Executive Summary

Strategic Studies Institute and U.S. Army War College Press

MAKING STRATEGIC SENSE OF CYBER POWER: WHY THE SKY IS NOT FALLING

Colin S. Gray

Generically viewed, the challenge that cyber power poses to our understanding is a familiar one. After all, within living memory (just about) we have had to try and make sense of air power, and then, a generation later, of nuclear weapons and their possible delivery by ballistic missiles. What unites our experience with air power, nuclear weapons, and now cyber, is the authority of strategic explanation conveyed in the general theory of strategy—Carl von Clausewitz's rules, even though he was ignorant of hydrogen fusion weapons and of networked digital computers.

Our challenge is the need to be thoroughly respectful of the science and engineering that generates the technology for cyber, while at the same time declining to be so dazzled by the technical wonders that are ours to command that we are unable to look beyond technology and tactics. To date, the networked computer has fueled a large library on the technology and the tactics of the emerging digital age, but very little of lasting note on the strategic meaning of it all. Senior people in the ranks of strategic studies have by and large ignored the growing cyber challenge, while those who are technically highly cyber knowledgeable typically have scant background in strategy. On the one hand, those who are technically competent have not been sufficiently strategically educated to know how to think about cyber strategically. On the other, those who have some serious credentials as strategic thinkers have been deterred both by their uncertain technical grasp of cyber and—it needs to be said—by the more pressing demands of other strategic challenges. In the 2000s, cyber has been "coming," but it has not been urgent in its need for attention today, unlike the problems associated more directly with terrorism and insurgency. Regarded historically, the American extended defense community strives to cope seriatim with the biggest issue of "now." As counterterrorism (CT) and counterinsurgency (COIN) have more than somewhat faded from high official interest in very recent years, so, predictably, there has been opportunity for the next new big conceptual challenge to dominate conference and seminar agendas—cyber.

The revolution in military affairs (RMA) theory of the 1990s (and the transformation theory that succeeded it) was always strategy- and politics-light. It is not exactly surprising that the next major intellectual challenge, that of cyber, similarly should attract analysis and assessment almost entirely naked of political and strategic meaning. Presumably, many people believed that "doing it" was more important than thinking about why one should be doing it. Anyone who seeks to think strategically is obliged to ask, "So what?" of his or her subject of current concern. But the cyber revolution did not arrive with three bangs, in a manner closely analogous to the atomic fact of the summer of 1945; instead it ambled, then galloped forward over a 25-year period, with most of us adapting to it in detail. When historians in the future seek to identify a classic book or two on cyber power written in

the 1990s and 2000s, they will be hard pressed to locate even the shortest of short-listable items. There are three or four books that appear to have unusual merit, but they are not conceptually impressive. Certainly they are nowhere near deserving (oxymoronic) instant classic status. It is important that cyber should be understood as just another RMA, because it is possible to make helpful sense of it in that context. Above all else, perhaps, RMA identification enables us to place cyber where it belongs, in the grand narrative of strategic history.

In addition to thinking about cyber in the context of strategy's general theory, also it is enlightening to consider cyber in the contexts of geography and of information. Much of the unhelpful undue technicism about cyber is suitably sidelined when the networked computer and its cyberspaces are framed both geographically and as only the latest stage in the eternal and ubiquitous story of information. To approach cyber thus is not to demote or demean it; rather, is it simply to locate cyber properly in our relevant universe.

Argument by historical analogy is commonplace and essential; indeed, it is unavoidable, because history is our sole source of evidence. We cannot help but argue from what we know to what we do not (and cannot) know. It is helpful to consider cyber with reference to its prospective utility in terms of net assessment, and to resort to analogical thinking strategically and tactically, being suitably respectful of the critical distinctions between them. In strategic analogy, cyber is entirely familiar. If we are able to think strategically about Landpower, sea power, air power, and Earth-orbital space power, ipso facto we can think strategically about cyber with its electrons. The EMS does not pose a challenge to the theory of strategy.

However, efforts to think tactically by analogy about cyber are certain to be seriously misleading and probably disastrously wrong. Cyber is as different from the military power of the other geographical domains as they are from each other. Indeed, because of the nonphysicality of cyber power (though not of the cyber infrastructure and its human operators), this fifth domain is uniquely different technically and tactically. The challenge to understanding is the necessity for us to be fully respectful of the distinctive "grammar" of cyber, without falsely assigning similarly unique meaning to its policy and strategy "logic. "

Four broad conclusions are compelling at this time. First, cyber power will prove most useful (or dangerous, as enemy cyber power) as an enabler of joint military operations. Horror scenarios of stand-alone (miscalled "strategic") cyber attacks are not persuasive. The United States should expect its cyber assets to be harmed in conflict, but, if disrupted as anticipated, the country will repair, recover, and fight on. A like judgment applies to our Landpower, sea power, air power, and space power.

Second, while it is probably true to claim that, for technical reasons, cyber offense usually is likely to achieve some success, more significantly, is it probably true that the harm we suffer is most unlikely to be close to lethally damaging. Thanks to the technology that makes cyberspace, our discretion in the re-creation of cyberspace should present our enemies with unsolvable problems. Cyber offense is swift, but it is not likely to be deadly, and it should not work twice. Cyber defense ought to prove good enough.

Third, it is sensible to try and remember that cyber power is only information. Moreover, cyber is only one among many ways in which we collect, store, and transmit information. As if that were not contextual caveat enough, it is important to recognize that there is a great deal more to conflict and actual warfare than information, no matter what the tools for gathering and transmitting data may be. From the beginning of time, armies have clashed in relative ignorance. This is not to demean the value of information, but it is to remind ourselves that information, even knowledge (or its absence), is not a wholly reliable key to strategic success or failure.

Fourth, overall, despite the acute shortage of careful strategic thought on the subject, and notwithstanding the "Cybergeddon" catastrophe scenarios that sell media products, it is clear enough today that the sky is not falling because of cyber peril. The fundamental reason we can be confident about this is because cyber power,

ours and theirs, is ruled by the general theory of strategy. Once we shed our inappropriate awe of the scientific and technological novelty and wonder of it all, we ought to have little trouble realizing that as a strategic challenge we have met and succeeded against the like of networked computers and their electrons before. The whole record of strategic history says: Be respectful of, and adapt for, technical change, but do not panic.

*****

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute's homepage at *www.StrategicStudiesInstitute.army.mil.*

*****

This Publication

SSI Website

USAWC Website