FOREIGN POLICY RESEARCH INSTITUTE
E-Notes
A Catalyst for Ideas | Distributed via Email and Posted at www.fpri.org | June 2012

CYBERPOWER AND INTERNATIONAL SECURITY

By David Betz

David Betz is a Senior Fellow of the Foreign Policy Research Institute and is a senior lecturer in the War Studies Department at King's College London. He is the head of the Insurgency Research Group there as well as the academic director of the master's program War in the Modern World. He also heads a 2-year US DoD Minerva-funded project on Strategy and the Network Society. Most recently, he is co-author (with Tim Stevens) of **Cyberspace and the State: Toward a Strategy for Cyber-Power.**

Like the shock paddles of a defibrillator on the chest of a heart attack victim the prefix 'cyber' has an electrifying effect on policymakers and strategists wrestling with the complexities of information age security—or more commonly today, "cybersecurity." Successfully attaching the term to this or that policy appears to markedly increase its chances of survival. Thus in recent years while public spending has been shrinking (or is expected imminently to shrink) we have seen a bonanza of resources dedicated to countering or mitigating threats to our economic vitality from "cyber espionage" and "cyber crime," societal cohesion from "cyber subversion" and "cyber terror," and ultimately our material being from "cyber war." "I dare say," said Deputy Secretary of Defence Ashton B. Carter in March 2012, "we'd spend a lot more if we could figure out where to spend it."[1]

Some venture to call this a panic, while others suggest a degree of alarm is justified. Both are partly right and partly wrong. The defense and foreign policy community is worried too much about the effect of cyber on the existing distribution of power among states in the international system. It is not worried enough about 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 high profile attacks of *Al Qaeda*, its affiliates and imitators in New York, Washington, Bali, Madrid, London, Mumbai and elsewhere are a part of the story. They are instances of what has been called cyberspace "touching the ground."[2] But they are not the whole of the story: 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.

> **What has been will be again, what has been done will be done again; there is nothing new under the sun.**
>
> ***Ecclesiastes 1:9***

The literature on cyber security is typified by two major preoccupations. The first is how "game changing" the technology is—even sidelining the Clausewitzean paradigm of war.[3] The second is a heavy analytical focus on

[1] Ellen Nakashima, "Pentagon Ups Ante on Cyber Front," *Washington Post* (19 March 2012), p. 1.
[2] Seymour Goodman, Jessica Kirk, and Megan Kirk, "Cyberspace as a Medium for Terrorists," *Technological Forecasting and Social Change*, Vol. 74, No. 2 (2007), pp. 193-210.
[3] James Adams, one of the first to write on "cyber war" described Clausewitz's theories as "outdated" and "ever more irrelevant" in *The Next World War* (New York: Simon and Schuster, 1998), p. 93.

computer science rather than social science. Both, while understandable to a degree, are unhelpful. The effect of connectivity on how war is conducted is potentially, although not yet shown in practice, considerably large. Its effect upon war's essence as a reciprocal act of force to compel one's enemy to do one's will is small, contrary to the claims of "cyber war" alarmists. All told, its effect upon strategic affairs is complex. On the one hand, it represents a significant advance in the "complexification" of strategy, understood in the sense of the production of intended effects as the philosopher Bertrand Russell described the function of power. 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.

> **"The Web is shifting power in ways that we could never have imagined. Cyberspace is reinventing warfare."**
>
> ***BBC, "The Virtual Revolution" (6 February 2010)***

Ours is not the first time in which it was claimed that technology was reinventing warfare. Beginning ninety years ago, the prophets of airpower writing in the shadow of the Great War's ghastly yet indecisive slaughters were equally convinced that aerial bombing of modern industrial societies, so vulnerable to disruption and terror they thought, would drastically increase the decisiveness of war. The Italian Giulio Douhet is the most famous of such theorists but others such as J.F.C Fuller and Basil Liddell Hart in Britain and William "Billy" Mitchell in the United States shared his views all or large part. One cannot help but hear echoed in today's "cyber doom" scenarios Stanley Baldwin's infamous 1932 House of Commons speech in which he warned "the bomber will always get through…"[4] That none of this proved true of airpower then does not mean that it might not be true of cyber power now. Some caution, however, about claims of discontinuous change in war might be in order.

> **"First you will come to the Sirens who enchant all who come near them. If any one unwarily draws in too close and hears the singing of the Sirens, his wife and children will never welcome him home again, for they sit in a green field and warble him to death with the sweetness of their song."**
>
> **Circe's warning to Odysseus in Homer's *The Odyssey*, Book XII**

Cyber power falls squarely in the tradition of what Eliot Cohen once described as airpower's "mystique," offering "gratification without commitment."[5] Moreover, it appears to offer other alluring properties which airpower does not: *anonymity* and *low "buy-in costs*." There is something to such claims. For instance, compared to ships and planes (the "hardware" of modern warfare) weaponized code seems relatively cheap. On closer inspection, though, it transpires that while relatively low-grade/low-potential-damage "cyber weapons" are indeed cheap and readily available, high-grade/high-potential-damage "cyber weapons" are not nearly so.[6] In historical perspective the Stuxnet virus that targeted the Iranian nuclear programme in 2010 will likely be regarded as the Zeppelin bomber of its day—whatever the cyber weapons that may follow it they are unlikely to be both cheap *and* effective. (At the time of writing a new piece of malware 'Flame' is in the news—designed for espionage rather than it sabotage, it is much larger than Stuxnet though it shares an apparently common lineage.) In short, cyber power is likely to make strong states stronger and weak states weaker.

The problem of anonymity has a similarly counterintuitive complexity. A devastating attack on national infrastructure by an unknowable attacker is an oft-heard nightmarish hypothetical.[7] However, the seeming ability of cyber power to deliver an almighty blow without triggering war's inherently escalatory nature is also seductive: it seems to offer the possibility of gratification without commitment whatsoever. But it is an exaggeration. The problem is not with the theoretical power of cyber espionage (possibly sponsored by foreign powers) to enervate economies that depend on secured intellectual property rights and electronic commerce[8]; it is, rather, that as a frame of analysis war as an act of force to compel our enemy *to do our will* is a distracting way to conceptualize the

---

[4] The full text of the Baldwin House of Commons speech from 10 November 1932 may be found on the "Airminded" blog, http://airminded.org/2007/11/10/the-bomber-will-always-get-through/; Baldwin was echoing the claims of the Italian air power theorist Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (New York: Faber and Faber, 1942).

[5] Eliot Cohen, "The Mystique of US Air Power," *Foreign Affairs*, vol. 73, no. 1 (January/ February 1994), p. 109.

[6] Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal*, Vol. 157, No. 1 (February/March 2012), pp. 6-13.

[7] Richard Clarke, *Cyber War* (New York, HarperCollins, 2010), pp. 67-68.

[8] One senses this recognition in The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

problem. Technology can alter the way in which force is applied but it does not obviate the necessity to declare one's will (even if after the event). Anonymity is as much a problem for the strategic aggressor as it is the defender. There is no way around this problem through gadgetry or subterfuge.

> **"Freedom is the freedom to say two plus two make four. If that is granted, all else follows."**
>
> **Winston Smith writing in his secret diary in George Orwell's *Nineteen Eighty Four***

Cyberspace, however, changes relations amongst non-state entities and between states and non-state actors in other significant ways. 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 or who act non-rationally cyber attack might yet prove a potent means of attack. More immediately, though, interconnectivity has proven to be an invaluable tool of social mobilization as may be seen in the "Arab Spring." There is controversy over these so-called "Twitter Revolutions": social media enthusiasts see the role of connectivity in them as inherently liberalizing while skeptics observe its eminent authoritarian utility. It is often said that cyberspace increases transparency, or what psychologists call "mutual knowledge" which, in turn, makes it harder to govern through repression. This is essentially the truth that Orwell's Winston Smith hit upon with his maxim of freedom consisting of the ability to speak one's mind. Big Brother's strength was the ability to prevent this, to deny people any environment, even in their own homes, in which they could speak openly. Thus having transformed every citizen into a solitary outpost of secret fear, physical control of the population was relatively easy.

The Spanish sociologist Manuel Castells describes what is happening as a paradigm shift from mass communications to mass self-communications. In our deeply networked public sphere social movements and "insurgent politics" have a greater ability to set agendas and shape discourse than ever before.[9] This is not academic fancy. Britain's chief of defence staff Sir David Richards has described the future of war in similar terms, arguing that the conflicts of our time are fought "through the medium of the Communications Revolution."[10]

> **"Find your tribe. Decide what you believe. Rally them around you."**
>
> **Matthew Reinbold, Salt Lake City Ignite Conference, March 2010**

[11]

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 makes it harder to govern full stop. Some argue that the way in which information now flows more freely into the public sphere has changed the "landscape of international relations" irrevocably.[12] Be this as it may, we can already observe that connectivity enhances the ability of movements to operate and organize in both the physical and virtual dimensions in ways that are hard to counter with the kinetic blows of a conventional campaign. Occupy Wall Street, which describes itself as a "leaderless resistance movement" utilizing the "Arab Spring tactic," is a case in point.[13] The use by the diverse "alter-globalization" of "smart mob" tactics using digital connectivity to deploy "swarming tactics" goes back to the 1999 "Battle for Seattle" protests against the World Trade Organisation is another.[14] In a wider sense we see signs of revolution adapting to the new public sphere as far back as the early 1990s Chiapas revolt in Mexico which skillfully exploited the then emerging cyberspace using email to internationalize its cause and find allies abroad. One sees the same trend exhibited in the umbrella group "We are Everywhere," which describes itself as an "unprecedented global rebellion of the oppressed and impoverished, a rebellion which is in constant flux, which swaps ideas and tactics across oceans, shares strategies between cultures and continents, gathers in swarms and dissolves, only to swarm again elsewhere."[15]

---

[9] Manuel Castells, *Communication Power* (Oxford: Oxford University Press, 2009), p. 302.

[10] General Sir David Richards, "Future Conflict and Its Prevention: People and the Information Age," International Institute for Strategic Studies (18 January 2010), http://www.iiss.org/recent-key-addresses/general-sir-david-richards-address/

[11] 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

[12] Carne Ross, "Wikileaks Whistle Blows Time on the Old Game," New Statesman (6 December 2010), http://www.newstatesman.com/society/2010/12/wikileaks-governments-cables

[13] From the Occupy Wall St webpage: http://occupywallst.org/

[14] Howard Rheingold, *Smart Mobs: The Next Social Revolution* (Cambridge, MA: Basic Books, 2002), pp. 160-162.

[15] Notes from Nowhere (eds.), *We are Everywhere: The Irresistible Rise of Global Anti-Capitalism* (London: Verso, 2003), p. 16.

It is easy to dismiss such groups. Their putative strengths of leaderlessness, diversity of membership, and constant internal debates over the desirability or otherwise of the use of force (the vast majority today are non-violent though some subgroups have embraced "black bloc" tactics, including property damage and sabotage as well as street-fighting) may just belie inept leadership, absence of real unity, and a general lack of seriousness of purpose. Today's "revolutionary" *zeitgeist* (in the West, at any rate) may serve no further purpose than the emotional sustainment of a small counterculture that possesses no potential of mass mobilization. And yet the potential for escalation in size and type of operation is real. As Starhawk (one of the major strategic thinkers in the movement) put it, one possibility is its evolvement into "an unpaid militant mercenary army."[16] The reason she concludes this would be wrong is important because it is not her personal conviction of non-violence that is germane so much as a shrewd strategic calculation that at the moment the political and economic system is already reeling toward collapse, violent tactics are "most likely to backfire and confirm the system's legitimacy."[17]

Whether or not Western society is really reeling towards collapse remains to be seen, although it is widely feared that the ongoing collapse of the Eurozone is leading to major social disorder.[18] Moreover, as opposed to Islamism, which in the West appeals to a minority within a minority, the "global justice" movement is powered by a widespread and deepening perception that the current order is significantly unjust. Cyberspace enables diverse movements to highlight some vital elements of a compelling strategic narrative, for instance in the case of "Occupy" economic victimization of the 99 percent by the 1 percent, and to organize in forms that are highly fluid and able to sustain protest over the long-term at low-cost. At the same time, it does not deliver on a platter another key ingredient: the plausible route to a better future which mass movements have always required in the past in order to truly mobilize. Were such to appear these groups would very rapidly scale the strategic agenda.

In the meantime and even without such a plausible end-state, the potential for new forms of simple disruption and attack of the *status quo* is worthy of concern. Social change is not *a priori* a bad thing—on the contrary, it is the hallmark of a healthy, dynamic and open society; it is, rather, that the range of known unknowns surrounding the emerging new hacker elite (in large part among 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. The Internet collective known as "Anonymous" is an example. In recent years it has "declared war" on everything from the Church of Scientology to the Zetas drug cartel. Yet despite having demonstrated the power to inflict pain and destroying wealth—the essential "bargaining power" of strategy—strategic studies has shown little interest in it. No doubt this is in part because the group, as its idiosyncratic target set and rationalization of their operations as being essentially "for the lulz" (i.e., laughs), is practically self-parodying. There are, however, similarities of outlook (if not organization and operational concepts) between Anonymous now and 19th and early 20th 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. Its championing of *Wikileaks* may be significant if it represents the development of a coherent ideological identity that can outweigh the well-established capriciousness of the group. Anonymous without an agenda is a nuisance; Anonymous with an agenda has the potential for quite serious mischief.

Connectivity has important implications for the practice of war but it does not alter its nature nearly as much as has been supposed. That said, we should not blind ourselves to the ways in which it is changing strategic affairs in the broader sense. 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 emergence of networked social movements that are building upon growing dissatisfaction with the *status quo* and embrace a "diversity of tactics" including purely electronic attacks conducted by a new hacker elite; and,

---

[16] Starhawk, *Webs of Power: Notes from the Global Uprising* (Gabriola Island, British Columbia: New Catlyst Books, 2008), p. 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).

[17] Starhawk, p. 150.

18 See UBS Investment Research, Global Economic Perspectives, "Euro break-up: The Consequences" (6 September 2011), http://www.scribd.com/doc/64020390/xrm45126

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

Perhaps most fundamentally for strategists the ever-greater number and interconnectedness of actors is highly problematic because it increases the inherent complexity of the strategic environment.

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. It seems to accelerate existing revolutionary tendencies and offer new coercive tools to 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. Contemporary events in the Middle East where old regimes toppled by spontaneous outpourings of public rage are being succeeded by more disciplined revolutionaries playing the vanguard game illustrate this duality.

In the West we appear to be seeing the "retribalization" of society, which the media guru Marshall McLuhan predicted in the 1960s in ways that are potentially very positive while also in ways that are decidedly negative. The extremist Anders Breivik who on the 22nd of July 2011 raided a youth camp of the Norwegian Labour Party shooting and killing sixty-nine people, most of them teenagers is an example of the latter which blends both cyberspace and "real space" elements inextricably: he chose his "tribe"—one which he defined on the basis of ideas almost entirely formed by his solitary on-line activities; he decided what he believed and what made him angry, which he explained in laborious detail in a 1,000-page-plus manifesto that he distributed to carefully selected individuals throughout Europe on the day of the attack; and he went out to make the world what he wanted it to be through an act of spectacular violence designed primarily as an "information operation" to galvanize his target constituency and win new adherents. Breivik's propaganda by deed was hardly the first of its kind; it is unusual as a variant that is highly adapted to the current communications paradigm and because of the degree of individual superempowerment it involved. It will not be the last.