Volume 10 (2010)

Interface: The Journal of Education, Community and Values

8-1-2010

Inside Cyber Warfare

Jeffrey Barlow
Pacific University

Inside Cyber Warfare

Description
This review of Jeffrey Carr's work, Inside Cyber Warfare, follows upon our discussion in the previous issue of Interface, "Cyber War and U.S. Policy: Part I, Neo-realism." That piece was informed in large part by a review of Richard A. Clarke and Robert Knake's recent work, Cyber War: The Next Threat to National Security and What to Do About It. The two books are on the same topic, and the two reviews are intended to be complementary.

Inside Cyber Warfare

Posted on **August 1, 2010** by **Editor**

Review Essay by Jeffrey Barlow

This review of Jeffrey Carr's work, *Inside Cyber Warfare*, follows upon our discussion in the previous issue of *Interface*, "Cyber War and U.S. Policy: Part I, Neo-realism." That piece was informed in large part by a review of Richard A. Clarke and Robert Knake's recent work, *Cyber War: The Next Threat to National Security and What to Do About It*. The two books are on the same topic, and the two reviews are intended to be complementary.

The works proceed, however, from different premises. While Clarke and Knake see the topic of cyber war as related to earlier forms of warfare, they also see cyber war as demanding a very different approach.

Carr in *Inside Cyber Warfare* sees continuities as more important than discontinuities. The work relies, much more than did Clarke and Knake, upon models derived from earlier forms of warfare.

The distinction arises, I believe, because the two works are intended for substantially different audiences, though clearly they overlap; the group concerned about cyber war is very large. Clarke and Knake see cyber war as a policy problem. But for Carr, the problem is essentially a military one. This may be in part because the group concerned with the threat of war in any form, is, of course, the military establishment. Today's high-ranking officers were trained for, and are experienced in, kinetic warfare. Attempts to present cyber war as discontinuous and requiring substantially new approaches are going to be less welcome than those which see it as just a new "battle space."

Clarke, however, is deeply suspicious of those in the American military who draw quick comparisons to past war-fighting technologies in which cyber space is viewed simply as another battlefield:

"...the U.S. military in general repeatedly characterizes cyberspace as something to be dominated. It is reminiscent of the Pentagon's way of speaking of nuclear war in the 1960s. The historian of nuclear strategy Lawrence Freedman noted that William Kaufmann, Henry

Kissinger, and other strategists realized that there was a need then "to calm the spirit of offense, potent in Air Force circles…[whose] rhetoric encouraged a view of war that was out-moded and dangerous." That same sort of macho rhetoric is strong in Air Force cyber war circles today, and apparently in the Navy as well [1]."

Jeffrey Carr is a "principal" at GreyLogic, a noted cyber security firm. Carr, and GreyLogic take a hard line on issues related to cyber War [2]. While having a significant financial stake in the cyber Security industry obviously does not disqualify an expert such as Carr from having a great deal to say on the subject, it does expose him to charges of self-interest and subjectivity. There clearly is a "cyber War industrial complex" already in existence, and there are billions to be made from solving the problems presented by cyber conflicts, but also from exploiting, even creating, fears. Some commentators have felt that at times the line between problem solving and exploitation grows a bit unclear [3].

Carr's credentials are first-rate; he consults frequently, publishes widely, and his access to insider sorts of studies and information—some studies done at GreyLogic, others in various military and think-tank venues. These provide *Inside Cyber War* with a great deal of urgency and credibility. He is, in this area, a consummate insider. His publisher, O'Reilly Media, is noted for narrowly focused expert analysis of a broad range of technical areas [4].

Another large difference between the two works is that Carr and his major sources reflect a sort of mirror image to Clarke and Knake in that while they certainly were concerned with the potentially violent impact of the Internet, their work focuses more on policy than on technology.

Carr's work is very much based in a close analysis of technology and technologically enabled opponents. Accordingly it largely treats solutions not as policy issues, but as technical ones facing the defense establishment. This is both its strength, and its weakness.

The strengths of *Inside Cyber Warfare*, however, are many. The work analyzes many examples of cyber conflicts. It also has very close analysis of the organizations and cyber conflict doctrines of potential adversaries, to Carr, clearly China and Russia. While Clarke and Knake saw a large part of the critical threat from cyber conflict to be a result of the wide dispersion of both tools and motives for engaging in cyber attacks among highly varied non-state actors around the world, Carr focuses upon potentially adversarial states.

While paying attention to criminal gangs and free-lance hackers, Carr sees the link between nation states and their hackers to be the truly threatening issue. Carr's material includes many useful brief summaries of hacker gangs, their WWW locales, and even of individual hackers, usually, of course, known by their on-line identities. These make fascinating reading and would provide the interested reader with a great deal of material for their own research, though a great deal of caution is in order in accessing some of the sites listed [5].

Carr's grasp of technology is very strong and chapters 7-10 could well constitute a manual for

white-hat hackers wishing to form a sort of counter-weight to the Russian criminal gangs and Chinese citizens' cyber militias which Carr sees as part of the strengths of those two potential adversaries. Some of the content is quite dense and in addition to providing step-by-step guidance to guarding against or tracking down threats, serves as an introduction to many useful sites which will doubtless evolve to stay abreast of future developments in this field.

The book grows a bit labored at times. The author simply incorporates parts of a large unpublished study by Lt. Cdr. Matthew Sklerov into chapter 4, and again into Chapter 13. Chapter 4 deals with the concept of "active defense," or what might fairly be termed immediate retaliation or even preemptive strikes for cyber attacks presumed to be imminent.

The problem in active defense, however, is attribution. That is, how do we know who has attacked? And even if we determine that an attack comes from say, China, how can we be sure that it was launched by the Chinese government and not by an ultranationalist Chinese teenager? Carr rather glosses over such issues, asserting that technological solutions and "predictive intelligence" can ultimately determine perpetrators. Clark and Knake, however, see this as a very difficult problem to be dealt with quite carefully in terms of policy.

The work itself, however, shows some of the problems raised in dealing with a potentially infinite number of threats. For example, a state often presumed to be adversarial is China. But Carr's own materials on China do not give us a great deal of confidence in at least his own ability to perform the snap-judgments necessary to respond to possible impending attacks on the part of some *unknown* foe.

While Carr might be excused for such cultural lapses as a compete misunderstanding of the Chinese system of names, in which family names come first and given names last, other problems are more serious ones. To Carr, Hong Kong and China are sufficiently the same that a threat from Hong Kong is one from China, and, presumably, vice-versa. This would astonish both mainlanders and "Hong Kong Belongers," each quite a distinct group.

And at pages 174-175 his analysis is at least laughable, if not downright racist. He takes an ancient Chinese book of military stratagems and by drawing very far-fetched analogies makes them warnings of potential Chinese evil intentions with regard to cyber war [6]. As Carr says, the "36 stratagems…still plays a large role in shaping Beijing's military strategy [7]." And don't forget the greatest of all Chinese criminal masterminds, Fu Manchu, either.

Skerlov, and by extension, Carr, after a great deal of logic-chopping on the former's part, finesse the problem of attribution by arguing that states are legally obliged to prevent cyber attacks [8], and hence it would be legal to immediately attack that state [9]. This is, of course, given the ability of teenagers to successfully launch cyber attacks upon the Pentagon from, say, a rural area of Alabama, let alone a Chinese Internet café, rather strange reasoning.

This chain of reasoning also ends, as Clarke and Knake point out, in justifications under certain

foreseeable circumstances for "kinetic responses"—i.e., conventional warfare attacks, given that the U.S. is so much weaker on the defense than some of its potential opponents (because it has so many more critical electronic sites to defend) and hence must rely on quick and violent counter-attacks.

At the last I must agree with Clarke and Knake that while extrapolations from warfare in the predigital age are useful, cyber conflicts are substantially new. Belabored attempts to face cyber conflicts into the moulds of kinetic ones are more dangerous than enlightening.

On balance, this is a very useful book. It provides a hard-nosed counterpoint to anyone suspecting that Clarke and Knake are ultimately appeasers, and a good insight into the very widespread, perhaps dominant, Realist perspective on cyber conflicts. Anyone wishing to fully understand cyber conflict and the various schools of thought on it should not neglect it. But it is probably most useful not as a manual or a final statement on cyber war, but as a resource which can open up a wide variety of sources and perspectives.

Endnotes

[1] Highlight Loc. 689-95, Kindle Edition, Clarke and Knake.

[2] For an understanding of GreyLogic's perspective on questions related to cyber war, see their WWW page at: http://greylogic.us/

[3] See a skeptical take on this issue see Robert X. Cringely, "The next cyber war will be for your wallet" In *InfoWorld*, at: http://www.networkworld.com/news/2010/030510-the-next-cyber-war-will.html

[4] http://oreilly.com/

[5] If you are not already well aware of some of the potential consequences of visiting some web pages, see our review of Nitesh Dhanjani's work, Hacking: The Next Generation

[6] "Hide a knife behind a smile," for example, is related to phishing schemes at p. 175, as is "tossing a brick to get a jade gem."

[7] p. 175

[8] pp. 62-68.

[9] See also Carr's article "Projecting Borders into Cyberspace"

This entry was posted in Uncategorized by **Editor**. Bookmark the **permalink [http://bcis.pacificu.edu/interface/?p=3817]** .

Inside Cyber Warfare provides fascinating and disturbing details on how nations, groups, and individuals throughout the world use the Internet as an attack platform to gain military, political, and economic advantages over their adversaries. You'll discover how sophisticated hackers working on behalf of states or organized crime patiently play a high-stakes game that could target anyone, regardless of affiliation or nationality. Inside Cyber Warfare goes beyond the headlines of attention-grabbing DDoS attacks and takes a deep look inside multiple cyber-conflicts that occurred from 2002 through summer 2009. Learn how cyber attacks are waged in open conflicts, including recent hostilities between Russia and Georgia, and Israel and Palestine. Discover why Twitter, Facebook, LiveJournal, Vkontakte, and other sites on the social web are mined by the intelligence services of many nations. Inside Cyber Warfare summary is updating. Come visit Mnovelfree.com sometime to read the latest chapter of Inside Cyber Warfare. If you have any question about this novel, Please don't hesitate to contact us or translate team. Hope you enjoy it.