Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed

DAVID BETZ
Department of War Studies, King’s College London

ABSTRACT This article explores the effect of connectivity on strategic affairs. It argues that the effect on war’s character is potentially, although not yet shown in practice, considerably large. Its effect upon the distribution of power among states in the international system is small, contrary to the claims of ‘cyberwar’ alarmists. All told, however, its effect upon strategic affairs is complex. On the one hand, it represents a significant advance in the ‘complexification’ of state strategies, understood in the sense of the production of intended effects. On the other hand, strategists today – still predominantly concerned with the conflicts and confrontations of states and organised military power – are generally missing the power which non-traditional strategic actors, better adapted to the network flows of the information age, are beginning to deploy. These new forms of organization and coercion will challenge the status quo.

KEY WORDS: Cyberspace, Cyberwar, Cyberpower, Airpower, Networks, Connectivity, Social Movements, Terrorism, Revolution, Strategy

‘Cyberwar! The threat from the Internet’, reads the leader of the July 2010 Economist, the words emblazoned across an illustration of a mushroom cloud looming over a burning city below.¹ ‘Be afraid, be very afraid’ is the not too subtle message echoed across the burgeoning cybersecurity industry and re-echoed in policy circles. Some venture to call this a panic, while others suggest that a degree of alarm is justified.² The simple question that this article asks is, how terrified should we really be? As strategists it behoves us to maintain a degree of perspective on events and processes that at close hand appear more threatening than they do with the respectful distance which history and


ISSN 0140-2390 Print ISSN 1743-937X Online/12/050689-23 © 2012 Taylor & Francis
http://dx.doi.org/10.1080/01402390.2012.706970
Clausewitzean theory of war provides us. That, essentially, is the object of this contribution, which advances two claims about cyberspace and conflict each of which turns on the central concept of escalation. First, contemporary strategists who reckon that ‘cyberwar’ represents a decisive new form of interstate conflict – one which ‘short circuits’ the inherently escalatory nature of war (which many have argued has caused major war’s obsolescence from the mid-twentieth century onwards) – are plain wrong. Second, strategists traditionally concerned with struggles between well armed and organized states ought to be more concerned with the ways in which digital connectivity is imbuing a wide range of novel globally networked social movements with a potential strategic significance not seen by non-state actors since 1648. The problem is not just Al-Qaeda: many other social movements employ the same strategy of using cyberspace for the mobilization of contention in support of diverse causes; most are not violent but a few are, and more are poised to escalate as the problems which animate them (in particular economic) grow increasingly acute; and several are experimenting with forms of digital coercion which have not been seen before.

The article explores these ideas in five parts. First, it locates cyberspace in the context of strategic theory. Second, through reference to interwar airpower theory it suggests how it is likely that ‘cyber-power’ might be affecting conventional war today. Third, it explains cyberpower’s seductive allure for strategists but why, ultimately, this allure is false. Then, fourth, shifting to the unconventional realm, it considers how ‘cyberpower’ is actually being employed by networked social movements to challenge governments. Fifth, it shows how hackers are attaching themselves to ‘revolutionary’ causes and experimenting with new forms of coercion.

**On Portmanteau War**

Overdrawn conclusions about changes in war’s character, usually assumed to be caused by technological change, constituting some profound shift in war’s fundamental essence are a recurrent feature of Western scholarship. Many have sought to overturn Clausewitz’s theories of war. The ‘cyber war’ literature falls squarely in this

---

intellectual tradition.\textsuperscript{6} Partially as a result, cyber security discourse is frequently both shrill and paradoxical speaking of existential digital threats which are yet vague and intangible.\textsuperscript{7} Viewed in historical context, however, not merely the period since the invention of the microchip or the World Wide Web but as another step in the more than a century-long period in which the decisiveness of major war for a mixture of political, economic and technological reasons is thought to have been gradually diminishing, the ‘threat from the Internet’ takes on a different hue. For the major armies of the world, formed by the conventions of the Industrial Age, twenty-first-century conflict seems unfathomably complex and ambiguous because war itself is a ‘contested concept’.\textsuperscript{8} As the strategist and World War I historian Hew Strachan has argued, ‘One of the central challenges confronting international relations today is that we do not really know what is a war and what is not.’\textsuperscript{9}

The same can be said of cyberspace which has proven also difficult to define because of its lack of conventional dimensionality. Perhaps the best available model is Libicki’s three-layered one which interposes a ‘syntactic layer’ (the software and protocols that govern how information flows in the network) between cyberspace’s ‘physical layer’ (i.e., routers, wires, and computers) and its ‘semantic layer’, which is where humans extract meaning from data on the web in the form of natural language.\textsuperscript{10} Cyberspace is an environment that defies easy categorization. Indeed, one of the key controversies in its study


\textsuperscript{7}Britain’s new national security strategy is a good example, describing the country as more physically secure than it has ever been while subject to terrible digital threat as a result of its connectedness. See HM Government, \textit{A Strong Britain in an Age of Uncertainty: The National Security Strategy} (London: The Stationery Office 2010), 3.


\textsuperscript{9}Hew Strachan, ‘The Changing Character of War’, Europaeum Lecture delivered at the Graduate Institute of International Relations, Geneva (9 Nov. 2006), 2.

\textsuperscript{10}Martin C. Libicki, \textit{Conquest in Cyberspace, National Security and Information Warfare} (New York: Cambridge UP 2007), 236–40. He also describes a fourth
concerns whether there is any difference between ‘real space’ and ‘cyberspace’ meaningful enough to support the distinction between the two.\textsuperscript{11} It possesses few of the definable parameters of the traditional domains of land, sea, air and space, which at least possess some form of integument.\textsuperscript{12} It is also characterized by non-linear dynamics in which effects are both unpredictable and potentially highly disproportionate to their causes. It is hard to fathom. Yet war too is non-linear – all the great commanders of history have recognized its inherent chanciness, as did Clausewitz who placed it squarely in the centre of his trinity of war: passion, chance, and political purpose;\textsuperscript{13} and what else is the fear of escalation than the realization of war’s natural tendency to grow to proportions beyond those which its proximate causes can justify? Thus of ‘cyber war’ we might say two things, at least in the abstract. First, it is a portmanteau of two concepts, cyberspace and war, which are themselves undefined and equivocal; it takes one complex non-linear system and layers it on another complex non-linear system. And second, as a result, it does not clarify understanding of the state of war today; it muddies waters that were not very transparent to start with.

\section*{Some Things Change, Some Things Stay the Same}

Strange though it may sound, there is more than a passing resemblance between the late nineteenth and early twentieth centuries and the late twentieth and early twenty-first centuries. There is today a similar technological surge – the nineteenth was known as the century of invention for good reason;\textsuperscript{14} a similarly politically revolutionary climate prevails in which \textit{anciens regimes} are the target of substantial subversion and political violence; and there is a similar popular feeling that the international order is shifting in some potentially tectonic way, for example. Cyberspace is by no means the only cause of these developments but there can be little doubt that the recent and radical change in the modality of communications which many regard as the dawning of an ‘Information Age’ is a major factor. ‘The Web is shifting power in ways that we could never have imagined’, warned

\textsuperscript{13}For more on this thought, see Alan Beyechen, ‘Clausewitz, Non-Linearity, and the Unpredictability of War’, \textit{International Security} 17/3 (Winter 1992/93), 59–90.
\textsuperscript{14}See Barry Buzan and Eric Herring, \textit{The Arms Dynamic in World Politics} (London: Lynne Rienner 1998), esp. chap. 2.
portentously a recent BBC documentary programme on *The Virtual Revolution* that cyberspace is ‘reinventing warfare’.\(^{15}\) Yet such things have been said before: 90 years ago Britain’s best-known strategists, J.F.C. Fuller and Basil Liddell Hart, writing in the shadow of the Great War’s ghastly yet indecisive slaughters, were equally convinced of the power of manned flight to decisively change war. In *The Reformation of War*, Fuller described an aerial attack on London causing the capitulation of the government within 48 hours with nil casualties on the attacker’s side.\(^{16}\) While Liddell Hart was impressed not only by the apparent puissance of the new means of warfare but also had an acute sense of the new fragility of modern industrial society.\(^{17}\)

Moreover, just as today one finds politicians echoing the apprehensions of the cyber security sector about cyber wars, so then did figures such as three times Prime Minister Stanley Baldwin proclaim in a famous House of Commons speech in November 1932 entitled ‘A Fear for the Future’ such flat warnings as ‘the bomber will always get through…’.\(^{18}\) This is not to say that what was true or not true of airpower need necessarily be the same of its cyberspace analogue; it is simply to inject some notes of caution about current claims of a technology-driven reinvention of warfare on the basis of lessons learned about a significant previous instance of the same. Perhaps the most germane of these is to beware of anything being sold as having *independent* war-winning effects – winning the war in 48 hours with nil casualties on the victorious side, as Fuller imagined, and as other prophets of airpower claimed too. This faith in airpower’s almost unique decisiveness has been very durable. Sixty years later in the early 1990s, building on his *Gulf War Air Power Survey* conducted on behalf of the USAF (at that time flush with the apparent success of the battering it had just delivered Saddam Hussein’s army) Eliot Cohen cautioned policy-makers about the ‘mystique’ of air power: ‘… an unusually seductive form of military strength, in part because, like modern courtship, it appears to offer gratification without commitment’.\(^{19}\) The addition, as a result of developments in

---

\(^{15}\)British Broadcasting Corporation, *The Virtual Revolution*, Episode 2 ‘The Enemy of the State?’, aired on BBC2 (6 Feb. 2010), [www.bbc.co.uk/programmes/b00n4j0r](http://www.bbc.co.uk/programmes/b00n4j0r).

\(^{16}\)J.F.C. Fuller, *The Reformation of War* (London: Hutchinson 1923), 150.


microelectronics, of precision-guided munitions to the mix merely added to airpower’s allure; it made it seem possible that the vast civilian casualties which had necessarily resulted from mass aerial bombing in the past could be avoided with a more ‘surgical’, less bloody but cheap and decisive form of warfare. The high point of this strategy of gadgets was the doctrine of ‘Rapid Dominance’, supposedly a way in which ‘shock and awe’ would be induced in an opponent by a combination of ‘near total or absolute knowledge and understanding of self, adversary, and environment rapidity’ with ‘operational brilliance in execution’.

In the heady days of the Cold War’s end and in the warm afterglow of the first Gulf War, when it was widely thought that we were witnessing the permanent triumph of liberal democracy and market capitalism, and that Western military forces empowered by high technology would henceforth triumph easily and cheaply over less sophisticated enemies, such thinking had a high degree of currency. Now, with the War on Terror (howsoever called) having acquired a sense of permanent indecisiveness, and in light of what can only be described charitably as Pyrrhic victory in Iraq and, most likely, plain defeat in Afghanistan, it seems rather tarnished.

The Siren Song of the Cyber Prophets

Enter cyberpower, which appears to offer similar things as well as two other properties which airpower does not: anonymity and low ‘buy-in costs’. The latter is particularly alarming to state strategists because, as it was put in a recent article in *Joint Force Quarterly*, as opposed to the ‘vastly more complex and expensive appurtenances of air and space warfare’ the instruments of cyberwar are cheap, allowing ‘Lilliputian adversaries to generate what one expert called “catastrophic cascading effects” through asymmetric operations against the American Gulliver.’ In truth, there is something potentially very disruptive here, as will be discussed further below, when it comes to non-state actors (to whom cyberspace extends a number of command, control, communications and intelligence capabilities which only the richest states

---

could afford two decades ago); but the picture is rather different with state use of cyberspace as a means of war. For one thing, as the Stuxnet virus, which targeted the Iranian nuclear programme, demonstrates very well, such capabilities do not come cheap. Indeed, expert analyses of Stuxnet point to it being the product of a well-resourced government (the best guess at present is that it was designed by the United States and Israel with the assistance, witting or otherwise, of Britain and Germany) with precise insider knowledge of the target it was seeking.

Much attention has been paid to the remarkable sophistication of the weapon. For the purposes at hand, however, the significant thing about Stuxnet (which in historical perspective may be seen as the Zeppelin bomber of its day – more important as a harbinger of what is to come than for its material contribution to the conflict at hand) is that it was not the work of hackers alone but of a deep-pocketed team which had both excellent technical skills and high-grade intelligence on the Iranian programme. In short, as with all other weapons systems (with the exception of the hydrogen bomb, arguably) it required the combination of significant other resources in order to achieve strategic effect. Moreover, far from demonstrating a smoothing of the existing asymmetry of power it actually shows a reinforcement of that asymmetry: cyberpower rewards already powerful states with even more capability and, when push comes to shove, it would appear that Western powers have thought hard about cyberattack and are pretty good at it.

Similarly counter-intuitively, the anonymity of cyberattack is less disruptive of the strategic relations among states than is popularly supposed. For instance, in his recent book, Cyberwar, Washington insider Richard Clarke (formerly National Coordinator for Security, Infrastructure Protection, and Counterterrorism under Bill Clinton), describes a hypothetical cyberattack on the United States which is utterly devastating ‘without a single terrorist or soldier ever appearing…’. Frightening stuff – such ideas are the essential underpinning of the ‘electronic Pearl Harbour’ rhetoric that is often invoked by cyber alarmists. Clarke is almost

---

27 Ibid.
28 Clarke, Cyber War, 67–8.
certainly correct that most future wars will be ‘accompanied by’ cyberwar.\textsuperscript{30} Indeed, this was the main point of the seminal 1993 article by John Arquilla and David Ronfeldt, ‘Cyberwar is Coming!’ in which the term was coined;\textsuperscript{31} but their vision was essentially tactical in orientation, a theory of battle in which greater combat power could be produced through the employment of better information systems – knowledge as power in a very literal and immediate sense – not a new theory of war per se. The problem is that when Clarke, and others, talk of ‘stand-alone’ cyberwars they are arguing a theory of a new form of war in which decisive results are achieved without triggering the thorny problem of escalation. The way in which this is supposed to work is based on the obscurity of attacker identity in cyberspace. If the originator of an attack is unknown,\textit{ergo} the victim does not know against whom he should retaliate – hence the problem of escalation does not materialize. This seeming ability of cyber power to deliver an almighty blow without possibility of return is even more seductive than airpower: it offers gratification without commitment whatsoever.

But it is a fallacy. The problem is not with the theoretical power of cyberattack: it is entirely likely that the prosperity of ‘knowledge economies’ whose intellectual property, creative industries, high-tech sector, financial services, and commerce thrive on connectivity is imperilled by threats to and from cyberspace.\textsuperscript{32} It is rather, as Clausewitz would remind us, that war is still an act of force to compel our enemy \textit{to do our will}. Technology can alter the way in which force is applied – perhaps (though it remains to be seen in practice) it enables an attacker to compel another bloodlessly but it does not obviate the necessity to declare one’s will (even if after the event): war \textit{requires} commitment. Anonymity is as much a problem for the strategic aggressor as it is the defender: if China, for instance, were to kill several thousands of Americans, or vice versa, and profoundly disrupt the lives of many millions of others through cyberattack in an attempt to bend its government to its will then the prefix cyber would be superfluous to the requirement of describing the state of relations which would exist

\textsuperscript{30}Clarke, \textit{Cyber War}, 31.
\textsuperscript{31}John Arquila and David Ronfeldt, ‘Cyberwar is Coming’, in J. Arquila and D. Ronfeldt (eds), \textit{In Athena’s Camp: Preparing for Conflict in the Information Age} (Santa Monica, CA: RAND 1997).
between the two countries. And because of the expanse and diversity of their interests and capabilities, the wounded state would likely retain or have the ability to reconstitute other means of reprisal. There is no way around this problem through gadgetry or subterfuge. Among states, escalation abides in the Information Age as it did in the Industrial Age.

**When I Know That You Know That You Know What I Know . . .**

While cyberspace changes less in the world of states than has been supposed, it changes relations amongst non-state entities and between states and non-state actors in a rather significant way. For one thing, as has been observed of non-state use of weapons of mass destruction, for enemies who possess no comparable infrastructure against which to retaliate, are motivated by transcendent beliefs which make nonsense of rational calculations of the utility of force, and/or simply seek to punish their enemies, cyberattack might yet prove a potent means. It must be said, however, that there are to date no known incidents of pure cyberterrorism (although it is thought some groups have contemplated them and, in theory, a combined physical and cyber attack, perhaps to disrupt emergency response, is plausible); and, moreover, the vast majority of analysts tend to scorn the likening of cyber to nuclear attack. A more immediately relevant way in which digital interconnectivity has already changed things is in the way that it has proven such an invaluable tool of social mobilisation, for good or for ill.

Among the most obvious examples of this at present is the wave of revolts against repressive regimes in the Middle East which started in late 2010. There is a high degree of controversy over the degree to which social media has driven these so-called ‘Twitter Revolutions’. On the one side, enthusiasts of social media see it as an inherently liberalizing force with literally revolutionary potential. Activists speak effusively of the way in which social media allows them to organize protest, document and publicize security force crackdowns, and seek moral and material support for their causes globally. On the other side, there are sceptics who warn of the dark potential of the technology to strengthen the control of authoritarian states, first through the provision to their populations of cheap but distracting entertainments and, second, by giving the state extensive new means of


detecting anti-regime speech (i.e., thought-crime).\footnote{Evgeny Morozov, \textit{The Net Delusion: How not to Liberate the World} (London: Allen Lane 2011).} No good historian would attempt to render judgment on how, ultimately, the balance of power between people and state may be realigned by digital connectivity. Zhou En Lai, Chinese foreign minister during the Nixon–Mao era of US–Chinese rapprochement, was perhaps too conservative when asked to assess the 1789 French Revolution he replied ‘too early to say’; nonetheless, the sentiment is apposite with respect to today’s apparently revolutionary climate which is still developing. Still, it is possible to put a finger on the essential dynamic that is at work, which is a shift in the way in which information is communicated, stored and analysed.

The Spanish sociologist Manuel Castells describes this as a shift in the paradigm of communication from one of mass communications in which a few privileged speakers (i.e., governments, corporations and powerful individuals who own major media outlets) can to a large extent control what is said publicly, to one of ‘mass self-communication’ in which many people can speak to many others relatively easily and cheaply about whatever they want. The consequences of this are profound across the spectrum of human affairs. In his words: ‘In a world marked by the rise of mass self-communication, social movements and insurgent politics have the chance to enter the public space from multiple sources.’\footnote{Manuel Castells, \textit{Communication Power} (Oxford: OUP 2009), 302.} In effect, increasingly the conflicts of our time will consist of revolutionary social actors aiming to animate their target constituencies through cyberspace. This is not merely academic speculation. Britain’s most senior military leader used similar terms to describe future wars: ‘Conflict today, especially because so much of it is effectively fought through the medium of the Communications Revolution, is principally about and for People – hearts and minds on a mass scale.’\footnote{Gen. Sir David Richards, ‘Future Conflict and its Prevention: People and the Information Age’, International Institute for Strategic Studies (18 Jan. 2010), <www.iiss.org/recent-key-addresses/general-sir-david-richards-address>.}

It is often said that cyberspace increases transparency – in a nutshell, it makes it harder to keep things secret; and this, in turn, makes it harder to govern.\footnote{See, for example, Micah Sifry, \textit{Wikileaks and the Age of Transparency} (New York: OR Books 2011).} At another level of abstraction we may understand what is happening as a change in the relative prevalence of what economists and logicians call ‘individual’ as opposed to ‘mutual’ or ‘common’ knowledge. Individual knowledge is that which person A
knows and which person B knows but which neither A nor B knows that each other knows; whereas mutual knowledge is that which person A and B know and which each know that the other knows. The strategic effects of a massive increase of mutual knowledge are non-trivial. For one thing, it is an accelerant to revolution – where there is substantial dissatisfaction with the status quo, increasing mutual knowledge increases the likelihood that change will be demanded because it makes the fear and loathing that prevails in repressed societies more transparent.

Authoritarian states have always worked hard to prevent this by controlling civil society institutions: by denying people any environment in which they can speak openly (even in the family home) the state destroys any possibility of people converting individual knowledge into mutual knowledge. Indeed, one may read George Orwell’s classic novel on authoritarianism, 1984, as an extended essay on this theme. Winston, the hero of the novel, keeps a secret diary in which he records his subversive thoughts. Among these is what he regards as an important axiom: ‘Freedom is the freedom to say two plus two make four. If that is granted, all else follows.’ The downfall of Colonel Gaddafi illustrates this well. In late February 2011 the dictator told an incredulous BBC interviewer, while riots raged across his country: ‘all my people love me, they will die to protect me.’ In actuality, the large majority of Libyans hated and feared him – seven months later a jubilant group of them would beat and sodomise him on camera before shooting him in the head, to general applause; and yet, as with two plus two equals four, it was not so much the fact that he was a dictator, loathed and feared, as it was the manner in which that knowledge was held that led to action – it is one thing to hate and fear ‘Big Brother’ silently alone, it is another thing to do so amongst multitudinous others in which condition feelings of fear are mitigated by feelings of solidarity.

40 For an example see Orlando Figes, The Whisperers: Private Life In Stalin’s Russia (London: Penguin 2007), in particular pp. 122–6, dealing with Pavlik Morozov, the 13–year-old boy who informed on his father who was subsequently arrested and killed and the killing thereafter of Pavlik by his remaining family.
Do-It Yourself Revolution

The consequences of information transparency, however, are hardly confined to authoritarian states. Albeit in less dramatic fashion, the publication of sensitive documents by Wikileaks illustrates the way in which cyberspace has effects that confound democratic states also. Much attention has been paid to Wikileaks’ head Julian Assange as the ‘Robin Hood of hacking’. Carne Ross, a former British diplomat who quit over the dissimulation of government communications in the lead-up to the Iraq War, argues that the ‘landscape of international relations’ has been changed irrevocably by the way in which information now flows more freely into the public sphere. In a nutshell, it makes it considerably more difficult for them to dissemble. Information transparency means they are more quickly fact-checked and held to account. The ‘politics of spin’ started to come unspun even as governments appeared to be mastering their techniques.

Governments are also confronted with the problem of some networked social movements cottoning on to the power of networks to multiply their violent capacity. Al-Qaeda, as has been richly described in the literature, is a superb example having turning itself into a ‘non-territorial network enterprise’ which has no territory but stretches around the world in geographically-isolated but digitally interconnected groups which share a common cause driven by a shared sense of outrage. Naturally, the literature has dwelled lengthily on this strikingly violent phenomenon that the terrorism analyst Marc Sageman describes as ‘leaderless jihad’; but there are many other movements which use some or all of the same ways as Al-Qaeda – notably resource mobilization via propaganda and propaganda by deed, ‘flattened’ hierarchy, decentralization, and self-organization which all depend on

---

networks. Some such as the environmental group Earth Liberation Front (ELF) use violence (though not on the scale or of the same viciousness as Al-Qa’eda) and are similarly intent on destroying Western civilization, which they regard as intrinsically hostile to and destructive of the Earth’s environment. With remarkably few changes in word choice, the ELF’s communiqué in response to the development of genetically modified organisms by several major corporations and universities could read like a suicide bomber’s ‘martyrdom’ video.

Others use networks to enhance their ability to organize various forms of protest including demonstrations that may end, deliberately or accidentally, in violent street battles. At the time of writing, the ‘Occupy’ movements, which have formed encampments in New York, London and other cities around the world, are on the news agenda. In its own words, Occupy Wall Street is a ‘leaderless resistance movement’ utilizing the ‘Arab Spring tactic to achieve our ends …’. A strong element of the ‘smart mob’ has been apparent in the global anti-capitalist (or ‘global justice’) movement since the 1999 ‘Battle for Seattle’ in which networked activists used mobile phones, websites and laptop computers to deploy ‘swarming tactics’ in protest against a World Trade Organization meeting in the city. The movement is avowedly global, the umbrella group ‘We are Everywhere’ (itself a telling formulation) describes it as an ‘unprecedented global rebellion’ of the oppressed and impoverished; yet many sense in it a decidedly ‘bobo’ (a French portmanteau of ‘bohemian’ and ‘bourgeois’) flavour with its overwhelmingly white middle class adherents calling for ‘anarchism’, and the rejection of ‘hierarchical institutions’ including the state, but without violence. It is easy to dismiss such ‘revolution’ because history provides so few instances of non-violent ‘change of self’ actually changing the existing political order. At some point, serious revolutionaries encountering

50From the Occupy Wall St webpage <http://occupywallst.org>.
52Notes from Nowhere (eds), We are Everywhere: The Irresistible Rise of Global Anti-Capitalism (London: Verso 2003), 16.
54Ibid., 22.
real resistance come up against a hard choice of whether to escalate to bloodshed or not. In 1964, while on trial by the Apartheid regime in South Africa for sabotage, Nelson Mandela explained the remorseless logic of contested change, eventually ‘we were placed in a position in which we had either to accept a permanent state of inferiority, or to defy the government. We chose to defy the law.’

Once the decision is taken to go beyond the law, claimed Mandela, there were four violent options in ascending order of severity – sabotage, guerrilla warfare, terrorism and open revolution. The global justice movement has been suspended on the cusp of political violence for at least a decade (notwithstanding the flirtation with violence – typically property damage and intimidation – practiced by some sub-groups). As Starhawk, one of the most prominent, thoughtful, and respected figures in the movement wrote in 2000: ‘We’re at a crucial point right now. We can evolve further into an unpaid militant mercenary army, travelling to actions that get more violent, smaller, more isolated, and less effective or …’. ‘Or’ indeed – that is the tricky part; Starhawk equivocates about what ‘or’ might be with platitudinous counselling not to wait for the revolution but to ‘live it’, echoing the aforementioned ‘change yourself, change the world’ syllogism without actually explaining it. There is more, however, than personal conviction of non-violence at play here; there is also a shrewd strategic calculation of the political landscape which is refreshing. In her own words,

Those who advocate highly confrontational tactics … are generally trying to strike blows against the system. But at the moment the system has been struck harder than we could have imagined, and is reeling toward fascism, not liberation. In the present climate, such tactics are most likely to backfire and confirm the system’s legitimacy.

Whether or not Western society is really reeling toward fascism remains to be seen, although it has been argued by some that the collapse of the Euro might lead to ‘some form of authoritarian or military government’

---

55Nelson Mandela (20 April 1964), may be found on The History Place, Great Speeches Collection, <www.historyplace.com/speeches/mandela.htm>.
56Starhawk, Webs of Power: Notes from the Global Uprising (Gabriola Island, British Columbia: New Catlyst Books 2008), 60; for a different vision of this prospect which imagines such a mercenary force going from strength to strength see the near-future science fiction novel by Adam Roberts, New Model Army (London: Orion 2010).
57Starhawk, Webs of Power, 150.
or war in Europe. Moreover, there is a long way to go still before anti-capitalism can develop a plausible end state with a real chance of mobilizing a sufficiently large part of the population to achieve revolutionary change. Without doubt, cyberspace enables movements to mobilize rapidly in forms that are highly fluid and hard to defeat. At the same time, it does not change the fact that revolutionary groups need to do more than disrupt and attack the status quo – they must also paint a convincing picture of a better future. It is significant, however, that as opposed to Islamism, which in the West appeals to a minority within a minority, the ‘global justice’ movement is thriving on a widespread and deepening perception that the current order is unjust. It is also apparent that a new elite is emerging (in large part amongst the most disaffected youth segment of the population) which derives its power from a greater than normal ability to delve between the layers of cyberspace: hackers, who are experimenting with new ways and means of inflicting pain and grief and destroying value – the essential currency or ‘bargaining power’ of strategy.

The irony of the current dark image of the hacker as a combination of vandal, thief, subversive and terrorist is that it could hardly be further from the crew-cutted and short-sleeved young men of MIT’s Tech Model Railway Club where the first ‘hackers’ emerged in the late 1950s. The first generation of hackers were essentially in it for the primal thrill of maximizing code, their main interest being attaining technical mastery of the clunky early digital machines. Indeed, they possessed a ‘hacker ethic’ that seemed to flow from the logic of the computer itself. ‘It was a philosophy of sharing, openness, decentralization, and getting your hands on machines at any cost to improve the machines, and to improve the world.’ From quite early on there was a connection between 1960s counter-culture and the emerging cyber-culture that is apparent in the slogan ‘information wants to be free’ coined by Stewart Brand, the founder of the hippie-classic Whole Earth Catalog who later co-founded the San Francisco-based WELL (for Whole Earth ‘Lectronic Link), the first ‘virtual community’. Thus we may see a certain duality in the ‘hacker ethic’, which is on the one hand essentially apolitical and technically focused while on the other hand subversive and profoundly ideological. While not very apparent in the days when the digital world

---

59The concept of force as ‘bargaining power’ is from Thomas C. Schelling, Arms and Influence (New Haven, CT: Yale UP 1966).
was small and the knowledge to operate in it so esoteric; nowadays, with
the number and power of computers and the networks between them so
much greater, subsequent generations of hackers have a much larger
‘canvas’ on which to express themselves, including politically, and ever
more sophisticated and powerful means of doing so.

The best current example of this new hacker type is the Internet
collective known as ‘Anonymous’. The group has been the cause of great
ingestion as much from its curiousness as an entity as for the efficacy
of its attacks. In the space of a few years it has ‘declared war’ on, inter
alia: the music industry and its legal representatives for cracking down
on music and video file-sharing; the Church of Scientology ‘for the good
of mankind and for our enjoyment’; the financial enterprises Visa,
Mastercard and PayPal, and the nation states United Kingdom and the
United States in order to punish them for the crackdown on Wikileaks
and the persecution of its founder; various regimes in the Middle East for
being repressive; and, most recently, the Zetas drug cartel in Mexico,
allegedly in retaliation for the kidnap of one of its members. It is,
however, far from clear what exactly Anonymous is. In its own words, it
is: ‘... not a single person, but rather, [it] represents the collective whole
of the internet ... devoid of humanity and mercy’. Neither is it clear
whether it possesses any leadership. The credibility of the few figures
who have self-identified as leadership figures – such as Barrett Brown
who claims to be a ‘senior strategist and propagandist’ – is difficult to
judge. One of the things that make Anonymous interesting is that it is
subversive in the sense of being disruptive of the existing order but its
goals do not seem to be constructive in the way which genuinely
revolutionary goals are thought to need to be. At present they are much
more like the nineteenth and early twentieth century anarchists with
whom many members seem to consciously identify. Whether there are
more disciplined revolutionaries within the movement employing the
dumb mass of other cheap ‘clicktivists’ or ‘hacktivists’ as ad hoc ‘shock
troops’ or not is unknown.

62For an overview, see Quinn Norton, ‘Anonymous 101: Introduction to the Lulz’,
63From the _Encyclopedia Dramatica_ entry on Anonymous, <http://encyclopediadrama-
tica.com/Anonymous>.
64See the post by David Betz and accompanying comments by Barratt Brown and
others on ‘Anonymous Spokesman Opens Nechayev’s Tomb, Becomes Possessed’,
_Kings of War_ (14 March 2011), <http://kingsofwar.org.uk/2011/03/anonymous-
spokesman-opens-nechaevs-tomb-becomes-possessed/>.
65On ‘hacktivism’, see: Tim Jordan and Paul A. Taylor, _Hacktivism and Cyberwars:
Rebels with a Cause?_ (Abingdon, UK: Routledge 2004); also, Otto von Busch and Karl
Palmas, _Abstract Hacktivism: The Making of Hacker Culture_ (London and Istanbul:
self-published and in collaboration with Openmute.org 2006).
Nonetheless, its attacks on organizations such as the reputable data security and malware response company HB Gary demonstrate that it has substantial technical capability to cause harm – that is to say, it has means to compel its enemies. The firm was targeted after the CEO of an associated company HB Gary Federal, Aaron Barr, announced that his company had infiltrated Anonymous, discovered its members’ real names and was going to publicize them. In return, Anonymous hacked HB Gary’s servers, defaced its website, downloaded tens of thousands of its corporate emails and posted them on the web, digitally harassed its CEO and other staff, ultimately causing the cancellation of the launch announcement of a major new software product. The last exchange between HB Gary’s CEO Greg Hoglund on Anonymous’ IRC (Internet Relay Chat) channel in which he pleaded in vain for his e-mails to stay private lends some credence to the group’s claim for ‘blunt immorality’ and absence of mercy: participants in the chat openly welcomed the destruction of the company; there is a distinctly rudderless fanaticism to the group (they clearly were not interested in accepting his surrender) tinged with capriciousness. When one of the participants in that discussion asked Hoglund ‘Do you understand why we do what we do?’ he could not assay an answer. But the question is highly apposite. The most common answer is for the ‘lulz’ (a corruption of LOL, online shorthand for ‘laugh out loud’) – Anonymous clearly makes it very easy for individuals to engage in high-impact but low-cost/low-effort activism; but it is hard to see how ‘lulz’ can constitute the ‘sacred cause’ which revolutionary groups have thus far always required to sustain their movements over the long term. Anonymous’ championing of Wikileaks may be significant in this respect; it remains to be seen, however, whether this foray into political contest will outweigh the inherent capriciousness of the group – that is to say if it can adopt a coherent ideological identity.

In this respect, Anonymous is emblematic of a range of polycephalous and segmented revolutionary movements that are perhaps best described as being in a state of ‘strategic latency’. The causes of the

---


67 The polycephalous (many headed) and segmented nature of revolutionary movements is not, however, altogether new. The anthropologist Luther Gerlach described them as such in ‘Movements of Revolutionary Change: Some Structural Characteristics’, American Behavioral Scientist 14/6 (July/Aug. 1971), 812–36; ‘Strategic latency’ is a condition which some analysts have used to describe ‘a condition in which that could provide military (or economic) advantage remains untapped.’ See Zachary Davis, ‘Strategic Latency and World Order’, Orbis 55/1 (Winter 2011), 69.
strategic latency of networked social movements are not technological: the means for them to exert noteworthy power – to compel, or attempt to compel, their enemies to do their will are available and growing in scale and sophistication. Nor are the causes of their power to be found in obscure ways: various techniques ranging from disruption and sabotage, both real and virtual, to violent physical actions which resonate in the global mediascape have been amply demonstrated and shown to be operationally effective. The cause of their latency is political: no networked social movements as of yet have attached existing, albeit new, ways and means to an end compelling enough to mass mobilize.

Conclusion

Connectivity has important implications for the practice of war but it does not substantially alter its nature as much as is commonly supposed. It does not with ‘cyberwar’ create a decisive new form of warfare that will reshape the international order in respect of the balance of power among states as we have come to know it. If anything it shores up the existing distribution of military power rather than undermining it. It has not, yet, obviated the strategic concept of escalation that has held back major war for many decades. This is not an invitation to be complacent, however, because new forms of business, economic, and social practice, including subversives and revolutionaries, have emerged to shape and take advantage of unprecedented levels of connectivity. Escalation is also a problem for these groups, but from a different angle: whereas states struggle to disentangle their policy desires vis-à-vis other states from the potential of force to escalate beyond rational utility; revolutionary social movements struggle to attach to their policy desires grievances and solutions that are sufficiently resonant to impel normal people to do abnormal things. There is a revolutionary Zeitgeist to our time and yet it is one that feels rather Ersatz. When Mandela embarked upon a course of sabotage, terrorism, and guerrilla war it was in the belief that there was no other choice between that and slavery. The Bolsheviks rode to power in Russia in 1917 on the slogan ‘Bread, Land, Peace’, which resonated with the peasantry because they were literally starving and actually landless and had just suffered nearly two million dead in war with Germany. Fortunately, Western society is under less existential pressures today – student loan debt and underemployment notwithstanding, the people are not starving nor are hundreds of thousands of lives being snuffed out in trench warfare.

We should beware of claims of changes in war’s nature but not be blind to the ways in which broad societal developments such as those
which cyberspace entails have caused change in strategic affairs. In capsule form, these might be said to include:

I. A vast increase in the number and type of potential strategic actors as more and more people and organizations find ways of using cyberspace to mobilize contention globally for causes which would likely have failed to find a constituency in a less densely networked age;

II. The ability of violent movements to organize in wispy networked forms which are difficult if not impossible to defeat with the kinetic blows of a conventional military campaign; and,

III. A change in the manner of identity-group formation and scale of data-availability that makes it ever more difficult for states and organizations to keep secrets as people share information with more enthusiasm in more sophisticated ways.

Taken together, these trends create a significant potential for disruption of the status quo. This must not be seen as a bad thing a priori. Cyberspace can be a powerful force for good. But it has a significant dark side also. For one thing the rapidity and ease of communications means that actions initiated in one place can have practically instantaneous effects in another, regardless of their geographical separation. And the limits beyond which there are no potential attacks are disappearing as national frontiers become more permeable. Perhaps more fundamentally, if one sees strategy as the art of applying power for the ‘production of intended effects’ then the ever-greater number and interconnectedness of actors is highly problematic. Thus we may see that cyberspace has a Janusian aspect in strategic affairs. It seems to accelerate existing revolutionary tendencies and offer new coercive tools with which such groups may escalate; and yet, paradoxically it seems also to enervate these movements – to impair their ability to escalate and to build disciplined cadres over the long term, which heretofore has been a hallmark of revolutionary success. It is individually empowering but that does not clearly scale up to grander social success.

Contemporary events amply illustrate this duality. On the one hand, the Arab Spring and the Occupy movements appear to show how positive social change can be enabled by connectivity. As it was put in a recent ‘aux armes [cyber] citoyens’:

You can’t just idly sit back and decide that somebody else is going to solve your problems ... The alternative is sitting in darkness, stumbling around victimized by boom and bust cycles ... take
action... get excited and make the world that you want. Find your tribe. Decide what you believe. Rally them around you.68

There is no question that the speaker here is talking about non-violent activism in pursuit of changes, which most people would regard as normatively positive. Yet the subtext is that the existing authority, the government, is unable or uninterested in changing the status quo because it is enslaved to corporate interests, which are the real enemy. It trumpets a grievance ‘victimization by boom and bust’ which resonates with youth, particularly urban, educated and middle class youth whose life prospects have been hit hard by the global economic crisis. It implies an ‘in-group’ and an ‘out-group’ and it ends with a rousing call to make the world what you want it to be. There is no call to violence – nor is any implied. On the other hand, a world of do-it-yourself revolution is one which would possess multiple variants among disparate groups embracing different ways and means to similar ends. Consider the case of the extremist Anders Breivik who on 22 of July 2011 raided a youth camp of the Norwegian Labour Party shooting and killing 69 people, most of them teenagers: he decided what he believed and what made him angry, which he explained in laborious detail in a 1,000 page plus manifesto; he chose his ‘tribe’ – one which was defined almost entirely by his solitary online activities; and he went out to make the world what he wanted it to be. Thus, in the end, we may conclude of cyberpower’s effect on strategic affairs rather as H.G. Wells once did of airpower a hundred years ago, that it is a potentially terrible but ultimately limited weapon: ‘neither unthinkable nor blessed’.69

Note on Contributor

David Betz is at Senior Lecturer at the Department of War Studies at King’s College London.

Bibliography


68 Matthew Reinbold, ‘Superempowerment, Networked Tribes and the End to Business as We Know It’ Ignite 4, Salt Lake City (4 March 2010), <http://igniteshow.com/videos/super-empowerment-networked-tribes-and-end-world-we-know-it>.
Cyberpower in Strategic Affairs


Arquila, John, and David Ronfeldt, ‘Cyberwar is Coming’ in J. Arquila and D. Ronfeldt (eds), In Athena’s Camp: Preparing for Conflict in the Information Age (Santa Monica, CA: RAND 1997).


British Broadcasting Corporation, The Virtual Revolution, Episode 2 ‘The Enemy of the State?’, aired on BBC2 (6 Feb. 2010), <www.bbc.co.uk/programmes/b00n4j0r>.


Cronin, Audrey Kurth, Ending Terrorism (Abingdon: Routledge for the IISS 2008).


Economist 1 July 2010, <www.economist.com/node/16481504>


Occupy Wall St webpage <http://occupywallst.org/>.


