# Dilating Pupils

## The Pedagogy of Cyber Power and the Encouragement of Strategic Thought

Col Richard J. Bailey Jr., PhD*

> *Actions taken and actions to be taken are weighty factors in the strategist's thinking, of course, but they are elements to be shaped and manipulated, not strict lessons leading to instructions that must be followed.*
>
> —Everett Carl Dolman
> *Pure Strategy* (2005)

The pedagogy of cyber power presents an interesting conundrum. Although cyberspace and its related technologies have been around for decades, our *thinking* about them has yet to mature. Given the prominence of cyber power in recent international struggles, however, the urgency of integrating the technology into military strategy introduces a particular challenge. How do we *use* cyber power when we have yet to *understand* it? On a related note, how do we *teach* cyber power, particularly to practitioners who are expected to incorporate it into strategic decision making, given this lack of understanding? An exploration of this puzzle requires that we first examine the challenges of teaching strategy, independent of the particularities of cyber power. Next, a study of the environment of cyberspace will expose its etymological frameworks and biases, perhaps informing how modern

*The author is an associate professor of strategy and security studies at the School of Advanced Air and Space Studies, Maxwell AFB, Alabama. He earned his BS in engineering sciences at the United States Air Force Academy in 1992, an MA in international affairs from Washington University in St. Louis in 1997, and a PhD in government from Georgetown University in 2006. His research interests include military strategy, civil-military relations, American sociopolitical behavior, and cyber power. His latest works include *Strategy: Context and Adaptation from Archidamus to Airpower* (Annapolis, MD: Naval Institute Press, 2016) (coeditor and contributing author); *The Baltic Security Puzzle* (Lanham, MD: Rowman and Littlefield, 2015) (chapter contributor); "Fighting More Fires with Less Water: Phase Zero and Modified Operational Design," *Joint Force Quarterly* 77 (2nd quarter 2015): 101–8 (coauthor); and "You Can't Take the Human Factor Out of Warfare," Opinion-Editorial, *US News and World Report*, 17 October 2014. Colonel Bailey plans to retire later this year and will serve as the next president of Northern New Mexico College.

This article was presented as a paper at the American Political Science Association Teaching and Learning Conference, Washington, DC, January 2015, and at the International Studies Association National Conference, New Orleans, February 2015. It will appear as a chapter in a forthcoming book on cyber strategy tentatively scheduled for publication by the University of Copenhagen Press.

society approaches new technologies. Finally, an analysis of the uncertainties inherent in cyberspace and cyber power will shed light on the major problems associated with designing and articulating strategy in this virtual domain.

## The Challenges of Defining—and Teaching—Strategy

The School of Advanced Air and Space Studies is often touted as the premier school of strategy in the United States Department of Defense. The rigorous yearlong graduate program prepares its students for the dizzying array of complex problems they will face as senior military officers. Ironically, if you ask the 14 members of its all-PhD faculty for their definitions of *strategy*, you will most likely hear 14 slightly (and not so slightly) different answers. That is, the school thrives on its reputation for encouraging a broadening of mind-sets, of "creating habits of mind and patterns of inquiry" that serve graduates well in their follow-on assignments.[1] In other words, as Professor Dolman's quotation at the beginning of the article reminds us, no precise answers exist where strategy is concerned. Therefore, a multitude of varying definitions actually enhances the educational experience; that is why we encourage our students to determine their own perceptions of strategy's meaning as a critical part of their educational journey. As for the faculty of the School of Advanced Air and Space Studies, each of us (as you may have guessed) brags about our personal definition as being more useful than our colleagues' offerings. The friendly rivalry, however, is important not only for keeping each other on our toes intellectually but also for enriching the educational experience of our high-powered students. The definition I propose for strategy in this article is useful for the encouragement of strategic thought regarding cyber power, particularly since we must approach such an enterprise with humility, an open mind, and a vigorous intellectual curiosity. Let us define *strategy*, therefore, as *a continual artistic endeavor to optimize competitive advantage through an understanding of one's environment and an adaptation to uncertainty*. Several words in this definition require clarifying explanation.

*Continual*—Strategy is not a temporally framed endeavor. If we follow Lawrence Freedman's prescription for "thinking about strategy as a story told in the future tense," then the application necessarily continues ad infinitum.[2] In a military planning effort, terms like *end point* or *termination point* allude to some sort of finality to an operational enterprise. These terms are important and helpful to frame a finite effort and to direct the use of limited resources accordingly. However, strategy is a different animal, in that it is an intellectually iterative exercise. That is, although goals and objectives are important to an operational initiative, strategy looks forward to determine how efforts shape the larger picture. For example, a strategist should ask, How does the completion of a particular task, if successful, change the behavior of the other actors in the scenario? Might it change an opponent's decision calculus? Are there constraints that this effort strengthens or weakens? Does the accomplishment of an objective open new avenues for tangentially related efforts? And so on. Strategy must be respected as a continual process so that as the environment changes, intellectual rigor adjusts to meet new demands.

*Artistic*—Prussian strategist Carl von Clausewitz famously wrote that "everything in strategy is very simple, but that does not mean that everything is very easy."[3] The complexities inherent in one's environment and the issues involved in adapting to uncertainty call for much more than the application of scientific principles. B. H. Liddell Hart opined, "However far our knowledge of the science of war be extended, it will depend on art for its application."[4] Simply put, for the strategist, neither perfect information nor perfect understanding exists. Therefore, students—and practitioners—of strategy require an innovative mind and a creative approach to problem solving to make the most of an endeavor.

*Optimize Competitive Advantage*—Strategy usually involves some type of an opponent. In the military, the opponent may be a declared enemy or enemies. In business, it can be one or more competitors for market share or perhaps market forces themselves. In any case, strategy aids in some sort of struggle. In the preface to his seminal book *Strategy: The Logic of War and Peace*, Edward Luttwak states that "as a vision of strategy emerged out of the shadows of words read, problems investigated, and warlike events actually experienced, I found that its content was not the prosaic stuff of platitudes, but instead paradox, irony, and contradiction."[5]

Luttwak uses the term *paradox* because of the presence of an intelligent opponent in strategic ventures. If strategy focuses inward at one's own resources, goals, and constraints, it completely misses the effects of a strategically minded opponent. Such a foe not only affects the dynamics of the environment but also adds to the uncertainty enveloping the engagement.[6]

*Environment and Uncertainty*—Ultimately, then, the primary aims of the strategist are to think deeply about his or her environment and to prepare for the probability—or eventuality—that things will not go exactly as expected. The environment is complex because of its dynamic nature and because of our imperfect perception of it. Our misunderstandings are a product of incomplete knowledge and of our own biases or improper frameworks. In addition, strategists constantly face the tendency to assume that greater access to information keeps the forces of uncertainty at bay. In fact, the reverse is often true. In the cyber domain in particular, often the challenge lies not in obtaining *enough* information but in determining *which* information to use from a seemingly endless trove. These two areas, environment and uncertainty, will guide the rest of the article to provide a potential framework for teaching cyber strategy.

Teaching strategy ultimately involves encouraging a broadening of perspectives and an understanding of one's own intellectual habits. Herein we find another paradox of learning strategy: if students gain a respect for what they *do not* know and, just as important, for what they *cannot* know, only then can they make the most of their strategic journey. Imagination, creativity, intellectual flexibility, and high-minded responsiveness are the tools that guide them as they prepare for both the study of strategy and its future applications.

In the cyber realm, deconstructing the environment and adapting to uncertainty are seemingly impossible tasks. However, if practitioners are expected to integrate cyber power into a larger strategic worldview, then they must explore these two avenues of thought. It is toward these two areas that we now turn.

## Understanding the Environment of Cyberspace

> *Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. . . . A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding. . . .*
>
> —William Gibson

In the 1984 science fiction book *Neuromancer*, William Gibson popularized the term *cyberspace*, which he had introduced in the short story "Burning Chrome" two years earlier. He probably did not recognize at the time that the term he attached to the virtual environment would become the standard moniker for everything we associate with today's digital world.[7] Thirty years later, the ubiquity of computer networks and their impact on the human experience present a conundrum. Without question, the technology affects almost every aspect of our lives, but its application vis-à-vis power dynamics and grand strategy has yet to be understood. No power dynamic is ever *fully* understood, but our nascent exploration of the cyber field still leaves us analogous to Laika on the rocket after liftoff. In other words, we have gained an immediate awareness that our environment has changed but probably do not understand the extent of those changes, how or why we got there, or where we are headed. To gain an appreciation for the context of cyber power, we must look at the etymology of cyberspace to reveal the biases and frameworks inherent in the terminology we use and explore the difficulties in defining the cyber domain.

### *The Etymology of Cyberspace*

The main argument presented in this section is that the terminology used to describe the elements of cyberspace affects the way we *think* about it. This proposition has had a profound effect on the development (or lack thereof) of a coherent strategy for its use and has made the teaching of cyber strategy incredibly difficult. To develop this line of argumentation, we look at cyber terminology to reveal how its particular semantics shape biases. If those biases create frameworks of understanding, then they may limit the way we think about the technology.

As blogger Mark Forsyth aptly noted, "New things need new words, but they usually end up with old ones."[8] Let us start with the term *cyberspace* itself. Even before Gibson's first popular use of the word, scholars and practitioners published a wide variety of related definitions, each with its own accompanying justifications. In the 1940s, Norbert Wiener, a professor of mathematics at the Massachusetts Institute of Technology, called for increased use of statistical analysis to explain societal phenomena. He interpreted the interaction of systems (biological, mechanical, and societal) as forms of *communication* with feedback mechanisms and, more importantly, predictive qualities. Wiener and his colleagues became the foundational pioneers of a transdisciplinary field of study he termed *cybernetics*. The root *cyber* comes from the Greek *kybernan*, a term meaning *to steer* or *direct*.[9] For Professor Wiener, cybernetics' etymology connoted a direction of order from disorder: "Guided by feedback, organic, mechanical, or social bodies create pockets of order, strong signals in an entropic sea of noise."[10] For many military strategists in the middle of the twentieth century, cybernetics offered hope that through feedback analysis, one might be able to learn enough about war to mitigate uncertainty in conflict. For decades, these strategists challenged Clausewitz's famous dictum that "war is the realm of chance."[11] Thus was born a revolution in military affairs (RMA), suggesting that information, if properly processed, could fundamentally change the essence of warfare. RMA literature embraced the 2,500-year-old philosophy of Chinese thinker Sun Tzu, who wrote, "One who knows the enemy and knows himself will not be endangered in a hundred engagements."[12] Critics of RMA literature claimed that cyberneticists' overconfidence in information as a panacea ignored the omnipresence of uncertainty in combat, leading for example to the "spectacular inefficiency and failure" of strategy in the Vietnam War.[13] Daily statistics on body counts and sorties did nothing to capture either the will of the North Vietnamese people or the eroding support from the American public.

How do semantics, then, ultimately affect our conceptualization of cyber strategy? Put simply, use of the root *cyber* in *cyberspace* and *cyber power* has always implied a mechanism for creating at least some order out of chaos. As experience shows, however, uncertainty is always present in warfare; thus, even though we use these terms, we must be aware of their limitations and remain mindful to keep them in the proper perspective. Cyber power, at its core, is fueled by information. However, even robust access to information will fall well short of clearing Clausewitz's fog of war. Students of strategy must respect this eventuality and prepare themselves for the intellectual challenges that it entails.

Let us consider the connotations of the second half of the term *cyberspace*. The word alludes to, or at least conjures up, an image of a physical *space*. Thus, the term itself is nothing more than a metaphor. However, if strategists think of cyberspace solely in physical terms, they run the risk of closing their minds to the potential of the technology and to missing its unique nonphysical characteristics. The mention of cyberspace in conjunction with the physical domains adds to this tendency. The United States Air Force, for example, clarified its mission statement in 2005, rallying its Airmen "to fly, fight, and win . . . in air, space, and cyberspace."[14] When cyberspace joins air and space as domains of military operations, it is natural for the mind to apply the analogy to an imagined geospatial entity and put it on equal footing with the physical domains.[15]

Even if we try to imagine cyberspace as analogous to a three-dimensional space, its boundaries would be impossible to identify. In reality, the only physical space involved in cyberspace is the architecture providing the infrastructure for its employment. Rather, cyberspace is a metaphor helping us to visualize a domain in which information "travels" via networked computer systems. One of the most complete definitions of cyberspace comes from Daniel Kuehl, who described it as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange information via networked information systems and physical infrastructures."[16] Martin Libicki was one of the first to identify three distinct layers of cyberspace: the physical (routers, wires, switches, etc.), the syntactic (the information systems themselves, along with the protocols for formatting and distributing information), and the semantic (the nexus between the transferred information and the human reception and understanding of that information).[17] Almost every early work on cyberspace emphasized that it is the only man-made military domain. The basic concept entails that, as opposed to other domains of military power (land, sea, air, and space), human-made objects must be present in order for cyberspace to exist. Although humankind creates objects to traverse and optimize the use of the physical domains, only in cyberspace is our intervention required to *create* the domain. However, even if we recognize this unique feature, what are its associated strategic implications? Ultimately, they are either nonexistent or irrelevant. The only possible connection exists either in a scenario in which someone or something destroys the global Internet architecture or through a cataclysmic event like a global electromagnetic pulse.

Because cyberspace has no physical boundaries, no simple rules exist for partitioning either responsibilities or control. Thus, military strategists have had to look beyond traditional assumptions about the application of military force in a physical setting. Consider, for example, the factor of distance. In a physical confrontation, the distance to an enemy target is critically important to a land or sea engagement and relatively important to an air attack but almost negligible in cyberspace. A skilled hacker with advance knowledge of an enemy's computer vulnerabilities can affect both his networks and perhaps his physical assets. No matter where the target is located, the hacker can engage it from practically anywhere on the planet in literally fractions of a second. Even extraterrestrial targets like satellites may be vulnerable.

The meaning of words can evolve and even transform over time. Consider the meaning of *computer.* The term has been used in the English language since the 1600s, but it has completely transformed to mean something fundamentally different. Before the twentieth century, the word denoted a human being who processed numbers by hand. However, with the advent of the microprocessor and the growing popularity of home computing in the 1970s and 1980s, society began to use *computer* to describe the mechanism more than the person who performed the function: "By that time, computers—like science-fiction cyborgs—had completed their transformation from human to machine."[18]

Why is terminology important to the student of strategy? Let us consider the dual meaning of words and phrases. According to linguistics professor Kate Kearns, a sentence "is composed of *lexical meaning*, which is the meaning of the individual words, and *structural meaning*, which is the meaning of the way the words are combined" (emphasis in original).[19] Even the lexical meaning can frame the way we approach a topic both intellectually and emotionally. Political lobbyists are highly skilled in this arena and use language to shape national discussion. Consider the abortion debate in the United States. Lobbyists (and politicians) opposed to *late term* abortions—those that take place in the second or third trimester of a pregnancy—were able to rename them *partial birth* abortions in the public sphere. The latter term is much more evocative and has the tendency to call up images of terminating a *living* human being. The language itself can frame how we might *think* or *feel* about a subject, just based on the lexical meaning of the words used to describe it.

It is helpful to extrapolate this understanding to the terms we use in cyberspace. Because the lexical meanings of the words we use to describe elements in cyberspace are rooted in understandings and perceptions of physical objects and concepts, their structural meaning becomes bound in archaic frameworks:

> A long-standing and influential view about language is that the meaningfulness of language amounts to its "aboutness." Words and expressions symbolize and describe—and are thus about—things and phenomena in the world around us, and this is why we can use language to convey information about reality. Accordingly, the meaningfulness of language consists of connections between words and expressions and parts of reality.[20]

How can budding strategists cope with this dilemma? Moreover, how can we teach cyber strategy in a way that counters this tendency? Ideally, we would come up with new terms for cyberspace and its elements that evoked a more expanded intellectual framework. Unfortunately, this effort would be futile. The words describing cyberspace have been around for decades, so the likelihood of changing the language at this point is remote. The only recourse is to understand the limitation of the terms and to fight to overcome the biases they subconsciously create. In any case, the education of cyber strategy must start with an understanding of the cyber environment—and a large part of that environment is founded in the language we use to describe it.

### *How Do We Experience New Technology? Polarization and Analogies*

An appreciation for the biases and frameworks provided by the language of cyberspace unlocks part of our understanding of its intellectual environment but does not offer a comprehensive picture. A complementary approach involves applying a sociological lens. In other words, we may gain a more thorough understanding of the cyber environment by exploring how society adapts to it over time. Two main patterns emerge when we apply this analysis: a polarization in the literature and a tendency to use analogies to past technological advances.

To explore the phenomenon of polarization in the literature, we must first ask why society tends to think about extreme positions when it experiences new concepts. A modified scenario from Alexander Wendt serves us well here.[21] Imagine turning on your television to live, late-breaking news that an alien spacecraft has landed in the middle of Central Park in New York City. Without any other information, what would your first thoughts be? What does the image of the spacecraft convey to you? To put it in popular movie terms, you may see this in one of two extreme camps. Perhaps you imagine the friendly, benevolent, kind-hearted visitors from *E. T. the Extra-Terrestrial* or the closing scene of *Close Encounters of the Third Kind*. Or maybe you picture the dark, ominous, resource-starved aggressors from *War of the Worlds* or *Independence Day*. Few people actually think of something in between. Put simply, most of us tend to explore the new or unknown with either feelings of trepidation or the hopeful promise of a panacea. James Gleick put it best: "Every new medium transforms the nature of human thought. In the long run, history is the story of information becoming aware of itself."[22] As human thought about cyberspace and cyber power evolves, the salvationists and alarmists are falling into their respective camps. A review of popular literature on cyber power reveals this phenomenon.

When Tim Berners-Lee created the World Wide Web, he was conscious of the social power it could enable. His design eschewed a proprietary approach. Instead, the Web "invited—*required*—its inhabitants to help build it. It was a World Wide effort" (emphasis in original).[23] Designers like Berners-Lee, however, just as the inventors of the Advanced Research Projects Agency Network before him, were far more conscious of the revolutionary potential of a borderless information source than any propensity for malfeasance: "The development of social machines requires the development of mechanisms that allow users of social machines to more freely share data without having to worry about it being used in inappropriate ways."[24] Thus, the floodgates opened, and access to both the benevolent and the nefarious became instantly possible.

To many people, cyberspace inspires hope—of information as a panacea to cure our social ills. In terms of warfare, cyber power might encourage an overall decrease in destructive violent action, a "computer-enabled assault on violence itself."[25] It also might spur organically (and peacefully) generated social and political change. Evgeny Morozov termed this concept *cyber utopianism*, a "naïve belief in the emancipatory nature of online communication that rests on a stubborn refusal to acknowledge its downside."[26] How many of us thought that the Arab Spring would continue to thrive based on people's growing access to good ideas? The ubiquity of information is only part of the picture. How audiences process messages and what they do in response are equally important. Morozov's sobering message is that while information can be a spark for positive change, regimes might also use it to continue their repressive control.

If we use sheer numbers as an arbiter, the alarmist side of cyber literature seems to be winning the debate over the cyber salvationists. Even a cursory review of popular literature on cyber power reveals a wide assortment of warnings about threats imposed by the technology and our related vulnerabilities. Richard Clarke, who served four separate presidential administrations as a counterterrorism expert, is very clear about the dangers of cyber power: "Cyber war is real. What we have seen so far is far from indicative of what can be done. Most of these well-known skirmishes in cyberspace used only primitive cyber weapons. . . . What the United States and other nations are capable of doing in a cyber war could devastate a modern nation."[27] Consider the now-famous 2007 cyber attacks on Estonia. When the Estonian government pressed to remove the *Monument to the Liberators of Tallinn* (now informally nicknamed the Bronze Statue) from a prominent spot in its capital city, the Russian people (including Estonia's ethnic Russian population) were infuriated. To them, the statue was a symbol of sacrifice and honor. However, to many other Estonians, it was a reminder of oppressive Soviet occupation. Two years after joining the North Atlantic Treaty Organization (NATO), several members in the Estonian government called for removal of the monument.[28] On 15 February 2007, the Parliament passed a bill calling for a ban on *any* structure memorializing the Soviet occupation, but President Toomas Hendrik Ilves, perhaps in an attempt to find a peaceful solution to the tension, vetoed the measure.[29] Months later, the local government decided to move the Bronze Statue from its central location to a spot outside the city. The move sparked an outcry from Tallinn's ethnic Russians. On 27 April, the first cyber attacks targeted several important Estonian websites. Among them were the Estonian presidency, Parliament, most government ministries, political parties, three of the country's six big news organizations, two of the biggest banks, and major communications companies.[30] Many pointed to the Russian government as the most likely perpetrator of the attacks. In any case, the strikes constituted one of the first well-known political uses of cyber power in what appeared to be an interstate conflict. Even though no one died as a direct result of the attacks, the social, political, and financial effects on Estonia were devastating, prompting the country to petition NATO for a military response.

States are not the only potential victims of cyber power's effects. One powerful example is the December 2014 cyber attack—allegedly by the North Koreans—on Sony Pictures in response to the theatrical release of *The Interview*, a comedy based on a plot to assassinate President Kim Jong-un. The attacks were so influential that Sony postponed the film's release. President Obama criticized Sony's capitulation: "If we set a precedent in which a dictator in another country can disrupt through cyber, a company's distribution chain or its products, and as a consequence we start censoring ourselves, that's a problem."[31] Although North Korea denied the attack, the government did threaten to engage in cyber attacks in the future. American pundits and politicians disagreed about how to characterize the strikes. Some, including President Obama, called it a form of cyber vandalism, but others characterized it as something far more sinister. In a Sunday morning talk show interview, Senator John McCain asserted that "it's more than vandalism. It's a new form of warfare that we're involved in and we need to react and we need to react vigorously."[32]

This recent example shows that even within the alarmist camp, there are disagreements about how to characterize the extent of the dangers. As with any exposure to a new technology or new experience, we tend to use analogies to aid in comprehension. Put another way, our framing of new ideas and new concepts is critical to our nascent understanding of them. Philip Ball put it best: "Science is driven by ideas, not numbers or measurements—and ideas only arise by people thinking about causative mechanisms and using them to frame good questions."[33] Yet, it is often our natural instinct to draw analogies to ideas or concepts with which we are familiar, similar to the way we use common language to describe them, even at the cost of creating problematic biases. In the cyber arena, a multitude of initial thinkers and writers explored society's early lessons with the airplane and airpower and used them as a blueprint (and in some cases a prediction tool) for our experiential journey through cyberspace and cyber power: "Airpower is similar to cyberpower because it is a domain dominated by technological advancements."[34] In many ways, the analogy can be helpful. Airpower, for example, started as a tool for reconnaissance and battlefield awareness but progressed into a fundamentally unique application of military force.[35] In other words, we could no longer think of airpower in the same way we thought of land power or sea power. Its three-dimensional nature and its ability to bypass or circumvent traditional battlefield considerations meant that airpower required a new way of *thinking* about warfare. The Center for Cyberspace Research at the Air Force Institute of Technology put it this way: "Cyberspace is a domain of military operations, and we need to begin growing a cyber culture. The challenge is that there is little or no published doctrine. . . . Nonetheless, we have to start somewhere. To a great extent, we are in the same situation as [Billy] Mitchell and [Giulio] Douhet when discussing [the] application of airpower."[36] In this sense, our early experiences with airpower are instructive for our early steps in cyberspace.

The application of cyber power is in many ways, however, fundamentally different from that of any military power preceding it. Therefore, we need to spend time thinking about these unique characteristics rather than simply applying constructs from the physical domains. Libicki was one of the first to recognize that a different mind-set would be necessary to thrive in a digital world:

> Over time, radical changes in technology are understood to involve radical changes in the organization of work and society as well. Initially the electric motor did not help productivity compared to the belt-driven machines it replaced; in time, vertical factories designed to minimize the amount of belting gave way to horizontal factories designed to help the flow of men and material. Similarly, computers cannot help most firms very much until they reengineer their work processes to accord with the silicon logic. Conflict both conventional and unconventional will perforce follow the same path—accommodating change first by incorporation, and next by reinvention.[37]

This is the irony of using analogies in cyberspace. The only thing helpful about applying an analogy to cyber power is that it warns us to avoid common frameworks—like analogies.

Budding strategists exposed to cyber power must come to grips with how society experiences new technologies, both to wade through the polarization of initial thinkers and to use—but be wary of—analogies to past technologies.

## Adapting to the Uncertainty Inherent in Cyberspace

> *The telescope . . . was powerful enough to make out those details that would ordinarily be beyond the commander's view, but not so powerful as to produce the administrative equivalent of Heisenberg's Uncertainty Law in physics, which says that subatomic particles can never be measured because the very attempt to measure them will cause them to change.*
>
> —Martin van Creveld

In *Command in War*, Martin van Creveld warns us that no matter how hard we try to create order from chaos, uncertainty is a timeless characteristic of war.[38] Cyberspace is our latest telescope. It offers us access to information that previously seemed unimaginable. Yet, even in an era of Big Data, uncertainty thrives. How should students of cyber strategy contend with this dilemma? As the definition of strategy at the beginning of this article reminds us, adaptation is the key. Successful adaptation depends on two endeavors: (1) understanding the dialectic nature of strategy and (2) gaining an appreciation of what—and how much—is still unknown.

### *The Strategy of Others*

Boxing champion Mike Tyson is famously quoted as saying that "everyone has a plan until they get punched in the mouth."[39] If strategy is about optimizing competitive advantage, then students of strategy must acknowledge that a thinking, strategic opponent has a vote in determining the outcome of any engagement. This fact alone creates uncertainty for the strategist. Therefore, it is incumbent on students of strategy—particularly cyber strategy—to consider the most prominent actors in the domain today. As Timothy Thomas put it, "Cyber strategists will be wise to become familiar with the methods, definitions, and concepts of the most capable cyber nation-states."[40]

The United States and Western Europe got a head start in the development of cyberspace tools and technologies. One need only look at *Forbes* magazine's list of the three most valuable worldwide brands today—Apple, Microsoft, and Google—to see where innovation generated huge profits.[41] As Joseph Nye pointed out, in many ways, that head start had a huge impact on the geopolitical distribution of power:

> In the twentieth century, science and technology added dramatic new dimensions to power resources. . . . Subsequently, the leading role of the United States in the information revolution near the end of the century allowed it to create a revolution in military affairs. The ability to use information technology to create precision weapons, real-time intelligence, broad surveillance of regional battlefields, and improved command and control allowed the United States to surge ahead as the world's only military superpower.[42]

However, this gap is arguably shrinking. China, Russia, and other state actors are spending considerable percentages of their military budgets on the development of offensive and defensive cyber technologies. According to a recent *TechRepublic* report, "Peter W. Singer, director of the Center for 21st Century Security and Intelligence at the Brookings Institution, said 100 nations are building cyber military commands. . . . There are about 20 that are serious players, and a smaller number could carry out a whole cyberwar campaign."[43] The biases and frameworks that cyberspace's etymology creates in English can become even more problematic on the international stage:

> Yet even before addressing divergences in attitude and threat perception, there is the more basic problem of absence of a common terminology between the major players in cyberspace. The definitions of such terms as cyber conflict, cyber war, cyber attack, cyber weapon, etc. used by the UK, USA, Russia and China do not coincide—even where official or generally recognised definitions exist in each respective language. Furthermore, direct translations of specific terms from Russian and Chinese which resemble English-language terms, and vice versa, can complicate matters further by giving the misleading impression of mutual understanding, while in fact referring to completely different concepts.[44]

State powers are not the only actors joining the fight. Although attribution is still a challenge in cyberspace—as discussed below—several high-visibility cyber attacks have been linked to nonstate actors.[45] As opposed to dominance in the physical domains, which may require either massive personnel numbers or sophisticated high-tech weaponry, cyber power's cost of entry is relatively low. Sophisticated knowledge is certainly a requirement, but the design of the Internet's architecture makes its users vulnerable to malfeasance from anywhere. Thus, students of strategy must ask the question, In terms of military power, do cyber capabilities serve as a leveling function for what used to be a hierarchical playing field? If so, how do militaries in an era of fiscal constraints prepare for the myriad of potential adversaries?

In addition, the strategist must attempt to comprehend—and appreciate—the way potential adversaries *think* about the use of power. For example, "China has a very long history of strategic thought. One need only access their military encyclopedia to get a feeling for the hundred or so Chinese terms that are defined and include the word *strategic*."[46] What does this mean for the Chinese use of cyber power, not just today but within the context of a much longer game plan? Moreover, perhaps more importantly, what security concerns would these decisions affect? The cyber strategist must use a combination of thoughtful research and freethinking imagination to tackle problematic questions like these in an effort to adapt to uncertainty caused by the presence of other actors in cyberspace.

### *The Cyber "Unknown"*

Uncertainty in cyberspace is not just dependent on the presence of intelligent foes. In fact, cyber power's own characteristics bring forth a level of uncertainty with which strategists must contend. Two classic examples are (1) attribution/forensics and (2) classification/cooperation. Ironically, one is a product of technological progress while the other is caused by our own national policies.

In 2007 it was easy to blame Russia for the attacks on Estonia. Their timing, the Russian government's passionate outcries about the removal of the Bronze Statue, the temper of ethnic Russians in the Baltics, and the capabilities exhibited by the Russian government on previous occasions all pointed to Moscow as the prime suspect. The same can be said for the attacks on Sony Entertainment in 2014. Their timing, the pending release of *The Interview*, and public statements by the North Korean government (even considering its denials) still pointed to Pyongyang. However, all of those factors in a court of law would amount to nothing more than circumstantial evidence. It may be a far greater challenge to attribute responsibility for an act in cyberspace than to determine the source of a nuclear catastrophe. Organizations like the Defense Threat Reduction Agency now have highly sophisticated nuclear forensics programs that can identify the source of harmful material from radioactive debris, even potentially pinpointing the area of origin.[47] Phantom Internet protocol addresses and other techniques for operations in cyberspace still make attribution a concern for cyber practitioners and a more significant one for geopolitics. How can leaders make national security decisions and endorse potential military-response actions without a clear picture of a perpetrator? For example, when Estonia petitioned NATO for a response to the attacks in 2007, NATO nations refused to act, not simply because of the confusion about whether the cyber attacks constituted acts of war but because they could not be *certain* that the attacks came from Russia (much less the Russian *government*). In essence, cyber operations have yet to reach the level of forensic sophistication that occurs in the physical domains. Consequently, uncertainty surrounding cyber acts can make even seemingly straightforward response decisions incredibly complex.

In time, cyber forensics may reach a level of sophistication comparable to that of the physical domains. Scientific research and development will pave the way. To a meeting of business executives on national security on 11 October 2012, then–secretary of defense Leon Panetta observed that "over the last two years, DoD [the Department of Defense] has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America."[48] At the time, many people questioned the validity of the statement and perceived the secretary's speech as more of a deterrent threat than an actual boast of improving capabilities. Although attribution in cyberspace is a difficult problem, improvements in cyber forensics are nevertheless developing.[49] Techniques to mask identity in cyberspace are evolving as well, so the attribution issue, at least in the near term, presents a problematic uncertainty to the cyber strategist.

Uncertainty caused by classification difficulties, however, is a human-made conundrum and the source of an interesting paradox between security and cooperation. The United States Presidential Website illustrates a prime example. On the one hand, the White House is very clear about the importance of protecting its classified information: "It's the classified military and intelligence networks that keep us safe." On the other hand, the same website trumpets the importance of international collaboration and cooperation: "Because cyberspace crosses every international boundary, we must engage with our international partners. We will work to create incentives for, and build consensus around, an international environment where states recognize the value of an open, interoperable, secure, and reliable cyberspace."[50] Anyone who has worked in a military cyber power capacity will tell you that the security classification procedures are incredibly robust—perhaps because of the perceived concept of *one-and-done* cyber weapons. In other words, if a cyber weapon exploits an enemy's particular network vulnerability and the enemy detects the act, he or she can do two things almost immediately: (1) patch the vulnerability to prevent similar weapons from having the same access and permitting the same damage and (2) use that same weapon in an offensive capacity against any other entity with the same vulnerability.

Thus, the concept of one-and-done weapons leads to two major behaviors. First, would-be users of the weapon may resist using it until absolutely necessary since they do not want to expose knowledge of the weaponry. This choice may in some ways reduce the likelihood of offensive attacks since actors may be incentivized to hold on to the potential use as long as possible—or at least until they feel they *really* need to use it. Second—and closely related—cyber actors want to keep a close hold on the capability to prevent that same awareness, so their tendency is to classify the capabilities (and the weapons themselves) at the highest possible level.

This situation presents a unique challenge to international cooperation efforts. Concern about the difficulty of maintaining classified information of any kind encourages actors to play their cyber cards incredibly close to their chests, leading to intensive (and sometimes exhaustive) security classifications. This behavior, however, runs completely counter to practices that facilitate international cooperation. Some examples of successful cooperation do exist—the NATO Cooperative Cyber Defence Centre of Excellence in Estonia stands out as a potential institutional blueprint. The center offers avenues for international information sharing and hosts international exercises and best-practice simulations. Such an agency, though, is only as effective as the information that member states choose to share with one another. In many cases, individual governments still classify their most advanced techniques at the highest national levels, prohibiting international sharing—even with their closest partner nations.

The US government's self-inspection after the attacks of 11 September 2001 offers an interesting framework. A report to the US Senate 10 years after the attacks pointed out that

> the attacks on 9/11 showed all of us that the Cold War "need to know" system for managing classified and sensitive information drove a culture of information security that resulted in countless stovepipes and secretive pockets of the nation's most valuable information. It may have worked in the Cold War, but it was not adequate to keep America safe in a world of asymmetric threats. Many realized that protecting America in this new threat environment would require the government to operate in an entirely new way.[51]

In a similar way, the asymmetric threats posed by cyber power today necessitate consideration of removing national stovepipes and traditional classification tendencies. This is not an argument for removing all national classifications from cyber tools and techniques, but strategists must recognize that cooperation without meaningful information sharing is akin to a paper tiger and ultimately may leave each member state more vulnerable.

Uncertainty is omnipresent in warfare. Cyberspace and its related technologies may have offered initial promise that robust access to information could create order from the chaos, but the opposite is closer to reality. Our present access to cyberspace in some ways has complicated the picture. The ubiquity of information, ironically, increases uncertainty by forcing the strategist to concentrate much more on *prioritizing* available information rather than *gaining access* to it, making adaptation and flexibility more important than ever—particularly to the strategist.

## Cyber Strategy Education in Action: A Few Examples

Over the last 20 years—and the last 10 in particular—several states have instituted cyber education programs to encourage strategic thinking about cyberspace and cyber power. A cursory review illustrates that many of these programs tend to focus more on tactical and operational skill training rather than on strategic thinking.

The United Kingdom offers an interesting example. In 2011 that country published its national cyber security strategy, highlighting four main strategy objectives:

- to make the UK one of the most secure places in the world to do business in cyberspace;
- to make the UK more resilient to cyber attack and better able to protect our interests in cyberspace;
- to help shape an open, vibrant and stable cyberspace that supports open societies;
- to build the UK's cyber security knowledge, skills and capability[52]

Based on the definition of strategy provided previously in this article, one can argue that the United Kingdom values strategic cyber thinking, but its national goals seem overwhelmingly tactical in nature. Even the fourth objective, although referring to increasing knowledge, seems more slanted toward tactical training than strategic education. In 2013 a governmental review of the strategy "identified a shortage of cyber security skills as a key challenge. . . . If the UK is to be equipped to respond to cyber threats, and the cyber security sector is to grow, we need to strengthen the pipeline of cyber talent and help prepare students for entry-level security career opportunities."[53] This stance has led to the Higher Education Academy and other educational programs instituting aggressive training programs in cyber skills. Such training is certainly valuable and indeed necessary for national defense given the impact of the cyber domain, but deeper-level strategic education must also be included.

The US professional military education (PME) program is designed to arc across an individual's entire military career. The Air Force's PME goal, for example, is to produce "professionals educated in the profession of arms who possess an intuitive approach to joint war fighting built upon individual Service competencies. The aim is to produce graduates prepared to operate at appropriate levels of war in a joint environment and capable of generating quality tactical, operational, and strategic thought from a joint perspective."[54] At different key nodes within a service member's career, military education programs foster both a refresher about the unique responsibilities of being a member of the profession of arms as well as an update of doctrine, tactics, and strategies involved with the employment of military power. At the Air Force Institute of Technology (AFIT), specific courses target both practitioners and supervisors of cyber power. In April 2015, AFIT invited the author to upgrade the strategy block of the curriculum for the Cyber 300 (upper-level supervisor) course. The course directors identified that their strategy block had been much more about national *policy* than national *strategy*. Thus, we have worked on broadening the lessons (and related exercises) to stimulate strategic thinking rather than simply review associated policies.[55]

NATO's Cooperative Cyber Defence Centre of Excellence is taking big steps to encourage strategic thought. Its website includes links to every member state's national strategies regarding cyberspace as well as any relevant legal documents.[56] The center may be best known, however, for a book it published in 2013. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is the first publication of its kind to attempt to codify international norms of cyber power.[57] Although not legally binding (NATO did not even formally review it), the manual at least establishes a framework by determining the extent to which cyber power fits within already-established legal standards for the physical domains. The *Tallinn Manual* was groundbreaking in that it was the first major attempt to codify international norms for cyber power. The center hosts tactical exercises that are gaining in popularity with member states each year and holds education programs in several areas, but its largest strategic education initiatives focus primarily on international legal issues.[58]

As demonstrated in this article, strategic thinking—particularly regarding cyberspace—requires a shift in mind-set. As Timothy Thomas puts it, "A holistic approach is required to develop a cyber strategist due to the global nature and blinding speed of digits."[59] The recent explosion of cyber training programs is a positive trend, showing that states are taking the effects of cyber technology seriously. However, *training* must be accompanied by *education*. If we are to cultivate future cyber strategists, then an introduction to cyber tools is just the beginning. A greater understanding of the dynamic cyber environment and a respect for the unexpected will be necessary elements of a more complete cyber strategy education.

## Conclusion: The Journey Continues

As this article illustrates, thinking strategically about cyber power is no easy task. Teaching and learning strategy are complicated enough, particularly considering the varied definitions—and perceptions—of strategy itself. If strategy is ultimately dependent on understanding one's environment and adapting to uncertainty, then we clearly still have much work to do in the cyber domain. Understanding the environment of cyberspace is often hampered by biases and frameworks, many of which are based on etymological foundations. In addition, contextual confusion often leads to a polarization in early literature and a tendency to use anachronistic analogies to aid in comprehension—both of which present challenges to strategic thinking. Uncertainty in cyberspace is a product of the dialectical nature of strategy and the limits to useful information—both organic and synthetic—inherent in cyberspace and in our application of cyber power. This situation makes adaptation critical to the cyber strategist.

Military practitioners face a daunting task. They are being asked to incorporate cyberspace and cyber power into an already complex suite of military applications. However, our nascent experience with the technology shows that we have yet to grasp fully the domain's intricacies. Students of cyber strategy must acknowledge and respect the enormity of the unknown. Designing and articulating a coherent strategy for cyber power will likely take several more years and require more intellectual rigor. In the interim, practitioners who desire to think strategically about cyber power must endeavor to understand the complex environment of cyberspace and be flexible enough to adapt to its ever-present uncertainties. Ultimately, cyberspace and cyber power are important subjects with which students of strategy must become familiar; reciprocally, however, this technology offers an intellectual harvest that when approached properly can assist in the development and cultivation of deeper strategic thought.

**Notes**

[1] Special thanks to Dr. Thomas Hughes for this insightful phrase.

[2] Lawrence Freedman, *Strategy: A History* (New York: Oxford University Press, 2013), xiv.

[3] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 178.

[4] B. H. Liddell Hart, *Strategy* (London: Faber and Faber, 1954), 323.

[5] Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: Belknap Press of Harvard University Press, 1987), xii.

[6] See also David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 229–30. He posits that five factors shape the nature of war, one of which is *paradoxical logic*, based on the presence of an intelligent foe.

[7] William Gibson, *Neuromancer* (Princeton, NJ: John Wiley, 1984), 51.

[8] Mark Forsyth, *The Etymologicon: A Circular Stroll through the Hidden Connections of the English Language* (New York: Berkley Books, 2011), 103.

[9] *Dictionary of Etymology: The Origin of American English Words*, ed. Robert K. Barnhart (New York: HarperCollins, 1995), 181.

[10] Adam Brate, *Technomanifestos: Visions from the Information Revolutionaries* (New York: Texere, 2002), 18.

[11] Clausewitz, *On War*, 101.

[12] Sun Tzu, *The Art of War*, trans. Ralph D. Sawyer (New York: Barnes and Noble, 1994), 179.

[13] Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 160.

14. The US Air Force publishes its mission statement on its public website, along with the organization's values, core competencies, and history. "Mission," US Air Force, accessed 9 May 2016, http://www.airforce.com/learn-about/our-mission/.

15. The concepts in this paragraph and the following two originated in an essay I wrote entitled "Four Dimensions to the Digital Debate," recently published as a chapter in Richard J. Bailey Jr., James W. Forsyth Jr., and Mark O. Yeisley, eds., *Strategy: Context and Adaptation from Archidamus to Airpower* (Annapolis: Naval Institute Press, 2016), 186–207.

16. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, 2009), 26.

17. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 8–9.

18. Justin Cord Hayes, *The Unexpected Evolution of Language* (Avon, MA: Adams Media, 2012), 67.

19. Kate Kearns, *Semantics*, 2nd ed. (London: Palgrave Macmillan, 2011), 3.

20. Ibid., 6.

21. Professor Wendt used the scenario to argue that social threats are not natural but socially constructed phenomena. See Alexander Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization* 46, no. 2 (Spring 1992): 405.

22. James Gleick, *The Information: A History, a Theory, a Flood* (New York: Pantheon Books, 2011), 12.

23. Brate, *Technomanifestos*, 231.

24. Jim Hendler and Tim Berners-Lee, "From the Semantic Web to Social Machines: A Research Challenge for AI on the World Wide Web," *Artificial Intelligence* 174, no. 2 (February 2010): 156–61.

25. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), xiv. Author's note: In a telephone interview with the author in the summer of 2013, Professor Rid articulated that despite his book title, his position was not necessarily an optimistic one. He simply argues that cyber power offers a less violent alternative to the conflict mechanisms of sabotage, espionage, and subversion, and that this option may lessen the propensity for overall violence.

26. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011), xiii.

27. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 30–31.

28. The most vocal element of the Estonian government at the time was the Pro Patria and Res Public Union (IRL). For more information, please see Joel Alas, "Bill Paves Way for Statue Removal," *Baltic Times*, 15 November 2006, http://www.baltictimes.com/news/articles/16812/.

29. For the full news story, please see "Law to Remove Memorial Vetoed by Estonia's Leader," *South Bend Tribune*, 23 February 2007, http://articles.southbendtribune.com/2007-02-23/news/26801820_1_bronze-soldier-president-toomas-hendrik-ilves-soviet-war-memorial.

30. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, 16 May 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia.

31. Jethro Mullen, "North Korea and the Sony Hack: The War of Words Escalates," *CNN*, 22 December 2014, http://www.cnn.com/2014/12/22/world/asia/north-korea-us-sony-hack-who-says-what/index.html.

32. Ibid.

33. Philip Ball, "Machine Envy," *Aeon Magazine*, 7 January 2014, http://aeon.co/magazine/science/science-is-becoming-a-cult-of-hi-tech-instruments/.

34. Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Waltham, MA: Elsevier-Syngress, 2011), 27.

35. For an analysis of the different stages of US Air Force thinking—and branding—see Paula G. Thornhill, "*Over Not Through*": *The Search for a Strong, Unified Culture for America's Airmen* (Santa Monica,

CA: RAND Corporation, 2012), http://www.rand.org/content/dam/rand/pubs/occasional_papers/2012/RAND_OP386.pdf.

36. Dr. Robert F. Mills, Dr. Richard A. Raines, and Maj Paul D. Williams, *Developing Cyberspace Competencies for Air Force Professional Military Education* (Wright-Patterson AFB, OH: Center for Cyberspace Research, Air Force Institute of Technology, 2007), 1.

37. Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, McNair Paper 28 (Washington, DC: Institute for National Strategic Studies, National Defense University, 1994), 3.

38. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 142.

39. Mike Berardino, "Mike Tyson Explains One of His Most Famous Quotes," *Sun Sentinel*, 9 November 2012, http://articles.sun-sentinel.com/2012-11-09/sports/sfl-mike-tyson-explains-one-of-his-most-famous-quotes-20121109_1_mike-tyson-undisputed-truth-famous-quotes.

40. Timothy Thomas, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic," *Defence Studies* 14, no. 4 (28 August 2014): 382.

41. Kurt Badenhausen, "Apple, Microsoft, and Google Are World's Most Valuable Brands," *Forbes Magazine*, 5 November 2014, http://www.forbes.com/sites/kurtbadenhausen/2014/11/05/apple-microsoft-and-google-are-worlds-most-valuable-brands/.

42. Joseph S. Nye Jr., *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004), 18.

43. Steve Ranger, "Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar," *TechRepublic*, 24 April 2014, http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/.

44. Keir Giles and William Hagestad III, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in *Proceedings: 5th International Conference on Cyber Conflict*, ed. K. Podins, J. Stinissen, and M. Maybaum (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 414–15.

45. For an in-depth look at the effects of nonstate actors in cyberspace, see Capt Johan Sigholm, "Non-State Actors in Cyberspace Operations," *Journal of Military Studies* 4, no. 1 (2013), http://www.ida.liu.se/~g-johsi/docs/JMS_4-1_Sigholm_Non-State_Actors_in_CyberOps.pdf.

46. Thomas, "Creating Cyber Strategists," 381.

47. See "Nuclear Technologies," Defense Threat Reduction Agency and USSTRATCOM Center for Combating WMD and Standing Joint Force Headquarters-Elimination, accessed 10 May 2009, http://www.dtra.mil/Research/NuclearTechnologiesDepartment.aspx.

48. Secretary of Defense Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," US Department of Defense, 11 October 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

49. James Steinberg and Michael E. O'Hanlon, *Strategic Reassurance and Resolve: U.S.-China Relations in the Twenty-First Century* (Princeton, NJ: Princeton University Press, 2014), 176.

50. "Foreign Policy: Cybersecurity," White House, President Barack Obama, accessed 9 May 2016, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

51. Senate, *Statement of Zoe Baird Budinger and Jeffrey H. Smith, Senate Committee on Homeland Security and Governmental Affairs: Ten Years after 9/11; a Status Report on Information Sharing*, 112th Cong., 1st sess., 12 October 2011, https://www.fas.org/irp/congress/2011_hr/101211smith.pdf.

52. Cabinet Office, *The UK Cyber Security Strategy: Report on Progress and Forward Plans*, December 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.

53. "Learning and Teaching in Cyber Security," Higher Education Academy, accessed 9 May 2016, https://www.heacademy.ac.uk/funding-call/learning-and-teaching-cyber-security.

54. Mills, Raines, and Williams, *Developing Cyberspace Competencies*, 3.

55. For a full description of AFIT's Cyber 200 and 300 courses, see "Cyberspace 200/300 Courses," AFIT Graduate School of Engineering and Management, 8 December 2015, http://www.afit.edu/CCR/programs.cfm?p=60&a=pd&page=162&tabname=Tab1A.

56. See "Cyber Security Strategy Documents," NATO Cooperative Cyber Defence Centre of Excellence, 3 August 2015, https://ccdcoe.org/strategies-policies.html.

57. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013).

58. For a list of available training and educational offerings at the center, see "Cyber Security Training events," NATO Cooperative Cyber Defence Centre of Excellence, accessed 9 May 2016, https://ccdcoe.org/events.html.

59. Thomas, "Creating Cyber Strategists," 390.