

4-1-2013

## Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling

Colin S. Gray Dr.

Follow this and additional works at: <https://press.armywarcollege.edu/monographs>

---

### Recommended Citation

Gray, Colin S. Dr., "Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling" (2013).  
*Monographs, Books, and Publications*. 529.  
<https://press.armywarcollege.edu/monographs/529>

This Book is brought to you for free and open access by USAWC Press. It has been accepted for inclusion in Monographs, Books, and Publications by an authorized administrator of USAWC Press.



Visit our website for other free publication  
downloads  
<http://www.StrategicStudiesInstitute.army.mil/>

[To rate this publication click here.](#)

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

---

Colin S. Gray

U.S. ARMY WAR COLLEGE  
**SSI**  
STRATEGIC STUDIES INSTITUTE

# STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically-oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

**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**

**April 2013**

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute and U.S. Army War College Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues.

\*\*\*\*\*

This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

\*\*\*\*\*

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

\*\*\*\*\*

All Strategic Studies Institute (SSI) and U.S. Army War College Press (USAWC) publications may be downloaded free of charge from the SSI website. Hard copies of this report may also be obtained free of charge while supplies last by placing an order on the SSI website. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and USAWC Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: *www.StrategicStudiesInstitute.army.mil*.

\*\*\*\*\*

The Strategic Studies Institute and USAWC Press publishes a monthly e-mail newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at *www.StrategicStudiesInstitute.army.mil/newsletter/*.

\*\*\*\*\*

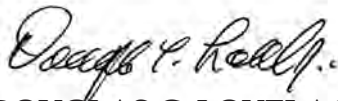
I would like to acknowledge Group Captain Shaun Harvey of the Royal Air Force (RAF) for his educational assistance to me in my preparation of this monograph. However, he is not at all responsible for the use that I have chosen to make of his knowledge and advice.

ISBN 1-58487-564-X

## FOREWORD

Cyber is now recognized as an operational domain, but the theory that should explain it strategically is very largely missing. As the military establishment accepted the revolution in military affairs as the big organizing idea of the 1990s, then moved on to transformation in the early-2000s, so the third really big idea of the post-Cold War Era began to secure traction—cyber. However, it is one thing to know how to digitize; it is quite another to understand what digitization means strategically.

With respect to cyber power, Dr. Colin Gray poses and seeks to answer the most basic of the strategist's questions, "So what?" He notes that the technical and even tactical literature on cyber is as abundant as the strategic theoretical treatment is both thin and poor. However, strategic sense can be made of our limited cyber experience. Gray argues that the general theory of strategy has authority over the cyber domain as the fifth geography of war, even though physical "force" cannot be generated directly by networked computers. Cyber power is not to be compared usefully with nuclear weapons; analyses that suggest or imply catastrophic perils from hostile cyber action are thoroughly unconvincing. Cyber is an important enabler, a team player, in joint operations. As a constructed environment, cyberspace(s) is very much what we choose to make it.



DOUGLAS C. LOVELACE, JR.  
Director  
Strategic Studies Institute and  
U.S. Army War College Press



## ABOUT THE AUTHOR

COLIN S. GRAY is Professor of International Politics and Strategic Studies at the University of Reading, England. He worked at the International Institute for Strategic Studies (London) and at the Hudson Institute (Croton-on-Hudson, NY) before founding the National Institute for Public Policy, a defense-oriented think tank in the Washington, DC, area. Dr. Gray served for 5 years in the Ronald Reagan administration on the President's General Advisory Committee on Arms Control and Disarmament. He has served as an adviser to both the U.S. and British governments (he has dual citizenship). His government work has included studies of nuclear strategy, arms control, maritime strategy, space strategy, and the use of special forces. Dr. Gray has written 25 books, including: *The Sheriff: America's Defense of the New World Order* (University Press of Kentucky, 2004); *Another Bloody Century: Future Warfare* (Weidenfeld and Nicolson, 2005); *Strategy and History: Essays on Theory and Practice* (Routledge, 2006); *Fighting Talk: Forty Maxims on War, Peace and Strategy* (Potomac Books, 2009); *National Security Dilemmas: Challenges and Opportunities* (Potomac Books, 2009); *The Strategy Bridge: Theory for Practice* (Oxford University Press, 2010); *War, Peace and International Relations: An Introduction to Strategic History*, 2nd Ed. (Routledge, 2011); *Airpower for Strategic Effect* (Air University Press, 2012); and *Perspectives on Strategy* (Oxford University Press, 2013), which is the follow-up to *Strategy Bridge*. Dr. Gray is a graduate of the Universities of Manchester and Oxford.





## SUMMARY

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 both 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 the high official interest of 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 the general theory of strategy, also it is enlightening to consider cyber in the contexts of geography and 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 it is simply to locate cyber properly in our relevant universe.

Argument by historical analogy is commonplace and essential—indeed, it is unavoidable—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. Cyberspace does not pose a challenge to the theory of strategy.

But 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 unique 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.”<sup>1</sup>

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 (mis-called “strategic”) cyber attacks are not persuasive. The United States should expect its cyber assets to be harmed in conflict, but, if they are 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, it is probably more significant that the harm we suffer is most unlikely to be close to lethally damaging. Thanks to the technology that makes cyberspaces, 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 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 that 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.

## ENDNOTES

1. Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, eds. and trans., Princeton, NJ: Princeton University Press, 1976, p. 605.



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

Strategic thought on cyberwar, on hostile action in cyberspace, is in its infancy.

Elinor C. Sloan, 2012<sup>1</sup>

No comparable [to Bernard Brodie's edited 1946 book, *The Absolute Weapon: Atomic Power and World Order*] comprehensive assessment of the impact of cyberwarfare capabilities exists. Outside the slowly emerging policy literature there is limited scholarly work on the topic, leaving important theoretical questions unexamined.

Adam P. Liff, 2012<sup>2</sup>

The rules of conduct for the use of code are evolving. As parties develop more sophisticated capabilities and acquire experience in their use, the picture will grow more complicated and nuanced. The strategic situation contains echoes of the period between the two world wars, when rapid developments in new technologies and domains of war-fighting preceded an understanding of how effectively to employ them operationally.

James P. Farwell and  
Rafal Rohozinski, 2012<sup>3</sup>

To ask whether cyberspace is the new high ground is just the latest version of the age-old question: which medium dominates war?

Martin C. Libicki, 2007<sup>4</sup>

### **INTRODUCTION: THE CHALLENGE**

The core question of the strategist is "So what?" Because strategy is all about the consequences of the



threat or use of military (and other, for grand strategy) means for political ends, the strategist must always ask what difference would possible ways and available means make to the course of events. There can be an agreeable ambiguity about "So what?" since the meaning of the spoken words is conveyed only by tone of voice, given the unavoidable absence of a clarifying question or exclamation mark. The "So what?" question is central to this analysis, because this strategist admits to having expressed the words frequently in both their recent meanings when striving to unravel the mysteries of cyber. The purpose here is to seek to provide an answer to the strategist's "So what?" question. What does cyber power mean strategically? What difference will it make to the course of strategic (and other) history?

My mission should be feasible for at least two significant reasons. First, I am able to draw heavily upon the understanding achieved by the scholars who have been grappling with many aspects of the cyber challenge over the past 20 years. Second, much of the novelty of cyber becomes rather less mysterious when it is contextualized historically. Indeed, it is a major challenge for this analysis to contextualize accurately the information technology (IT) revolution of cyber, without inadvertently appearing to understate the quantity and quality of very recent and contemporary change. Nonetheless, it is essential for the understanding of cyber that it should be located in strategic history. We humans have a habit of allowing the latest technological marvels to overwhelm our more critical strategic sense. Enthusiasts for the new technology with military application, direct or indirect, have a long history of perceiving the objects of their favor as the terminating move in a game of strategy that has blighted

the past. The “revolution” of the day is expected to provide the technical means to reduce adversaries to helpless victims, as conflict ceases meaningfully to be a duel.

There has long been a debate over the important issue of whether ideas direct, or at least shape, military practice, or whether military practice provides most of the fuel for ideas. This is not so much an academic controversy over the interpretation of historical evidence, but rather fuel for policy dispute today. The immaturity of strategic theory for cyber typically is accepted as an inevitable and none-too-troubling consequence of its novelty. An understanding of what cyber power means strategically is expected, somewhat complacently, to emerge once the practice of cyber conflict yields evidence of what is and is not possible. I believe that a relaxed attitude toward the strategic meaning of cyber is neither prudent nor necessary. The historical record of the relationship between muscle and brain is more than a little mixed.<sup>5</sup> Certainly, however, it is not the case that very typically, let alone universally, theory was written up to explain what the practical people had found to be good enough practice. Theory and doctrine asserting authoritatively what is believed to be the best practice has led practice as often as vice versa. But, the relationship between military theory and military practice is truly a complex one, with theory and practice comprising essentially a single unified subject. Theory, be it general strategic, or military-specific (i.e., for Landpower, sea power, air power, space power and now also cyber power—at the environment level), is always about strategic and military practice. When theory and doctrine do not adapt in the light of the actual experience of conflict, they are in a pathological condition.

The relationship between theory and practice is important for this study because the evidence of cyber war is entirely absent thus far. Cyber war, needing careful definition, may be “coming,” as John Arquilla and David Ronfeldt claimed in an exciting article in 1993, but it has not come yet.<sup>6</sup> Unfriendly cyber activity there has been and is in abundance, but state-to-state computer network attacks there have not been. Espionage, yes, of course; irritating hacktivism, certainly; but cyber war, no, at least not by a careful definition.<sup>7</sup> The lack of evidence of cyber performance of several kinds in warfare has contributed, one can assume, to the immature condition of the strategic understanding of cyber attested to in the epigraphs to this monograph.

It is my contention that we do know enough now, with sufficient confidence, to make strategic sense of cyber. But, as so often is true of strategic subjects, absent contextualization does gratuitous damage to understanding. Assuredly we do not have available today a book of intellectual merit on cyber power equivalent to Brodie’s edited work, *The Absolute Weapon*.<sup>8</sup> But it so happens that his fairly prescient work is conceptually dominant, far more with the inestimable value of hindsight, than was evident in the late-1940s. There is usually a theorist or two who gets it right early on, even before “it” appears (though not, of course, in the case of the A-bomb). But that fact, verified by historical audit, itself can mean little for contemporary understanding, let alone conduct.<sup>9</sup> The atomic bomb had been “coming” for a while, but its practicability, demonstration, and use in 1945 was such a well-kept secret that there was extant no strategic assessment of its meaning beyond the most obvious and immediate.

Cyber is different in several respects, though there are also some similarities. The scientific story behind

the atomic bomb had a provenance of the better part of a century prior to 1945, that of our contemporary IT revolution centered around the computer and its exploitation, is easily traceable to Alan M. Turing in 1936, with his paper "On Computable Numbers. . ." <sup>10</sup> However, the roots of 21st-century IT can be identified very plausibly in the early-19th century. In that regard, it is probably no exaggeration to argue that the electric telegraph in the 1840s, leading to the wiring of the world, was a more significant technological invention and development than was the computer in the late-20th century. Telegraph wires, the atomic bomb, and the computer all have made a large strategic difference to the conduct of war (and peace). <sup>11</sup> Whether Brodie and his colleagues at Yale were somewhat in the right about the atomic bomb in 1946, serious nuclear debate about the strategic meaning of the technology was not concluded until the mid-1960s. Strategic speculation by scholars pertinent to IT, if not quite to cyber explicitly, dates only from the early-1990s. But even then the conceptual meeting with cyber was measured, if not tardy. The reason may well have been that cyber was somewhat subsumed strategically in public prominence by the seductive attractions of revolutions in military affairs (RMA), transformation and, in the 2000s, by the apparent demands of the "War on Terror."

It appears that the U.S. defense community has difficulty addressing more than one big concept (and believing adjunct elements) at a time. Cyber power undoubtedly was present at the table of U.S. strategic thinking and defense planning from the 1970s until today. Yet, the full-on consideration of cyber had to wait its turn, partly pending its own technical maturity, but also pending official and public exhaus-

tion on other more pressing concerns (e.g., RMA, al-Qaeda, *et al*). Today, the United States seems bored with al-Qaeda and recognizes that Iraq and Afghanistan, though well-intentioned projects, were not successes. At this time, cyber power “catches the wave,” as one might put it, of an American official and public mood that strongly wishes the country to substitute stand-off power, kinetic and electronic, for boots on the local ground across oceans.<sup>12</sup> With drones and electrons, the American public favors a change in the strategic, though possibly not policy, course in its still continuing commitment to police selectively what has to pass for a tolerable world order. Lest I be misunderstood, this monograph is not about U.S. national security policy. The intention here is strictly educational and scholarly, to contribute to the strategic understanding of cyber power – whatever the political purposes to which that power is committed.

It is necessary for me to venture briefly and with caution into highly dangerous terrain, bearing upon the quantity and quality of the strategic literature on cyber, or, more accurately, its relative shortage – relative, that is, to cyber’s potential strategic importance. The literature is also historically scarce, when compared with the community of theorists who addressed, eventually to the point of conceptual exhaustion by the mid-1960s, the last great technology-driven revolution – the nuclear. I suggested above that other subjects seemed more urgent to professional strategists in the 1980s, 1990s, and (most of the) 2000s. However, the current state of the strategic understanding of cyber – of the content of strategic theory for cyber – seems to this strategist to be notably attributable to two plausible facts unmentioned thus far.

First, I suspect that many strategists with only a modest technical background have felt themselves

somewhat disenfranchised from cyber commentary beyond the most obvious. The sheer “technicity” of this subject, and its scientific and technological dynamism over the past 20 years, have discouraged both critical and genuinely strategic assessment of the meaning of it and – dare it be said – may have dazzled unduly those who were intimidated by the real and apparent wonders of cyber. Generational ebb and flow may serve to explain this, but strategic thinkers who are not primarily technical in their expertise have not as a class risen to the strategic challenge of attempting to explain cyber. High-quality strategic theory about cyber simply is not there in the literature during the 1990s and most of the 2000s.<sup>13</sup> The negative comparison with the nuclear debate in the 1950s is almost extraordinary in its scale and quality; or, at least, it would be, were the challenge posed by cyber to be judged seriously analogous to that posed 60 years ago by nuclear weapons. As I argue later in this monograph, there are good reasons for contemporary strategists to be less than wildly excited about the promise and perils of cyber power, but, nonetheless, even that judgment should have been interesting enough to generate a larger publishable debate.

Second, for a reason closely related to the first, the acute shortage over most of the past 20 years of high-quality strategic literature on cyber has not meant that little has been published about networked computers. What has happened, inevitably, is that the rapidly growing cyber library has been filled with technical and tactical assessments. To risk understatement, most of this literature, though no doubt valuable in its own right, has been innocent of, or naïve about, strategic considerations. This claim is not directed as a charge against those who wrote largely technically

and sometimes tactically about cyber power because that is what they knew. Rather it is a charge against those of us strategists who did not rise to the cyber challenge in a timely fashion (*mea culpa!*). As a general comment that bears on the missing strategic scholarly debate about cyber, it may be worth noting that even strategists who are not themselves highly technically proficient are apt to be unhealthily attracted to the apparent promise of high technology.

The plan of attack now moves on from the description of the conceptual challenge, to the explanation of the unity in strategic theory and its relevance to the cyber domain. Next, the analysis considers the strategic historical experience of RMAs, and then proceeds to examine the strategic promise in cyber power. The monograph concludes with recommendations for useful thought and action about cyber power.

## **CONTEXTS: CYBER IN THE FIVE DOMAINS OF WAR**

It is important to be as clear as possible in the use of key organizing concepts, while avoiding academic pedantry in definition and explanation. To that end, thus far I have spared the main body of these introductory pages and argument definitions of the concepts most important to this analysis. However, the analysis cannot proceed further without a brief pause for definition and comment on terms. Three concepts dominate the leading edge of cyber debate as it pertains to the mission here: cyberspace; cyber power; and cyber strategy. I select two definitions of cyberspace and suggest that these should be regarded as mutually compatible, though the first one, by Daniel T. Kuehl, is the more satisfactory:

Cyberspace is 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.<sup>14</sup>

Additionally, one may choose to agree with Andrew F. Krepinevich in understanding that cyberspace comprises all of the world's:

computer networks, both open and closed, to include the computers themselves, the transactional networks that send data regarding financial transactions, and those networks comprising control systems that enable machines to interact with one another.<sup>15</sup>

For cyber power, the admirable Daniel T. Kuehl advises that:

[C]yberpower . . . is the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.<sup>16</sup>

My preferred definition of cyber power is an adaptation of my preferred definition of air power, which I borrowed gratefully from General William "Billy" Mitchell. He was admirably nonspecific, robust, inclusive, and yet clear. Adapted to fit the fifth geographical domain, my definition holds that cyber power is the ability to do something strategically useful in cyberspace.<sup>17</sup> This wording more than compensates in clarity of meaning for what it lacks in literary elegance, and the ambiguity is both deliberate and useful.



The third vital concept that should be written and thought about is strategy for cyber, not cyber strategy. Kuehl employs the latter wording, which inadvertently encourages misunderstanding. Strategy is strategy, whether it is for cyber power, Landpower, sea power, or whatever. To conceive of cyber strategy risks giving the appearance of licensing the view that cyber is the dominant partner over strategy. Strategy for cyber is syntactically useful, because it should reduce the risk that people will believe that the strategy can be intellectually as distinctive as cyberspace is unique.

The concepts of cyber war and cyber warfare mentioned briefly earlier are more heavily laden with political, legal, and moral issues than are cyberspace, cyber power, and strategy for cyber. The dispute about the exact meaning of these three big ideas can fuel much heat as well as light, but it lacks obvious powder trails to dangerous real-world consequences. This is not the case with reference to cyber war and cyber warfare. There can be seriously harmful consequences to defining some cyber activity as warfare and possibly war. All political communities understand themselves to be in different political, legal, and moral terrain when they are in a condition of war and are conducting, certainly are in receipt of, acts of warfare — as contrasted with a condition of nonwar. In other words, whereas cyberspace, cyber power, and strategy for cyber essentially are concepts most fit for technical definition, cyber war and warfare are subjects for judgment and choice.

Much as it is necessary to locate the Cold War in the whole stream of strategic history, notwithstanding the novelty and awesomeness of the nuclear fact, so likewise the Information Age, the IT revolution, or cyber (pick a preferred label) require conceptual and

historical contextualization. Whereas technically focused strategists once wrote as if their strategic world bore little if any relation to the whole course of history prior to July 1945, so it is that in their turn many of our contemporary cybernauts can scarcely imagine strategic and other life before the arrival of the electronic computer. I exaggerate, but not by much. Indeed, in the 1970s, I wrote an article critical of those whose cognitive realm of historical relevance began unarguably only in 1945, and possibly in 1952, with the testing of thermonuclear weapons.<sup>18</sup> The full meaning of a new technology cannot be grasped solely on its own scientific and technical terms, essential though that is. New technologies have life cycles, and they may have story arcs – to borrow from Hollywood – within yet greater life cycles and story arcs that probably have no end point reachable soon by purposeful human endeavor.

Technologies such as nuclear weapons and computers exist in context, and their contexts in turn also have context. When we marry the potent idea of context to the persistent reality of useful analogy, we have at least the beginnings of the historical and conceptual forensic toolkit necessary to make strategic sense of cyber. This is not to deny that context can be an overly demanding conceptual tool, because, as Dr. Antulio Echevarria has insisted correctly, it does not have natural frontiers.<sup>19</sup> There is always context to context, without logical end: it helps explain everything, but in such a way that it can thwart explanation. However, it is necessary to approach cyberspace, cyber power, and strategy for cyber in their historical and other contexts, and, in doing so, it is also necessary to be open to what we might learn by analogy.

On the evidence of their writings, most of the people who write expertly about the dynamic cyber frontier

know little strategic history and have few credentials in strategic theory. As always, there are exceptions, and I do not intend these remarks as criticism of our cybernauts. There is no reason why excellence in technical understanding of the digital revolution should equip a person with strategic sense about the net capabilities of his or her machines. But, it is an enduring reality that politics abhor a vacuum, meaning that the absence of strategic expertise among cyber inventors, developers, and heavy users will not remain a void for long. When those educated in (grand and military) strategy are not on the job, those who are strategically uneducated soon will be; at least they will be on the job as they understand it, very largely in the technical and tactical terms that construct their comfort zone of expertise.

Our journey toward a better strategic understanding of cyber can begin with the recognition of three vital contexts: the theory (meaning the general theory) of strategy, geography (meaning the distinctive geographical domains), and information.

### **Context 1: Strategy's General Theory.**

First and foremost, it is necessary to register the fact that cyber in all its technological, psychological, political, military, and other aspects is under the intellectual authority of strategy's general theory. Given that we seem to have made enough strategic sense of nuclear weapons thus far, though admittedly with caveats and many prayers, cyber power presents little difficulty. With a sole exception that is not likely to be a game changer for human conflict, cyber power should be understood as just another category of weapon (and a weapon should be understood to be anything that

is used for the purpose of causing harm).<sup>20</sup> As such a category, cyber undeniably is far more pervasive and intrusive than are other environmentally classifiable types of weapon, but that granted, in tactical application it is a tool of policy and strategy in common with Landpower, sea power, air power, and space power. Such geographical categories are seriously challenged by the increasingly joint and even integrated character of contemporary military operations, but such porosity does not render irrelevant, nor can it invalidate, the importance of the distinctiveness of the five geographies (domains) of war.

Regardless of its geographical affiliation, all weaponry and strategic endeavor are under the authority of a unified general theory strategy. The attached appendix is my version of that theory, presented in the summary form of "22 Dicta."<sup>21</sup> Of the 22 Dicta, only one appears to be lethally contradicted by cyber. Specifically, Dictum 2 defines military strategy as "the direction and use made of force and the threat of force for the purposes of policy as decided by politics." This Clausewitzian definition may seem incompatible with, or at least very uncomfortable with, a cyber power that can neither kill people directly nor, as a general rule, wreak physical damage. These realities of electronic "warfare" should not be permitted to paralyze strategic sense. Hostile behavior in cyberspace and the potential of cyber action to assist in joint warfare that includes lethal physical contact render cyber a category of weapon, albeit one that distinctively does not, indeed cannot, itself apply force.<sup>22</sup> Cyber warfare is not, however, entirely unprecedented in its potential to do harm to people without applying force directly.

For example, economic warfare in the two World Wars was confined not only to the infliction of harm

kinetically, but also by the manipulation of commodity and other markets in neutral countries, in order to starve belligerent populations and deprive their industries of necessary raw materials. Cyber is an extreme case of nonkinetic agency, but the legal problems (in the laws of war) created by regarding combat electrons effectively as equivalents to agents of force ought to be overwhelmed by strategic sense. Cyber plainly is different from Landpower in the way it can work, but nonetheless it is obviously a weapon. Hostile intent, motivation, rules this judgment, not careful analysis of the nature of the electronic agents aimed to do harm.

With the sole exception just discussed, which poses only superficial difficulty, there is nothing in the general theory of strategy that does not apply vitally to cyber. The obvious fact that cyberspace is geophysically different from the other environments is close to banal. The function of this general theory is to explain the nature and key working of the subject. The general theory's value for us now includes its high merit in allowing us to de-particularize cyber, or, indeed, any other environmentally specific category of (military) power. The general theory provides the essentials of a common language for cognition that rules over any and all kinds of strategic projects, regardless of their specific character and purpose. The theory of strategy says, silently but unmistakably by inclusive meaning, that cyber is just another rather fuzzy category of power. While every technical and tactical detail important to the generation and every intended use of cyberspace requires close attention in detail, recognition of the general theory's sway permits cybernauts to see themselves and their special duties in the appropriate strategic context. Cybernauts are doing

strategy, meaning that they are employing cyber ultimately for the same higher ends of political advantage as our military tools, which make physical contact with the enemy. For morale, as well as for reasons of necessary tactical and technical expertise, it is important for troops to be proud of their “specialness.” But such pride needs to be guided by the strategic sense that the general theory of strategy insists should suffuse all of a community’s belligerent efforts, no matter how one’s own portion of that project is understood tactically and technically. The general theory helps to contextualize cyber crucially and properly, not to demote it.

## **Context 2: Geography.**

It is convenient to regard cyberspace, which should really be cyberspaces, as a fifth geographical domain for war, peace, defense preparation, and strategy. It is somewhat counterintuitive to attempt to think of cyberspace in geographical terms, given its essential placelessness.<sup>23</sup> It is more appropriate to consider cyberspace as comprising any number of networked (and perhaps networkable) spaces that people choose to construct. Although the proposition that cyberspace is simply one of five geographical domains is expedient, there are perils in the geographical claim. I have said here only that approaching cyberspace as a fifth geography for strategic attention is convenient and expedient; I have not asserted that it is either scientifically or social-scientifically right to do so. The preferred characterization of cyberspace remains a cognitive work still in progress.

There is some danger in the expedient categorization of cyberspace as a geographically nameable op-

erational domain. In particular, we are nearly certain to be seduced by the familiarity of geographical identification into making inappropriate analogies from other operational domains with their own unique geographies. The absence of meaningful physicality in cyberspace and cyber power amounts to an uncomfortable intangibility. This ethereality is sufficiently alien, even intellectually, to kinetic thinkers, for them to be motivated to attempt to translate cyber into terms more friendly to their military culture than it is or can be. Familiarity will be identified, whether or not it is present or could be created by digitally expressed human will.

It has long been a feature of strategic history that people respond to new challenges largely on the basis of what they understand strategically about answers to old challenges. To risk anticipating later argument unduly, there is extraordinary peril in theorizing by analogy when the subject of contemporary concern (cyber) has either no, or only distinctly challengeable, history in strictly defined warfare. Moreover, the RMA theory that seeks to explain episodic important changes in the character of warfare is itself none too reliable. When debating the strategic meaning of cyber, it is important for our necessary intellectual humility that we recognize that, in effect, we are working with two “maybes” and trying to construct a positive story on shaky foundations. This is not necessarily to be highly critical of RMA theory or of current judgments about what is or may be evidence of cyber warfare. However, I would like to remind people that bold and attractive explanations of allegedly great strategic historical changes really are only theories. RMA theory, for the case in point, is a family of intellectual constructions by scholars put upon complex processes that usually

can bear more than one dominant narrative of causes and claimed effects.

The discussion above seeks to register as strategically important the claims that: although cyberspace is radically different geophysically from the land, sea, air and Earth-orbital environments, it is still very much a geographical context as the others.<sup>24</sup> There is physical geography to cyberspace, comprising user people, dedicated machinery, and the interactive consequences of cyber in joint and integrated action on extra-cyber geographies. Much as we can find it difficult to allow historical education sufficient, but not overmuch, weight in our strategic learning, so it is not always easy to be both properly respectful of what is unique about cyberspace, but not accord that uniqueness a strategic significance it may not merit. Contextual examination cannot lift the peril of underappreciation or overappreciation of change—technical change in this case—but it should serve to reduce the danger of such.

It may be unduly hazardous to say this, but it is most prudent to regard cyber as just another geographical domain (for politics, conflict, and strategy), but one that is unique. Admittedly, the nonphysicality of cyber is a domainal singularity, but one should hesitate before being overimpressed by the strategic meaning of this geophysical fact of intangibility. We have always thought, theorized, moralized, and legislated about armed force—an historical reality that helps explain the strategic strangeness of the electromagnetic spectrum (EMS) in its cyber manifestations. Obviously, the EMS and its cyberspace(s) that we construct pose an unusual challenge to strategic thought and practice. But the domainal assignment that today finds favor, albeit not unarguably, is right enough, if to



a degree over-simple. Theory, which is to say, explanation, of cyber as a geography of conflict, including warfare, may be rather rough, but it is ready enough to serve the practical purposes of strategic conceptualization for good-enough strategic practice.

### **Context 3: Information.**

Concepts and the words chosen to express them have histories and, as cultural artifacts, they are apt to have unsteady life stories as circumstances and fashions change. Thus far, I have claimed that there is value in contextualizing cyber both intellectually – as yet another subfield over which the general theory of strategy must enjoy authority – and also as but the latest distinctive environmental domain for strategy. The third contextual perspective that can help us understand the EMS and our constructed cyber realm(s) is that of information. Information enjoyed great popularity as an organizing idea in the 1990s, before closer study and much experience of its use and misuse revealed that it was so close to being conceptually boundary-free that it lacked forensic value. This conceptual demotion from the premier league of concepts believed to carry the seeds of strategic decisiveness, or some such elevated aspiration, was well enough deserved, but it came at a cost that was unfortunate for the understanding of cyber that we need.

What is strategically new and very different – at best, unfamiliar – about cyber is now fairly obvious, but what is not so obvious is just what this technical novelty means strategically. There is a nontrivial danger that our contemporary anxiety about, even fear of, cyber power and cyber warfare will promote and consolidate a body of alleged Great Truths that

will be nothing of the kind. One way in which we can help understand what cyber is about, what it means, and what its historical trajectory as a toolkit may be, is to contextualize it functionally. To do so is not to demean or demote cyber, but it is to remind ourselves that we do have more or less accessible the political or strategic history of our species over the past 2 1/2 millennia—and, functionally regarded, cyber has serious provenance, there is a *longue durée* of relevant context. To state the blindingly obvious, cyber is information and the communication of this information for all manner of strategic purposes.<sup>25</sup> It takes scarcely a moment's reflection to recognize the familiarity of these concepts. Assuredly, cyber is technically extraordinary, but so too was the electric telegraph in the 1840s. The telephone, radio, and television were each on the frontier of technological achievement for a short while. In the 1920s and 1930s, notwithstanding its introductory experience in belligerent action from 1914 to 1918, motorization and mechanization was a cumulatively startling strategic reality. It bore a somewhat uncertain, though assuredly awe-inspiring and potentially awful, strategic narrative. Rival theories contended for public attention, official endorsement, and funding in defense planning.<sup>26</sup>

Whatever else cyber power may be, for certain it is information and its communication. Cyber power has to be expressed as, in, and through networks with physical architecture.<sup>27</sup> It is no great challenge to recognize the historical longevity of much of the cyber function. Without for one moment ceasing to be deeply impressed by cyber's novel features—speed and potential ubiquity, for example—it would be helpful to place cyberspace and cyber power in strategic historical perspective. If cyber is quintessentially about the communication of information, leaving aside for now

the particulars that that wording conceals, it ought to be reasonable to argue that cyber is only the latest of mankind's efforts to facilitate the information (and its communication) function. Information in its many human and technical aspects has historical form shaped significantly in its characteristics by enduring factors. It follows that we should be able to learn much from historical experience about the benefits and costs and perhaps, but only perhaps, the course frequently taken by technical change, which can be disconcertingly rapid. However, it is helpful to our understanding to strip away the toolkit of the period, any period, that handles the communication of information, and grasp as firmly as one can that the technical excitement of the moment really relates only to the enabling tools. Cyber power is not about computers and their networks; rather, it is about what networked computers are able to do in passing on information and what the consequences might be.

It should be recalled that the strategist's most vital question is always "So what?" The answer to that question is what the strategist needs to understand about the technically wonderful, if frustratingly somewhat intangible, world of cyber. Cyber will do what strategists want done faster, over longer range, and perhaps far more stealthily, than ever before. But functionally regarded, cyber fits unexceptionally into the course of strategic history. The technology certainly changes, but the general theory of strategy is not interested in that incontestable fact. If cyber is only the latest way to perform familiar tasks, what does that imply for its strategic significance? Also, is it possible that cyber power is or will be so different from other kinds of power that it cannot prudently be regarded and treated simply as a team player in the ever-evolving joint and possibly integrated narrative of warfare?

## **RMA Theory and Cyber.**

It is commonplace to regard modern IT as having sponsored, triggered, and enabled strategic changes worth labeling as revolutionary. Today, it is believed an IT-enabled RMA either has occurred or plainly is occurring in real time. This is not usually understood to be an assumption, but rather is accepted in the category of verified facts.<sup>28</sup> Without necessarily challenging the claim that an IT-led RMA is well under way in strategic affairs, it is appropriate to set strategic thought about cyber in some historical context viewed with a healthy skepticism. The issue of high moment here is not the reality of cyberspace and its dynamic technical improvement, but rather the strategic significance of these electronic and physical actualities. When viewed by a strategist thinking strategically, cyberspace and cyber power invite, indeed, demand, plausible answer(s) to the fundamental question, "So what?"

Cyber thought and directly relevant behavior is easily traceable to the mid-1980s, while its subsequent amble, canter, and then gallop to today has been technically so glittering that its conceptual understanding for strategy has been neglected, or perhaps, more delicately expressed, postponed.<sup>29</sup> Because the technology that enables cyber has been technically so successful, few people with skills in strategic reasoning have felt moved to provide strategic explanation of the obviously burgeoning IT revolution carried by the electronic computer. The situation today is that cyber—networked computers—has advanced technically and tactically at high speed, as has compliant policy and its politics, to the limited degree to which they have been required to provide a site license. But, not for the

first time in modern history, strategy has largely been absent. In other words, networked computers have been blessed politically, and there has been a rush to adopt and exploit them as best as we have been able while the technology has been moving on us rapidly. Missing from the ever-more-highly paced action, which is to say, from the technical adoption and the practical doing, has been a serious endeavor to understand what it all means strategically.

Lest I should be accused of exaggeration, I can cite in my support recent parallel judgments by other analysts. The first two epigraphs above both point explicitly to the contemporary immaturity of strategic thought about cyber, while in his examination of cyber perils for evidence of a nuclear option, Krepinovich contrasts early thought about atomic weapons with the paucity of thought on cyber over the past 15 years.<sup>30</sup> There is no shortage of candidates to blame for the strategic poverty in the cyber literature, but there is possibly an imperial one that has escaped much notice. Because this particular contributor to the suppression of strategic thought has not attracted attention and continues to have influence, it needs to be aired and assayed. The arguable villain is RMA theory, considered in the context of a defense community not overly skilled in strategic thought or practice.

Scientific excitement, technological novelty, and the uncertainty that must attend innovation, business opportunism, and the political and bureaucratic advantages that are apt to reward genuine enthusiasm, formed a heady brew difficult to imbibe prudently. Indeed, there seemed to be a sense almost of surrender to an untamed and, for a while, untamable technical change, following which – to hypothesize rather boldly – a time would come for mature reflection. There

has been a sense in which defense communities, led by the United States thus far, have all but surrendered to science and technology, possibly safe enough in the historically well-founded belief that “one day,” we, or someone, will sort out what all this computer-led change means strategically. Contrary to appearances, this attitude of somewhat strategically uncomprehending acceptance of scientific and technical change often is as realistically necessary as it proves actually to be safe enough.

The consequences of great scientific and technical changes are rarely predictable. Even when hindsight allows us to identify the prophets who were mainly correct, it is unusual for our honor roll to correlate closely with those who were most respected at the time. Railroads, radio, aircraft, television, nuclear weapons, and now electronic computers did not exactly appear fully and strategically comprehended when first they appeared. Moreover, even nuclear weapons experienced a decade and more of consideration, as well as technological change, before a theory adequate to explain them strategically took firm shape. Serious policy and strategy debate about nuclear weapons was not concluded until 1966. This means that those who seek to compare and contrast unfavorably the history of strategic thought on cyber with the early years of nuclear thought can be on shaky ground historically.

Krepinevich may mislead when he offers the following historical comparison:

Yet, despite its enormous potential consequences for the security and well being of the world’s leading economic powers, the issue of catastrophic cyber attacks is only now emerging, even though we are perhaps 15 years or more into the era of cyber weapons and warfare. This stands in striking contrast to the concen-

trated and persistent efforts of many of the world's best strategic thinkers to understand the implications of nuclear weapons in the decades immediately following their introduction in 1945.<sup>31</sup>

The fact is that the world's best strategic thinkers did not engage impressively in a debate over nuclear weapons until the H-bomb arrived after 1952 and the Dwight Eisenhower administration endeavored to make strategic sense of its nuclear inheritance. In an outstanding intellectual history of American thought about nuclear strategy in the early years of the Cold War, Marc Trachtenberg has shown convincingly and unsurprisingly that much was misunderstood by Brodie in 1946, and that the most creative period of American strategic thought—at least in its nuclear dimension—can be dated most convincingly to the period 1955–66. Argument today claiming fairly plausibly that cyber has yet to benefit from profound strategic thought is not much aided by unsound reference to the late-1940s and early-1950s.<sup>32</sup> The debate over nuclear strategy had not been over-impressive when the weaponry was only of a fissionable nature, but it flared into active life with the arrival of fusion weapons. The decade 1955–66 can be called the “golden era” of American strategic thought.<sup>33</sup> By the mid-1960s, the subject of nuclear strategy was intellectually exhausted. If Krepinevich's analogy is taken seriously, today we are in 1960 on the nuclear timeline, and, indeed, cyber is lagging by nuclear comparison. However, it is a mistake to regard the late-1940s and early-1950s as a period of lively and bold strategic theorizing about things nuclear. Among other caveats, we need to be attentive to the huge difference in the strategic context affected by the arrival of the H-bomb.

The need for strategic common sense about cyber is pressing, notwithstanding the difficulties that impede its provision. Politicians and civil servants unwisely are addicted to the concept of a “foreseeable future,” which is, alas, substantially fictitious as it is typically casually employed. However, the future can be foreseen in the sense of anticipated, even though it cannot be predicted in detail. The practical challenge is to understand how best to use what we think we know with high reliability about the future of cyber in its strategic meaning. Strange as it may seem to some, and poverty-stricken though we have to be about the detail of cyber’s future scientific and technical course, we are reasonably well supplied with theory to explain by our variable access to millennia of strategic history.

Strange though it may appear to many of those who are busy technically developing, doing, and making use of cyber, there is to hand (perhaps to brain) useful strategic theory that can aid understanding. The advice in the general theory of strategy cannot educate about technical detail and tactical doing, but assuredly, it contextualizes the technology and tactics of cyber. In so doing, it carries plain implications for the likely character of this latest wave in strategic history.

RMA theory strives to make strategic sense of the past 7 centuries, and in the main, it has shed useful light. But what is an RMA, and how can we distinguish it from antecedent and succeeding phenomena? The most widely used definition was coined by Krepinevich and deployed to lasting effect in an article published in 1994.

What is a military revolution? It is what occurs when the application of new technologies into a significant



number of concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict. It does so by producing a dramatic increase—often an order of magnitude or greater—in the combat potential and military effectiveness of armed forces.<sup>34</sup>

This popular and influential definition appeared sophisticated in its inclusivity (i.e., “concepts and organizational adaptation,” not only “new technologies”), but it was essentially tactical in focus—just possibly operational, but not strategic or political. This tactical perspective on military change was limited in its utility by limitations more than marginally obscured by the fact that it was presented as the ambitious conceptual key to a sweeping explanation of historical change. Of importance for this analysis is not so much the challengeable historical merit of RMA theory, but rather the consequences of that theory for the understanding of cyber. The American defense community that woke up in the later-2000s to its need to make some strategic sense of its relatively unfamiliar cyber assets, and of possible threats by the like assets of others, was a community already robustly on board for a theory of historical change keyed near exclusively to technology. By the early-2000s, American military thinkers had been captured by the RMA argument, had moved on to the transformation thesis, and were ready for the next big idea and its basket of associates, among which was cyber.

How should one think about cyberspace? What was the promise in digital change? The defense community had spent a busy if navigationally rather uncertain decade teasing out any and probably every variant of meaning of the RMA thesis. It had passed on from RMA, and was well into transformation as

the brightest current guiding light, when along came real conflict in Afghanistan, Iraq, and then Afghanistan again. While the U.S. (and some allied) military struggled to understand, and then, hopefully, to do consequentially what seemed necessary to be done in the 2000s, the technical momentum of military revolution was posing a growing challenge to strategic comprehension. What happened was that the pace of technical change in digitization had transcended understanding of what it meant strategically.

The RMA theory outlined by Krepinevich and many other analysts mainly in the early- and mid-1990s, was significantly bereft of strategic content. This fact was not widely appreciated at the time, as a review of the literature makes unambiguously clear (and as this theorist recalls all too plainly). The high-tech dazzle of RMA, and the evident sophistication of the argument recognizing the vital roles of concepts and organizations, when pursued in a near-vacuum of major threat in the 1990s amounted to a strategy-free enterprise. Why was the United States pursuing the latest RMA in the 1990s? What desirable consequences were anticipated? What was the strategic narrative that made sense of the project? This is to criticize neither the RMA enterprise per se, nor its product and models of transformation. But it is to claim that the whole effort was vitally short of strategic guidance. The ends, ways, means—and assumptions—of the 1990s, were critically short on holistic coherence. When exciting means and the ways to employ them are not connected intelligently to prudent political ends (policy), strategy worthy of the name cannot function. So it was for many years when RMA was the technology-led, certainly enabled, vision that came to function for many as an end in itself. Admittedly, this

is an ungenerous judgment fueled more than marginally by hindsight.

Missing from the unofficial, but conceptually dominant, RMA theory of the period, was an adequate understanding of war and strategy. The technology-led theory summarized tersely in the words of Krepinevich quoted earlier should be regarded only as pertaining to the components of strategic effectiveness in crisis and war. What was wrong with the RMA theory of the 1990s was that it confused unilateral combat power with the net effectiveness that produces outcomes in strategic history.<sup>35</sup>

I offer two perilously bold historical judgments in support of the argument just made. First, in none of the greater wars of modern history has technological inferiority, or related conceptual weakness, been a dominant cause of strategic success or failure. Of course, the elements mentioned explicitly by Krepinevich matter seriously—technologies, concepts, and organizations—but they do not constitute a viably full-enough inventory of inputs to the making of strategic performance. It should be obvious from any strategic historical evidence that war and its warfare cannot reliably be tamed conceptually and physically by an explanation of effectiveness that omits everything beyond the equipment, organization, and employment of one belligerent's military assets. Second, it ought to occur to us that there has been a strange contrast between what we believed to be the leading edge of conceptual sophistication in our maturing theory of RMA, then of transformation, and the brutal, humiliating reality of the lack of convincing success in Iraq and Afghanistan. How could it happen that the world's sole true superpower, one educated by deep immersion in the RMA and beyond (but like) theoriz-

ing of more than a decade, could have performed so poorly in the field? After all, strategic theory is invented and developed only for the purpose of advancing the prospects for success in strategic practice.<sup>36</sup> The United States that waged war as it did in the 2000s was a country misinformed by an explanation of historical change carried in notable part by a theory of revolution that was not fit for the purpose. This RMA theory and its descendants are alive and well in recent efforts to make strategic sense of cyber.

The lack of strategic content worthy of the label has been noticed in the cyber literature, but it is what one would expect from the organizations that generated the RMA theory of the 1990s and their defense analysts. The point is not that the theory was wrong in most of its content, but rather that the content could not aspire plausibly to account for the entire reality of politics and war. A defense community seemingly happy enough with an RMA-cum-transformation theory of change in strategic history was never likely to be one sensitive to the lack of strategic explanation about the technically exciting realities of digital networking. The current situation of technological feast and strategic famine over cyber shows a faithful linearity from the RMA thought of the 1990s. Indeed, the linearity can be traced to the 1950s and 1960s, as noted by Brodie in his *War and Politics* in 1973.<sup>37</sup>

Regarded at the human and tactical level, war—and certainly its warfare—is all about the experience of combat; as Clausewitz insisted, war has a pervasive “climate,” consisting of “danger, exertion, uncertainty, and chance.”<sup>38</sup> However, war is not about those four potent elements. Clausewitz is subtle, reasonable, yet unmistakably clear on the role of policy and the politics that generate it. Given the prominence of tech-

nology in our thinking about cyber and its uses, pausing to reflect briefly on the great Prussian's advice is highly valuable. He says:

If we keep in mind that war springs from some political purpose, it is natural that the prime cause of its existence will remain the supreme consideration in conducting it. That, however, does not imply that the political aim is a tyrant. It must adapt itself to its chosen means, a process which can radically change it; yet the political aim remains the first consideration. Policy, then, will permeate all military operations, and in so far as their violent nature will admit, it will have a continuous influence on them.<sup>39</sup>

Our subject ultimately, as it was for Clausewitz, is war, not the waging of war. The military means of war are, of course, vital, and they must be allowed to influence—even “radically change”—the political aim. But whether the military means and the grammar of its use in combat radically shifts political ambition, the conduct of war is about politics. Definitions of strategy are unambiguous on this conceptually dominant organizing nostrum: military strategy is the direction and use made of force and the threat of force for the purposes of policy as decided by politics.

It follows from the logic in the paragraph above that computer-led RMA is not and cannot be about science and technology, anymore than air power is about aeronautics or nuclear weapons are about nuclear physics and engineering. When considered strategically, all three relatively recent RMAs—air power, nuclear weapons, and cyber—are about policy and its politics. This is not to deny that the technical and tactical realities of these three RMAs have been so demanding, even seductive of attention, that their political purpose frequently slips out of mind and sight.

If today's military cybernauts would pause briefly to recognize that their particular realm of technical fascination is but the latest in a long line of innovations that have high strategic relevance, they might appreciate that the general theory of strategy has meaning for them and their networked computers, as it did—indeed, still does—for networked railroads, telephones, and much else. The technical and tactical story of digital IT is important and has to be appreciated on its own technical and tactical terms, as Clausewitz plainly allowed, but that story is not the story for contemporary strategy.<sup>40</sup> It is very important for us not to forget that cyber truly is distinctive as an environmental domain for strategic behavior, in that its features are not geographically constrained as are those that bear on Land-power, sea power, air power, and Earth-orbital space. We construct cyberspace, or more accurately stated, we can construct cyberspaces and reconstruct them very rapidly indeed. Yes, the laws of physics do rule, but those laws do not pose notable limitations on our or our enemies' cyber competence. When approached strategically, cyberspace can be what we and our enemies make it. This can prove a challenging tactical reality for us to grasp as fully as we should.

If it is reasonable to regard our ongoing digital revolution as an RMA, there should be some value in considering our historical experience with other RMAs in the past. The considerable body of theory and arguable but suggestive historical experience with past RMAs from the early-14th century to the 20th (with atomic, then hydrogen bombs heralding the nuclear age) provide some basis for a prudent view of cyber.<sup>41</sup> Historical perspective encourages today's cybernauts to attempt to place the RMAs in the stream of time. It should be reassuring, perhaps usefully humbling,

to realize that in the past, innovators and exploiters of then-exciting new manifestations of science and technology needed to be understood militarily and strategically for the political purposes of their day. One ought not to venture on a journey into speculative thought about cyber unless one is first exposed to the theory and history of railroads, the telegraph, the telephone, aircraft, and nuclear weapons. The reason is not that one needs to know who did what, when, and to whom, or even what it meant at the time and later (in answer to the “So what?” question). Rather, the reason is simply to situate cyber by logical implication in the flow of strategic history. As is so often the case in strategic inquiry, appreciation of context is essential.

Cyber unquestionably is of major importance, but the assumptions that one makes about it before examining it closely can hardly help but shape the assessment. Engineers and tacticians who are making sense of networked computers for current use can hardly help but be over impressed by the technical wonder of the machinery at their disposal. But if we are to understand what is happening with the computer – whither it is likely to proceed, and what this is likely to mean strategically – we need help derived from the historical context of past RMAs and from the conceptual context, which can only be provided by the general theory of strategy.

## STRATEGIC EFFECTIVENESS

### Net Assessment.

War and its warfare are decided by superiority in net strategic effectiveness.<sup>42</sup> Many factors contribute to that effectiveness, and the strategic leverage granted by each factor varies from war to war and even over time and in different geographies in the same war. However, the constituents of strategic effectiveness comprise a constant list, even though their specific values are highly variable. The general theory of strategy tells us what makes strategic effectiveness, and not least among its dicta is the insistence that strategy is pervasively adversarial in nature and in character. When enemies are not plainly identifiable, defense communities need to hypothesize about future perils. We know too little for true comfort about the identity and intensity of future insecurities, but we can be certain that feelings of danger – close or more distant – assuredly lurk in the years to come. Also, we know that our objective and subjective security situation in the future has to be anticipated and then judged by net assessment.<sup>43</sup> The strength of America cannot be the issue, because this has meaning for strategy only when it is understood as a relational variable.

Our cyber literature is generally unsatisfactory in its treatment both of prospective strategic benefit to us and in its limited grasp of the necessary contextualization in war and warfare. Unsound analogy is part of the explanation for these weaknesses. The first step that needs to be taken toward understanding the strategic meaning of cyber is recognition that when it is appreciated strategically, rather than tactically or technically, America's cyber performance is a team



player prospectively opposing other countries' teams. In other words, American cyber would contribute to American strategic performance against enemies who assuredly will be different from America in many respects, but not when weighed in the ever-shifting assay of net strategic effectiveness. No matter how asymmetric belligerents may be, in a vital and objective sense the net merit in their competitive strategic endeavors is graded and registered in a single unique course of events.

One needs always to bear in mind that the international strife of the day and its occasional realization in military action are always about politics. Moreover, political objectives are gained or frustrated in good part by net strategic effectiveness. This argument does not diminish cyber; rather, it reminds the cyber community that it too is on the team and is not the whole national security team itself. Debate about cyber sometimes strays toward the claim that cyber power might be the strategy team.

Because cyberspace is geophysically so extraordinary, there is indeed an important sense in which it is extra-physical, beyond geography. This line of thought has some limited merit, but it is obvious that much of what helps to make cyberspace, let alone those who make it, is distinctly physical. However, even if cyberspace truly were as geophysically extraordinary in its uniqueness as some like to argue and emphasize, *ipso facto* that would not mean that this domain has the potential to be exploited for exceptional strategic effectiveness. One must hasten to point out that the idea that cyber power could be a war-winner, or, at least, the key player on the national security team, is by no means absurd. Indeed, it is prudent for defense analysts today to explore and examine the net strategic

promise in cyber power to see how great its strategic benefits and dangers might be.

While much about cyber is cloaked either in official secrecy or is shrouded in a fog of uncertainty because of the subject's immaturity, nonetheless it is safe enough to say now that cyber peril should not be regarded as a nuclear-like danger or set of dangers. This is not necessarily to claim that we should be relaxed about the inherent risks in our computer-networked existence, but it is to insist that cyber attack is not at all credibly comparable to a nuclear option. This claim is controversial to those of a "Cybergeddon" persuasion, but it would be a useful step forward for strategic net assessment were the more extreme disaster scenarios labeled clearly as the nonsense that they are. Krepinevich is convincing when he argues that:

[D]espite the assertions of some, it also seems likely that cyber weapons have nowhere near the ability to inflict catastrophic destruction as that of a major nuclear attack. . . . Simply put, nuclear weapons remain in a class all their own.<sup>44</sup>

The same judgment is advanced by a technically more expert source on cyber, Martin C. Libicki, who holds that "[n]uclear warfare trumps all other forms."<sup>45</sup> Libicki may be wrong, but he advances and defends this conviction with no little authority. Given our ignorance of future technical feasibility, it has been necessary to examine the full range of possibility on the scale of threats by cyber. But the extra-physicality of the menace, and its substantially discretionary character – dependent as the menace has to be on our technical and tactical choices – means that nuclear menace continues unchallenged as a survival-level danger that could be caused by hostile strategic intent.

In short, on the evidence of careful, if limited, assessment to date, cyber is not akin to nuclear peril, and hypothetical nuclear analogies are more likely to mislead governments and frighten the public needlessly than they are to educate and warn prudently.<sup>46</sup>

### **Analogy, Tactical and Strategic.**

It matters profoundly whether nuclear analogy is appropriate for cyber. It is ironic, and it may even be one of strategic history's few paradoxes, that somehow we have learnt to live with ineradicable nuclear facts. This is reality, despite the continuing awesome uncertainties that surround its likely meaning if expressed in violent military behavior. To some, indeed possibly to many, people who have sought to understand cyber power, its possibilities have appeared strategically unbounded. It can be difficult, if not impossible, to prove a negative. How can we be sure that cyber threats are not of a scale, notwithstanding their definitional nonphysicality, that begs plausibly for comparison with what is now usually regarded in the main as yesterday's menace — nuclear attack?

Several categories of response can be offered to the alleged relevance of nuclear analogy, but suffice it for now to cite but two. First, except for highly unusual cases, cyber power is confined in its damaging effects to cyberspace. This is not to understate the problems that can be caused by cyber attack, but it is to claim firmly that the kind of damage and disruption that cyber might affect cannot compare with the immediate and more lasting harm that nuclear weapons certainly would cause. This is not guesswork. It is simply foolish to argue that understanding of cyber peril can be much advanced by nuclear analogy.

Nonetheless, analogy is critically important in our efforts to grasp what cyber power means strategically. Because strategy must be done tactically, it is not possible to assess cyber strategically without grasping the tactical (and technical) narrative. That plainly being so, the understanding of cyber must be founded upon our best contemporary judgments regarding what is and is not possible in and through cyberspace. Analysts have drafted an analogy to help unravel cyber's nature, character, and meaning. While respectful of their efforts and achievements, I believe that the most helpful way to enlist an analogy for enhanced understanding is to recognize the relevance of the analogy in critically distinguishing between strategic and tactical enquiry. This elementary and commonplace binary distinction is preferable to an elaborate conceptualization that requires historical data to serve an evidential function that is beyond it.

1. Strategic analogy: Cyber is an informational tool of a particular kind, totally dependent on the exploitation of the EMS. But the technical and tactical detail of cyber is of no relevance to the matter of cyber's identity and role(s) as a tool of strategy. Of course, those details are important, but they are important only with respect to the strategic tasks that cyber can and cannot perform. The general theory of strategy explains functionally what its instruments do and why they do it. Each of the five operational domains of national military strategy has a unique technical and tactical story, albeit with considerable overlap among them; the geophysical domains of land, sea, air and Earth-orbital space are each somewhat porous, as elements of other domains have some influence on, through, and because of them. Even the extra-physicality of the electrons of the EMS assembled

and directed as the information collected and moved as cyber cannot be immune to the material context in which and for which those electrons are employed. But the specific technical and tactical details scarcely signify comprehension as agents of strategy, as it is generally understood. The understanding of cyber has to begin with the general theory of strategy, because if it does not, it is very likely that strategically undereducated people will confuse the tactical with the strategic. For example, the theory of cyber in war (i.e., cyber warfare) may well be mistaken for the theory of war as a whole. This happened with air power, came close to happening with sea power, and with some, but only some, good reason, did happen for a while with nuclear weapons. All weapons have to be located conceptually and unambiguously under the common conceptual umbrella provided by the general theory of strategy. This is both logically correct and politically and militarily essential for the purpose of keeping tools properly labeled only as such, no matter how novel and exciting they appear at the time.

2. Tactical analogy: Cyber power is not like other kinds of military power; all of the others have physical reality and can engage physically with the rest. Cyber can be assaulted physically by action against the machines and people that generate it, but cyber attack is utterly different in its essential nonphysicality. When considering cyber action, one needs to put to one side the kinetic and maneuverist ideas that in the main have shaped and then driven our military enculturation, no matter which physical environment is our principal focus. In part because cyber has come to be appreciated and discussed as a weapon, friendly or hostile, it is easy to forget that functionally regarded, it should be located in the long history of informa-

tion and communication. This can be so obvious an enduring fact that it is neglected, and soldiers may be straining against physics as they strive to conceptualize computer networks in terms, and even for some purposes, that are fundamentally alien to what can be done via the EMS. Cyber has to be approached and can be exploited only on its own scientific terms. It is perhaps ironic that the physics of cyberspace on the one hand are rigidly nonpermissive of physical action, while on the other they are thoroughly permissive of discretionary construction effort. Cyberspaces, emphatically plural, are very much what we choose to make them.

This is not so for the other four geographies of warfare. Gravity and the laws of planetary motion codified by Johannes Kepler (1571–1630) are absolute sources of physical constraint on military effort. The physics of seawater cannot be ignored and evaded in ship design and propulsion, while the technical challenges of aeronautics continue to be nontrivial. As for Landpower, terrain, vegetation, climate, and weather, these are all permanent sources of some limitation. The cyberspace we use is that which we have chosen. If that cyberspace is found vulnerable to attack, or unexpectedly prone to technical failure, the fault will be ours. This cannot be said in these terms of the land, sea, air, and Earth-orbital military domains. This important, even crucial argument, has been made convincingly by those who are steeped in the science and technology of cyber, but still, appreciation of it is nowhere near as widespread as it should and needs to be. If we are lethally vulnerable to harm in our use of cyberspace, it will largely, if not wholly, be our own fault.

The contrast with nuclear danger could hardly be more obvious. Because of their nature, nuclear weapons have never (since the early-1950s at least) offered the plausible prospect of use in a war that we could choose to conduct with only acceptable friendly damage being the most likely result. Arguably, air defense and later missile defense have been more possible and strategically useful than the dominant theory and official U.S. position held. But even if optimistic judgment about active defense was substantially correct, though doctrinally unpopular, there is little doubt that national survival was always potentially at risk.<sup>47</sup> The contrast with cyber peril is stark. Such danger certainly is avoidable by our own endeavors for cyber security, while cyber damage has to be accepted as a tolerated cost of superpower duty that we anticipate and with which we intend to cope well enough. Our cyberspace will be disrupted, harassed, and hurt, but that can be said sadly with confidence of our Landpower, sea power, air power, and also space power, to resort to a familiar thought, though with an exclamation mark rather than a question mark, “So what!”

We cannot safely learn about cyber’s meaning through tactical and technical analogy from the other military domains. However, when we plug cyber into a conceptual world view educated by the general theory of strategy that is alert to the course of events over the long term, the technology and the tactics of our EMS exploitation today become much easier to understand. War and strategy for its conduct are to be thought of as a deadly duel. Also, because (unlike nuclear weapons) cyber power is not potentially an instrument of mass destruction—probably not even of long-lasting mass disruption if we choose to be attentive to cyber security—there is no obvious reason why the entirely standard dynamics of competition

will not apply. Yes, cyber power is radically different, but it is not different in ways that must hinder fatally the working of the offense-defense relationship that has been familiar in the other geographies of strategic concern for so long. Although it continues to be orthodox to assert that cyberspace is by its scientific nature an environment friendly to offense, rather than defense, this fashionable belief almost certainly either is wrong, or, to be generous, is seriously misleading. On November 10, 1932, Stanley Baldwin was not correct when he claimed that “the bomber will always get through,” at least it would not get through well prepared defenses in strategically lethal numbers able to attack critical targets.<sup>48</sup> Some bombers certainly would penetrate air defenses, but so what? Britain prepared to be able to accept damage but to fight on. This is the approach that appears most suitable to the challenge of damage from cyberspace. Cyber offense will register some success, but so what?

In the context of all the factors that play in international politics, war, strategy, and warfare, the strategic history of cyber must reflect the course and relative weight of tactical success and failure. As indicated earlier, it is important not to strip cyberspace, cyber power, and the strategy for cyber of the context that is absolutely required to give them meaning. The latest focus of military and strategic interest, which is to say, nuclear weapons in the recent past and the networked computer (cyber) today have an attractive power, an all but gravitational pull, deriving in part from the excitement they promote in a distinctly technically oriented American defense community. The technical experts do not so much reject the politics and strategy that alone are sources of meaning; rather, they largely ignore them.



It is somewhat reassuring to be able to reach the interim conclusion registered in the secondary title to this monograph, "The sky is not falling." Undoubtedly, the Information Age in cyberized form is still young. Indeed, it is so young that one should hesitate before declaiming any firm position on the strategic meaning of cyber. That said, it is useful to record a short list of the more important apparent facts about cyber power that have clear strategic implications. What I have done is select the more significant candidate facts and judgments about cyber power. I must preface this shortlist with the historical comment that every one of the now traditional (including Earth-orbital space) environmental domains has recorded a technical-tactical narrative of offense and defense. There has been a persisting pressing reason for this competitive dynamic. When a geography becomes militarily and usefully exploitable, the logic is inexorable that holds that such exploitation is worth denying to rivals and enemies. Technical accomplishment in the offense-defense nexus fluctuates with the technological achievements of the period, but over the longer term, military (and militarily relevant) machines themselves rarely can be claimed credibly to have been the decisive factor in strategic history.

If some belligerents enjoyed superior mechanical military muscle, there were broader societal and political reasons quite distinct from the technology why that was so. Weapons do not win and lose wars; people and their societies do. Nuclear weapons appear not incredibly to be historically distinctive, even unique, in that their unit destructiveness is so great, albeit variable, that the standard dynamics of offense and defense have yet to produce a true tactical balance. But as best we can tell today, cyber has little in

common with nuclear weaponry. So thoroughly does cyber power depend upon the details of humanly constructed cyberspaces that it is not scientifically accurate to conceive of a single cyberspace as constituting a single great common, akin to the sea, the air, and Earth-orbital space. This is not mere academic pedantry, because the effectively limitless possibilities of constructed cyberspace(s) mean that cyber offense should confront a tactical-technical challenge in which the systemic advantage resides inherently with the defender. It is true that offensive success in cyberspace may be achievable by surprise, but repair and recovery by the defender ought to be fairly routine. Good practice in cyber security includes preparation to suffer some disruption, but then to recover rapidly, not seriously impaired. I do not imply that this is easy or cheap, but on the limited evidence of experience to date, and in the light of the physics of the EMS, this approach appears to be the most prudently realistic.

## **CONCLUSIONS AND RECOMMENDATIONS: THE SKY IS NOT FALLING**

This analysis has sought to explore, identify, and explain the strategic meaning of cyber power. The organizing and thematic question that has shaped and driven the inquiry has been “So what?” Today we all do cyber, but this behavior usually has not been much informed by an understanding that reaches beyond the tactical and technical. I have endeavored to analyze in strategic terms what is on offer from the largely technical and tactical literature on cyber. What can or might be done and how to go about doing it are vitally important bodies of knowledge. But at least as important is understanding what cyber, as a fifth

domain of warfare, brings to national security when it is considered strategically. Military history is stocked abundantly with examples of tactical behavior unguided by any credible semblance of strategy. This inquiry has not been a campaign to reveal what cyber can and might do; a large literature already exists that claims fairly convincingly to explain “how to . . .” But what does cyber power mean, and how does it fit strategically, if it does? These Conclusions and Recommendations offer some understanding of this fifth geography of war in terms that make sense to this strategist, at least.

1. Cyber can only be an enabler of physical effort. Stand-alone (popularly misnamed as “strategic”) cyber action is inherently grossly limited by its immateriality. The physicality of conflict with cyber’s human participants and mechanical artifacts has not been a passing phase in our species’ strategic history. Cyber action, quite independent of action on land, at sea, in the air, and in orbital space, certainly is possible. But the strategic logic of such behavior, keyed to anticipated success in tactical achievement, is not promising. To date, “What if . . .” speculation about strategic cyber attack usually is either contextually too light, or, more often, contextually unpersuasive.<sup>49</sup> However, this is not a great strategic truth, though it is a judgment advanced with considerable confidence. Although societies could, of course, be hurt by cyber action, it is important not to lose touch with the fact, in Libicki’s apposite words, that “[i]n the absence of physical combat, cyber war cannot lead to the occupation of territory. It is almost inconceivable that a sufficiently vigorous cyber war can overthrow the adversary’s government and replace it with a more pliable

one."<sup>50</sup> In the same way that the concepts of sea war, air war, and space war are fundamentally unsound, so also the idea of cyber war is unpersuasive.

It is not impossible, but then, neither is war conducted only at sea, or in the air, or in space. On the one hand, cyber war may seem more probable than like environmentally independent action at sea or in the air. After all, cyber warfare would be very unlikely to harm human beings directly, let alone damage physically the machines on which they depend. These near-facts (cyber attack might cause socially critical machines to behave in a rogue manner with damaging physical consequences) might seem to render cyber a safer zone of belligerent engagement than would physically violent action in other domains. But most likely there would be serious uncertainties pertaining to the consequences of cyber action, which must include the possibility of escalation into other domains of conflict. Despite popular assertions to the contrary, cyber is not likely to prove a precision weapon anytime soon.<sup>51</sup> In addition, assuming that the political and strategic contexts for cyber war were as serious as surely they would need to be to trigger events warranting plausible labeling as cyber war, the distinctly limited harm likely to follow from cyber assault would hardly appeal as prospectively effective coercive moves. On balance, it is most probable that cyber's strategic future in war will be as a contributing enabler of effectiveness of physical efforts in the other four geographies of conflict. Speculation about cyber war, defined strictly as hostile action by networked computers against networked computers, is hugely unconvincing.

2. Cyber defense is difficult, but should be sufficiently effective. The structural advantages of the of-

fense in cyber conflict are as obvious as they are easy to overstate. Penetration and exploitation, or even attack, would need to be by surprise. It can be swift almost beyond the imagination of those enculturated by the traditional demands of physical combat. Cyber attack may be so stealthy that it escapes notice for a long while, or it might wreak digital havoc by complete surprise. And need one emphasize, that at least for a while, hostile cyber action is likely to be hard (though not quite impossible) to attribute with a cyberized equivalent to a "smoking gun." Once one is in the realm of the catastrophic "What if . . .," the world is indeed a frightening place. On a personal note, this defense analyst was for some years exposed to highly speculative briefings that hypothesized how unquestionably cunning plans for nuclear attack could so promptly disable the United States as a functioning state that our nuclear retaliation would likely be still-born. I should hardly need to add that the briefers of these Scary Scenarios were obliged to make a series of Heroic Assumptions.

The literature of cyber scare is more than mildly reminiscent of the nuclear attack stories with which I was assailed in the 1970s and 1980s. As one may observe regarding what Winston Churchill wrote of the disaster that was the Gallipoli campaign of 1915, "[t]he terrible 'Ifs' accumulate."<sup>52</sup> Of course, there are dangers in the cyber domain. Not only are there cyber-competent competitors and enemies abroad; there are also Americans who make mistakes in cyber operation. Furthermore, there are the manufacturers and constructors of the physical artifacts behind (or in, depending upon the preferred definition) cyberspace who assuredly err in this and that detail. The more sophisticated—usually meaning complex—the

code for cyber, the more certain must it be that mistakes both lurk in the program and will be made in digital communication.

What I have just outlined minimally is not a reluctant admission of the fallibility of cyber, but rather a statement of what is obvious and should be anticipated about people and material in a domain of war. All human activities are more or less harassed by friction and carry with them some risk of failure, great or small. A strategist who has read Clausewitz, especially Book One of *On War*,<sup>53</sup> will know this. Alternatively, anyone who skims my summary version of the general theory of strategy will note that Dictum 14 states explicitly that “Strategy is more difficult to devise and execute than are policy, operations, and tactics: friction of all kinds comprise phenomena inseparable from the making and execution of strategies.”<sup>54</sup> Because of its often widely distributed character, the physical infrastructure of an enemy’s cyber power is typically, though not invariably, an impracticable target set for physical assault. Happily, this probable fact should have only annoying consequences. The discretionary nature and therefore the variable possible characters feasible for friendly cyberspace(s), mean that the more dangerous potential vulnerabilities that in theory could be the condition of our cyber-dependency ought to be avoidable at best, or bearable and survivable at worst. Libicki offers forthright advice on this aspect of the subject that deserves to be taken at face value:

[T]here is no inherent reason that improving information *technologies* should lead to a rise in the *amount* of critical information in existence (for example, the names of every secret agent). Really critical information should never see a computer; if it sees a computer, it should not be one that is networked; and if the computer is networked, it should be air-gapped.<sup>55</sup>

Cyber defense admittedly is difficult to do, but so is cyber offense. To quote Libicki yet again, “[i]n this medium [cyberspace] the best defense is not necessarily a good offense; it is usually a good defense.”<sup>56</sup> Unlike the geostrategic context for nuclear-framed competition in U.S.–Soviet/Russian rivalry, the geographical domain of cyberspace definitely is defensible. Even when the enemy is both clever and lucky, it will be our own design and operating fault if he is able to do more than disrupt and irritate us temporarily.

When cyber is contextually regarded properly—which means first, in particular, when it is viewed as but the latest military domain for defense planning—it should be plain to see that cyber performance needs to be good enough rather than perfect.<sup>57</sup> Our Landpower, sea power, air power, and prospectively our space systems also will have to be capable of accepting combat damage and loss, then recovering and carrying on. There is no fundamental reason that less should be demanded of our cyber power. Second, given that cyber is not of a nature or potential character at all likely to parallel nuclear dangers in the menace it could contain, we should anticipate international cyber rivalry to follow the competitive dynamic path already followed in the other domains in the past. Because the digital age is so young, the pace of technical change and tactical invention can be startling. However, the mechanization RMA of the 1920s and 1930s recorded reaction to the new science and technology of the time that is reminiscent of the cyber alarmism that has flourished of recent years.<sup>58</sup> We can be confident that cyber defense should be able to function well enough, given the strength of political, military, and commercial motivation for it to do so. The technical context here is a medium that is a constructed one, which provides

air-gapping options for choice regarding the extent of networking. Naturally, a price is paid in convenience for some closing off of possible cyberspace(s), but all important defense decisions involve choice, so what is novel about that? There is nothing new about accepting some limitations on utility as a price worth paying for security.

3. Intelligence is critically important, but information should not be overvalued. The strategic history of cyber over the past decade confirms what we could know already from the science and technology of this new domain for conflict. Specifically, cyber power is not technically forgiving of user error. Cyber warriors seeking criminal or military benefit require precise information if their intended exploits are to succeed. Lucky guesses should not stumble upon passwords, while efforts to disrupt electronic Supervisory Control and Data Acquisition (SCADA) systems ought to be unable to achieve widespread harmful effects. But obviously there are practical limits to the air-gap option, given that control (and command) systems need to be networks for communication. However, Internet connection needs to be treated as a potential source of serious danger.

It is one thing to be able to be an electronic nuisance, to annoy, disrupt, and perhaps delay. But it is quite another to be capable of inflicting real persisting harm on the fighting power of an enemy. Critically important military computer networks are, of course, accessible neither to the inspired amateur outsider, nor to the malignant political enemy. Easy passing reference to a hypothetical “cyber Pearl Harbor” reflects both poor history and ignorance of contemporary military common sense. Critical potential military (and other)



targets for cyber attack are extremely hard to access and influence (I believe and certainly hope), and the technical knowledge, skills, and effort required to do serious harm to national security is forbiddingly high. This is not to claim, foolishly, that cyber means absolutely could not secure near-catastrophic results. However, it is to say that such a scenario is extremely improbable. Cyber defense is advancing all the time, as is cyber offense, of course. But so discretionary in vital detail can one be in the making of cyberspace, that confidence—real confidence—in cyber attack could not plausibly be high. It should be noted that I am confining this particular discussion to what rather idly tends to be called cyber war. In political and strategic practice, it is unlikely that war would or, more importantly, ever could be restricted to the EMS. Somewhat rhetorically, one should pose the question: Is it likely (almost anything, strictly, is possible) that cyber war with the potential to inflict catastrophic damage would be allowed to stand unsupported in and by action in the other four geographical domains of war? I believe not.

Because we have told ourselves that ours uniquely is the Information Age, we have become unduly respectful of the potency of this rather slippery catch-all term. As usual, it is helpful to contextualize the allegedly magical ingredient, information, by locating it properly in strategic history as just one important element contributing to net strategic effectiveness. This mild caveat is supported usefully by recognizing the general contemporary rule that information per se harms nothing and nobody. The electrons in cyberized conflict have to be interpreted and acted upon by physical forces (including agency by physical human beings). As one might say, intelligence (alone) sinks

no ship; only men and machines can sink ships! That said, there is no doubt that if friendly cyber action can infiltrate and misinform the electronic information on which advisory weaponry and other machines depend, considerable warfighting advantage could be gained. I do not intend to join Clausewitz in his disdain for intelligence, but I will argue that in strategic affairs, intelligence usually is somewhat uncertain.<sup>59</sup> Detailed up-to-date intelligence literally is essential for successful cyber offense, but it can be healthily sobering to appreciate that the strategic rewards of intelligence often are considerably exaggerated. The basic reason is not hard to recognize. Strategic success is a complex endeavor that requires adequate performances by many necessary contributors at every level of conflict (from the political to the tactical).

When thoroughly reliable intelligence on the enemy is in short supply, which usually is the case, the strategist finds ways to compensate as best he or she can. The IT-led RMA of the past 2 decades was fueled in part by the prospect of a quality of military effectiveness that was believed to flow from “dominant battle space knowledge,” to deploy a familiar concept.<sup>60</sup> While there is much to be said in praise of this idea, it is not unreasonable to ask why it has been that our ever-improving battle space knowledge has been compatible with so troubled a course of events in the 2000s in Iraq and Afghanistan. What we might have misunderstood is not the value of knowledge, or of the information from which knowledge is quarried, or even the merit in the IT that passed information and knowledge around. Instead, we may well have failed to grasp and grip understanding of the whole context of war and strategy for which battle space knowledge unquestionably is vital. One must say “vital” rather

than strictly essential, because relatively ignorant armies can and have fought and won despite their ignorance. History requires only that one's net strategic performance is superior to that of the enemy. One is not required to be deeply well informed about the enemy. It is historically quite commonplace for armies to fight in a condition of more-than-marginal reciprocal and strategic cultural ignorance. Intelligence is king in electronic warfare, but such warfare is unlikely to be solely, or even close to solely, sovereign in war and its warfare, considered overall as they should be.

4. Why the sky will not fall. More accurately, one should say that the sky will not fall because of hostile action against us in cyberspace unless we are improbably careless and foolish. David J. Betz and Tim Stevens strike the right note when they conclude that "[i]f cyberspace is not quite the hoped-for Garden of Eden, it is also not quite the pestilential swamp of the imagination of the cyber-alarmists."<sup>61</sup> Our understanding of cyber is high at the technical and tactical level, but remains distinctly rudimentary as one ascends through operations to the more rarified altitudes of strategy and policy. Nonetheless, our scientific, technological, and tactical knowledge and understanding clearly indicates that the sky is not falling and is unlikely to fall in the future as a result of hostile cyber action. This analysis has weighed the more technical and tactical literature on cyber and concludes, not simply on balance, that cyber alarmism has little basis save in the imagination of the alarmists. There is military and civil peril in the hostile use of cyber, which is why we must take cyber security seriously, even to the point of buying redundant capabilities for a range of command and control systems.<sup>62</sup> So seriously should

we regard cyber danger that it is only prudent to assume that we will be the target for hostile cyber action in future conflicts, and that some of that action will promote disruption and uncertainty in the damage it will cause.

That granted, this analysis recommends strongly that the U.S. Army, and indeed the whole of the U.S. Government, should strive to comprehend cyber in context. Approached in isolation as a new technology, it is not unduly hard to be over impressed with its potential both for good and harm. But if we see networked computing as just the latest RMA in an episodic succession of revolutionary changes in the way information is packaged and communicated, the computer-led IT revolution is set where it belongs, in historical context. In modern strategic history, there has been only one truly game-changing basket of technologies, those pertaining to the creation and delivery of nuclear weapons. Everything else has altered the tools with which conflict has been supported and waged, but has not changed the game. The nuclear revolution alone raised still-unanswered questions about the viability of interstate armed conflict. However, it would be accurate to claim that since 1945, methods have been found to pursue fairly traditional political ends in ways that accommodate nonuse of nuclear means, notwithstanding the permanent presence of those means.

The light cast by general strategic theory reveals what requires revealing strategically about networked computers. Once one sheds some of the sheer wonder at the seeming miracle of cyber's ubiquity, instantaneity, and (near) anonymity, one realizes that cyber is just another operational domain, though certainly

one very different from the others in its nonphysicality in direct agency. Having placed cyber where it belongs, as a domain of war, next it is essential to recognize that its nonphysicality compels that cyber should be treated as an enabler of joint action, rather than as an agent of military action capable of behaving independently for useful coercive strategic effect. There are stand-alone possibilities for cyber action, but they are not convincing as attractive options either for or in opposition to a great power, let alone a superpower. No matter how intriguing the scenario design for cyber war strictly or for cyber warfare, the logic of grand and military strategy and a common sense fueled by understanding of the course of strategic history, require one so to contextualize cyber war that its independence is seen as too close to absurd to merit much concern.

Because cyber threats, unlike nuclear threats, should not be able to menace the integrity of the game table on which politics is played internationally, there is good reason to endorse the proposition that the networked computers that generate cyber power are entirely understandable in the terms long made familiar to us in the pages of the classic books on strategy and statecraft written by Thucydides, Clausewitz, and Sun-Tzu. Furthermore, our contemporary troubles in understanding what cyber power may mean strategically are different only in technical and tactical character from the challenges posed by past RMAs. Cyber is different in its character, but not in its nature, when it is approached in strategic context.

## ENDNOTES

1. Elinor C. Sloan, *Modern Military Strategy: An Introduction*, Abingdon, UK: Routledge, 2012, p. 97.

2. Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *The Journal Strategic Studies*, Vol. 35, No. 3, June 2012, p. 402.

3. James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival*, Vol. 54, No. 4, August-September 2012, p. 108.

4. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge, UK: Cambridge University Press, 2007, p. 291.

5. I address this important issue in Chap. 1, *Perspectives on Strategy*, Oxford, UK: Oxford University Press, 2013.

6. John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, Vol. 12, No. 2, Spring 1993, pp. 141-165. This article is reprinted in the important book, John Arquilla and David Ronfeldt, ed., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, CA: RAND, 1997, pp. 23-60.

7. It needs to be understood that definitions are not truths; rather, they are chosen meanings for words. This caveat is particularly relevant to the debate about cyber. Strategic studies continue to be blighted by unduly casual use and misuse of key terms. Cyber war and cyber warfare have attracted misuse of a familiar kind. Cyber warfare can be defined adequately as "[t]he actions by nation-states and non-state actions to penetrate computers or networks for the purpose of inserting, corrupting, or falsifying data; disrupting or damaging a computer or network device; and inflicting damage or disruption to computer control systems." Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option?"* Washington, DC: Center for Strategic and Budgetary Assessments, 2012, p. 82. Confusion arises when cyber warfare is not distinguished from cyber war. The points that tend to be lost because of the confusion are that there is more to war than warfare, and that wars in the future will have a broader canvass

than that provided strictly by cyberspace. A cyber war should refer to a war conducted solely by cyber action between the cyber warriors of belligerents. An air war or a sea war would similarly be environmentally restricted as specified. It is important not to lose the military and other contexts for cyber power. Misuse of the concept of cyber war encourages decontextualized thought, and just possibly, action. For another term deployed in my text: “*Hactivism* is usually understood as the manipulation of digital information to promote a political ideology.” Irving Lachow, “Cyber Terrorism: Menace or Myth?” in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*, Washington, DC: National Defense University Press, 2009, p. 439. An alternative variant of the definition that is marginally clearer is that specifying that “[h]activism (a portmanteau of *hack* and *activism*) is often understood as the writing of code, or otherwise manipulating bits, to promote political ideology.” Stuart H. Starr, “Toward a Preliminary Theory of Cyberpower,” in Kramer, Starr, and Wentz, eds., *Cyberpower and National Security*, p. 570, endnote 33.

8. Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order*, New York: Harcourt, Brace, 1946.

9. See Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd Ed., Basingstoke, UK: Palgrave Macmillan, 2003, Chaps. 1-4.

10. George Dyson, *Turing’s Cathedral: The Origins of the Digital Universe*, London, UK: Allen Lane, 2012, is essential, while James Gleick, *The Information: A History, a Theory, a Flood*, London, UK: Fourth Estate, 2011, Chap. 7, is useful. Gleick is particularly valuable for the historical context that he provides persuasively.

11. See Tom Standage, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century’s Online Pioneers*, London, UK: Weidenfeld and Nicolson, 1998. The strategic value of telegraphic cable is illustrated and explained admirably in Paul M. Kennedy, “Imperial Cable Communications and Strategy, 1870–1914,” in Kennedy, ed., *The War Plans of the Great Powers, 1830–1914*, London, UK: George Allen and Unwin, 1979, pp. 74–98. Martin van Creveld offers helpful commentary on the strategic meaning of the electric telegraph in his *Command in War*, Cambridge, MA: Harvard University Press, 1985, pp. 107–109; and *Technology and War: From 2000 B.C. to the Present*, New York:

The Free Press, 1989, pp. 168-170. In the former book, van Creveld ventures the characteristically exciting claim that the telegraph was “the first real technological advance in the field of communications to take place in millennia” (p. 107).

12. I wish to recognize with gratitude the study by John Ferris, “Catching the Wave: The RAF Pursues a RMA, 1918–39,” in Talbot C. Imlay and Monica Duffy Toft, eds., *The Fog of Peace and War Planning: Military and Strategic Planning under Uncertainty*, Abingdon, UK: Routledge, 2006, pp. 159-178.

13. To seriously misquote the old saying, “Strategic theorists ride, or these days type, to the sound of the guns.” And the electronic guns of cyber power evidently were not sounding loud enough to mobilize responsive, let alone, prudent, anticipatory, theorizing. I have often quoted Raymond Aron on the subject of motivation for strategic thought. Accepting the regrettable fact of repetition, I must quote him yet again, because his judgment is, I believe, of enduring and extraordinary value: “Strategic thought draws its inspiration each century, or rather at each moment of history, from the problems which events themselves pose.” Raymond Aron, “The Evolution of Modern Strategic Thought,” in Alastair Buchan, ed., *Problems of Modern Strategy*, London, UK: Chatto and Windus, 1970, p. 25.

14. Daniel F. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in Kramer, Starr, and Wentz, eds., *Cyberpower and National Security*, p. 28.

15. Krepinevich, *Cyber Warfare*, p. 82.

16. Kuehl, “From Cyberspace to Cyberpower,” p. 38.

17. See Colin S. Gray, *Airpower for Strategic Effect*, Maxwell AFB, AL: Air University Press, February 2012, p. 9. For the Mitchell original, see William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power – Economic and Military*, 1925; New York: Dover Publications, 1988, p. xiii.

18. Colin S. Gray, “Across the Nuclear Divide: Strategic Studies Past and Present,” *International Security*, Vol. 2, No. 1, Summer 1977, pp. 24-46.



19. Antulio J. Echevarria II, "American Strategic Culture: Problems and Prospects," in Hew Strachan and Sibylle Scheipers, eds., *The Changing Character of War*, Oxford, UK: Oxford University Press, 2011, pp. 432-433.

20. The nonkinetic nature of cyber power provides much fuel for controversy over whether or not cyber power should be regarded as a source of weaponry, given its inability to be applied as force. See the recent discussion of this issue in Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal*, Vol. 157, No. 1, February/March 2012, pp. 6-13; and Farwell and Rohozinski, "The New Reality of Cyber War," pp. 107-120.

21. The 22 Dicta of the general theory of strategy are presented tersely in Colin S. Gray, *Perspectives on Strategy*, Oxford, UK: Oxford University Press, 2013 forthcoming, p. 13. A slightly (only 21 Dicta) earlier version is explained in Colin S. Gray, *The Strategy Bridge: Theory for Practice*, Oxford, UK: Oxford University Press, 2010, Chaps. 1-2.

22. The use of cyber as a weapon teamed as a contributor to the effectiveness of joint warfare is a major theme viewed by and large favorably in Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND, 2009, Chap. 7. Libicki terms such use of the cyber weapon "operational cyberwar."

23. I debated Martin C. Libicki on geography, geopolitics, and the arguable placelessness of cyberspace back in 1996. See Colin S. Gray, "The Continued Primacy of Geography," *Orbis*, Vol. 40, No. 2, Spring 1996, pp. 247-259; Martin C. Libicki, "The Emerging Primacy of Information," *Orbis*, Vol. 40, No. 2, Spring 1996, pp. 261-274; and "Rejoinder by Colin S. Gray," pp. 274-276.

24. On the exploitation of the EMS in warfare, see Abdul Karim Baram, *Technology in Warfare: The Electronic Dimension*, Abu Dhabi, United Arab Emirates: The Emirates Center for Strategic Studies and Research, 2008.

25. See Gleick, *The Information*. Also see Gregory J. Rattray, *Strategic Warfare in Cyberspace*, Cambridge, MA: The MIT Press, 2000, which is not without merit. However, Rattray's conceptual

frailty in misusing the adjective “strategic” in “strategic information warfare” is troubling, while from the perspective of today this generally well-regarded book should be read in good part as a period piece of and from the late-1990s.

26. The literature is large, but the following books are especially helpful: Williamson Murray and Allan R. Millett, eds., *Military Innovation in the Interwar Period*, Cambridge, UK: Cambridge University Press, 1996; David E. Johnson, *Fast Tanks and Heavy Bombers: Innovation in the U.S. Army, 1917–1945*, Ithaca, NY: Cornell University Press, 1998; David R. Mets and Harold R. Winton, eds., *The Challenge of Change: Military Institutions and New Realities, 1918–1941*, Lincoln, NE: University of Nebraska Press, 2003; and Joe Maiolo, *Cry Havoc: How the Arms Race Drove the World to War, 1931–1941*, New York: Basic Books, 2010.

27. The fundamental physicality of the architecture that enables the Internet is emphasized effectively in Andrew Blum, *Tubes: A Journey to the Center of the Internet*, New York: HarperCollins, 2012. The International Institute for Strategic Studies (IISS) claims as a:

fact that the global systems of undersea fibre-optic cables through which most Internet traffic passes was configured such that the bulk of the world’s Internet communications physically transited the United States. At the turn of the millennium, this figure was in excess of 80%; and although alternative cabling routes have since been developed, it remains on the order of 60%.

*Strategic Survey 2012: The Annual Review of World Affairs*, Abingdon, UK: Routledge for the IISS, 2012, p. 34.

28. For the theory and considerably argued historical evidence of RMA, see MacGregor Knox and Williamson Murray, eds., *The Dynamics of Military Revolution, 1300–2050*, Cambridge, UK: Cambridge University Press, 2001; Colin S. Gray, *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*, London, UK: Frank Cass, 2002; and Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, Stanford, CA: Stanford University Press, 2010.

29. On some of cyber's "missing" history, see Jason Healey, "Claiming the Lost Cyber Heritage," *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012, pp. 11-19.

30. See Krepinevich, *Cyber Warfare*, pp. 4-5.

31. *Ibid.*, p. 4.

32. Marc Trachtenberg, *History and Strategy*, Princeton, NJ: Princeton University Press, 1991, Chap. 1, "Strategic Thought in America 1952-1966."

33. See Colin S. Gray, *Strategic Studies and Public Policy: The American Experience*, Lexington, KY: The University Press of Kentucky, 1982, Chaps. 3-4. Appreciated today for its width, depth, and context, the most notable strategic analysis from the period was from Bernard Brodie, *Strategy in the Missile Age*, Princeton, NJ: Princeton University Press, 1959.

34. Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest*, Vol. 37, Fall 1994, p. 30.

35. See Gray, Chap. 5, *The Strategy Bridge*; and *Perspectives on Strategy*, Chap. 5.

36. On theory and practice with respect to RMA, see Adamsky, *The Culture of Military Innovation*.

37. Bernard Brodie, *War and Politics*, New York: Macmillan, 1973, Chap. 10.

38. Clausewitz, *On War*, Michael Howard and Peter Paret, eds. and trans., Princeton, NJ: Princeton University Press, 1976, p. 104.

39. *Ibid.*, p. 87.

40. Clausewitz's first paragraph in Chap. 2 of Book Two of *On War*, p. 133, should speak volumes to us as we strive to make strategic sense of networked computers. He distinguishes care-

fully, pointedly, and purposefully between the “preparation of the forces” and their military and strategic employment. “It [the preparation of forces] stood in about the same relationship to combat as the craft of the swordsmith to the art of fencing. It did not yet include the use of force under conditions of danger, subject to constant interaction with an adversary, nor the efforts of spirit and courage to achieve a desired end.”

41. Knox and Murray, eds., *The Dynamics of Military Revolution, 1300–2050*, is the place to start, notwithstanding its overambitious dating.

42. See Gray, Chap. 5., *The Strategy Bridge*

43. Two books of outstanding value are Williamson Murray and Allan R. Millett, eds., *Calculations: Net Assessment and the Coming of World War II*, New York: The Free Press, 1992; and Williamson Murray, *Military Adaptation in War: With Fear of Change*, Cambridge, UK: Cambridge University Press, 2011.

44. Krepinevich, *Cyber Warfare*, p. 79.

45. Libicki, *Cyberdeterrence and Cyberwar*, p. 41.

46. Another recent study from the ranks of those who are strategically, as well as technically, literate also endorsed the “DON’T PANIC” judgment advice of Krepinevich and Libicki. See David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power*, London, UK: International Institute for Strategic Studies, November 2011, espec. p. 127. “DON’T PANIC” is borrowed from the front cover of science fiction author Douglas Adams’s book, *Hitchhikers’ Guide to the Galaxy*, as deployed effectively by Betz and Stevens.

47. See Keith B. Payne, *The Great American Gamble: The Theory and Practice of Deterrence from Cold War to the Twenty-First Century*, Fairfax, VA: National Institute (for Public Policy) Press, 2008.

48. In a debate on disarmament in the House of Commons, Stanley Baldwin, Conservative leader and at that time the Lord President of the Council, claimed that “[n]o power on earth can protect the man in the street from being bombed. Whatever peo-

ple may tell him, the bomber will always get through." Quoted in Uri Bialer, *The Shadow of the Bomber: The Fear of Air Attack and British Politics, 1932-1939*, London, UK: Royal Historical Society, 1980, p. 14. Baldwin was right, but his somewhat accurate prediction encouraged people to draw notably incorrect conclusions out of excessive, though inchoate, fear.

49. I am profoundly suspicious of scenario writing as an aid to planning for national security strategy, but the exercise probably is unavoidable. The problem lies not so much with the scenarios that are designed of future peril, but rather with the influence that they may have on the attitudes and assumptions of American officials to whom they are addressed as heuristic imagination expanders. All national security scenarios conceived to illustrate hypotheses of future dangers need to be accompanied by severely worded caveats about the necessity for a skeptical view. With mixed feelings, I recommend Andrew F. Krepinevich, *7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century*, New York: Bantam Books, 2009, particularly Chap. 5, "China's 'Assassin's Mace'."

50. Libicki, *Cyberdeterrence and Cyberwar*, p. 119.

51. *Ibid.*, p. 177.

52. Winston Churchill deployed the "if" word promiscuously and effectively, albeit largely for self-excusatory purpose, in his history-memoir, *The World Crisis, 1911-1918*, London, UK: Odhams Press, 1938, Vol. I, p. 208; also see Vol. I, pp. 688-689, and Vol. II, pp. 930-931.

53. See Clausewitz, *On War*, pp. 119-121.

54. See Appendix, "The General Theory of Strategy in 22 Dicta."

55. Libicki, *National Security and Information Warfare*, pp. 105-106: "An *air gap* is the lack of an electronic connection between the system and the rest of the world." Libicki, *Cyberdeterrence and Cyberwar*, p. 19, endnote 24.

56. Libicki, *Cyberdeterrence and Cyberwar*, p. 176.

57. I emphasize the high relevance of the “good enough” standard in my article, “Strategic Thoughts for Defence Planners,” *Survival*, Vol. 52, No. 3, June-July 2010, pp. 159-178.

58. Consider Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: HarperCollins Publisher, 2010, in the context of the fear of bombing in the 1930s, analyzed in Bialer, *The Shadow of the Bomber*.

59. See Clausewitz, *On War*, pp. 117-118.

60. See Bill Owens, *Lifting the Fog of War*, New York: Farrar, Straus, and Giroux, 2000, pp. 100-101. Owens’s book was a hubristic period piece. An earlier offering from the same school of thought was Harlan Ullman and James Wade, *Shock and Awe: Achieving Rapid Dominance*, Washington, DC: National Defense University Press, November 1996.

61. Betz and Stevens, *Cyberspace and the State*, p. 129.

62. Amidst the ever-growing library of works on cyber perils and defense, these recent books are particularly helpful: Tarek Saadawi and Louis Jordan, eds., *Cyber Infrastructure Protection*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, May 2011; Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, New York: The Penguin Press, 2011; and Jeffrey Carr, *Inside Cyber Warfare*, 2nd Ed., Sebastopol, CA: O’Reilly Media, 2012.



## APPENDIX

### THE GENERAL THEORY OF STRATEGY IN 22 DICTA\*

#### **Nature and Character of Strategy.**

1. Grand strategy is the direction and use made of any or all of the assets of a security community, including its military instrument, for the purposes of policy as decided by politics.

2. Military strategy is the direction and use made of force and the threat of force for the purposes of policy as decided by politics.

3. Strategy is the only bridge built and held to connect policy purposefully with the military and other instruments of power and influence.

4. Strategy serves politics instrumentally by generating net strategic effect.

5. Strategy is adversarial; it functions in both peace and war, and it always seeks a measure of control over enemies (and often over allies and neutrals, also).

6. Strategy usually requires deception, very frequently is ironic, and occasionally is paradoxical.

7. Strategy is pervasively human.

8. The meaning and character of strategies are driven, though not dictated and wholly determined, by their contexts, all of which are constantly in play and can realistically be understood to constitute just one compounded super-context.

9. Strategy has a permanent nature, while strategies (usually plans, formal or informal, expressing contingent operational intentions) have a variable character, driven but not mandated by their unique and changing contexts, the needs of which are expressed in the decisions of individuals.



## **Making Strategy.**

10. Strategy typically is made by a process of dialogue and negotiation.

11. Strategy is a value charged zone of ideas and behavior.

12. Historically specific strategies often are driven, and always are shaped, by culture and personality, while strategy in general theory is not.

## **Executing Strategy.**

13. The strategy bridge must be held by competent strategists.

14. Strategy is more difficult to devise and execute than are policy, operations, and tactics: friction of all kinds comprise phenomena inseparable from the making and execution of strategies.

15. The structure of the strategy function is best explained as comprising political ends, chosen ways, and enabling means (especially, but not exclusively, military) and the whole endeavor is informed, shaped, and may even be driven, by the reigning assumptions, both those that are recognized and those that are not.

16. Strategy can be expressed in strategies that are: direct or indirect; sequential or cumulative; attritional or maneuverist-annihilating; persisting or raiding (more or less expeditionary); or a complex combination of these nominal alternatives.

17. All strategies are shaped by their particular geographical contexts, but strategy itself is not.

18. Strategy is an unchanging, indeed unchangeable, human activity in thought and behavior, set in a variably dynamic technological context.

19. Unlike strategy, all strategies are temporal.
20. Strategy is logistical.
21. Strategic theory is the fundamental source of military doctrine, while doctrine is a notable enabler of, and guide for, strategies.

### **Consequences of Strategy.**

22. All military behavior is tactical in execution, but must have operational and strategic effect, intended and otherwise.

\*This Appendix is provided with the permission of Oxford University Press. It is published in Colin S. Gray, *Perspectives on Strategy*, Oxford, UK: Oxford University Press, 2013, p. 13.

**U.S. ARMY WAR COLLEGE**

**Major General Anthony A. Cucolo III  
Commandant**

**\*\*\*\*\***

**STRATEGIC STUDIES INSTITUTE  
and  
U.S. ARMY WAR COLLEGE PRESS**

**Director  
Professor Douglas C. Lovelace, Jr.**

**Director of Research  
Dr. Steven K. Metz**

**Author  
Dr. Colin S. Gray**

**Editor for Production  
Dr. James G. Pierce**

**Publications Assistant  
Ms. Rita A. Rummel**

**\*\*\*\*\***

**Composition  
Mrs. Jennifer E. Nevil**



U.S. ARMY WAR COLLEGE



PARAMETERS

U.S. Army War College  
**SLDR**  
Senior Leader Development and Resiliency



FOR THIS AND OTHER PUBLICATIONS, VISIT US AT  
<http://www.carlisle.army.mil/>

ISBN 1-58487-564-X



9 781584 875642

9 0000 >



This Publication



SSI Website



USAWC Website