


December 2014

## Publisher's Corner: Don't Call It Cyberspace

Roger G. Harrison  
Roger.g.harrison@edu.edu

Follow this and additional works at: <https://digitalcommons.unomaha.edu/spaceanddefense>

 Part of the [Asian Studies Commons](#), [Aviation and Space Education Commons](#), [Defense and Security Studies Commons](#), [Eastern European Studies Commons](#), [International Relations Commons](#), [Leadership Studies Commons](#), [Near and Middle Eastern Studies Commons](#), [Nuclear Engineering Commons](#), [Science and Technology Studies Commons](#), and the [Space Vehicles Commons](#)

Please take our feedback survey at: [https://unomaha.az1.qualtrics.com/jfe/form/SV\\_8cchtFmpDyGfBLE](https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE)

### Recommended Citation

Harrison, Roger G. (2014) "Publisher's Corner: Don't Call It Cyberspace," *Space and Defense*: Vol. 7: No. 0, Article 8.

DOI: 10.32873/uno.dc.sd.07.01.1131

Available at: <https://digitalcommons.unomaha.edu/spaceanddefense/vol7/iss0/8>

This Article is brought to you for free and open access by DigitalCommons@UNO. It has been accepted for inclusion in Space and Defense by an authorized editor of DigitalCommons@UNO. For more information, please contact [unodigitalcommons@unomaha.edu](mailto:unodigitalcommons@unomaha.edu).

## Publisher's Corner: Don't Call It Cyberspace

Roger G. Harrison

It is said of human beings that we are a pattern discerning species. We tend to search for or invent patterns even where none exist—hence the popularity of power point.<sup>1</sup> When we deal with something truly unprecedented, our tendency is nonetheless to find some precedent for it, or, failing that, to fall back on analogy, metaphor or simile, all tools the mind uses to confront the unknown future with the familiar—which is one reason that large organizations faced with unique challenges almost invariably get it wrong.

We are in danger of doing that again as we organize to deal with challenges to national security presented by the unique phenomenon of cyber, and do so based on comparisons between cyber and space—or, more radically, on the notion that these are, for practical purposes, aspects of the same thing. This is the synergy thesis, on the basis of which Air Force Space Command is now charged with the responsibility for cyber as well. Former Assistant Secretary of the Air Force Jeffrey Harris told a recent symposium at CSIS that in his view space and cyber were ‘merging and aligning.’

It isn't immediately clear what any of this means. How do you ‘merge’ a tangible, physical

---

<sup>1</sup> It is a mark of the essential difference between cyber and space that the latter can be represented adequately on a power point slide (or more commonly a very large number of them) whereas the former cannot be. Power point is good at describing structure but very bad dealing with abstraction, and cyber is an abstraction, representing our efforts to imagine a universe compounded of billions of independent transactions from millions of sources, some known, some unknown, and some potentially generated by the environment itself. Such a phenomenon cannot be represented visually, which saves it (or should) from power point's intellectual death grip. Note that the cyber ‘cloud’ (itself a metaphor) is most often represented in power point presentations not by lengthy explanation, or by bulleted talking points, but by a drawing of a cartoon cloud.

environment like space, with an intangible, virtual environment like cyber? In what way do they align? How do we capitalize on the mutually reinforcing (synergistic?) characteristics of a domain like space where doctrine changes at the speed of bureaucracy, and a domain like cyber which is so much in flux that even the concept of doctrine doesn't seem to apply?

The thesis here is precisely the opposite, i.e., that cyber is something truly new and unique in human experience. Nothing like it has existed before. So we will have to do the tedious work of conceiving, *ab initio*, an entirely new approach to management, collaboration, procurement, organization, and strategy. And we will have to cultivate a new kind of strategic mind that can lead in this unique environment.

Defenders of the synergy thesis will point out in rebuttal the similarities between cyber and space. For example, attribution of attack is a problem for both space and cyber warriors; deterrence therefore presents some of the same problems in the two domains.<sup>2</sup> Satellites are one conduit (although only one) for cyber communication, and cyber is one possible vector for interfering with or disabling satellites. Both space and cyber depend on electromagnetic spectrum, and this dependence makes both vulnerable to attack from a variety of national and non-national actors with relatively limited resources.<sup>3</sup> Both are arguably offense-

---

<sup>2</sup> The problems are much more difficult, and perhaps impossible, to resolve in cyber, another mark of essential difference between cyber and space. Both the Eisenhower Center and Rand Corporation published studies of how deterrence might apply in space, given the right combination of hardware and policies. The most prominent study of cyber deterrence concludes, on the contrary, that it is simply not possible.

<sup>3</sup> This mutual vulnerability is not symmetrical. An interruption of that portion of cyber communication carried by satellites would be a serious inconvenience; a compromised cyber network could render the

dominant environments, i.e., environments in which technology favors the attacker—particularly preemptive attack—over defense. And mission assurance in both domains is critical to national security.

Still, these “points of contact” are to some degree incidental<sup>4</sup> and in any case pale before the differences between the two domains. Indeed, space and cyber are not just different but essentially antithetical, and the real question is not how we combine their strengths (although we should when we can) but how we keep them safely distinct and prevent the culture of space—with its endless procurement cycles, hierarchical management structures, overlapping and mutually hostile bureaucracies, glacial response times, derivative strategic concepts, and aging, entrenched work force—from seeping over into the cyber environment.

Is antithetical too strong a word? It might be argued that some differences between the two domains are simply matters of degree. The most obvious example is the need in cyber for much greater speed in research, planning, procurement, and training. The problem—a problem inherent in the nature of the environment—is that the traditional bureaucratic space management structures are incapable of that kind of speed.<sup>5</sup> Because operating in space is so expensive, their emphasis is (properly) on redundancy and robustness of systems, adherence to proven protocols, and, above all, avoidance of mistakes. Cyber, on the other hand, changes so rapidly that yesterday's protocols may be obsolete today and self-defeating tomorrow. Because the cost of entry in cyber is low, the opportunity and reward for experimentation and innovation are correspondingly high. Space may be ‘contested,’

---

information provided by satellites useless—or, at worst, malicious.

<sup>4</sup> Lists like this do not imply any existential connection between cyber and space. Similar lists could be constructed in relation to any two strategic domains, for example space and air, or space and undersea.

<sup>5</sup> The business plan of “new space” companies like SpaceX is based on bringing cyber management practices to traditional space operations, especially launch. Whether it will work or not is open to question.

but in relation to cyber it is truly a peaceable kingdom where the incidents of intentional interference are rare. Our cyber networks, by contrast, are attacked thousands of times every day. We may be surprised in space as potential adversaries attain capabilities more quickly than we had anticipated, but that evolution will likely measure in years and even decades. We can only vaguely discern the challenges that will face us in cyber a year from now; indeed, we are uncertain of our grasp on those we confront at present.<sup>6</sup>

These are not just differences in degree; they are differences in kind and will require different kinds of management structures, a different lexicon of terms, and a new sort of strategic mind. Applying the slow but certain model to cyber (treating it as we treat space) is not just inappropriate but potentially disastrous.

The commercial world provides a model of the sort of management structures that work. Companies that succeed in the cyber world tend—at least initially—to be small and entrepreneurial. Management structures are flat; talent is rewarded regardless of rank (and rank in the traditional sense is rare); innovation is favored; received wisdom is treated with skepticism; power is dispersed; doctrine is suspect; dogma is rejected. The atmosphere reminds many in the older generation of that which existed in the space community forty years ago. The problem for cyber companies is how to maintain those characteristics as they succeed, and therefore become larger and more bureaucratized, that is, more like government. This raises the question of whether government—and in particular the military—can run a successful cyber operation. How can it become more like these entrepreneurial companies? More of that below.

---

<sup>6</sup> The Obama Administration Space policy refers to the possibilities of international agreements, including arms control, for space. Historically, arms control agreements only become possible when contending sides believe that they understand the terrain sufficiently to conclude that neither they nor their adversaries can achieve unilateral advantage at acceptable cost. This is, arguably, true of space, but not of cyber, where the terrain is so uncertain that even the parameters of theoretically stabilizing international agreements are far from clear.

In the meantime, it is likely that success in national security cyber will require an unprecedented level of cooperation with commercial operators, whose experience is vital and whose interests in cyber are essentially the same as those of government. The old divisions between government and industry, the public sector and the private, will have to be (and are being) re-drawn.<sup>7</sup>

The sort of new lexicon we will need is more difficult to describe. Perhaps the key here is to understand the state of mind we need rather than the concepts themselves, which are beyond the scope of this brief paper. This state of mind might be described as radical skepticism when it comes to the application to cyber of any concept (metaphor, analogy, or simile) developed in other domains for other purposes.

To resort to these will be the inevitable tendency, not because the concepts are applicable but because we are comfortable with them and because adopting them requires no new and painful bureaucratic consensus building. What constitutes offense and defense in cyber? What is meant—or can anything be meant—by deterrence, by escalation, by security and preemption in the cyber domain? It may be that some or all of these terms are useful, just as the concept of merging domains may be useful, but only if we can describe (and then agree on) what they mean in this unique new world, and only if cyber stabilizes sufficiently to ensure that they mean the same thing from one planning cycle to the next.

Finally, we will need a different kind of strategic mind, accustomed to irregularity, ready to make mistakes, free of doctrine, hostile to dogma, and alert to the principal thing (among many) that makes cyber as a strategic environment something new—that it is, in every sense, a product of our imagination. When we enter space we encounter what amounts to a toxic sea that erodes our bodies

and our machines; but space is indifferent to our presence and imposes the same limitations on all who operate there. When we enter cyber, we encounter ourselves—the human psyche electronically enhanced. Cyber exhibits all the virtues and vices of our species: it is creative, dynamic, perverse, innovative, evolutionary, elusive, and constantly evolving. We can (at least in theory) develop a doctrine for space and be reasonably certain that it will still be applicable a decade from now. Opponents can counter strategize, but they labor under the same physical limitations we do. In a sense, every punch will be telegraphed; whether we are agile enough to react, of course, is another issue.

There is no such assurance in cyber, where threats come from everywhere, opponents appear and disappear, motives other than greed can be obscure, and doctrine (if we have any) will have to be *ad hoc*, developed on the fly and discarded just as quickly. We are not on a level playing field in cyber; we are limited by law, others—freelance individuals or non-state networks—are not.

Which begs the previous question: where, aside from the commercial sector, will we find examples of how this threat can be countered, and the leaders to do it?

The answer, paradoxically enough, is: the military, or more specifically the Army and the Marine Corps under pressure of combat. The habits of mind that cyber requires are being developed at the moment in the conflict with insurgencies, particularly in Afghanistan. Brian O’Keefe described the phenomenon in a recent issue of “Fortune” magazine (March 22, 2010). Industry was, O’Keefe wrote, “skeptical of structure” and therefore looking to the military veterans of the wars in Iraq and Afghanistan for the kind of young leaders who are “comfortable with complexity,” and capable of “dealing with ambiguity” and “challenging paradigms.”

A former Army captain now at Google was quoted as saying this: “I think the people who are doing interesting stuff in the military are entrepreneurial in mindset. And they don’t look up for approval and permission to do stuff. They are just doing it, and then after a while, the chain

---

<sup>7</sup> Large cyber companies like Google and Intel already operate as quasi-sovereign entities, as the recent contretemps between Google and China (a severing of relations, then partial rapprochement) demonstrate. This is also true, not incidentally, of supra-national commercial space operators like Intelsat, now headquartered in Luxembourg.

of command recognizes that what they're doing has value, and they kind of put a veneer of respectability around it." In other words, doctrine in fast developing environments like counter insurgency and cyber follows rather than informs tactics. Confusing that kind of world with the world of space—or, for that matter, the cyber challenge with any other we have faced in our history—is to mire ourselves in false analogy. There really is something new under the sun.