We encourage you to e-mail your comments to us at: strategicstudiesquarterly@maxwell.af.mil.

Deciphering Cyberpower

Strategic Purpose in Peace and War

John B. Sheldon

What is the strategic purpose of cyberpower? All too many works on cyberspace and cyberpower are focused on the technical, tactical, and operational aspects of operating in the cyber domain. These are undoubtedly important topics, but very few address the strategic purpose of cyberpower for the ends of policy. Understanding its strategic purpose is important if policy makers, senior commanders, and strategists are to make informed judgments about its use. Cyberpower does indeed have strategic purpose relevant to achieving policy objectives. This strategic purpose revolves around *the ability in peace and war to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment.*

While it is proper to pay attention to the technological, tactical, and operational implications, challenges, and opportunities of cyberspace, this article concerns itself with its use—"the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power"—for achieving the policy objectives of the nation.[1] Transforming the effects of cyberpower into policy objectives is the art and science of strategy, defined as "managing context for *continuing advantage according to policy*" (emphasis in original).[2] The definition provides the overall strategic impetus for the use of cyberpower. To fully understand the power of cyber, one must acknowledge the character of cyberpower and cyberspace. The linkage between strategic context, strategy, and

The author wishes to thank Derek Reveron, Naval War College; Col Harold J. Arata, USAF, and his exemplary team at the Center for Cyberspace Research; Drs. Harold R. Winton, Richard Muller, James W. Forsyth Jr., Stephen Wright, and Stephen D. Chiabotti at the School of Advanced Air and Space Studies; and Lt Col William E. Young, USAF, currently at Air War College.

John B. Sheldon, PhD, is professor of space and cyberspace strategic studies at the School of Advanced Air and Space Studies and deputy director of the AF Space and Cyber Strategy Center, Maxwell AFB, AL. He also teaches cyber strategy at the AF Institute of Technology's Cyber 200 and Cyber 300 courses at Wright-Patterson AFB, OH. Prior to his current duties, he served in Her Britannic Majesty's Diplomatic Service.

Disclaimer
The views and opinions expressed or implied in the SSQ are those of the authors and should not be construed as carrying the official sanction of the United States Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

cyberpower is also essential. Ultimately, cyberpower stems from the ability to manipulate the strategic environment, and this requires a theory of cyberpower.

The Character of Cyberspace and Cyberpower

It is worth noting the difference between the terms *cyberspace* and *cyberpower*. Cyberspace is the domain in which cyber operations take place; cyberpower is the sum of strategic effects generated by cyber operations in and from cyberspace. These effects can be felt within cyberspace, as well as the other domains of land, sea, air, and space, and can also be cognitively effective with individual human beings. With this in mind, we turn our attention to some of the main characteristics of cyberspace.

Cyberspace relies on the electromagnetic spectrum (EMS). Cyberspace cannot exist without being able to exploit the naturally existing electromagnetic spectrum. Without the EMS, not only would millions of information and communications technologies (ICT) be unable to communicate with each other, but the ICTs themselves would be unable to function. Integrated circuits and other microelectronic devices depend on electrons to function. Fiber-optic cables are nothing if they are unable to propagate light. Networks of ICTs are also dependent upon the myriad properties of the EMS for their essential connectivity via radio frequencies and microwaves.[3]

Cyberspace requires man-made objects to exist. This makes cyberspace unique when compared to the land, sea, air, and space domains. Without integrated circuit boards, semiconductors and microchips, fiber-optics, and other ICTs, there would be no cyberspace capable of hosting the EMS. Space would still exist if humankind were not able to place satellites in Earth orbit; the sea would still exist if humans had been unable to master the intricacies of buoyancy; and similarly, the air would still exist if the principles of flight had not been discovered. Cyberspace would not exist were it not for the ability of human beings to innovate and manufacture technologies capable of exploiting the various properties of the EMS. Without such technologies the EMS would be nothing more than the "Luminiferous Ether" promulgated by the scientist Albert A. Michelson in the late nineteenth century—in other words, though it can be said to exist, the velocity of the earth's orbit around the sun has no discernable effect on it.[4]

Cyberspace can be constantly replicated. As an entity, there is only one air, one sea, one space, and one land. In contrast, there can be as many cyberspaces as one can possibly generate. In reality, there is only one portion of the air, sea, or land that is important: that portion that is being contested. The air over the United States is pretty much the same as that over Afghanistan. The only difference is that the air over the United States is not contested like the air over Afghanistan (or at least, it is contested in principle if not in practice). The same goes for the oceans. One could set off across the Atlantic tomorrow and have a more or less pleasant passage to Europe on the same ocean that, several thousand miles away off the Horn of Africa, is infested with pirates. With cyberspace, however, there can be many in existence at any one time—some contested, some not. For the most part, nothing is final in cyberspace.[5] With airpower, enemy aircraft can be destroyed, and there the matter ends. In cyberspace, a jihadist website can be purposefully shut down, only for the same jihadists to start a new website within hours on a different server using a different domain name. Similarly, networks can be quickly repaired and reconstituted, thanks to the relatively inexpensive and readily available hardware.[6]

The cost of entry into cyberspace is relatively cheap. The resources and expertise required to enter, exist in, and exploit cyberspace are modest compared to the resources and expertise required for exploiting the land, sea, air, and space. Generating strategic effect in cyberspace does not require a budget of billions, manpower in the thousands, tracts of land, or divisions/fleets/wings/constellations of hardware that cost yet more billions of dollars. Rather, modest financial outlays, a small group of motivated individuals, and access to networked computers that are accessible to a large portion of the world's population can provide entry to the cyber domain.[7] Deep computer expertise is always an advantage but not always necessary. Computer science and programming knowledge need be only modest to generate strategic effect in and from cyberspace. As Col Stephen Korns points out, many cyber "weapons" are now commoditized and can be easily purchased "off the shelf" at affordable prices, such as denial-of-service software that can be downloaded onto a personal computer and deployed against its target.[8] The commoditization of cyber capabilities is evidenced by the cyber attacks that took place against Estonia in April/May 2007 and against Georgia in August 2008, when individuals—the vast majority of whom were not experts in programming or computer science—downloaded readily available software to mount the denial-of-service attacks.[9] This is not to imply that deep cyber expertise cannot bring about an advantage or that the investment of billions of dollars into a cyber effort will not have a significant strategic return—far from it. Rather, the character of cyberspace is such that the number of actors able to operate in the domain and potentially generate strategic effect is exponential when compared to the land, sea, air, and space domains.

For the time being, the offense rather than the defense is dominant in cyberspace. This is due to a number of reasons. First, network defenses rely on vulnerable protocols and open architectures, and the prevailing network defense philosophy emphasizes threat detection, not fixing vulnerabilities.[10] Second, attacks in cyberspace occur at great speed—for all intents and purposes to a human observer they seem instantaneous—putting defenses under immense pressure, as an attacker has to be successful only once, whereas the defender has to be successful all of the time. Third, and related to the previous reason, range is not an issue in cyberspace as it is in the other domains. Attacks can emerge from literally anywhere in the world.[11] Fourth, attributing attacks is for the most part problematic, thus complicating any possible response.[12] Fifth, and lastly, the overwhelming reliance on cyberspace throughout modern society, not just in the military, presents any attacker with a target-rich environment, again placing great strain on the ability to successfully defend the domain.[13]

Cyberspace consists of four layers, and control of one layer does not mean control of the others. Cyberspace consists of infrastructure, physical, syntactic, and semantic layers. The infrastructure layer consists of the hardware, cabling, satellites, facilities, and so on. The physical layer consists of the myriad properties of the EMS—electrons, photons, frequencies, and so forth—that animate the infrastructure layer.[14] The syntactic layer consists of the formatting of information and the rules that instruct and control information systems that make up cyberspace. The semantic layer consists of information useful and comprehensible to human users and is essentially the cyber-cognitive nexus. Controlling the infrastructure layer of cyberspace does not necessarily translate into control of the physical, syntactic, and semantic layers. Similarly, semantic control does not require infrastructure control, as evidenced by the prevalence of cyber crime today that effectively exploits the semantic layer. While this proposition is generally true, there are exceptions that depend upon what one is trying to do. If one is trying to destroy and disable a network, then attacking the infrastructure layer alone may well be effective. If, on the other hand, one is trying to spoof an enemy commander into making certain decisions, then control of the infrastructure layer is largely irrelevant, but control of the semantic layer is everything.[15]

Cyberpower is ubiquitous. Land, sea, air, and space power are able to generate strategic effect on each of the other domains, but nothing generates strategic effect in all domains so absolutely and simultaneously as cyberpower.[16] Given the cyber dependencies of the military, economy, and society in a growing number of countries, and given that cyberspace critically enables land, sea, air, and space power—as well as other instruments of power, such as diplomacy, media, and commerce—cyberpower is ubiquitous. Land, sea, air, and space power can return to barracks, ports, airfields, or, in the case of satellites, be tasked on to another target. Cyberpower does not go back to its sender, nor is it expended.

Cyberpower is complementary. Unlike land, sea, and airpower, but in many ways like space power, cyberpower is largely a complementary instrument, especially when used autonomously. It is indirect because the coercive ability of cyberpower is limited and likely to remain so. For example, consider the cyber attack against Estonia in spring 2007. It is often forgotten that the attacks occurred along with violent protests in Estonia and a political warfare campaign allegedly perpetrated by the Russian government against Estonian interests. None of these—the protests, political warfare campaign, Russian threats and diplomatic protests, or the cyber attacks—swayed the Estonian government. This is even more remarkable given that Estonia is widely regarded as one of the most cyber-dependent countries in the world. It can certainly be argued that the cyber attacks were damaging, disruptive, and a nuisance, but they were not coercive.[17] It is even more evident that the cyber attacks during the short conflict between Russia and Georgia in August 2008 were likewise not coercive. Georgia, especially at the time, was not a particularly cyber-dependent country, and the Russian military campaign was relatively swift and decisive in achieving its objectives against the Georgians. The associated cyber attacks—which have never been publicly attributed to the Russian government but seemed to have been impeccably timed to peak just as Russian forces crossed into South Ossetia and Abkhazia—certainly caused major disruption to Georgian Internet services and several means of communication, but it is implausible to suggest that the Russian military campaign would have been in any way less decisive had the cyber attacks not taken place or had failed.[18]

The assertion that cyberpower is a complementary instrument rests, of course, on the little-observed use of meaningful cyberpower over the past few years. The nightmare scenarios of cyberpower used to switch off power grids, disrupt air traffic control, or bring down Wall Street with a few keystrokes, so beloved by Hollywood, have thankfully yet to occur. This may well change at some point in the future, and in that case the assertion should be thoroughly revised. But for this to happen, coercion must be proven. Shutting down a power grid via cyberpower, for example, would undoubtedly have catastrophic consequences, but rather than coercing its victim to concede to an attacker's demands, it may in fact only invite an even more catastrophic response. Similarly, for all the press about the damage caused by the Stuxnet worm in recent months,[19] it has plainly not coerced Iranian leaders to abandon their nuclear program.[20] Until such time that cyberpower might prove its coercive ability, it can be said, at best, that it is a complementary instrument.

Cyberpower can be stealthy. One of cyberpower's attractions for many users is the ability to wield it surreptitiously on a global scale without it being attributed to the perpetrator. Malicious software can be planted in enemy networks without knowledge until the cyber weapon is activated and causes its intended damage. Databases can be raided for classified or proprietary information, and the owners of that information may not be any the wiser as terabits of data are stolen. Similarly, private citizens can go about their innocent lives only to discover that cyber criminals have ruined their credit rating and maxed out their credit cards because of stolen identity. This ability to stealthily use cyberpower, aided by the inherent difficulties of attributing the identity and motivation of most attackers, makes it a very attractive instrument for governments and other actors.[21]

Other theorists might feasibly identify more attributes of cyberpower than described here, but the preceding discussion has identified the most prominent characteristics pertinent to the wider ensuing discussion. Before addressing the strategic purpose of cyberpower, however, it is necessary to briefly describe the strategic context in which it is emerging as an instrument of power and its relationship to the enduring nature of strategy.

The Strategic Context of Cyberpower

Along with land, sea, air, and space power is a strategic tool that can be used either alone or in combination with other instruments of military and national power. Cyberpower can be used in peace and war because, among its many other attributes, it is stealthy and covert, relatively cheap, and its use both favors the offense and is difficult to attribute to the perpetrator. Of course, these very same attributes render our own networks vulnerable to cyber attack by others. But, with a more robust cyber-security culture and a more realistic understanding of the limits of cyberpower, we should consider that its value as an instrument to manipulate the strategic environment to one's advantage outweighs the risks.

Cyberspace is but the latest collection of technologies in the history of information processing. The printing press, telegraph, telephone, and wireless communication technologies such as radio and television have each revolutionized society, and in turn military affairs, in their own ways.[22] Cyberspace, however, is different from its technological predecessors because it is not just a means of communication but also the predominant form of creating, storing, modifying, and exploiting information.[23] The technological predecessors of cyberspace—with the possible exception of the book—have always been means of exchanging (transmitting and receiving) information; the creation, storage, modification, and exploitation of that information did not occur within those technologies.

Today, information and communication technologies permeate every function and level of the US military, including the Air Force.[24] An ICT can be anything from a personal computer or cell phone to supervisory control and data acquisition (SCADA) devices that monitor the functioning of utilities, infrastructure, facilities, and other complex hardware.[25] Their use is extensive, pervasive, and growing throughout the US military and beyond. Furthermore, most military hardware is now digitized, making most platforms reliant on ICTs for both their internal functioning and for their coordinated use in both peace and war. When ICTs communicate, or network, with each other it can be said that cyberspace exists.[26] Reliance on ICTs is both spreading and deepening, and not just in the military. Throughout the US economy and society, ICTs play a critical role in the everyday functioning of the country, and the same is also true not only of other industrialized developed countries but emerging and developing countries as well.[27]

This expanding, deepening, and increasingly pervasive reliance on cyberspace is part of the mosaic of the shifting geopolitical and economic global environment that provides the strategic context for the use of cyberpower. Admittedly, this strategic context is challenging for policymakers, commanders, and scholars to comprehend, as fundamental power shifts are still underway and geopolitical alignments are in flux. Safe to say, however, that the United States and its allies, while still the most important fulcrum of power in the international system, are not necessarily the sole focus of international affairs. As Philip Stephens of the *Financial Times* recently pointed out,

> A multipolar world has been long predicted, but has always seemed to be perched safely on the horizon. Now it has rushed quite suddenly into the present . . . The lazy way to describe the new geopolitical landscape is one of a contest between the west and the rest—between western liberal democracies and eastern market economy autocracies. Neat as such divisions may seem, they miss the complexities. None are more determined, for example, than Russia and China to keep India from securing a permanent seat on the UN Security Council. Few are more worried than India by China's military buildup . . . The rising nations prize state power over international rules, sovereignty over multilateralism. The transition to a new order is likely to see more rivalry and competition than co-operation. The facts of interdependence cannot be wished away but they will certainly be tested. It is going to be a bumpy ride.[28]

Compounding these rapid, and at times dramatic, changes is the fact that cyberpower as a strategic tool has diffused widely among all actors—state and nonstate alike. The United States may continue to hold the preponderance of land, sea, air, and space power, and may well do so with cyberpower, but other actors in the strategic environment are also cyber empowered and are often wielding their cyberpower to some effect.[29] With the strategic context summarized, now consider the relationship between strategy and cyberpower.

Strategy and Cyberpower

Cyberpower is technically, tactically, and even operationally distinct from the other instruments of military power, but it is not beyond strategy; nor does it subvert the enduring nature of war that is unchanging throughout history. Yet while the nature of war is unchanging, its character changes all the time along with changes in society, political actors, technology, geopolitics, and the emergence of new exploitable domains such as the sea, air, space, and more recently, cyberspace.[30] A general understanding of strategy, and in particular, an understanding of the strategic meaning of cyberpower, can help senior commanders and policymakers comprehend what is enduring, what is new and unique, and what is important and unimportant in cyberpower.

Cyberpower is subservient to the needs of policy, and strategy is the process of translating those needs into action. Cyber operations take place in cyberspace and generate cyberpower, but they do not serve their own ends; they serve the ends of policy. Strategy is the bridge between policy and the exploitation of the cyber instrument. The notion that cyber operations (along with land, sea, air, and space operations) must serve their own imperatives is a thoroughly astrategic one. For example, the capability may exist through cyber means to shut down the power grids in foreign nations, disable their networks, or read every digital message they transmit and receive, but the needs of policy will often demand that the power be kept on, the networks remain unmolested, and intelligence garnered from passively monitoring enemy e-mail activity not be used. Such restraint may stem from a variety of reasons, ranging from the very limited and nuanced objectives of policy, to restraint based on proportionality, to fear of unknown consequences from certain cyber actions. Additionally, one may not wish to tip one's hand by demonstrating a capability for a short-term goal that may only be used a couple of times at best before the enemy can devise a plausible defense. Ultimately, cyberpower may be able to deliver the required strategic effect, but leaders may want to rely on other forms of military power, or even other instruments of national power, in any given instance.

It is vital that commanders and senior officials develop a greater understanding not only of the strategic purpose of cyberpower but also its relationship to strategy. Education, experimentation, and experience will be essential in comprehending the relationship and in identifying the strategic purpose of cyberpower.

Manipulating the Strategic Environment through Cyberpower

The characteristics and attributes of cyberpower previously discussed are just some that can be ascribed to it but do not ultimately explain to the strategist what makes it a unique instrument. The key strategic attribute of cyberpower is *the ability in peace and war to manipulate the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment*. This strategic utility extends to all the other strategic domains (or, if one prefers, media), given their ubiquitous dependence upon cyberspace. Indeed, the strategic environment is now something that is comprehended and refracted increasingly through cyber technologies, and as a result, the strategic potential of cyberpower will increase accordingly. Its ability, therefore, to manipulate an adversary's perception of the strategic environment to one's advantage is a real, if not growing, prospect. Such manipulation produces the strategic effect of misdirection and deception that in turn allows other military and national instruments of power to achieve policy objectives directly. Ultimately, this means that successful applications of cyberpower will be those used in support of, and in conjunction with, other military and national instruments of power to allow these instruments greater leverage and prospects of success.

The currency of cyberpower is information that can be disseminated via a variety of means across, in, and to all the other media. The aim of the cyber strategist is to maximize to the greatest extent possible the various tools (or cyber "weapons") that can, among other things, disrupt and sabotage adversary cyber-dependent activities; deny adversary cyber-dependent communications; steal information that is valuable to the adversary; monitor and spy on adversary activities through cyberspace; and deceive cyber-dependent adversaries into making decisions (or *not* making decisions) that are favorable to the perpetrator through the manipulation of adversary information by cyber means. Ultimately, these and a variety of other actions through cyberpower—used autonomously and in conjunction with other instruments of power—provide the strategic potential to complicate adversary decision making, buy time to allow other instruments of national power a greater chance of success by disrupting or deceiving adversary information, and ultimately subvert, deny, steal, and even destroy information vital to the functioning of a group, society, or economy as part of a wider strategy of punishment or coercion in conjunction with other forms of military power.

Employed autonomously, cyberpower is unlikely to emerge as an independent coercive instrument. Yet its capabilities do provide real strategic value, as events of the past several years have demonstrated. The Stuxnet computer worm has disrupted and, as a result, delayed the Iranian nuclear program by sabotaging the computer operating system used to power its centrifuges.[31] The denial-of-service operation against Georgian cyberspace during the Russian invasion of August 2008 contributed greatly to the inability of Georgian elites to communicate with each other and the outside world during the military campaign, thus retarding their ability to react to events in a timely manner.[32]

China is using cyberspace to conduct extensive espionage operations against political, governmental, industrial, and military targets throughout the West to gain access to critical Western technologies and glean the strategic and economic intentions of its rivals.[33] One US official claims that Chinese intelligence services have essentially stolen enough classified and proprietary information to fill the Library of Congress.[34] Finally, millions of people—to include members of Congress, the government, and the military—are potential victims of various "phishing" scams that attempt to illicitly obtain sensitive user ID and password information to access proprietary databases and spoof messages from individuals in positions of authority and command to sow confusion, create deception, and dissolve trust within networks.[35] All of these activities are of serious consequence but, in and of themselves, are not coercive. The reason is relatively simple: no matter how effective the autonomous use of cyberpower may be, one cannot underestimate the resilience of adversaries nor forget that they will almost always have recourse to the use of physical violence to resist and strike back.[36]

Indeed, the ubiquitous nature of cyberspace—thanks in turn to the ubiquity of ICTs—has critical implications for military command, defined by Martin van Creveld as "a function that has to be exercised, more or less continuously, if the army is to exist and to operate."[37] Because cyberspace shrinks organizational scope and can reach up, down, and across echelons and stovepipes, it offers military commanders the potential for greater control. Yet, as van Creveld effectively points out, to use a communications technology solely for control of every tactical and operational activity is to abrogate effective command and stifle, if not strangle, tactical and operational performance.[38] Present-day cyber-enabled commanders would do well to emulate Helmuth von Moltke and his judicious use of the telegraph during the late nineteenth century rather than Field Marshal Haig's "telephonitis" during the catastrophic Battle of the Somme in the First World War.[39] The ubiquity of cyberspace may well tempt many commanders to interfere at the lowest echelon and reach forward into tactical fights, yet the imperatives for effective command in the information age are the same as they were in the days of the Roman Empire. These imperatives consist of the ability of the commander to grasp the strategic context of the time; bring internal and external coherence to the force under command; create a design for how the force is to be used; have the moral and intellectual courage to take action; possess nerve in the face of extreme pressure and uncertainty; create a persona to inspire those under command to not only obey orders in the face of mortal danger but to also follow the commander who inspires them; possess a great intellect that is creative, bold, and curious; possess expertise in the practice of arms, without which there is no credibility; and finally, identify those rare individuals who not only possess the capacity to carry out such imperatives but also epitomize them.[40]

Cyberpower in the hands of a commander who is able to exercise all the imperatives of command will be a very powerful tool. As van Creveld convincingly demonstrates, those commanders who shaped their command structure according to the mission to be accomplished, rather than the technology at their disposal, won. Those commanders who became slaves to the technology at their disposal—be it the telegraph, telephone, or wireless radio—have tended to exert control at the lowest echelons, thus strangling initiative and adaptability. Rather than leading their forces, they were cocooned by their favored means of communication.[41] Thus, in the wrong hands cyberpower will likely amplify the pathologies of poor senior commanders, stifle the ability of junior officers and senior noncommissioned officers to lead and adapt, and render the entire structure of command reliant on the durability and survivability of what is, in essence, a collection of fragile and vulnerable communication links.

Profound implications arise out of these assertions. First, future wars against cyber-savvy adversaries will have to be fought using command systems that anticipate having to fight in a degraded, if not denied, cyber environment. In other words, these systems must be structured in such a way that they can survive when information is not only unreliable but also scarce. Second, senior commanders will have to delegate tactical and even operational authority to subordinate commanders and guide them through the use of mission orders that specify the minimum that must be achieved. And third, for a force to succeed in an information-deprived environment, a greater onus on unit cohesion, training, and (especially for commanders) education in the strategic arts becomes imperative.

Cyberspace, as already mentioned, is fragile and vulnerable to myriad methods of attack and disruption ranging from jamming of the EMS to the hacking of software, insertion of malware into operating systems, or denial-of-service attacks. This vulnerability, when taken together with the ubiquity of cyberspace and the reliance built upon it, means that cyberpower is an offensive instrument that is ideal for manipulating the strategic environment to one's advantage and ultimately disrupting and even denying the ability of an adversary deprived of individuals steeped in the imperatives of command to effectively command its instruments of national power. In future wars in which cyberpower will feature most prominently, victory will favor the side able to effectively command forces deprived of information while at the same time using it to deceive, deny, demoralize, and disrupt enemies to the extent that their ability to comprehend the strategic environment is sufficiently deprived. Threats to cyberspace are myriad, and as earlier described in the strategic context of cyberpower, there are many sources of this threat. Even with better cyber defenses, especially in the United States, the effective use of cyberpower will see networks disrupted and unreliable for effective communications and use. That said, however, sufficient resilience measures should be instituted as quickly as possible to help facilitate offensive cyber operations.[42]

Strategically this means policy makers and commanders who are today used to making decisions and commanding in an information-saturated environment will have to become accustomed to carrying out their function in the face of information scarcity and, thus, uncertainty. Perhaps the most profound implication of all is future leaders will find that enduring traits of command and strategic acumen will be just as, if not more, important as ever before. Cyberpower not only adds a new layer of fog to war but also to peace, and this will apply to all who utilize it. Continuing advantage will likely turn on both the ability of leaders and commanders to think and act strategically *and* having the most resilient cyberspace networks that while degraded may provide the information edge. As David J. Lonsdale states, "A little information power can go a long way,"[43] but only if leaders and commanders have the strategic acumen to properly manipulate it to their advantage. Uncertainty, not certainty, will be the default condition in a world of cyberpower. To help future leaders and commanders cope, work must begin, albeit incrementally, on building a theory of cyberpower.

Toward a Theory of Cyberpower

It would be wrong to suggest that no attempt has been made to craft a theory of cyberpower to date. Greg Rattray has done the field a great service with his excellent book, *Strategic Warfare in Cyberspace*, and Stuart

H. Starr attempted to lay a framework for a theory of cyberpower in a chapter he contributed to the eminently useful collection of essays, *Cyberpower and National Security*.[44] Both works have contributed much to building a theory of cyberpower, yet both also have drawbacks. Rattray's work is arguably the superior of the two and has many strategic "nuggets" to offer the careful reader, however, it also tends to overemphasize the technological and organizational dimensions at the expense of other pertinent dimensions and relies exclusively on the analogy of strategic airpower.[45] Starr, on the other hand, usefully employs Harold Winton's taxonomy of what a theory should look like but then immediately delves into the tactical and technical weeds and fails to relate cyberpower to its political and strategic context.[46]

Under the rubric of the eternal logic of strategy should be a theory of cyberpower that can aid the commander and cyber operator to maximize its usefulness as an instrument of policy. Land, sea, air, and space power all have a canon of military theory that includes Jomini and von Moltke for land power, Mahan and Corbett for sea power, Douhet and Mitchell for airpower, and Dolman and Klein for space power.[47] To this day these works are taught in the respective staff and war colleges of all the services around the world. Likewise, a theory of cyberpower is deemed useful because "it is based on the proposition that before one can intelligently develop and employ [cyberpower], one should understand its essence."[48] Similarly, ADM J. C. Wylie, USN, one of the finest strategic thinkers of the twentieth century, noted,

> Theory serves a useful purpose to the extent that it can collect and organize the experiences and ideas of other men, sort out which of them may have a valid transfer value to a new and different situation, and help the practitioner to enlarge his vision in an orderly, manageable and useful fashion—and then apply it to the reality with which he is faced.[49]

A theory of cyberpower, then, might just be of some practical use. But what is such a theory supposed to do? What should it, in broad terms, look like? Winton provides five criteria for developing military theory that can be applied to cyberpower and which, at the very least, should be addressed in any attempt.

Define the field. This criterion would delineate what cyberspace and cyberpower are and what they are not. Daniel T. Kuehl recently identified at least 14 definitions of cyberspace, revealing that the study of the strategic application of cyberpower is immature.[50] Reaching some kind of consensus on definitions of cyberspace and cyberpower is ultimately important if a plausible theory is to emerge.

Categorize into constituent parts. The next criterion of a theory is to break the field of study down into its constituent parts. Imagine cyberpower as a citrus fruit, cutting it up into slices, examining each, and then putting them back together to remake the whole. This involves identifying the component parts of what constitutes cyberspace—its infrastructure, physical, syntactic, and semantic layers—and the various tools (or weapons) that can be used to generate effects.

Explain. With cyberpower defined and the workings of its constituent parts understood, the next criterion of a theory is to explain how it does what it does. Ultimately, "theory without explanatory power is like salt without savor—it is worthy only of the dung heap." Here a theory must explain how cyberpower achieves its desired effects in the strategic environment, such as disruption, deception, denial, and so forth. Furthermore, a theory must attempt to identify the circumstances in which cyberpower will be most effective.

Connect to other fields. A theory must then be able to connect cyberpower to the wider universe. In what ways does it interact with the other domains? In what ways is cyberpower mitigated by friction, differences in cultures, economics, and so on? Such a description need not be exhaustive but should at least demonstrate the place of cyberpower within the strategic cosmos.

Anticipate. A good theory should be able to identify those aspects of cyberpower that are likely to be timeless long after society and technology change.[51] Anticipation is not the same as prediction (which is impossible), but is possible by identifying the larger influences of cyberpower that are scalable in the future. It should, of course, be noted that a theory of cyberpower will have its limitations. It will never be able to fully reflect reality and all the random and complex variables that occur. It is impossible for theory to capture such complexity, but it can educate the mind to cope with the complexity and act with purpose despite it.[52] Furthermore, elements such as technologies, actors, and the political context change at alarming and rapid rates, and theory cannot be expected to capture such changes, but a good theory will recognize that change is inevitable. The best a theorist of cyberpower can expect is to get the big things right enough.

Conclusion

The technological and tactical story of cyberpower has been an exciting (if not disquieting) one to date. Yet the strategic story has been slow to develop, partly due to the fact that little effort has gone into identifying exactly what it is that cyberpower strategically provides to its employer. Cyberpower does have a strategic purpose, and it can be understood by exploring its character, strategic context, and relationship to strategy. Ultimately cyberpower translates into the ability to manipulate perceptions of the strategic environment, and this task requires a theory of cyberpower. There is much that is eminently debatable about cyberpower that doubtlessly others will take issue with, but the growing community of cyber thinkers must focus on the strategic implications as a matter of urgency lest they lead the unwitting into catastrophe. SSQ

Notes

1. This article uses Daniel T. Kuehl's definition of *cyberspace*: "A global domain within the information environment *whose distinctive and unique character is framed by the use of electronics and* the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." Daniel T. Kuehl, "Cyberspace and Cyberpower," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, 2009), 28.

2. Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (London: Frank Cass, 2005), 6.

3. See David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 179–200; Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, 30; and Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 5, 29.

4. Albert A. Michelson, "The Relative Motion of the Earth and the Luminiferous Ether," *American Journal of Science* 22, nos. 127–32 (July–December 1881): 120–29. See also Gerald Holton, *Thematic Origins of Scientific Thought: Kepler to Einstein* (Cambridge, MA: Harvard University Press, 1973), 261–352. My thanks to Dr. Stephen Chiabotti of the School of Advanced Air and Space Studies, Maxwell AFB, for relating this useful point to me.

5. Libicki, *Conquest in Cyberspace*, 5–6.

6. Ibid., 84–85.

7. See Col Stephen W. Korns, USAF, "Cyber Operations: The New Balance," *Joint Force Quarterly* 54 (3rd Qtr. 2009): 97–98.

8. Ibid., 99–100.

9. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Ecco, 2010), 11–21.

10. For a critique of the lack of robust cyber defenses in the United States, see ibid. 103–49.

11. Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, 255–56.

12. Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009).

13. On US dependence on cyber, see Clarke, *Cyber War*, 170–75.

14. Libicki refers to the infrastructure layer as the physical layer. I have added the EMS physical layer to Libicki's taxonomy. See his *Conquest in Cyberspace*, 8–10.

15. Ibid.

16. David J. Lonsdale makes a similar point in his *Nature of War in the Information Age*, 184–86.

17. Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy* 27, issue 3 (May 2008): 227–47.

18. See Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008–09): 60–76; US Cyber Consequences Unit, *Overview by the US–CCU of the Cyber Campaign against Georgia in August of 2008* (Norwich, VT: US–CCU, August 2009), http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf; Stéphane Lefebvre and Roger N. McDermott, "Intelligence Aspects of the 2008 Conflict Between Russia and Georgia," *Journal of Slavic Military Studies* 22, no. 1 (January 2009): 4–19; and Timothy L. Thomas, "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia," ibid., 31–67.

19. On Stuxnet, see, among others, Paul K. Kerr, John Rollins, and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (Washington: Congressional Research Service, December 2010); and David Albright, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* (Washington: Institute for Science and International Security, December 2010).

20. See Daniel Dombey, "US fears faster Iran nuclear arms progress," *Financial Times* (London), 29 December 2010.

21. See, among others, Brenner, *Cyberthreats*; and Clarke, *Cyber War*, 197–200.

22. See, for example, Elizabeth C. Hanson, *The Information Revolution and World Politics* (Lanham, MD: Rowman & Littlefield, 2008), 13–45.

23. See Daniel T. Kuehl's definition of cyberspace cited in note 1.

24. On the dissemination of ICTs throughout the military see, among others, John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (2nd Qtr. 1993); 142–44; Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001), 312–14; and the collected essays in David S. Alberts and Daniel S. Papp, eds., *The Information Age: An Anthology on Its Impacts and Consequences*, vol. 1, pt. 1, *The Information and Communication Revolution* (Washington: National Defense University, June 1997).

25. On SCADA, see Robert A. Miller and Irving Lachow, "Strategic Fragility: Infrastructure Protection and National Security in the Information Age," *Defense Horizons* 59, January 2008.

26. Capt David R. Luber, USMC, and Col David H. Wilkinson, USMC, "Defining Cyberspace for Military Operations: A New Battlespace," *Marine Corps Gazette* 93, no. 2 (February 2009): 40–46.

27. On the dissemination of ICTs throughout societies around the world, see Manuel Castells, *Communication Power* (New York: Oxford University Press, 2009), 54–136; Martin Campbell-Kelly and William Aspray, *Computer: History of the Information Machine*, 2nd ed. (Boulder, CO: Westview Press, 2004), 141–279; and Eric G. Swedin and David L. Ferro, *Computers: The Life Story of a Technology* (Baltimore: Johns Hopkins University Press, 2005), 131–49.

28. Philip Stephens, "On the way to a new global balance," *Financial Times* (London), 16 December 2010.

29. See Joseph S. Nye Jr., "The Future of American Power: Dominance and Decline in Perspective," *Foreign Affairs* 89, no. 6 (November/December 2010): 2–12, for a judicious view of America's prospect in a rapidly changing geostrategic context.

30. On the nature and character of war and cyberpower, see Lonsdale, *Nature of War in the Information Age*, 19–48; and Lonsdale, "Clausewitz and Information Warfare," in *Clausewitz in the Twenty-First Century*, eds. Hew Strachan and Andreas Herberg-Rothe (Oxford: Oxford University Press, 2007), 231–50.

31. Daniel Dombey, "US says cyberworm aided effort against Iran," *Financial Times* (London), 10 December 2010.

32. Korns and Kastenberg, "Georgia's Cyber Left Hook," 60.

33. Northrop Grumman, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, prepared for the US–China Economic and Security Review Commission (McLean, VA: Northrop Grumman, October 2009), http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

[34] Clarke, *Cyber War*, 58–59.

[35] On "social engineering" methods, such as "spear-phishing," see Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly, 2010), 146–50.

[36] A point eloquently raised by Lonsdale, *Nature of War in the Information Age*, 166.

[37] Martin van Creveld, *Command in War* (Cambridge: Harvard University Press, 1985), 5.

[38] Ibid., 261–75.

[39] On Von Moltke's style of command, see ibid., 103–47. See also Daniel Hughes, ed., *Moltke on the Art of War: Selected Writings* (Novato, CA: Presidio Press, 1995); Geoffrey Wawro, *The Austro-Prussian War: Austria's War with Prussia and Italy in 1866* (Cambridge, UK: Cambridge University Press, 1996); and Wawro, *The Franco-Prussian War: The German Conquest of France in 1870–1871* (Cambridge: Cambridge University Press, 2003). On Haig's style of command, see Van Creveld, *Command in War*, 155–68. See also Paddy Griffith, *The Great War on the Western Front: A Short History* (Barnsley, UK: Pen & Sword Military, 2008), 43–55; and David Stevenson, *1914–1918: The History of the First World War* (London: Allen Lane, 2004), 168–71.

[40] Lt Col Christopher Smith, Australian Army, *Network Centric Warfare, Command, and the Nature of War*, Study Paper no. 318 (Canberra: Land Warfare Studies Centre, February 2010), 49–56.

[41] Van Creveld, *Command in War*, 261-75.

[42] There are various views, and a lively debate, regarding cyber defense in the United States. See, among others, Clarke, *Cyber War*, 151–78; Edward Skoudis, "Information Security Issues in Cyberspace," and John A. McCarthy, Chris Burrow, Maeve Dion, and Olivia Pacheco, "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts," both in *Cyberpower and National Security*, 171–205 and 543–56, respectively; Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington: CSIS, December 2008); and *Cyberspace Policy Review: Assuring a Trusted and Resilient Informational and Communications Infrastructure* (Washington: The White House, April 2009).

[43] Lonsdale, *Nature of War in the Information Age*, 193.

[44] Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, 43–88.

[45] See Rattray's use of faulty strategic analogies in *Strategic Warfare in Cyberspace*, especially his chapters on "Development of Strategic Airpower, 1919–1945: Challenges, Execution, and Lessons," (pp. 235–308) and "The United States and Strategic Information Warfare, 1991–1999: Confronting the Emergence of another Form of Warfare," (pp. 309–459).

[46] Starr at least provides a starting point, and for that we are in his debt. Starr, "Toward a Preliminary Theory of Cyberpower."

[47] See Baron Antoine Henri de Jomini, *The Art of War* (1838; London: Greenhill Books, 1996); Hughes, *Moltke on the Art of War*; Alfred Thayer Mahan, *The Influence of Sea Power upon History, 1660–1783* (1890; Boston: Little, Brown & Co., 1918); Julian S. Corbett, *Some Principles of Maritime Strategy* (1911; Annapolis, MD: Naval Institute Press, 1988); Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1921; Washington: Office of Air Force History, 1983); William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military* (1925; Port Washington, NY: Kennikat Press, 1971); Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (London: Frank Cass, 2002); and John J. Klein, *Space Warfare: Strategy, Principles and Policy* (Abingdon, UK: Routledge, 2006).

[48] Harold R. Winton, "On the Nature of Military Theory," in *Toward a Theory of Spacepower: Selected Essays*, ed. Charles Lutes et al. (Washington: NDU Press, 2011), 19–35

[49] J. C. Wylie, *Military Strategy: A General Theory of Power Control* (1967; Annapolis, MD: Naval Institute Press, 1989), 31.

[50] Kuehl, "From Cyberspace to Cyberpower," 26–27.

[51] Winton, "On the Nature of Military Theory," 2–5.

[52] See Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 141.