Cyberspace Superiority

A Conceptual Model

Lt Col William D. Bryant, USAF

The Airman seeks air superiority; the Sailor, maritime superiority. Does cyberspace superiority exist? Currently we have no clear consensus regarding that question. Some authors, such as RAND's cyber expert Martin Libicki argue that "cybersupremacy is meaningless and, as such, is not a proper goal for operational cyberwarriors."[1] The US Air Force disagrees, identifying cyberspace superiority as a key concept. According to Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, cyberspace superiority represents "the operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference."[2] Joint doctrine takes the middle ground. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, includes definitions for air, maritime, and space superiority but not cyber superiority. To confuse the issue further, it notes that full-

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberspace Superiority: A Conceptual Model	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute (AFRI) ,155 N. Twining Street,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**20**	

spectrum superiority is the "cumulative effect of dominance in the air, land, maritime, and space domains and information environment (which includes cyberspace)."[3] Much of the confusion over cyberspace superiority stems from the difficulty of intuitively grasping what it looks like. This article seeks to overcome this difficulty by proposing a conceptual model of how cyberspace superiority works.

By its very nature, a model is not the thing itself and is significantly simplified to facilitate comprehension and analysis. However, to be useful, the model must have sufficient fidelity, and any proposed model in strategy must account for the dynamic nature of strategy whereby "the enemy gets a vote" and both sides make decisions in response to each other. Carl von Clausewitz captured this interaction in his analogy of two struggling wrestlers, each attempting to throw the other.[4] The model must do the same.

We must also note that the cyberspace superiority discussed here has to do with conflicts between nation-states. Although "hacktivists" and cyber criminals utilize some of the same tools and techniques as nation-state attackers, they have fundamentally different objectives, and their operations are not "the continuation of politics by different means."[5] In nation-state conflict, cyberspace is generally considered a global common, much like the sea, and its normal state is not to be commanded or controlled by any party.[6]

Cyberspace superiority is not an end in itself; winning the battle for such superiority does not necessarily equate to winning the overall conflict—but it certainly makes it easier. Combatants will not feel the most important effects of cyberspace superiority in cyberspace but in the other war-fighting domains. Those who operate in the land, air, maritime, and space domains rely heavily on cyberspace to carry out their missions, and a modern military would have considerable difficulty operating effectively without its information systems. To convey what cyberspace superiority means and how control of cyberspace can produce desired effects in other domains, the article builds a model reflecting the production of superiority in the air domain.

A Model of Domain Control

Because of the difficulty of comprehending something not purely physical, such as cyberspace, we begin by building a model of domain control in a more familiar environment (fig. 1). Specifically, the literature includes a great deal of discussion about air superiority, and one can examine numerous wars and case studies to determine the characteristics, elements, and interactions pertaining to the air domain. Notably, the model developed here deals only with "means" (what produces superiority in the domain) and "ways" (what those means can do both in and out of the domain). The means are the tools, and the ways are what can be done with those tools. The model remains silent regarding how those ways may or may not contribute to the overall ends of the strategy.

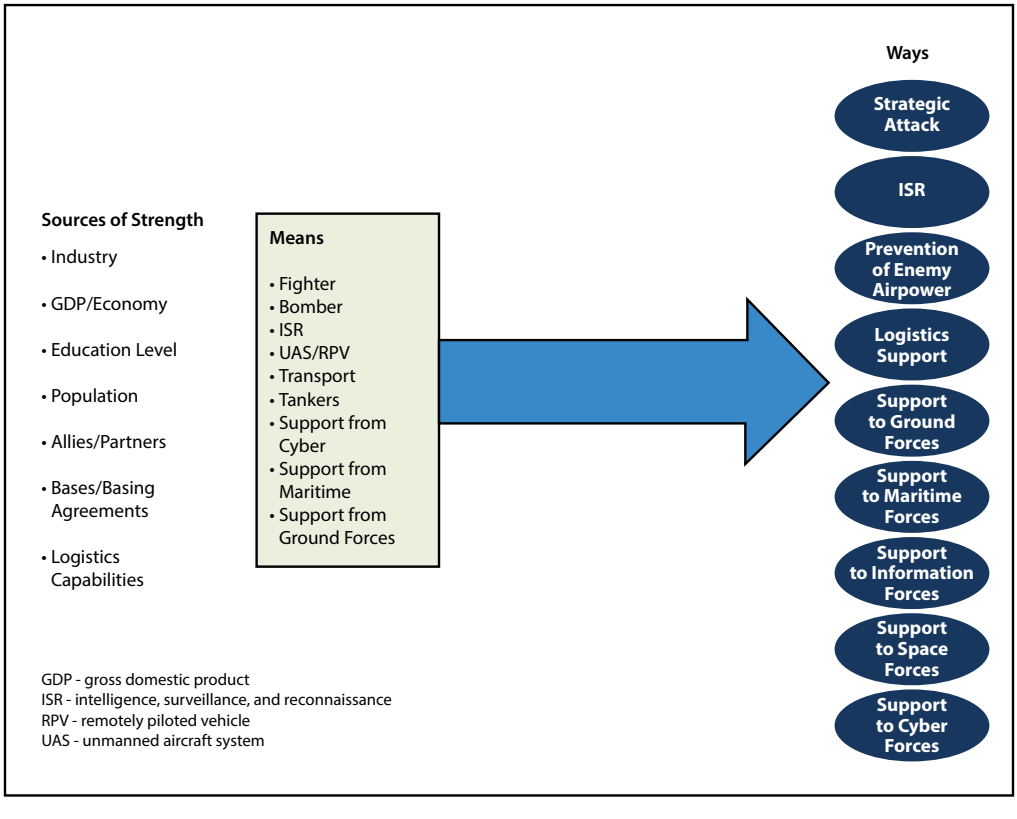

Figure 1. The means and ways of air superiority

A nation's sources of strength, such as industry and population, produce its airpower means (e.g., fighters, bombers, and tankers). The country then uses these means against an enemy to generate the airpower ways—the things that airpower can do—such as conduct strategic attack or support ground forces. However, as Clausewitz observed, "In war, the will is directed at an animate object that *reacts*" (emphasis in original).[7] The enemy will not sit idly by during an attack but will try to prevent the opponent from utilizing his means. Figure 2 depicts some of the more common ways an enemy can employ to block airpower.

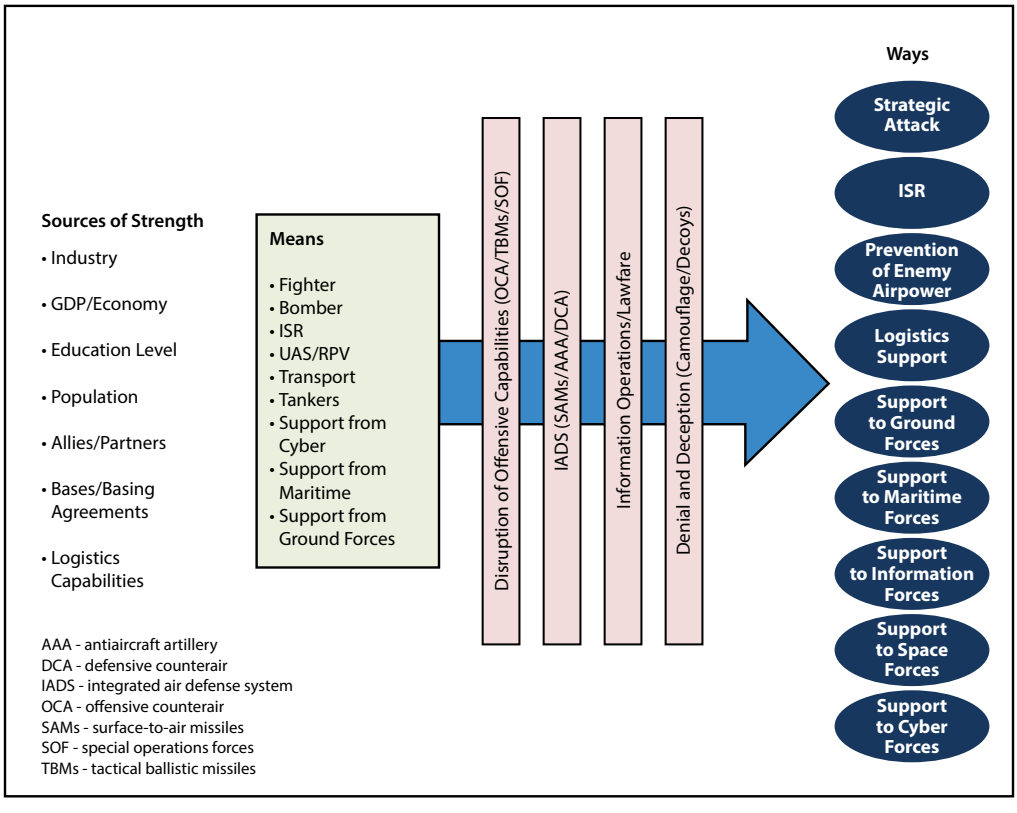

Figure 2. The means and ways of air superiority with adversary blocking

However, the dynamic nature of strategy, in which every action generates a reaction from the enemy, has not yet concluded. The initiator of the action can also react to the enemy's action by bringing into play a number of well-known and potentially effective measures. Figure 3, the complete model of air superiority, illustrates some of the attacker's potential mitigation strategies.

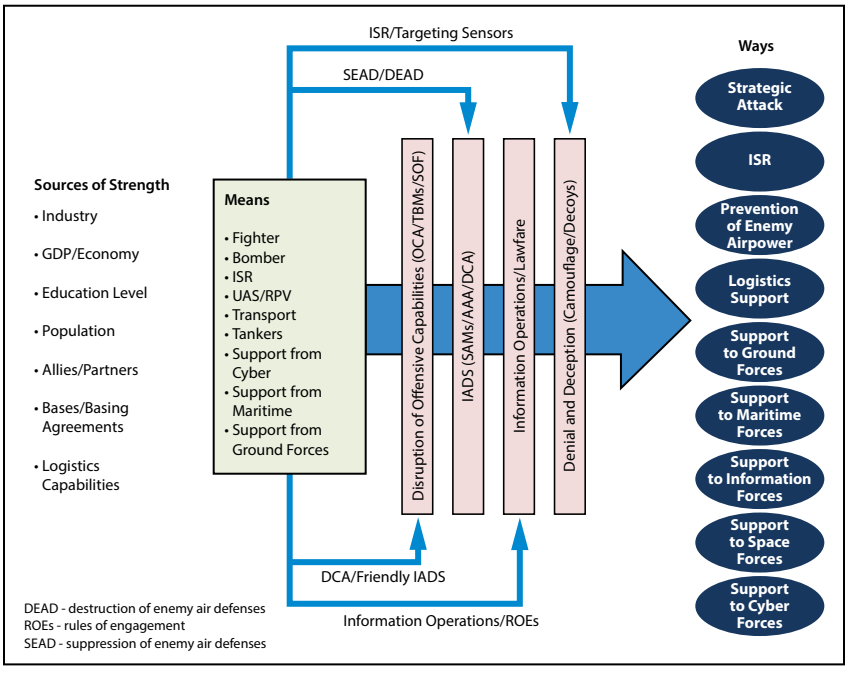

Figure 3. Air superiority model

Of course, reactions to reactions may go on ad infinitum, but moving only two levels up is sufficient to make the dynamic nature of the contest apparent. The model shows elements the initiator needs to strengthen, options the enemy has to block him, and choices for weakening those blocks along with the ways available to the initiator. All of this is relatively uncontroversial in the air domain, but the unique characteristics of the cyber domain lead to very different elements in the model.

Unique Characteristics of the Cyberspace Domain

Building a model of cyberspace superiority requires accounting for the distinctive characteristics of the cyberspace domain. Because the domain is man-made (the first characteristic), its geography is always subject to change by the combatants or third parties. Gregory Rattray, author of *Strategic Warfare in Cyberspace*, remarks that "cyberspace is unique in that the interactions are governed by hardware and software that is manmade, so the 'geography' of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the flick of a switch; they can be created or 'moved' by insertion of new coded instructions in a router or switch."[8] This mutability goes beyond the ability to move "geographical" features; we can also copy the rivers, mountains, and oceans of cyberspace; store them at will; and reinsert them later if the need arises. As data-storage costs continue to plummet, it becomes ever more practical for combatants to have multiple copies of everything. Libicki maintains that since cyberspace is replicable, it is also repairable—a notion that has significant implications for the persistence of effects in cyberspace.[9]

As is the case with the air and maritime domains, combatants access cyberspace via technology but at far less cost. The ports and ships of the maritime domain as well as the aircraft and airfields of the air domain demand an immense expenditure of resources generally available only to nation-states. In contrast, the port or airfield of cyberspace is as close as the nearest Internet service provider or Internet café, and the delivery vehicle for an attack can be a simple laptop purchased nearly anywhere for less than $500. Significant capability can prove extremely resource intensive and take years to develop, but the initial cost of entry remains quite low. Furthermore, the resources necessary for success ordinarily take the form of highly trained and competent personnel as opposed to major expenditures in infrastructure and equipment.

We must also recognize that control of cyberspace is unlikely to win the war by itself. Although the uncertainty generated by the enemy's

knowledge that the opponent can manipulate his information systems can be important, it probably won't make him give up the objectives he was willing to fight for in the first place. Possession of land can prove significant—possession of cyberspace less so. However, cyberspace superiority allows us to do things with the information resident in cyberspace and to produce effects in other domains through cyberspace. For example, the fact that an enemy can access a US logistics system is noteworthy because he could obtain information that shows where forces are going and could manipulate the system to make those forces less effective in other domains by reducing their supplies. The fact that an adversary has hacked into the control system of a power plant has significance because of the effect he could generate in other domains by affecting the power plant through cyberspace.

Another characteristic of cyberspace, the asymmetry between offense and defense, also applies to some extent in the air domain since an asymmetry exists between offensive airpower and ground-based defenses in modern air combat. A modern integrated air defense system utilizes surface-to-air missiles, antiaircraft artillery, fighters, and surveillance assets integrated with command and control. With the exception of multirole fighters, these defenses cannot perform offensive missions into enemy territory; they can only target incoming aircraft. A similar asymmetry exists between the defense and offense in cyberspace, where defensive and offensive systems are neither similar nor interchangeable. This asymmetry contrasts the situation in sea warfare, in which a destroyer can operate either offensively or defensively, much like a tank or an infantryman. A firewall and a worm, important elements of cyberspace, are fundamentally different and no more interchangeable than a Patriot missile and a B-52.

Because they rely on deception for access, cyberspace weapons are extremely frangible. Like glass swords, they can be sharp and lethal but may break on the first swing. Upon recognizing an enemy exploit, the defender will engineer patches to stop further attacks that use the same opening. Additionally, like glass swords, cyberspace weapons are

difficult to detect. Cyberspace offensives that utilize unknown, exploitable flaws are referred to as "zero day" attacks because the timer on the vulnerability starts at zero when the first strike occurs and then rises in increments as software engineers scramble to develop a patch. Defenders unaware of the specific vulnerability rely on systems that look for generic signatures—often with only moderate success. Thus they consider zero-day exploits important and guard against them carefully after discovery. Given these characteristics, we can now build a model of cyberspace superiority.

Cyberspace Superiority Model

Employing some concepts from the other domains as well as the characteristics of cyberspace, figure 4 presents the means and ways of cyberspace.

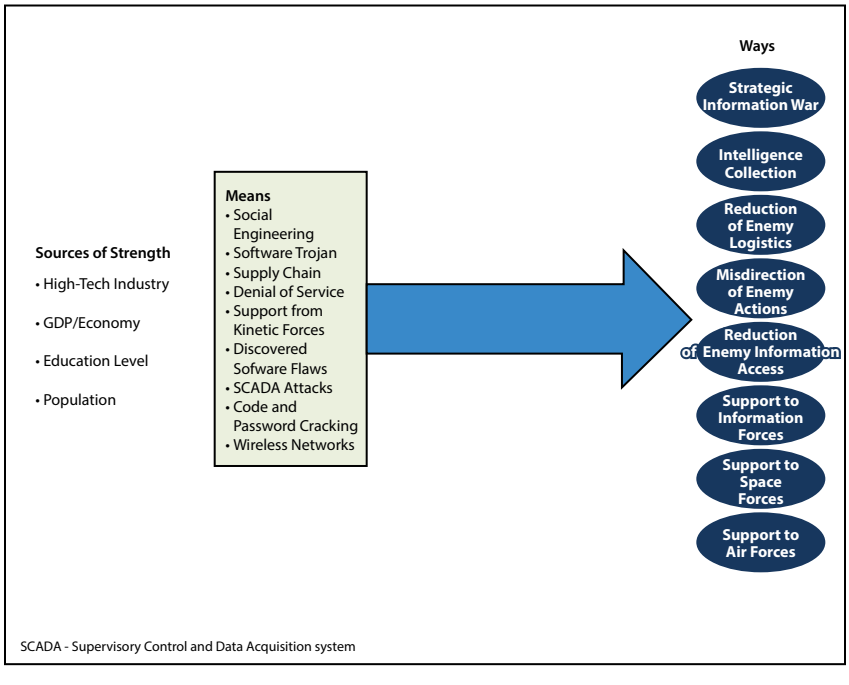

Figure 4. The means and ways of cyberspace superiority

Cyber Means

A nation's cyberspace sources of strength produce the capabilities or means currently available in cyberspace. By means of social engineering, the attacker convinces users to unknowingly take some action that lets him into the system. He can also develop software "Trojan horses" or strike an enemy supply chain where some sort of access port or capability is manufactured into either the software or hardware used by the defender. Additionally, the enemy may utilize denial-of-service attacks, overwhelming a defender's systems with so many false requests for information that they cannot function effectively. He may physically take apart an information system by some kinetic means, whether a Joint Direct Attack Munition dropped by a fighter or a pack of C4 plastic explosive delivered by a special operator. Cross-domain effects can proceed both from the physical world to cyberspace and vice versa. Discovered software flaws are the "crown jewels" of any attacker's arsenal because they allow him to develop specific strikes to gain access and carry out his intent. Such flaws are useful in inverse relation to the information technology community's familiarity with them. Generally, defenders can quickly produce a patch for a widely known problem and begin to close the attacker's window of opportunity. It normally does not close completely since many users and system administrators fail to patch their systems properly, but conducting an attack becomes much more challenging.

A special category of cyber attacks targets Supervisory Control and Data Acquisition systems, which operate infrastructure such as power plants, dams, water-treatment facilities, and so forth. Alarmists usually cite these systems when they want to make apocalyptic predictions of cyberspace attacks to generate funding from Congress. In theory, such a strike could shut down almost any modern system. Depending on the specific system under attack, sometimes an adversary can do far more damage than he can by simply turning something off that the defender can immediately turn on again. For example the Stuxnet worm, which can carry out a very sophisticated assault on a control system,

allegedly caused the physical destruction of components while reporting that all was well to the system's engineers.[10] Further, code and password cracking can facilitate entry or retrieve information, and wireless networks provide another potential port of entry for attackers—even into "air-gapped" systems (those not directly plugged into the broader Internet).

Cyber Ways

These means can accomplish a number of different ways in pursuit of strategic end states. First, an attacker can use them in strategic information warfare, during which a nation uses cyberspace to directly attack centers of gravity. According to Maj Eric Trias and Capt Bryan Bell, "The goal of strategic attack is to apply force systematically against enemy centers of gravity in order to produce the greatest effect for the least cost in dollars and lives."[11] Just as bombers strike a city to punish civilians and convince them to pressure their government to change its policy, so would a cyberspace attack inhibit or destroy the infrastructure of a city in an attempt to produce the same effect.

The majority of cyberspace intrusions by nation-states during peacetime appear focused on intelligence gathering and cyber espionage, which also has great importance during a conflict. Examples include breaking into an enemy's system to read his war plans or check on the readiness of his forces or capabilities.

Attackers can choose to launch their assaults against enemy logistics systems. Modern militaries rely on their information systems for logistical support; because multiple users in various locations must access these systems, they are often on unclassified networks and open to attack. Misdirection that sends supplies to the wrong places, changes inventory information, or alters timetables could have a tremendous impact on a campaign, particularly if the enemy relies heavily upon moving large numbers of forces a great distance in a short period of time. Obviously, the United States is especially vulnerable in this area.

Reducing the enemy's access to information will lessen the effectiveness of his forces. A more subtle approach involves misdirecting him and shaping his actions by altering his picture of what is happening around him. This technique can include false information, but the availability of multiple sources of data can hinder its success. Such an approach generally works best when it reinforces something the enemy is inclined to believe anyway—witness the operation to convince Hitler that the Allies would land at Calais, not Normandy. Rather than use false data, these attacks can employ technically true information to build a misleading picture. The attacker seeks to shape the decision space around the enemy to make him more likely to do something he wants him to do.

Cyberspace also provides critical support to all of the other warfighting domains.[12] For instance, a cyberspace attack could fool an enemy's integrated air defense system into not seeing an airborne strike package or could disable his space jamming system. As is the case with airpower, though, the enemy probably will not endure these actions passively but will try to block them (fig. 5).

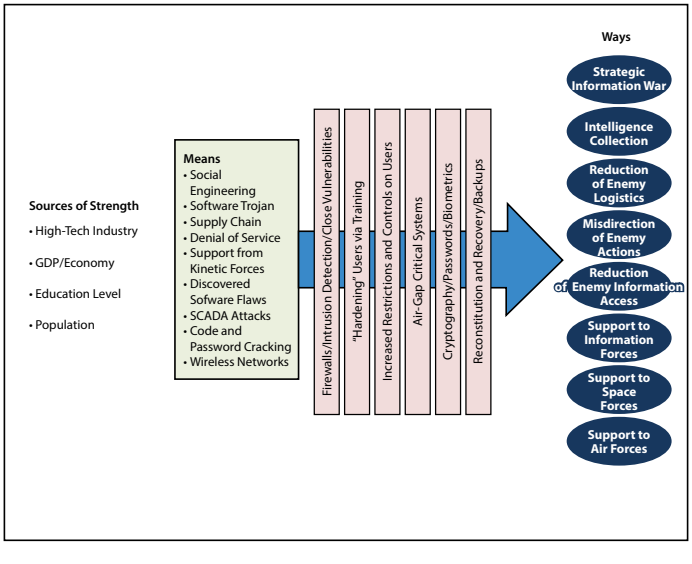

Figure 5. The means and ways of cyberspace superiority with defensive blocks

Cyber Defensive Blocks

Defenders can utilize a number of methods to protect themselves from cyberspace attacks. One of the most common entails preventing unauthorized access by installing firewalls, intrusion detection, and authentication systems. Closing known vulnerabilities is also critical since many systems do not have the latest patches.

Users are the bane of system administrators the world over, and many attacks rely on finding individuals who can be tricked into doing something that they should not. Because most users have only a rudimentary knowledge of computer security, the time and money spent on training them can produce a significant payoff.

Systems administrators can also decrease the risk posed by users by increasing restrictions and controls, but reducing connectivity can come at a substantial cost. Information systems exist to process and share information; if overzealous administrators can be convinced to shut off systems from the outside world, they may give the attacker exactly what he wants because such an action significantly reduces capability. Defenders must find the right balance between access and security so that they can avoid doing the attacker's work for him.

Moreover, defenders can air-gap (disconnect) systems from direct access to the Internet—an appropriate action for highly sensitive and critical systems such as those associated with nuclear weapons. Air-gapping offers no guarantee against attack, however, since a clever adversary may find other methods of access. Options include physical access to the system, enabled wireless-networking capabilities, and mistakes by users who inadvertently connect the air-gapped system into the wider Internet.

A system may also continue to use the backbone of the Internet while relying on encryption to keep information out of unfriendly hands. The use of passwords is standard practice now on most systems as a means of denying attackers access to them. Furthermore, if imple-

mented properly, biometric identification or token identification such as common access cards can help keep intruders out of systems.

A final way of blocking attackers makes use of backups and resiliency. Despite the media attention given to major worms such as Melissa or Slammer, most information technology operations recovered fully in a couple of days.[13] An attacker who penetrates all defenses and completely erases the data in a logistics system can cause severe problems for defenders. If the latter have a backup on removable media that the attacker did not know about or could not access and if they can have the system up and running in a day, then the effects of the strike may prove minimal. The completed cyberspace superiority model illustrates several methods that the attacker can use to reduce the effectiveness of these attempted blocks (fig. 6).

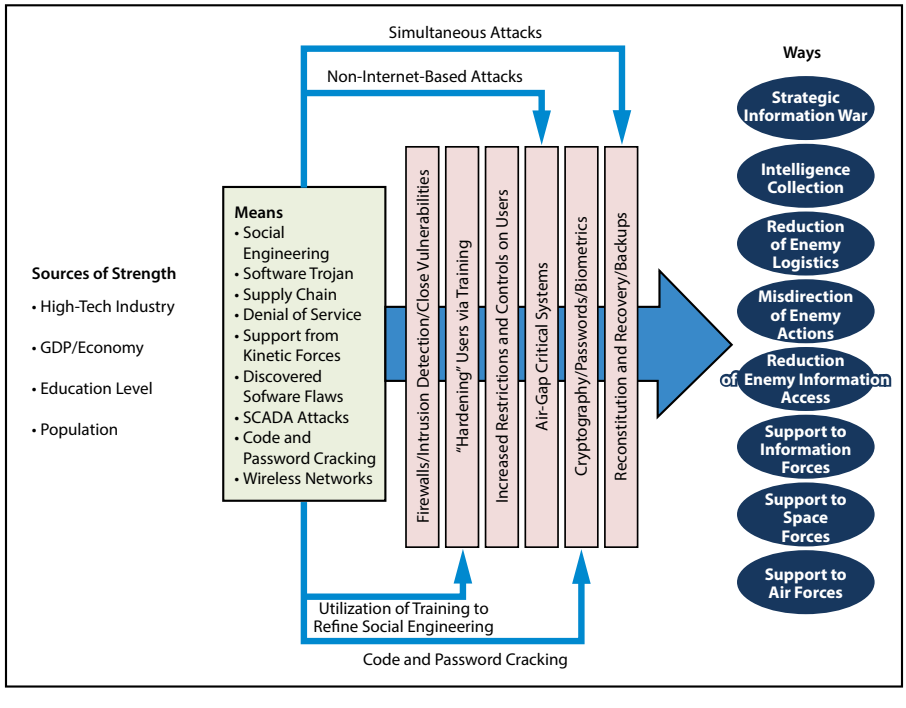

Figure 6. Cyberspace superiority model

Cyber Attackers' Counters to Defensive Blocks

If the enemy carefully examines the defender's training program, he can refine his social engineering to focus on methods not covered in the training or on those similar to training examples deemed acceptable. Just one user making a mistake can open a window of opportunity. Adversaries can use non-Internet-based attacks to access air-gapped systems—perhaps by way of a wireless modem inadvertently left out or turned on, insertion of malicious code in the defender's supply chain, or physical access to the system through espionage or special operations. Moreover, code and password cracking can defeat encryption, particularly if a clever attacker finds a technique to access the encryption keys so that he does not have to resort to brute force. Finally, an adversary can use simultaneous strikes to go after backup as well as primary systems to prevent easy copying of data as a means of protection. Although Internet hoaxes about viruses that can melt computers into a puddle of goo are overstated, it may be possible to attack the hardware itself and thus increase the amount of time necessary to recover functionality.

This model will not remain static; rather, it will change with newly developed techniques and procedures. As with the airpower model, new technology will produce new capabilities for both the offense and defense. Each side maneuvers in relation to what the other does, and Clausewitz's wrestling match will continue.

Measurement of Cyberspace Superiority

Testing of the proposed model requires specific metrics, such as those developed by US Joint Forces Command (fig. 7). In the figure, the lower levels feed into the higher ones, and it is important to note the possibility of multiple indicators for each measure of effectiveness (MOE), multiple MOEs for each effect, and multiple effects for each objective. Further, depending on the situation, there may be only one effect per objective, and so forth.

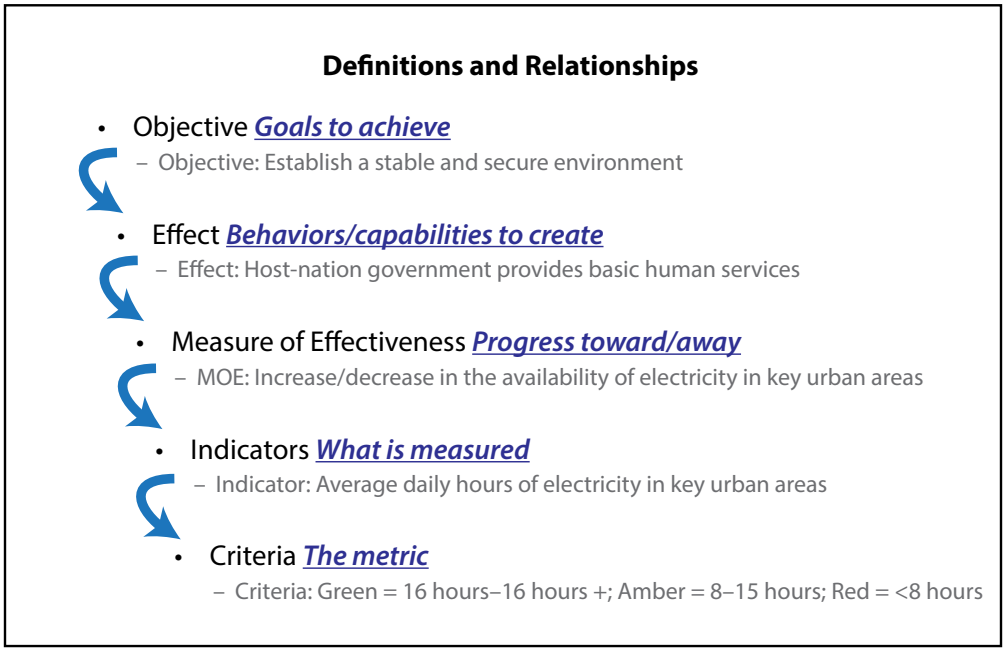

Figure 7. Effects component summary. (Adapted from Department of Defense, US Joint Forces Command, "Tactics, Techniques, and Procedures: Assessment of Joint Operations," 10 March 2008, I-6, fig. I-3.)

Cyberspace superiority will be local and transient. In accordance with the definition in AFDD 3-12, mentioned previously, when a friendly force can "conduct operations at a given time and in a given domain without prohibitive interference," it has attained cyberspace superiority. Such superiority is not global and comprehensive; it is relative to what the attacker in a conflict attempts to accomplish. In the cyberspace model suggested in figure 6, the objective or goal is the way that the attacker seeks. For example, an adversary might want to reduce his enemy's logistical capability by producing the desired effect of immobilizing the enemy's armored forces due to a lack of supplies. The attacker's corresponding MOE could involve a change in the supply status of enemy armored divisions, indicated by the level of supply possessed by specific divisions in the regular categories of supply. The following could serve as a metric for an attacker: for a specific enemy

division, green represents fuel reserves of 24 hours or fewer; amber, 24–72 hours; and red, more than 72 hours.

The cyber component in the above example could entail a concentrated attack on the enemy's computerized logistical system to misdirect fuel away from the divisions that the attacker intends to engage. This overly simplistic example illustrates several important issues with measuring cyberspace superiority. First, an attacker probably would not rely solely on cyberspace strikes to decrease the enemy's fuel supply but use other kinetic means as well. The fact that the armored division is out of fuel does not mean that cyberspace operations are responsible. Perhaps the attacker also wrecked bridges, hit fuel dumps, and destroyed the defender's fuel trucks. Since combat situations are not repeatable, it is not possible to run a campaign, note the outcome, and then reset and conduct the same campaign again without utilizing cyberspace attacks to determine whether a difference exists.

Applying the Model

The cyber attack on Aramco, which occurred in 2012, offers an example of how we can apply this model to a real case. Some of the details remain murky and highly classified by the various governments involved, but open-source literature includes sufficient information to justify an examination of this incident. According to the *New York Times*, the attackers—who claimed to belong to an activist group called the Cutting Sword of Justice—were attempting to shut down Aramco's production of oil and natural gas.[14] US intelligence officials, however, maintain that Iran orchestrated the attack in retaliation for the Stuxnet attack on its nuclear program.[15] In the cyberspace superiority model, the attacker's way involved the use of strategic information warfare and cyberspace attack to directly affect a physical target. Evidently, the selected means called for social engineering and a "spear phishing" attack.[16]

More specifically, the attacker sought to shut down Aramco's production of oil and natural gas and wished to produce the desired effect of halting its production. The MOE was a change in that production, indicated by the amount of oil and natural gas produced by Aramco. Although we do not know the attacker's criteria, we can use the following example: less than 50 percent production = green, 50–75 percent = amber, and 75–100 percent = red. In this case, it is easy to determine whether or not the attacker attained cyberspace superiority because despite affecting 30,000 computers, the strike did not reduce production at all.[17] By utilizing the cyberspace superiority model, we can clearly see why the attack proved unsuccessful. Specifically, because Aramco segregated its office computers from those that controlled oil and gas production, the attack could not get past the air gap. Figure 8 illustrates the elements of the Aramco cyber attack and the successful block.

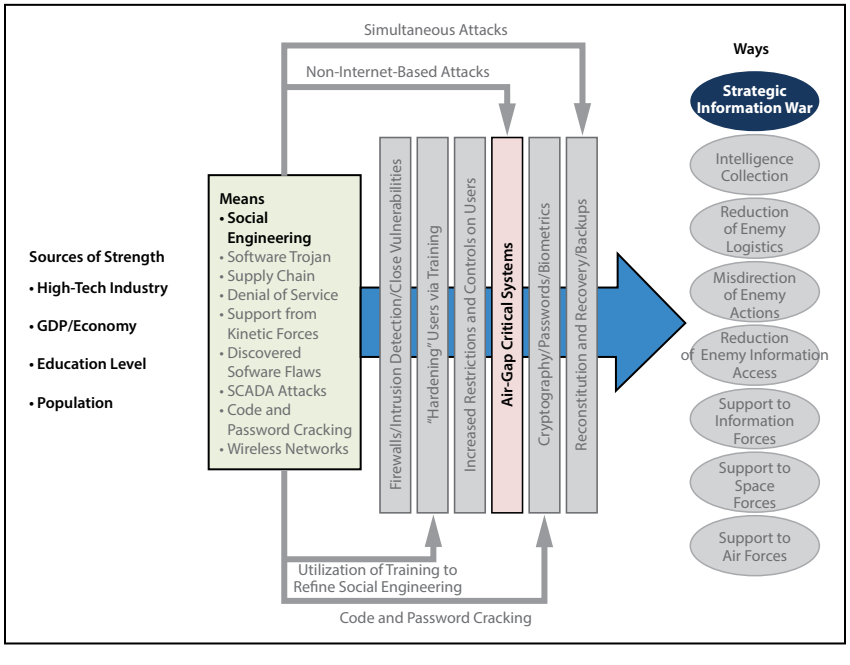

Figure 8. Aramco cyber-attack elements of the cyberspace superiority model

In this case, a successful defense prevented the attacker from attaining cyberspace superiority. This is not to say that the strike accomplished nothing at all; indeed, it inflicted a tremendous amount of damage on Aramco's systems and increased uncertainty in the Middle East. However, the attacker did not realize his stated goal of shutting down the production of oil and gas and thus could not execute operations in cyberspace without prohibitive interference.

Conclusion

This proposed model can be used to analyze cyber attacks, defenses, and the interactions between the two across multiple different types of cyber assaults. Though useful, without careful application, the model could become merely a backwards-looking measurement that includes elements of battle damage assessment and lessons learned. What we did yesterday is important—but mostly as a jumping-off point to assess what we can do tomorrow. Commanders want to know how much cyber superiority they have today, whether it is enough to do what they need to do tomorrow, and, if not, how they can get more. The proposed model can help answer these questions if we apply it deliberately in a forward-looking manner. If an air gap blocked yesterday's attacks, what can we do to find a way around that obstacle? If today's attack succeeded but the avenue became compromised and the defender has now closed it, do we have another path for tomorrow's attack? We must also add up the results across multiple objectives. If a commander has eight missions to carry out but expects success in two of them, that is not cyberspace superiority because the enemy is producing prohibitive interference. The model offers a structured way to think about superiority in the cyber domain that can help identify opportunities and risks which enable cyber warriors to better posture themselves for success.

War gamers can also use it as a template in both gaming and exercises to model the environment, as can commanders interested in looking at the defensive end of the model. Although this article em-

phasized cyber attack, defenders can just as easily apply the model to look at their plans to determine where they could strengthen them, always bearing in mind that the enemy will meet every action with a reaction.

The real utility in the proposed model is not that it will inform defenders that they need firewalls or alert attackers to software flaws. Everyone already has a good grasp of these concepts. Not as well understood, however, are the dynamic interactions between the various elements of cyberspace attack and defense. Clausewitz's wrestling match continues into cyberspace. This is where the proposed model has the most utility, and even though it will undoubtedly require refinement over time, it offers a useful framework for understanding the dynamics of cyberspace superiority. ✪

Notes

1. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 141, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.
2. Air Force Doctrine Document 3-12, *Cyberspace Operations*, 15 July 2010 (incorporating change 1, 30 November 2011), 2, http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-12/afdd3-12.pdf.
3. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 16 July 2013), 115, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
4. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.
5. Ibid., 7.
6. David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 185.
7. Clausewitz, *On War*, 149.
8. Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Dulles, VA: Potomac Books, [2009]), 256.
9. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 5.
10. Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, 15 April 2011, 2, http://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf.

11. Maj Eric D. Trias and Capt Bryan M. Bell, "Cyber This, Cyber That . . . So What?," *Air and Space Power Journal* 24, no. 1 (Spring 2010): 91, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj10/spr10/aspj_en_2010_1.pdf.

12. Shawn Brimley, "Promoting Security in Common Domains," *Washington Quarterly* 33, no. 3 (July 2010): 122, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA536657.

13. Libicki, *Conquest in Cyberspace*, 37.

14. Reuters, "Aramco Says Cyberattack Was Aimed at Production," *New York Times*, 9 December 2012, http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0.

15. Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, 23 October 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.

16. Wael Mahdi, "Saudi Arabia Says Aramco Cyberattack Came from Foreign States," *Bloomberg,* 9 December 2012, http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html.

17. Ibid.

Lt Col William D. Bryant, USAF

Lieutenant Colonel Bryant (USAFA; MA, American Military University; MA, George Washington University; MSS [Master of Space Systems], Air Force Institute of Technology; MAAS [Master of Airpower Art and Science], School of Advanced Air and Space Studies) is a student at the Air War College at Maxwell AFB, Alabama. A former operational support squadron commander and director of operations, he has served on numerous operational and staff assignments. As a career fighter pilot, Lieutenant Colonel Bryant has more than 1,500 hours in the F-16.