military actors in cyber attacks is an important and valid one. Giles makes the point that a state such as Russia may see virtue in forging links with civilian hackers, since the sorts of skills and motivations needed to be a high-level hacker are rarely found in those who want to work for the government or the military, or indeed in those that are happy to be conscripted to the army. Rather than fight this dichotomy therefore by co-opting the skills into the public sector, it may make more sense to contract out the requirements to private hackers.[29]

However, the cases of Ryan Cleary and Lulzsec show that to deal with such private hackers can be a dangerous business, and that the motivations of the hackers cannot always be guaranteed. These cases also show that the involvement of private hackers in cyber attack is not confined to non-Western countries. Another interesting case is that of the shadowy hacker dubbed "the Joker", who appears to be conducting a sole campaign against Jihadist websites on the internet and with whom a German newspaper claimed to have conducted an interview.[30] The Joker did not reveal much other than that he or she was a former soldier. Assuming this is true and that Western governments are not directing the work of this hacker, this shows that patriotic hackers will not always be confined to non-Western countries. Conversely, it is also clearly the case that not everyone in Russia or China is happy with the state and its ideology, and may be inclined in some cases to undermine or attack the state from within. It is perhaps dangerous to see the populations in such countries in monolithic, ideological terms. The question from a policy point of view is whether and how such people can be controlled or directed, or indeed whether the task is to interdict them and disrupt their activities.

All of these factors mean that if analogies are useful for determining counter-cyber war strategies then we may be dealing with something that looks a lot more like terrorism than war. Attacks may be carried out primarily by individuals or groups of individuals with varying degrees

DOI: 10.1057/9781137399625.0007

of connection with state sponsorship. Where state sponsorship can be definitively established (such as identifying a link between Hezbollah and the Iranian government, for example) pressure can be placed on states to cease their support of terrorism. Where individuals can be interdicted, they can be considered as having broken civil and criminal laws and can be prosecuted accordingly. This is what happened to Ryan Cleary and the other members of Lulzsec, although in their case motivation was not state-ideological but a perplexing mixture of grievance and an adolescent desire to make a mark on the world. In many ways, this is not entirely unlike much terrorist activity at the individual level.

Similarly, the nuclear analogy may be the wrong one to draw in considering cyber war; the analogy of chemical or biological weapons may be much more apt. Lawson lends much support to a biological analogy: biological weapons are, like cyber weapons, difficult to direct and control fully; usually have limited impact before they are dispersed or interdicted; and are usually of "one-time only" utility, in the sense that, once unleashed, the victim of the attack can see how the weapon was designed and develop an antidote or patch.[31] Furthermore, if a biological weapons analogy is useful in conceptualising the problem, then it might also offer some ideas for cyber security policy. A March 2011 report by the DHS in the US suggested that something akin to the Center for Disease Control could be developed, which monitors outbreaks of disease and provides analysis and advice to the international community on countering the threats.[32] At the moment, private cyber security companies such as Symantec, Kaspersky Labs and numerous others perform a service something along these lines by analysing new pieces of malware as they emerge and issuing detailed reports about how they are designed, and their strengths and weaknesses. It may be possible to formalise this process and make it a more international service. Similarly, it may be appropriate to leave it to the private sector to disseminate such information as they regularly do.

Staying with the nuclear line of thinking, Clarke and Knake offer a detailed strategy for the US in the face of the threat of cyber war called the "Defensive Triad". This draws on the nuclear triad concept of the Cold War, whereby a nuclear missile strike capability based on land, at sea and with a fleet of long-range strategic bombers was deemed to provide a flexible capability that ensured the ability to conduct a second strike after an initial attack. This in turn acted as a deterrent to any aggressor, under the principle of Mutually Assured Destruction. Clarke

DOI: 10.1057/9781137399625.0007

and Knake adapt this idea to the cyber context and attempt to overcome the political dilemma they have observed whereby the state talks about the criticality of the infrastructure and the need to defend it, but then refuses to mandate regulation or security standards for the private sector. This, they claim, leads to an impasse in which no useful policy is implemented.[33]

The first element of the triad is a commitment to protect the tier 1 Internet Service Providers (ISPs), namely the ones forming the core backbone of the internet rather than the myriad of smaller sub-networks. This would involve mandating a system of deep packet inspection (DPI) on the network to spot and interdict malware, designed in such a way that was both fast enough to avoid slowing down the traffic and automated and anonymised enough to avoid accusations of government spying on its citizens. This part of the strategy would ensure that the core communications network stayed running, even if parts of it were attacked and compromised. The second element involves identifying the core elements of the electricity grid's industrial control systems (ICS) and mandating protection of those, again to ensure that the core of the network remained operating even if parts of it failed. The final element focuses on protection of the Department of Defense's (DoD) own networks, so that it could keep operating and conduct cyber counter-strikes or even direct kinetic operations, even if parts of the national infrastructure were attacked. The principle of the triad is that it involves a combination of limited government regulation and security controls mandated for critical parts of the privately owned and operated network, with control of critical military networks, and thus avoids attempting to "boil the ocean" and tackle the enormity of the network and its infrastructure. The first two elements are primarily defensive while the third is primarily deterrent, in the sense that the overall message is that a major cyber attack on the US will not only fail, but will invite a comprehensive response.

The proposals have much logic and offer a limited yet feasible approach which may have great practical value and ensure that policy proceeds beyond grand statements and fine ideals. There are, of course, a number of issues which would have to be debated. First is the fundamental question of whether a major destructive cyber attack on critical infrastructure is a real possibility at all. If it is not and the threat has been greatly blown out of proportion, as many critics suggest, then a major and expensive strategy of this nature may not be needed. If we are incorrectly thinking

DOI: 10.1057/9781137399625.0007

of the threat in terms of war rather than terrorism, sabotage or even vandalism then we have to think of the most appropriate and proportionate response to the real threat. It may be that many of the problems can be thought of more as civil criminal issues which international police and judicial co-operation could tackle, as was the case with Lulzsec. Similarly, rather than the government mandating standards and controls for elements of the private sector, it may be the case that the existing flow of analysis and information about cyber threats and how to counter them within the industry itself may be sufficient to ensure that protection of critical infrastructure keeps pace with the threat organically. Thus, the free flow of information may be the greatest weapon against the threats.

At the same time, if states are involved in these attacks but are hiding behind private individuals then international criminal law and co-operation will cut little ice. China is unlikely to give up members of APT1 to US prosecutors, for example. In this way, it may not be enough to allow the problem to sort itself out within the private sector.

Another key issue is whether the technology is up to the task, particularly in the area of DPI. Clarke and Knake recognise this issue but consider that technology is progressing quickly enough that massive data rates can be analysed and monitored without causing an intolerable burden on the throughput of data.[34] However, they also recognise the potentially more thorny problem of public disquiet over the government's surveillance capabilities. As we have seen, this has been the problem for states such as the UK in various areas. The revelations by Edward Snowden through 2013 on the degree to which Western intelligence agencies have been intercepting communications data have only added to the vociferous lobby against extending states' monitoring powers. In the immediate future, this factor could prove to be as difficult for cyber security strategies as the technical issues.

Notes

1 M. Dunn Cavelty (2013) "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review* 15, 117.

2 S. Lawson (2012) "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States", *First Monday* 17/7, http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270, date accessed 10 November 2013.

DOI: 10.1057/9781137399625.0007

3 Cited in Lawson, "Putting the 'War' in Cyberwar".
4 J.A. Lewis (2005) "Aux Armes, Citoyens: Cyber Security and Regulation In the United States", *Telecommunications Policy* 29, 825.
5 Richards, *A Guide to National Security.*
6 Cited in Richards, *A Guide to National Security*, p. 6.
7 HM Government (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: TSO), pp. 29–30.
8 HM Government, *A Strong Britain*, p. 30.
9 *Guardian* (8 June 2011) "More Than 1000 Cyber-Attacks on mod, Says Liam Fox", http://national-security.governmentcomputing.com/news/2011/jun/08/1-000-cyber-attacks-on-mod-says-liam-fox, date accessed 7 July 2011.
10 M. Weber (1991 [1946]) *Max Weber: Essays in Sociology* (Abingdon: Routledge), p. 78.
11 P.W. Singer (2007) *Can't Win With 'Em, Can't Go to War Without 'Em: Private Military Contractors and Counterinsurgency* (Washington DC: Brookings. Policy Paper no.4), p. 3.
12 Lewis, "Aux Armes, Citoyens", p. 827.
13 Clarke and Knake, *Cyber War*, p. 116.
14 Clarke and Knake, *Cyber War*, pp. 114–5.
15 Clarke and Knake, *Cyber War*, p. 118.
16 J.S. Nye Jr. (2011) "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, p. 18.
17 Clarke and Knake, *Cyber War*, p. 155.
18 Nye, "Nuclear Lessons", p. 22.
19 Rid, *Cyber War Will Not Take Place,* p. 170.
20 See K. Geers (2010) "The Challenge of Cyber Attack Deterrence", *Computer Law and Security Review* 26/3, 298–303.
21 See J. Arquilla (26 July 2009) "Click, Click ... Counting Down to Cyber 9/11", *San Francisco Chronicle*, p. E2.
22 M.D. Young (2010) "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power", *Journal of National Security Law and Policy* 4, 177.
23 Dunn Cavelty, "From Cyber Bombs", p. 113.
24 G. Lucas, "Permissable Preventive Cyberwar", Presentation at University of Oxford: Ethics, Law and Armed Conflict, 23 November 2011.
25 See BBC News (8 November 2013) "Marine Guilty of Afghanistan Murder", http://www.bbc.co.uk/news/uk-24870699, date accessed 9 November 2013.
26 P. Olson (4 August 2013) "We Are Legion, Expect Us", *The Sunday Times Magazine*, 14–19.
27 Barrett, "Information Warfare", p. 687.
28 Giles, *Information Troops*, p. 54.
29 Giles, *Information Troops*, pp. 54–5.

DOI: 10.1057/9781137399625.0007

30 F. Flade (30 June 2010) "Hacker macht Jagd auf Online-Dschihadisten", *Die Welt*, http://www.welt.de/politik/article8236634/Hacker-macht-Jagd-auf-Online-Dschihadisten.html, date accessed 10 November 2013.
31 Lawson, "Putting the 'War' in Cyberwar".
32 Lawson, "Putting the 'War' in Cyberwar".
33 Clarke and Knake, *Cyber War*, p. 160.
34 Clarke and Knake, *Cyber War*, p. 161.

DOI: 10.1057/9781137399625.0007

6

Conclusions: A Pathway through the Forest

Abstract: *The conclusion reprises a three-tier categorisation of cyber warfare threats developed throughout the book. In the first tier are modern, cyber-enabled examples of traditional information operations which can happen both during conflict and in peacetime scenarios. In the second tier are cyber-attack activities which enable and shape the prosecution of conflict in the physical realm. The third tier comprises those activities over which, it is argued, there is most scepticism at present: namely cyber attacks which cause real physical death and destruction. Predicting the future, however, is a risky business. For this reason, policymakers need to continue to model and plan for such contingencies, while not allowing them to pervert the overall assessment of cyber security priorities.*

Richards, Julian. *Cyber-War: The Anatomy of the Global Security Threat*. Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399625.0008.

In this book I have attempted to define the anatomy of cyber war as a contemporary national security threat. I have taken a pathway through the dense forest of debate on this issue by breaking the question down into a number of constituent parts. First is the question of what cyber war is, and how it is being defined in official national security discourses. On the latter point, I have identified that a normative discourse is developing both in official policymaking circles and in academic discussion that identifies the threat of cyber war as a real and contemporary risk that is substantial if not existential for the state. The threat is identified as constituting a broad spectrum of activities, from information theft and denial to attacks on networks that have a real-world destructive outcome. Defining the threat in this way means that states have identified the need for a comprehensive and robust response in terms of capability and policy, even if the nature of that response has proved to be difficult to define at the present time.

In taking a critical look at this official securitisation of the threat of cyber war, we have identified that it breaks down into three dimensions. First is the dimension of information operations or information warfare (noting that definitions of the latter are sometimes more narrow than of the former, restricting themselves to specific information-related attack activities within the confines of actual military conflict). In the contemporary world, I have identified a number of examples of such activities. Sometimes these are closely associated with managing, shaping and perverting information around actual conflicts, such as was the case with the 2008 war between Russia and Georgia, or indeed the ongoing struggle between the state of Israel and the militant group Hezbollah. Numerous other examples could be cited and, I would argue, this dimension of conflict is likely to be a perennial feature from now on. Other examples concern situations that are not necessarily declared wars or conflicts but diplomatic disputes between states in the international arena, or disputes between civil organisations or identity-groups, or even attacks on organisations or states by individuals or loose groupings motivated loosely by ideology or a need to display technical prowess. Into this category fall the examples of the Syrian Electronic Army (SEA), the cyber attacks on Estonia in 2007, and the activities of groups such as Lulzsec. The blurring of boundaries between war and other types of dispute and conflict is, I would argue, a central element of this aspect of cyber war. Similarly important is the blurring of actors involved in these activities between military and civilian identities.

DOI: 10.1057/9781137399625.0008

An important point to note with this first category of cyber war is that events can sometimes be exaggerated and rendered as examples of "war", when they should more precisely be described as examples of criminality, activism or vandalism. The case of Estonia is particularly pertinent in this regard. When the attacks happened in 2007, many observers were quick to proclaim the outbreak of cyber war and to suggest that the world had crossed over from theoretical possibility to reality. More sober analyses after the event suggested – correctly in my view – that the attacks could not appropriately be called acts of war as such, but more acts of large-scale activism and vandalism. (We could, with some trepidation, also talk of an example of cyber terrorism here.) This is not to suggest that such acts are not serious threats to a state and its citizens, or that they are not indicative of the possibility for more ambitious and disruptive attacks in the future. The Estonians were right to point out at the time that the attacks represented a serious escalation in the history of cyber threats. But they are episodes which require a response more associated with criminal and judicial co-operation and interdiction than with military action at this time.

In the second category of the cyber war threat are risks that can be associated with more traditional notions of information warfare, namely attacks on military networks and associated systems that accompany and enable the prosecution of actual conflict. Since the end of the Cold War, the symbiotic link between rapidly accelerating advances in ICT and military development has led to the latest Revolution in Military Affairs (RMA), which is one very much rooted in technology. In a sense, this was a natural evolution of military affairs that had been underway throughout the twentieth century and particularly since the two World Wars, when electronic and automated systems such as radar and other forms of communications became part-and-parcel both of offence and defence in the military theatre. By the end of the century, these technologies had advanced to such a point that modern conflict – at least that involving advanced nations – was now very much "network-centric warfare", with military forces displaying a fundamental reliance on advanced networked communication capabilities in the successful prosecution of battle.

This means that modern warfare is accompanied and enabled by a host of cyber activities which target, shape and seek to disrupt networked communications in and around the military theatre. Capabilities such as Suppression of Electronic Air Defences (SEADs), for example,

DOI: 10.1057/9781137399625.0008

are generally central to any advanced contemporary military campaign. Again, the 2008 Russia–Georgia conflict displayed these attributes, as did a host of recent conflicts and skirmishes such as the Israeli bombing of the Syrian nuclear facility in 2007, and NATO campaigns in Yugoslavia and Libya to name but a few examples. It is entirely appropriate for modern militaries to develop tactical capabilities in these areas both in terms of being able to disrupt an adversary's tactical military communications in the event of battle, and being able also to protect their own networks from attack. Interestingly, such cyber capabilities combine seamlessly with more traditional kinetic capabilities, in that shaping and disrupting pivotal military communications nodes and systems can be conducted both by physical force and by electronic attack, and will often involve both. Such cyber activities are now an integral element of modern advanced warfare.

As we have discussed, the third category of the threat is the most controversial and disputed one at the present time. This is the notion of cyber attacks which have a real effect in the physical world in terms of death and destruction, and which could thus be described in similar terms to traditional attacks using armed force. There are several elements to this debate. First is the question of legal definitions. As we have seen, the only real framework we can adopt in trying to answer the question as to whether cyber attacks can be described as acts of war, is the existing collection of international treaties and norms which constitute the Law of Armed Conflict (LOAC). Davis Brown offers an interesting analysis of this question, looking both at the Geneva Conventions on the prosecution of conflict and the Hague law governing methods and means of warfare.[1] He concludes that while cyber space is different in fundamental ways from real space and, thus, existing legal concepts are difficult to apply, if one adopts an "effects-based" approach then there is no reason why cyber attacks could not be placed against similar legal tests as in other types of attack.[2] Thus, if a DDoS attack on a system led to the failure of a critical part of national infrastructure which in turn led to real harm amongst a part of the population, then the original attack could be said to have had the same effect as a kinetic military strike on the same piece of infrastructure.

In this way, attacks such as that on the Natanz nuclear facility in Iran using the Stuxnet malware fall into a contentious category. On the one hand, the attack caused real physical damage to the centrifuges in the plant in the same way that a physical attack might have caused. On the

DOI: 10.1057/9781137399625.0008

other hand, despite many observers heralding Stuxnet as the first example of a military-grade cyber weapon in action, the attack probably did not cause much more physical damage than would a saboteur wielding a metal bar. Certainly, this was an attack that may have caused considerable disruption to the Iranian military nuclear programme, but whether it was an act of war, militarily or legally, is dubious.

Of course, as with the case of the Estonian cyber attacks, Stuxnet may have more significance for its demonstration of what might be possible in the future, rather than what actually happened at the time. As we have discussed, critics such as Rid[3] and Lewis[4] doubt whether catastrophic cyber attack will ever be seen. Technically, achieving such an attack is a much more difficult task than is normally supposed. It is almost certainly beyond the capability of any sub-state terrorist group, and even a well-resourced state might find it difficult to achieve. At the same time, there is much interest around examples of where attacks on critical infrastructure have or could have caused real-world destruction. One is an attack in the Spring of 2000 in Australia. Here, a disgruntled citizen attacked the SCADA system of a sewage plant in Maroochy Shire in Queensland, causing a spill of more than a million litres of raw sewage into the surrounding area. It transpired that the 49-year-old attacker was unhappy at having been rejected for a job at the Maroochy Shire Council.[5] A more recent example concerned a test conducted by the US Department of Energy at a laboratory in 2007, dubbed the Aurora test, in which hackers successfully disabled by cyber attack a large electricity generator to the point of destruction.[6]

The obvious question is this: if low-level attacks by an individual or a small group of individuals can cause damage of this extent to elements of critical national infrastructure, could not a much larger and more focused hacking effort cause a much more serious level of disruption using cyber techniques? Critics would suggest that the answer is still "no", for two reasons. First, even if one particular system could be attacked and disrupted in a focused onslaught, whether a range of systems which together constituted a substantial element of the critical national infrastructure could be attacked simultaneously is still doubtful from a technical point of view. This not to say that serious disruption could not be caused by determined attackers, but whether an existential threat to security could be achieved is still very much subject to doubt.

Second, as we have discussed in Chapter 4, is the question of strategic considerations when looking at the likelihood of catastrophic cyber

DOI: 10.1057/9781137399625.0008

attack. The Chinese government, as we have seen, has often accused those in the West who are complaining vociferously about the threat of cyber war of being stuck in an old-fashioned Cold War mentality. They argue that the rise of nations such as Russia and China, within the context of growing power multi-polarity in the post–Cold War world, does not have to mean a zero-sum game of military confrontation with the traditional hegemon, the US. Just because Russia and China have fundamentally different ideological outlooks from the West, their rise does not have to mean that their power accumulation is incompatible with peaceful co-existence alongside Western states, they argue. Whether or not this is true, I have argued that discussion of the threat of cyber warfare in Western policymaking arenas could usefully encompass further attention on Robert Jervis's "perceptions and misperceptions" thesis around the hostile intentions of states.[7] Whether it makes strategic political or economic sense for the likes of China to effectively launch a Third World War against the US using cyber means should be subjected to very serious scrutiny. I would argue that some of the fictional scenarios of catastrophic cyber attacks on Western societies do not necessarily help to understand the nuanced strategic picture, even if they have some utility in exploring the extremes of technical possibilities. Red Teaming is probably happening a lot inside Western military and intelligence installations at the present time, but I suggest it should happen a lot more, and especially around this issue.

It is interesting to note that one of the key technical issues that complicates the picture of whether or not states are involved in large-scale cyber attack is that of attribution of attacks over networks. The principle of contemporary multi-stage and multi-layered attacks, which are often referred to as Advanced Persistent Threats (APTs), is that they are conducted over multiple international boundaries using a very complex and bewildering sequence of computers, many of which are unwitting staging-posts for passing traffic and are selected merely by dint of having an open connection to the internet. The ability to trace an attack all the way back through multiple stages to the original author is becoming increasingly difficult, if not impossible. China itself has pushed for a greater degree of attribution to be appended to IP addresses, in advance of the transition from IP version 4 to version 6, including a state-level flag on all IP addresses.[8] At one level, this might seem an unlikely proposition if China was the author of many attacks and wished to obscure that fact. At the same time, China is clearly worried about information

DOI: 10.1057/9781137399625.0008

control across its own population, and wishes to see if its own citizens are downloading prohibited publications from overseas networks.

The question of attribution is, nevertheless, a key consideration when it comes to considering military policy in countering cyber attack. A key element of a deterrent strategy is the need to make it clear to potential attackers that they will be punished for their actions, either by a large cyber attack in return or by more kinetic attack methods, or indeed by a combination of the two. But the power of a deterrent is making it plain that threats will sometimes be backed up by action, and such action is only possible if a defending nation can be absolutely certain about who has attacked. At the moment, words are all that can be directed at China, for example, since the latter can not unreasonably claim that there simply is not sufficient evidence to show that the PLA is the author of most of the major cyber attacks being directed at Western networks. With a considerable strengthening of state-level attribution the whole diplomatic equation could change very substantially. In positive terms, this could mean a greater level of international co-operation and agreement on curbing cyber attacks.

One of the key questions, therefore, is whether and how the attribution problem can be solved. For states with major cyber capabilities and aspirations of their own, the equation is an extremely complex one. On the one hand, attribution will allow potentially better controls on the threat and better possibilities for deterrence and counter-attack. On the other hand, clearer attribution will also curb the activities of defending states themselves, since they will also be restricted in their ability to gather intelligence and conduct covert cyber operations without being spotted. One solution, again adopting traditional thinking about international agreement on LOAC, is to accept that cyber war will happen in the same way that traditional war will sometimes happen, but to agree "rules of the road" around how such war is conducted. The existing Hague law principles of military necessity, humanity and chivalry could apply to cyber attack as much as to any other form of armed conflict, providing the major international actors could agree on such conventions.

However, there has also been much debate about whether adopting existing traditional notions of warfare and the laws governing it can be a suitable approach in the face of a technology that it fundamentally different and new. Perhaps all the existing rulebooks need to be thrown out of the window when considering how to regulate the cyber threat.

DOI: 10.1057/9781137399625.0008

In this sense, technical solutions to issues such as attribution may not be the best or the only answer. Analysts of APTs such as Barnum[9] have pointed out that it cannot be assumed that the attacker holds all the aces in conducting APT attacks. As with all malware attacks, cyber operations are fundamentally "fire and forget" attacks. Once the methodology and technique are out of the barracks, they are immediately open to scrutiny and mitigation. The multi-faceted nature of APTs means that mitigation strategies that can keep the defender sufficiently upstream and proactive in the process, rather than downstream and reactive, are undoubtedly difficult and increasingly so as technology improves. But the technology improves for the defender as well as for the attacker, and successful mitigation is therefore more than possible. As Hutchins, Cloppert and Amin argue, and I have argued above in the context of the threat from China, a successful cyber defence operation is as much about understanding the "why" of the attacker (namely their motivations, objectives and capabilities) as about the "what" they are doing in a technical and physical sense.[10]

This leads to a consideration that behavioural and political analyses need to be an integral part of cyber security policy formation. There is also a need to think creatively about response strategies and to try to avoid the trap of falling into traditional notions of threat and protection. If we take the hypothesis that contemporary threats of cyber war are more in the realm of political activism, crime and possibly lower-level terrorism than in that of an all-out catastrophic warfare, then responses need to be designed accordingly. There is also the question, discussed extensively in the previous chapter, of the confusing crossover between public and private sectors in the contemporary cyber threat landscape. We have seen the paradox for countries such as the US, where an elevation of the threat in public discourse, and the very visible formation of capabilities such as Cyber Command, are coupled with the need for minimal interference and imposition of red tape on private industry. When some estimates suggest that as much as 95 percent of the communications traffic of the Department of Defense in the US travels over privately installed and owned network infrastructure,[11] the policy conundrum is a challenging one.

The director of UK's Government Communications Headquarters (GCHQ) Sir Iain Lobban is among many senior policymakers in this area who have suggested that there needs to be an unprecedented and symbiotic relationship between government and private industry in the

DOI: 10.1057/9781137399625.0008

area of cyber security. Indeed, in a rare public statement, Lobban used the word "resilient" in describing the cyber security posture needed by the overall state.[12] One of Lobban's forebears at GCHQ Sir David Omand has discussed the notion of resilience in the context of the way in which modern security threats have evolved from the existential threat of nuclear war during the twentieth century. When faced with contemporary security threats such as terrorism, or indeed even those from factors such as extreme weather events or climate change, there can be no "absolute security". At the same time, leaving security to chance is not an option.[13]

A security policy that is structured around resilience rather than absolute security is perhaps more suited to the contemporary twenty-first century environment than is the thinking adopted during the Cold War. Such a policy has a number of inherent factors, not least the notion that protecting against attack, and preparing for mitigation of the effects when an attack does occur, can be as appropriate and effective as attempting to identify and robustly respond to an attack. What this means in the cyber context is that improved cyber security of networks, in both physical and behavioural terms, coupled with better monitoring, analysis and mitigation of attacks, when they do occur, could provide most of the answers to the threat. This may be doubly appropriate given the technical complexities, bordering on impossibility, of being able to accurately identify the author of a cyber attack. This approach also means that much of the work will need to be done in the private sector, where most of the networks constituting the critical national infrastructure are now situated. It may even become commercially beneficial to demonstrate to users a high degree of information security, much as has happened with the virtues of demonstrating "green credentials" in recent years. This does not mean that government can just sit back and absolve itself of all responsibility. As Lucas has argued, contemporary cyber security "will almost certainly require government intervention, legislation, and perhaps funding".[14]

It is clear, therefore, that conceptualising cyber war and the appropriate strategies needed in response is a hugely complex business. Not surprisingly, a range of different analogies have been tried out in the process. Seized with the existential potential of cyber war, many have settled on the analogy of the threat of nuclear war in the twentieth century, both in terms of conceptualising the degree of threat and of considering how states and the international community respond to the sort of military

DOI: 10.1057/9781137399625.0008

threat that has not been seen before. However, others have suggested that cyber weapons are more akin to chemical or biological weapons than to nuclear weapons. This is because cyber weapons are difficult to target precisely, can have unexpected and potentially indiscriminate effects, but at the same time are somewhat limited in their destructiveness and can quickly be mitigated once they are released. Yet others would say that this is still too far to go in considering cyber weapons. Cyber warfare, or even cyber terrorism, are not the real threats, but rather cyber activism, vandalism and crime. The vanguard of the application of cyber security should be the police, and not the military.

I have argued that catastrophic cyber attack has not yet been seen, and is unlikely to be seen in the near future, for a combination of reasons relating to technical complexity and the strategic motivations of attackers. However, I would not go so far as to say that it will never be seen. The co-founder of Intel Corporation Gordon Moore has an informal rule of thumb that is perhaps pertinent in this area of discussion. Moore's Law says that technical progress in computing (with particular reference to the degree to which semiconductor capacity increases) will outstrip progress seen in any previous industries, both in terms of capability and pace. For this reason, I would suggest that governments and militaries will need to continue thinking about the possibilities for cyber war for some years to come, and to watch developments very closely with an eye to developing appropriate counter-strategies and responses.

Notes

1 D. Brown (2006) "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict", *Harvard International Law Journal* 47/1, 179–221.
2 Brown, "A Proposal", pp. 187–8.
3 Rid, *Cyber War will Not Take Place*.
4 J.A. Lewis (2002) *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington DC: Center for Strategic and International Studies (CSIS)).
5 Rid, *Cyber War will Not Take Place*, p. 74.
6 J. Meserve (26 September 2007), 'Sources: Staged Cyber Attack Reveals Vulnerability in Grid', *CNN*, http://edition.cnn.com/2007/US/09/26/power.at.risk/, date accessed 10 November 2013.
7 Jervis, "War and Misperception".

DOI: 10.1057/9781137399625.0008

8 D.D. Clark and S. Landau (2010) "Untangling Attribution", *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy,* p. 34.
9 S. Barnum (2013) *Standardizing Cyber Threat Intelligence information with the Structured Threat Information eXpression (STIX)* (Maclean VA: The Mitre Corporation), p. 3.
10 E.M. Hutchins, M.J. Cloppert and R.M. Amin (2010) "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", *Proceedings of the 6th International Conference on Information Warfare and Security* (ICIW 11), p. 7.
11 Brown, "A Proposal", p. 194.
12 Iain Lobban, address at the International Institute of Strategic Studies, London, 12 October 2010. Cited in Rid, *Cyber War will Not Take Place*, p. 111.
13 Cited in Richards, *A Guide to National Security*, p. 33.
14 Lucas, "Privacy, Anonymity, and Cyber Security", p. 108.

DOI: 10.1057/9781137399625.0008

Bibliography

C. Albanesius (16 October 2013) "Indonesia Tops China as Cyber Attack Capital", *PC Mag.com*, http://www.pcmag.com/article2/0,2817,2425836,00.asp, date accessed 18 November 2013

R.J Aldrich (2010) *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: HarperPress)

J. Anderson (2007) "The HUMINT Offensive from Putin's Chekist State", *International Journal of Intelligence and Counterintelligence* 20: 258–316

J. Arquilla (26 July 2009) "Click, Click ... Counting Down to Cyber 9/11", *San Francisco Chronicle*

J. Arquilla and D. Ronfeldt (1993) "Cyberwar Is Coming!", *Comparative Strategy* 12/2: 141–65

R. Ayers (1999) "The New Threat: Information Warfare", *The RUSI Journal* 144/5: 23–7

S. Barnum (2013) *Standardizing Cyber Threat Intelligence information with the Structured Threat Information eXpression (STIX)* (Maclean VA: The Mitre Corporation)

B.M. Barrett Jr. (2005) "Information Warfare: China's Response to US Technological Advantages", *International Journal of Intelligence and Counterintelligence* 18: 682–706

BBC News (8 November 2013) "Marine Guilty of Afghanistan Murder", http://www.bbc.co.uk/news/uk-24870699, date accessed 9 November 2013

Z. Bijian (2005) "China's 'Peaceful Rise' to Great Power Status", *Foreign Affairs* 84/5: 18–24

DOI: 10.1057/9781137399625.0009

D. Brown (2006) "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict", *Harvard International Law Journal* 47/1: 179–221

B. Buzan, O. Waever and J. De Wilde (1998) *Security: A New Framework for Analysis* (London: Lynne Riener)

K.M. Campbell (2002) "Globalization's First War?", *The Washington Quarterly* 25/1: 5–14

A.K. Cebrowski and J.J. Garstka (1998) "Network-Centric Warfare: Its Origin and Future", US Naval Institute, *Proceedings Magazine* 124/1/1

W.G. Chapman (1996) *Organizational Concepts for the "Sensor-to-Shooter" World: The Impact of Real-Time Information on Air-Power Targeting* (School of Advanced Airpower Studies, Alabama), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA349387, date accessed 18 November 2013

D.D. Clark and S. Landau (2010) "Untangling Attribution", *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*

R.A. Clarke and R.K. Knake (2010) *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins)

CNN (16 August 2007) "Hezbollah Video Game; War with Israel", http://edition.cnn.com/2007/WORLD/meast/08/16/hezbollah.game.reut/, date accessed 12 December 2013

Daily Mail (21 November 2011) " 'Russian' Hackers Seize Control of US Public Water System by Remotely Destroying Pump", http://www.dailymail.co.uk/sciencetech/article-2064283/Hackers-control-U-S-public-water-treatment-facilities.html, date accessed 12 December 2013

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

M. Dunn Cavelty (2013) "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review* 15: 105–22

Economist (4 August 2012) "The Company That Spooked the World", http://www.economist.com/node/21559929, date accessed 18 November 2013

J.P. Farwell and R. Rohozinski (2011) "Stuxnet and the Future of Cyber War", *Global Politics and Strategy* 53/1: 23–40

DOI: 10.1057/9781137399625.0009

F. Flade (30 June 2010) "Hacker macht Jagd auf Online-Dschihadisten", *Die Welt*, http://www.welt.de/politik/article8236634/Hacker-macht-Jagd-auf-Online-Dschihadisten.html, date accessed 10 November 2013

Foxnews (25 February 2013) "Chinese Hackers Seen as Increasingly Professional, Experts Say", http://www.foxnews.com/tech/2013/02/25/chinese-hackers-seen-as-increasingly-professional-experts-say/, date accessed 18 November 2013

D. A. Fulghum, R. Wall and A. Butler (2007) "Cyber Combat's First Shot: Attack on Syria Shows Israel Is Master of the High-Tech Battle", *Aviation Week and Space Technology* 167/21

J.L. Gaddis (1972) *The United States and the Origins of the Cold War, 1941–1947* (New York: Columbia University Press)

K. Geers (2010) "The Challenge of Cyber Attack Deterrence", *Computer Law and Security Review* 26/3: 298–303

K. Geers (2011) *Strategic Cyber Security* (Tallinn: CCD COE)

R.Z. George (2004) "Fixing the Problem of Analytical Mindsets: Alternative Analysis", *International Journal of Intelligence and Counterintelligence* 17: 385–404

K. Giles (2011) "Information Troops – A Russian Cyber Command?" In C. Czosseck, E. Tyugu and T. Wingfield (eds) *Proceedings of the 3rd International Conference on Cyber Conflict* (Tallinn: CCD COE)

D. Gregory (2010) "War and Peace", *Transactions of the Institute of British Geographers* 35: 154–86

S.B. Griffith (1971) *Sun Tzu: The Art of War* (Oxford: Oxford University Press)

Guardian (8 June 2011) "More Than 1000 Cyber-Attacks on mod, Says Liam Fox", http://national-security.governmentcomputing.com/news/2011/jun/08/1-000-cyber-attacks-on-mod-says-liam-fox, date accessed 7 July 2011

L. Harding and C. Arthur (30 April 2013) "Syrian Electronic Army: Assad's Cyber Warriors", *The Guardian*

S. Herzog (2011) "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security* 4/2: 49–60

K. Hille and P. Taylor (24 April 2013) "Huawei 'Not Interested in us Any More' after Repeated Denials for Market Access", *CNN*, http://edition.cnn.com/2013/04/24/business/huawei-not-interested-us/index.html, date accessed 18 November 2013

M.S. Hirshberg (1993) "Consistency and Change in American Perceptions of China", *Political Behavior* 15/3: 247–63

DOI: 10.1057/9781137399625.0009

HM Government (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: TSO)
A. Hodges (1992) *Alan Turing: The Enigma* (London: Vintage)
D.E. Hoffman (27 February 2004) "CIA Slipped Bugs to Soviets", *The Washington Post*
M.F. Hopkins (2007) "Continuing Debate and New Approaches in Cold War History", *The Historical Journal* 50/4: 913–34
S.P. Huntington (1993) "The Clash of Civilizations?", *Foreign Affairs* 72/3: 22–49
E.M. Hutchins, M.J. Cloppert and R.M. Amin (2010) "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", *Proceedings of the 6th International Conference on Information Warfare and Security* (ICIW 11)
R. Jervis (1978) "Cooperation under the Security Dilemma", *World Politics* 30/2: 167–214
R. Jervis (1988) "War and Misperception", *The Journal of Interdisciplinary History* 18/4: 675–700
Joint Chiefs of Staff (2012) *Electronic Warfare*. Joint Publication 3-13.1
D. Kahn (2001) "An Historical Theory of Intelligence", *Intelligence and National Security* 16/3: 79–92
J. Kraska (2010) "How the United States Lost the Naval War of 2015", *Orbis* 54/1: 35–45
R. Langner (2011) "Stuxnet: Dissecting a Cyberwarfare Weapon", *IEEE Security and Privacy* 9/3: 49–51
S. Lawson (2012) "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States", *First Monday* 17/7, http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270, date accessed 10 November 2013
A. Leland and M-J. Oboroceanu (2010) *American War and Military Operations Casualties: Lists and Statistics* (Washington DC: Congressional Research Service)
J.A. Lewis (2005) "Aux Armes, Citoyens: Cyber Security and Regulation in The United States", *Telecommunications Policy* 29: 821–30
J.A. Lewis (2012) *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. (Washington DC: Center for Strategic and International Studies (CSIS)
Q. Liang and X. Wang (1999) *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House)

DOI: 10.1057/9781137399625.0009

G.R. Lucas Jr. (2013) "Privacy, Anonymity, and Cyber Security", (VU University Amsterdam: Amsterdam Law Forum), http://www.ojs.ubvu.vu.nl/alf/article/download/311/485 date accessed 12 December 2013

W.J. Lynn III (2010) "Defending a New Domain: The Pentagon's Cyerstrategy", *Foreign Affairs* 89/5: 97–108

M. Macdonald (8 October 2012) "China Slams 'Cold War Mentality' in US report", *International Herald Tribune*

J. Mackinlay (2001) "'Intervening in Conflict: The Policy Issues'", *Conflict, Security and Development* 7/1: 167–99

Mandiant (2013) *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria VA: Mandiant)

V. Mangin and C. Freeman (10 November 2012) "Chinese Official Accuses Washington of 'Cold War' mentality", *The Telegraph*

M. McConnell (28 February 2010) "How to Win the Cyber-War We're Losing", *The Washington Post*

J. Meserve (26 September 2007) "Sources: Staged Cyber Attack Reveals Vulnerability in Grid", *CNN*, http://edition.cnn.com/2007/US/09/26/power.at.risk/, date accessed 10 November 2013

MOD, DCDC (2010) *The Future Character of Conflict* (Bicester: DSDA Operations Centre)

M. Mylrea (15 November 2009) "Brazil's Next Battlefield: Cyberspace", *Foreign Policy Journal,* http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/, data accessed 18 November 2013

NATO (2010) *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, Adopted by Heads of State and Government in Lisbon: Active Engagement, Modern Defence (Brussels)*, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf, accessed 16 September 2011

S. Nider (21 May 2003) "Transformative Military Plan Vindicated in Iraq", *The Hill*, http://www.dlc.org/ndol_cif23c-2.html?kaid=85&subid=65&contentid=252695, date accessed 18 November 2013

R. Norton-Taylor (18 January 2010), "UK Military Chiefs Clash Over Future Defence Strategy", *The Guardian*

J.S. Nye Jr. (2010) *Cyber Power* (Harvard Kennedy School: Belfer Center for Science and International Affairs)

J.S. Nye Jr. (2011) "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly:* 18–38

DOI: 10.1057/97811373996250009

P. Olson (4 August 2013) "We Are Legion, Expect Us", *The Sunday Times Magazine*
D. Rapoport (2002) "The Four Waves of Rebel Terror and September 11", *Anthropoetics* 8/1
K. Rawlinson (1 November 2011) "China and Russia Accused of Orchestrating Cyber Attacks", *The Independent*
J. Richards (2010) *The Art and Science of Intelligence Analysis* (Oxford; Oxford University Press)
J. Richards (2012) *A Guide to National Security: Threats, Responses and Strategies* (Oxford: Oxford University Press)
T. Rid (2012) "Cyber War Will Not Take Place", *Journal of Strategic Studies* 35/1: 5–32
T. Rid (2013) *Cyber War Will Not Take Place* (London: Hurst and Co)
N.M Ripsman and T.V. Paul (2010) *Globalization and the National Security State* (Oxford: Oxford University Press)
H. Rulong (20 April 2013) "Letters: Cyberspace and the State", *The Economist*
S. Saad, S. B. Bazan and C. Varin (2011) "Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a New Strategic Battlefield", *Proceedings of the WebSci Conference 2011, Koblenz*, http://journal.webscience.org/526/, date accessed 18 November 2013
M.N. Schmitt (1999) *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework* (Wright-Patterson AFB, OH: US Air Force, Institute for Information Technology)
R. Silverstein (11 May 2013) "Advanced Israeli Drone Hijacked by Iran or Hezbollah, then Destroyed by Israel", *Tikun-Olam*, http://www.richardsilverstein.com/2013/05/11/advanced-israeli-drone-hijacked-by-unknown-hostile-party-then-destroyed-by-israel/, date accessed 18 November 2013
P.W. Singer (2007) *Can't Win With 'Em, Can't Go to War Without 'Em: Private Military Contractors and Counterinsurgency* (Washington DC: Brookings. Policy Paper no.4)
J. Smith (4 October 2011) "Rogers: US Must Confront "Intolerable" Chinese Espionage", *National Journal*, http://www.nationaljournal.com/njonline/rogers-u-s-must-confront-intolerable-chinese-cyberespionage-20111004, date accessed 10 November 2013
M. Soares (12 June 2010) "ikiLeaked Cable Says 2009 Brazilian Blackout Wasn't Hackers, Either", *Wired,* http://www.wired.com/threatlevel/2010/12/brazil-blackout/, date accessed 10 November 2013

DOI: 10.1057/9781137399625.0009

State Journal Register, Springfield, Illinois (2 December 2011) "Vacationing Contractor Talks about 'Cyber Attack' That Wasn't"

J. Swaine and R. Sanchez (11 March 2013) "China must stop 'unprecedented wave of cyber attacks', says Obama administration", *The Telegraph*

M.C. Waxman (2011) "Cyber-Attacks and the Use of Force", *The Yale Journal of International Law* 36: 421–59

M. Weber (1991 [1946]) *Max Weber: Essays in Sociology* (Abingdon: Routledge)

M.D. Young (2010) "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power", *Journal of National Security Law and Policy* 4: 173–96

DOI: 10.1057/9781137399625.0009

Index

DOI: 10.1057/9781137399625.0010

DOI: 10.1057/9781137399625.0010

DOI: 10.1057/9781137399625.0010