H-Diplo | ISSF
Partnership

A production of H-Diplo with the journals *Security Studies*, *International Security*, *Journal of Strategic Studies*, and the International Studies Association's Security Studies Section (ISSS).

http://issforum.org

H-Diplo/ISSF Article Review Editors: **Thomas Maddux and Diane Labrosse**
H-Diplo/ISSF Web and Production Editor: **George Fujii**
Commissioned for ISSF by **Thomas Maddux**

H-**Diplo | ISSF Article Review 32**

Chris McGuffin and Paul Mitchell. "On Domains: Cyber and the Practice of Warfare."
International Journal 69:3 (2014): 394-412. DOI: 10.1177/0020702014540618.
http://dx.doi.org/10.1177/0020702014540618

Reviewed by David J. Betz, King's College London

Originally Published by ISSF on **22 January 2015**
Reissued on 4 October 2015
https://issforum.org/articlereviews/32-on-domains-cyber
http://issforum.org/ISSF/PDF/ISSF-AR32.pdf

Over the last few decades one of the hottest subjects of debate in the social sciences has been the emergence of 'cyber' and its effects on all manner of social relationships and human communities.[1] The term itself is chronically contested and the understanding of the nature of cyberspace in the literature (i.e., its delimitation, composition, and relations with other sorts of space) has a certain buffet quality to it, meaning one thing to some scholars and something else to others.[2] The most influential literature on the subject largely steers clear of the term in the search for the essence of the problem at hand. The sociologist Manuel Castells, for instance, has described the arrival of what he calls the "network society." The basic idea, in a nutshell, is that the recent (or, perhaps better, ongoing) putative 'revolution' in information technology has, in turn, given rise to a

[1] Barry Wellman, ed., *Networks in the Global Village* (Boulder, CO: Westview Press, 1999) represents a foundational example.

[2] On which point, see David Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue* 44:2 (2013), 147-164.

paradigmatically new form of organization of human activities—political, economic, and cultural—that is structured around network *flows* of information, wealth, and, ultimately, power.[3]

Naturally, the major armies of the world, and it must be said a good number of their non-state and quasi-state challengers, have been struggling with how to integrate network-centricity in their own praxis: war—the compelling of one's enemy to do one's will by force or the threat of the use of force.[4] Many have concluded that 'cyber' represents a vital new domain of warfare alongside the domains of land, sea, air, and space—and scarce funding and resources have flowed towards it accordingly. Chris McGuffin and Paul Mitchell's paper questions the logic of this development. Their conclusions, that there is "insufficient doctrinal commonality between physical domains and cyberspace for it to warrant the status of a domain" and that cyber exists as an enabler of force rather than a force in its own right, are compellingly made (411).

The method by which they arrive at this view is essentially a systematic comparison of the qualities of cyber with those of the above-noted more established domains. This discussion is solidly grounded in military theory and history and more broadly in a concept of war that is, though *On War* is not specifically mentioned, I think fairly described as Clausewitzian.[5] The gist of their difficulty of including cyber as a stand-alone domain of warfare very largely relates to its artificiality and malleability—as opposed to the naturally occurring domains governed by the laws of physics, cyberspace is a human-made thing governed (in part though not whole) by software code—and its inherent lack of dimensionality. While there is a degree of overlap between the traditional domains (force, for example, can be applied from the air and sea to the land and vice versa), ultimately:

"The physical environment of each domain directly shapes the conduct of activity therein. The ability to direct activity, observe, move, strike, defend, and preserve those abilities is key to the projection of military force and influence that results in direct control of activities taking place within them" (404).

Cyberspace, by contrast, has no physical boundaries by which it may be demarcated from other domains. Moreover, the ability to use cyber *independently* in order to create physical effect is very small.[6] None of this is to deny the importance of it in combined military operations both actual and potential, a point that the authors highlight in their final line suggesting that cyber warfare is yet in a period of immaturity akin to that of air power before the world wars. Somewhat enigmatically, though, they also write that "Cyber war is an extension of the theories that evolved from information warfare, command and control warfare, and network-centric warfare, concepts with which militaries

[3] See Manuel Castells, *The Information Age*, Vol. 1, *The Rise of the Network Society* (London: Blackwell, 1996), Vol. 2 *The Power of Identity* (London: Blackwell, 1997), and Vol. 3, *The End of Millennium* (London: Blackwell, 1998), as well as *Communication Power* (Oxford: Oxford University Press, 2009), and *Networks of Outrage and Hope: Social Movements in the Internet Age* (Cambridge: Polity, 2012).

[4] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy of Cyberpower* (London: International Institute for Strategic Studies, 2011).

[5] See Carl Von Clausewitz (Michael Howard and Peter Paret, eds.), *On War* (New York: Alfred A. Knopf, 1993).

[6] Martin Libicki, a key figure in the literature, has explored this point in great detail through a series of publications, but exceptionally well in *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007). More recently, Thomas Rid has penned a forceful rejoinder to the cyberwar rhetoric in "Cyberwar Will Not Take Place," *Journal of Strategic Studies* 35:1 (2012).

have struggled since their introduction" (411), which left me wondering whether they meant since the introduction of these particular hypothesized hyphenated and/or portmanteau war types or since the advent of war itself.

The latter is an eminently defensible point of view. During the Second World War the Allies defeated the German Navy's attempt to strangle Britain by submarine attack on its vital naval commerce by cracking the encryption of German military communications and by developing a command and control system for convoys and their escorts based on a very near real-time intelligence picture of the whole North Atlantic battlespace.[7] Was that cyber warfare? In 1917, Britain leveraged its dominance of worldwide telegraphic communications and the cryptologic capability of 'Room 40' (part of the British Secret Service) to crack the Zimmerman telegram—a German diplomatic proposal to Mexico that they should ally—a masterful propaganda coup that helped greatly to bring the United States into the First World War alongside Britain and France.[8] Was that cyber warfare? During the 1870-1871 siege of Paris in the Franco-Prussian War, the efforts of Prussian military intelligence to prevent French leaders from communicating with their still intact armies outside the encircled capital included (after all the telegraph cables had been severed) the deployment of specially trained falcon squadrons around the city to interdict the return flight of carrier pigeons that the French high command had exchanged with subordinate headquarters before the outbreak of hostilities.[9] Was that cyber warfare? A key task of Confederate cavalrymen during the American Civil War was not only to destroy Union telegraph communications (a technology that was then barely twenty years old) where they could, they also intentionally switched communications to the wrong destinations, transmitted false orders to Union forces, and generally acted in order to 'shape the information environment' of the war, as contemporary jargon would put it.[10] Was that cyber warfare?

In other words, McGuffin and Mitchell's thesis provides some disquieting food for thought: leave aside its status as a domain, has there ever been in the history of war a time when the sorts of operations that now often have the prefix cyber attached to them were not integral to the art of warfare? 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—theirs was a vision that was essentially tactical in orientation, a theory of battle in which greater combat power could be produced through the employment of better information systems.[11]

Would replacing the word cyber in current doctrine with the words 'computer network' lose anything? For that matter, no student of military history would dispute that electronic warfare has

[7] See Don E. Gordon, *Electronic Warfare: Element of Strategy and Multiplier of Combat Power* (New York: Pergamon Press, 1981), chap. 7.

[8] Patrick Beesly, *Very Special Intelligence* (London: Doubleday, 1978), 1-2.

[9] Alex Butterworth, *The World That Never Was: A True Story of Dreamers, Schemers, Anarchists, and Secret Agents* (New York: Vintage Books, 2010), 18.

[10] Alfred Price, *The History of US Electronic Warfare, First Ed.*, (Arlington, VA: Association of Old Crows, 1984), 1-2.

[11] John Arquila and David Ronfeldt, "Cyberwar is Coming," in Arquila and Ronfeldt (eds), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND 1997).

been an indispensable pillar of power for over a century. Thirty-five years ago one analyst described it thus:

"Electronic warfare includes all actions in the entire electromagnetic spectrum to intercept, analyze, manipulate, or suppress the enemy's use of the spectrum as well as to protect friendly use of the spectrum from similar attack by an enemy…"[12]

If we define cyber narrowly, as comprising "all existing computer networks and all the devices connected to those networks" (405) does that suggest it is incompatible with the rich body of military science encapsulated in the definition of electronic warfare above? What does cyber really bring to the table full stop? The introduction of McGuffin and Mitchell's paper contains an anecdote that hints at its true utility:

"Every fortnight the senior civilian and military leaders of Canada's Department of National Defence meet as a Programme Management Board (PMB) to decide the fate of key projects and initiatives. These leaders, representing the army, navy, air force, and each of the other departmental Level 1 organizations, have a keen interest in the allocation of resources. Decisions regarding the staffing of new positions are particularly contentious at a time when the Canadian Armed Forces' (CAF's) strength is being reduced due to budgetary limitations. Nonetheless, when the PMB chairperson, the vice chief of the defence staff, raised the subject of staffing for the CAF Cyber Task Force, the board members approved the immediate allocation of 20 persons to undertake the new assignments" (394-395).

It is not just in Canada, either—the same sort of scene has played out across a range of defence establishments within NATO on both sides of the Atlantic and further abroad. In a climate of general budget austerity with defence spending trending downward across practically every category, spending on cyber is untypically trending sharply upward.[13] Cyber does not constitute a new domain of warfare. As a term of use in strategic discourse it does more to obscure than to illuminate and it should be allowed to fade out of policy and back into science fiction. It has undeniable power over the imaginations and purse strings of politicians, however, so probably it will not.

David Betz is Reader in Warfare in the War Studies Department of King's College London. His publications include *Cyberspace and the State: Toward a Strategy for Cyberpower* (IISS, 2011) and the forthcoming *Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power* (Hurst 2015). His current research centres on security issues and network flows, war and the built environment, and the renewal of fortification in strategic thinking.

[12] Gordon, 9.

[13] The UK stands as a particularly good example. See Malcolm Chalmers, 'The Lean Years: Defence Consequences of the Fiscal Crisis', in Michael Codner and Michael Clarke (eds.), *A Question of Security: The British Defence Review in an Age of Austerity* (London: I.B. Tauris for the Royal United Services Institute, 2011), pp. 33-75.