CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org.uk
F: +44 (0)20 7957 5710 www.chathamhouse.org.uk
Charity Registration Number: 208223

Working Paper

The Vulnerabilities of Developed States to Economic Cyber Warfare

Paul Cornish

Head, International Security Programme and Carrington Professor of International Security, Chatham House

June 2011

INTRODUCTION

The central features of the 'cybered' world of the early 21st century are the interconnectedness of global communications, information and economic infrastructures and the dependence upon those infrastructures in order to govern, to do business or simply to live. There are a number of observations to be made of this world. First, it is still evolving. Economically developed societies are becoming ever more closely connected within themselves and with other, technologically advanced societies, and all are becoming increasingly dependent upon the rapid and reliable transmission of ideas, information and data. Second, where interconnectedness and dependency are not managed and mitigated by some form of security procedure, reversionary mode or redundancy system, then the result can only be a complex and vitally important communications system which is nevertheless vulnerable to information theft, financial electronic crime, malicious attack or infrastructure breakdown. Third, while 'developed states' and their occupants are generally assumed to be the target of so much of this nefarious activity, it does not necessarily follow that a political structure invented in 1648 – the sovereign state – will be the most appropriate means to deal with cyber-vulnerability. Yet it is not clear what alternatives to the sovereign state – if any – might be available.

The more fundamental observation is that developed societies seem unwilling or unable to take counsel of their fears about cyber space. Perhaps because the world is so interconnected, and perhaps because societies depend so much on the complex of infrastructures for what is needed and desired, there is a reluctance to accept, and in some quarters an inability to understand that these highly developed societies have made themselves vulnerable to miscreants, criminals and aggressors. Technological strength and superiority has, unfairly though it might seem to its originators and beneficiaries, prompted what military analysts would describe as 'asymmetric' vulnerability, where a fleet-footed and sharp-witted adversary can manoeuvre so fast and so decisively that the strongest and most elaborate defences are turned into a cumbersome liability and a disadvantage. Since too little is known about who might wish to use cyber space against developed societies, and to what end, it is at least notionally possible that developed societies might be comprehensively, structurally vulnerable to a well organised and capable cyber aggressor of some sort, able to turn a society's dependencies into vulnerabilities and strengths into weaknesses. If developed states could be vulnerable in this way, then this should be considered a strategic challenge of

the highest order. The easiest, perhaps child-like response to such a possibility is to refuse to contemplate it at all and instead to believe fervently in a more positive and wholesome outcome. There can also be a more mature, if rather fatalist response which leads to a broadly similar position – that of the ostrich with its head buried firmly in the sand. During the Cold War, at the height of the doctrine of east-west mutual assured destruction (MAD), there appeared to be little preparation (at least in public) given to running the country after a massive nuclear onslaught. After all, why be concerned with such things when those who survive would be doomed to spend their remaining days in scenes similar to Cormac McCarthy's *The Road*? Perhaps, therefore, the complete dependence on the cybered world is generating a complacency and fatalism similar to that caused by the complete vulnerability to MAD.

This discussion paper is concerned with states and societies (rather than businesses or individuals) and their vulnerability, through interconnectedness and dependence, to aggressive economic action either from, or facilitated by cyber space. This paper is not, therefore, an analysis of the extent and gravity of financial cyber-crime; that subject has been discussed fully elsewhere.[1] Neither does the paper examine child exploitation and other forms of computer-based crime, important though these are. Instead, I ask whether economic cyber warfare should indeed be considered a strategic problem. In the words of the 2010 UK *National Security Strategy*, national strategy must be 'a combination of ends (what we are seeking to achieve), ways (the ways by which we seek to achieve those ends) and means (the resources we can devote to achieving the ends).'[2] Reversing the trajectory, I ask whether the economy might be the way, and cyberspace the means with which to attack the organisation and coherence of a modern developed state; not for financial or criminal gain, and not in order to achieve a terrorist 'spectacular', but for maximal political or strategic ends?

I take a stepwise approach to answering this question, beginning with a discussion of *economic warfare* and then of *cyber warfare*, before discussing the possibility of the composite idea of *economic cyber warfare*. What might be the incentives and disincentives to partake in economic cyber warfare, how seriously should it be taken and is the modern state the best organisation to deal with this security challenge?

---

[1] See most recently UK Cabinet Office and Detica, The Cost of Cyber Crime: A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office (Guildford, Surrey: Detica Limited, 2011).
[2] HM Government, A Strong Britain in an Age of Uncertainty: The National Security Strategy (London: TSO, Cm 7953, October 2010), p.10.

ECONOMIC WARFARE

Economic warfare has long been associated with military tactics and operations; a relatively low level of activity albeit with a very high potential for damage and destruction. Throughout history, the most able and successful military commanders have sought to identify their opponent's critical strength or weakness (the 'centre of gravity', in Clausewitzian terms) and then to attack it in order to bring the conflict to a quick and decisive end. To the extent that the opponent might be dependent on aspects of a functioning economy for access to food, water, transport, ammunition and military equipment, then it can make sense militarily (if not in humanitarian terms) to attack and destroy the economic infrastructure which produces these commodities or provides these services.

There have been many examples of this so-called 'scorched earth' policy in time of war. The Scythians famously destroyed food supplies and poisoned wells in order to defeat the invasion by Darius I of Persia in 512 BCE. In 1868 General William Sherman, the Union general observed that 'Amerindian troubles' would cease only with 'the ringleaders … hung [sic], their ponies killed, and such destruction on their property as will make them very poor.'[3] The Russians used scorched earth tactics against the invading armies of both Napoleon and Hitler, and there have been many other variations on the theme including the forcible resettlement of local populations and large scale defoliation using chemical agents. By the late twentieth century the deliberate infliction of damage on civilians and non-combatants had become so extensive that it was banned under international humanitarian law:

It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out the civilians, to cause them to move away, or for any other motive.[4]

---

[3] Douglas Porch, 'Imperial Wars: from the Seven Years War to the First World War', in Charles Townshend (ed.), *The Oxford Illustrated History of Modern War* (Oxford University Press, 1997), p.95,

[4] Additional Protocol 1 (1977) to the Geneva Conventions 1949, Article 54.2. Adam Roberts and Richard Guelff, *Documents on the Laws of War* (Oxford University Press, Third Edition, 2000), p.450.

For all the death and destruction they cause, these activities could nevertheless all be described as *tactical* or *operational* variants of economic warfare, ancillary to the main military effort. There is also the national strategic level to consider, where the goal is to use all available levers of national power in order to achieve the desired effect before, or even as an alternative to the threat or use of armed force.[5] *Strategic* economic warfare is intended to limit an adversary's capacity to make war in the first place, by destroying the economy that would sustain such an effort. Naval blockades, economic sanctions, commerce raiding and the use of strategic air power against cities and industrial centres would all come under the rubric of strategic economic warfare. More recently, Saddam Hussein's decision to destroy oil fields as he withdrew from Kuwait in 1991 seemed intended to limit both the case for military action against Iraq and the capacity to do so. And efforts in Afghanistan since 2001 to eradicate opium poppy cultivation have, in part, been driven by the need to destroy the Taliban's economic base of activity.

Yet in spite of activities in Afghanistan, economic warfare is widely considered to be a thing of the past: partly because of the objection, on humanitarian grounds, to its indiscriminate nature; partly because national economies are considered to be more tightly intertwined in the global trading and investment system than ever before; and partly, finally, because it has been widely assumed to have failed in recent years to prevent conflict or even to modify the behaviour of oppressive regimes towards their domestic populations. Yet this brief survey of economic warfare does raise three questions to be asked of its putative cyber variant. First, what would be the motives and goals of those undertaking economic cyber warfare? Second, at what levels of activity, political and military, would economic cyber warfare take place? And finally how, if at all, might economic cyber warfare be regulated? Would it be constrained by international humanitarian law in the same way that its non-cyber predecessor has been, or would it best be understood as a strategic-level equivalent of digital brigandage?

[5] See Colin Gray, *Modern Strategy* (Oxford University Press, 1999), p,162.

CYBER WARFARE

'Cyber warfare' is becoming a much-used term, albeit with very little agreement as to its precise meaning. Some see cyber warfare (or even full-scale, self-contained cyber *war*) as the new paradigm for inter-state conflict. Others see it as little more than a string of alarmist anecdotes, which often seem closer to the world of science fiction than public policy. The median position is to suggest that cyber warfare is at least becoming one aspect of inter-state conflict with several distinguishing features. In some cases, the parallels with conventional and economic warfare are clear. But in other respects cyber warfare would require new thinking and new practice where conflict between states is concerned.

As with conventional and economic warfare, the cyber variant could take place on various levels. It could be undertaken tactically and operationally, for example, in order to 'write down' the capability of an adversary's armed forces. For the present at least, cyberspace is arguably best understood as the 'fifth battlespace', alongside the more traditional arenas of land, sea, air and space. By this view, cyber warfare is a new but not entirely separate component of the multifaceted environment in which modern conflict takes place. Cyber warfare also holds out the possibility of achieving political and strategic goals without the need for armed conflict, by making it possible to attack the machinery of state, financial institutions, the national energy and transport infrastructure and public morale. Another parallel with economic warfare is that in cyberspace the boundaries are blurred between the military and the civilian, prompting familiar ethical and legal questions over the requirement to ensure discriminate and proportionate effect in targeting doctrine and in rules of engagement.

Where there are similarities between economic and cyber warfare there are also important differences. In the first place, it is more accurate to say that cyber warfare *dissolves* the boundaries between the physical and the virtual worlds, thus making it extraordinarily difficult to answer the ethical and legal questions mentioned above. Cyber warfare cannot yet be described as a politically constrained phenomenon, where international humanitarian law (or the law of armed conflict) can be applied in a reasonably straightforward fashion. In a sense cyberspace is *terra nullius*, currently beyond the reach of mature political discourse. And it is precisely the *absence* of a constraining political framework that could be seen to operate around and within cyber warfare that makes cyberspace so attractive as a place in which to pursue aggressively cultural, religious, economic, social and even – paradoxically –

political goals. There is a beguiling and dangerous argument that cyber warfare can be preferable as a 'painless' or 'bloodless' form of conflict that can nevertheless deliver decisive outcomes. Yet victory and defeat might be far from recognizable in cyberspace. These concepts have little traction in a domain where political, ideological, religious, economic and military combatants could 'fight' for varying reasons according to different timescales, and apply their own code of conduct to the fight. The result would be a particularly chaotic sphere of conflict in which it is not yet obvious that a common framework of ethics, norms and values could apply.

The second area of divergence concerns the distribution of power and influence. Governments and major commercial enterprises have considerable authority in cyberspace, just as they do in the physical world. But cyberspace is characteristically more anarchic; power and influence can be distributed very widely, giving disproportionate strength to small and otherwise insignificant non-state actors and even individuals. Cyber warfare might even be the archetypal illustration of the 'asymmetric' style of conflict mentioned above, in which one opponent might be weak in conventional terms but is clever and agile, while the other is strong but complacent and inflexible. Operating behind false internet addresses, foreign servers and aliases, these actors could act with almost complete anonymity and relative impunity, at least in the short term, while achieving very significant destructive effect (as demonstrated by the 'clickskrieg' against Estonia in 2007).

The third and final distinction to be drawn between conventional and economic warfare on the one hand, and cyber warfare on the other would be in the rapidity with which security threats and challenges could evolve and be met. The pace of change in cyberspace could be so abrupt as to render the action/reaction cycle of traditional strategy out of date before it has even begun. In the past, whenever one side fielded a new technology or weapon system the opposing side would react with crown that development with its own innovation and so the balance of advantage would swing back and forth. This action/reaction cycle would often be measured in years; a process which can only be described as ponderous when decisive cyber innovation can be measured in days and weeks.

It seems that cyber warfare, like economic warfare, could usefully be analysed in terms of ends, ways and means. What would be the motive behind a large-scale cyber attack? At what level would such an attack take place, and what techniques would be used? But it is in the matter of political constraints and legal regulation that economic warfare and cyber warfare appear to be most dissimilar. In the first place, there would be difficulties in

identifying the identity of a cyber aggressor, making it almost impossible to assess their intent. Their techniques could be equally opaque, given the speed at which cyber threats might evolve. It would appear, therefore, that for the present the initiative in cyberspace lies with the aggressor rather than with the large and unwieldy defender (in this case the developed state with its complex economy).

ECONOMIC CYBER WARFARE

As a composite of *economic warfare* and *cyber warfare*, 'economic cyber warfare' embodies two ideas which lead in different directions. Most national economies could be said to be inter-connected and inter-dependent within a global economic system. It should follow that even 'pariah' or 'rogue' states would be wary of conducting economic warfare against the United Kingdom (or any other developed and integrated economy) for fear of being damaged themselves in the process. The only conceivable exception to this rule might be an autarkic state, entirely immune from the vagaries of the international economy. Yet such a state, even if it were to exist, is unlikely to have the capacity to wage economic warfare in the first place.

Cyber warfare, however, raises another possibility. If in cyberspace, as I have suggested, the initiative lies with the attacker, then rather than wage *war* against a target state, the technologically proficient aggressor might use cyberspace to *exploit* the strengths and capabilities of the target state rather than seek to disrupt, defeat or destroy it. By this view, economic cyber warfare could offer a low-cost, low-risk alternative to both conventional warfare and economic warfare, both of which would cause grave damage to an increasingly interconnected global economy. This is a rather different prospect from the 'cyber armageddon' or 'cyber Pearl Harbour' which some commentators claim to be possible, if not likely.[6]

The anonymity of cyberspace could indeed dramatically reduce the risks associated with state-sanctioned espionage and intellectual property theft, making it possible for the predator company or state covertly and continuously to benefit from the knowledge, inventiveness and investment of its target. In 2010 for example, according to Foreign Secretary William Hague, the United Kingdom experienced a 'deliberate attack on our defence industry': 'A malicious file posing as a report on a nuclear Trident missile was sent to a defence contractor by someone masquerading as the employee of another defence contractor.'[7] This incident suggests that it could be in the economic interests of the predator to preserve and exploit, rather than attack and destroy the target economy and its cyber infrastructure.

---

[6] See for example Richard Clarke, 'Seven Questions: Richard Clarke on the Next Cyber Pearl Harbor', *Foreign Policy*, 2 April 2008, http://www.foreignpolicy.com/articles/2008/04/01/seven_questions_richard_clarke_on_the_next_cyber_pearl_harbor, accessed 23 March 2011.

[7] William Hague, 'Security and freedom in the cyber age – seeking rules of the road', Speech at the Munich security Conference, 4 February 2011, http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=545383882, accessed 20 March 2011.

This might indicate that only highly committed, adversarial non-state actors (such as terrorist organisations) would wish to use cyberspace in order to inflict severe economic disruption on a developed state, on the grounds that the organisation carrying out the attack would have little or nothing to lose economically in the process. Yet so far terrorist groups have been more interested in cyberspace as a means to fund their core activities rather than as a preferred medium of attack. It is certainly the case, as Joseph Nye puts it, that 'the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost.'[8] Yet it remains to be seen whether any non-state actor or terrorist group would have either the interest or the capacity to prepare and sustain an economic cyber warfare campaign, as opposed to a single 'spectacular' attack against a national financial centre or banking system. It might of course be that a state could use such a non-state actor as a proxy, using 'plausible deniability' to minimise the risk of discovery, but that state would still not be immune from the damage to the global economy that might ensue. An aggressor state which chose to make a direct attack on the economic stability of another country would also have to be extremely proficient in offensive cyber operations. And in either case – direct attack or by proxy – the aggressor state would have to be able to manage the economic shocks and turbulence that would result.

Economic cyber warfare might therefore best be understood as parasitism; a protracted campaign of espionage, 'corporate insurgency' or intellectual property theft, rather than all-out war against the economy of an adversary. But there is another possibility to consider. At a conference organised by the Jamestown Foundation in Washington in February 2011, the Chinese were described as 'seeing digital attacks differently than (sic) US planners.' China would play a 'long game' in which they would, essentially, prepare the battlefield of a subsequent, more traditional conflict by ensuring that US supply and logistic chains could be degraded at the critical moment. In order to infiltrate core networks, China would allow exported hardware to be inspected for security but would then 'introduce malicious software via upgrades, maintenance, and other post-buy actions.'[9] Economic performance is usually judged over months and years rather than hours and days; a 'long view' which could advantage those able to play the 'long game' of slowly but deliberately compromising and/or undermining national economic capabilities. Other analysis and information point to broadly similar conclusions: 'Acts of

[8] Joseph S. Nye, Jr., *Cyber Power* (Cambridge MA: Belfer Center, May 2010), p.4.

commercial espionage indicate that the Chinese are looking as closely at economic secrets as they are military or economic secrets.'[10] And the British industrialist James Dyson is reported to have warned that 'Chinese students are infiltrating British universities to steal technological and scientific secrets and even planting software bugs to relay the information to China.' Dyson is quoted as follows: "I've seen frightening examples. Bugs are even left in computers so that the information continues to be transmitted after the researchers have returned home."[11] The Chinese embassy in London refuted Dyson's claim as 'shocking and entirely unfounded and illogical' and a 'damaging slander to all Chinese students.'[12]

If an economic cyber warfare attack were to occur, whether via a non-state proxy or directly by one state against another, or after a 'long game', the damage could be considerable. Yet it is difficult, if not impossible to know with any degree of accuracy the cost to the UK government of economic cyber warfare. Assessments of the cost of cyber crime vary widely, even though this is an area which has been extensively researched and analysed. Calculating the cost of economic cyber warfare must, at least for the present, be an even less exact science, although there has been some speculative analysis. A recent paper by the Australian Kokoda Foundation, for example, notes that the cost to the United States of cyber espionage and intellectual property theft could have been as much as US$1 trillion between 2010-2011.[13] What can be said with more confidence is that the international trading and banking systems are highly dependent upon information and communications technology (ICT). In many cases, currency and commodity trading is automated; requiring especially advanced (and secure) ICT systems. Yet as I have argued, where there is dependence there is also vulnerability.

In the worst case, a cyber attack against trade and banking systems could undermine the most important commodity of all – confidence. In early 2011 there were reports that the London Stock Exchange (LSE) trading system, although not based on the internet, had nevertheless encountered 'suspicious circumstances' on at least two occasions in 2010, which some speculated could have been a major cyber attack. The result of these incidents was a loss of confidence in the LSE, if only temporarily, and the beginnings of a

---

[9] Richard Bejtlich, *TaoSecurity* (blog), http://taosecurity.blogspot.com/2011/03/experts-talk-us-china-security-issues_07.html, accessed 20 March 2011.
[10] Timothy L. Thomas, 'Google Confronts China's "Three Warfares"', *Parameters* (Summer 2010), p.103.
[11] 'Dyson: China has spy bugs in UK universities', *The Sunday Times*, 27 March 2011.
[12] 'Embassy: Dyson spy claim is groundless', China Daily, 6 April 2011, www.chinadaily.com.cn/cndy/2011-04/06/content_12276301.htm accessed 27 April 2011.

'close dialogue' between the LSE and UK security services.[14] A successful trading and investment environment needs not only to be stable and secure, it must also be seen to be such, and to be more stable and secure than alternative environments. Trade and investment require the balance between risk and reward to be favourable and, above all, predictable. When that predictability diminishes, investors will lose confidence. Governments might then compensate by increasing interest rates in order to make the market more attractive to investors, but only at the risk of increasing the cost of credit and stifling business activity generally. Nationally-based icons of international business might suffer particularly badly as a result of the flight of confidence, as alternative markets begin to appear more stable and therefore more attractive. And in the resulting turbulence, as national economic 'soft power' is undermined, so it will become ever more difficult to sustain investment in the 'hard power' of a costly and, in economic terms, non-productive national defence posture, as the current situation in the United Kingdom illustrates.[15]

---

[13] John Blackburn and Gary Waters, *Optimising Australia's Response to the Cyber Challenge* (Canberra: Kokoda Foundation, Kokoda Paper No.14, February 2011), p.9.
[14] 'London Stock Exchange 'under major cyberattack' during Linux switch', Computerworld UK, 31 January 2011, www.computerworlduk.com/news/open-source/3258808/london-stock-exchange-under-major-cyberattack-during-linux-switch/, accessed 23 March 2011.
[15] See Paul Cornish and Andrew Dorman, 'Dr Fox and the philosopher's stone: the alchemy of national defence in the age of austerity', *International Affairs* (87/2, March 2011), pp.335-353.

CONCLUSION

It is difficult to assess with much certainty the likelihood, the character and the consequences of economic cyber warfare, and therefore to gauge the United Kingdom's vulnerability to such a challenge. This paper is, therefore, necessarily speculative. As its name suggests, if and when economic cyber warfare were to take place it would combine some characteristics of economic warfare with some of cyber warfare. The first of these is a largely historical phenomenon, with a less than distinguished record (in both senses of that term), while the second is, for the present at least, rather more a matter of conjecture than of fact. For policy makers seeking to identify genuine security challenges and then to anticipate them, economic cyber warfare is of doubtful credibility and, consequently, its suitability for the allocation of scarce security and defence resources must be open to question. This brief essay suggests, nevertheless, that while the idea of economic cyber warfare might not merit a full-scale policy response at present, it would be prudent to subject it to sustained and careful scrutiny in coming years. Economic cyber warfare could, in other words, be an ideal candidate for the risk-based approach to national security, risks and challenges introduced in the 2010 UK National Security Strategy.[16]

In a world of interconnected and interdependent economies we could expect an element of self-deterrence to be associated with economic cyber warfare; it would surely be irrational for any state to undermine, damage or destroy the system upon which it depended for its economic security and stability. Non-state actors such as terrorist groups might be attracted by economic cyber warfare. But for the most part terrorist groups have so far seen cyberspace as a source of criminal income rather than a preferred area of operations. A more worrying possibility is that cyberspace offers a low-cost, low-risk alternative to both conventional and economic warfare. I have described this as parasitism, whereby the attacker seeks to exploit the target economy through espionage and intellectual property theft, rather than to destroy or impede it. Most disconcerting of all is the idea of the 'long game', whereby strategically significant economic ICT systems are gradually infiltrated through apparently benign means in order that at some point in the future they might be corrupted as part of a broader campaign.

All of these possibilities place a premium on information, personnel and network security and on the need for rapid detection and attribution of attacks

and infiltrations. Above all, even the faintest possibility of economic cyber warfare points to the need for a more agile and mutually supportive relationship between national governments and critical sectors of the economy such as science and innovation, manufacturing and industry, and the financial and banking sector. Otherwise, the first casualties of economic cyber warfare are likely to be the credibility of national government and the confidence and predictability upon which a national economy depends.

[16] *The National Security Strategy*, pp. 25-31.

ABOUT THE AUTHOR

Dr Paul Cornish is Carrington Professor of International Security and Head of the International Security Programme at Chatham House. His recent publications cover many aspects of contemporary security and defence policy including reports and articles such as his most recent article *Dr Fox and the Philosopher's Stone: the alchemy of national defence in the age of austerity* (International Affairs, March 2011). Dr Cornish's most recent major publications include *Strategy in Austerity: the Security and Defence of the United Kingdom* (Chatham House, October 2010) and *On Cyber Warfare* (Chatham House, November 2010). In the field of cyber security studies he is co-author with David Livingstone and Rex Hughes of *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (Chatham House, March 2009).