Chief of warfighting integration and chief information officer for Office of Secretary of Air Force discusses cyber security during seminar at Barksdale Air Force Base (U.S. Air Force/Chad Warren)

Cyber Power in 21st-Century Joint Warfare

By E. Lincoln Bonner III

> *For, in war, it is by compelling mistakes that the scales are most often turned.*
>
> —B.H. Liddell-Hart
> *Strategy: The Indirect Approach* (1941)

Lieutenant Colonel E. Lincoln Bonner III, USAF, is Director of Operations at the Space Operations Squadron Aerospace Data Facility–Colorado.

In 2008, Russian military forces, supported by cyber attacks, rapidly defeated opposing Georgian forces and seized territory later traded in exchange for Georgia's granting greater autonomy to pro-Russian governments in South Ossetia and Abkhazia. *Cyber power* is the ability to exploit cyberspace to create advantages and influence events, and *cyberspace* is the interdependent and interconnected networks of electronics and the electromagnetic spectrum where information is created, stored, modified, exchanged, and exploited.[1] The 2008 Russia-Georgia war marks the only public incidence of cyber power integrated with traditional kinetic military operations. To date, however, little attention has been paid regarding how to integrate cyber power into conventional military operations. Rather, research has tended to focus on the independent use of cyber power for espionage and as a means of strategic attack to punish and/or compel a state to do one's will.

This article addresses this research gap by focusing on how cyber power can best be integrated into joint warfare to fight and win the Nation's wars. Using the Russia-Georgia war as an illustrative case, this article argues that the principal value of integrating cyber power into a joint military campaign is that it compels the enemy to make mistakes by performing three main warfighting tasks: reconnaissance, superiority, and interdiction. It begins with a description of how cyber power's main warfighting tasks support kinetic operations by degrading/disrupting the enemy decision cycle. The cyber aspects of the Russia-Georgia war are then analyzed to show how pro-Russian forces employed cyber power to degrade the Georgian decision cycle in support of kinetic military operations. Finally, implications for present and future integration of cyber power into joint warfare are discussed.

Reconnaissance, Superiority, and Interdiction

Cyber power has evolved similarly to early airpower and will likely make contributions to joint warfare now and into the foreseeable future, namely to conduct cyber reconnaissance, gain and maintain cyber superiority, and conduct cyber interdiction.

In World War I, the advantages of aerial reconnaissance gave birth to the battle for air superiority. Aerial reconnaissance "warned of any movement or change in the enemy camp, and with few exceptions it foretold the enemy's offensive and helped guarantee that it would fail."[2] As a result, the requirement emerged to gain and maintain air superiority, thereby securing the information advantage flowing from aerial observation. Despite its value to effective land operations, aerial reconnaissance could not directly degrade or defeat enemy operations.

In the same manner, cyber power's military development can trace its roots to reconnaissance. As the recent Mandiant report about Chinese cyber espionage highlights, much of the impetus to develop cyber power arises from the advantage that accrues to the side that can conduct more effective cyber reconnaissance operations.[3] In turn, effective cyber reconnaissance and the information advantage that comes with it depend on possessing at least a degree of cyber superiority. Like airpower, cyber reconnaissance and cyber superiority can make friendly operations more effective, but they cannot directly degrade or defeat enemy operations.

In 1936, 18 years after World War I ended, Sir John Slessor of the Royal Air Force described how airpower could be integrated with land operations to directly and substantially degrade or defeat an adversary's warfighting capability in airpower and armies. Using evidence from British military operations in the Middle East, Slessor deduced that in addition to aerial reconnaissance, airpower's main warfighting tasks in a joint air-land campaign were to gain and maintain air superiority and to interdict enemy land lines of communication and supply. Air superiority continues to provide friendly forces with the ability to exploit airpower for reconnaissance, mobility, and attack without prohibitive enemy interference.[4] Air interdiction destroys or interrupts those elements of an enemy's system of supply or communication for a sufficient time that the degradation will immediately or in due course prove fatal to his continuance of effective operations.[5]

Cyber superiority and cyber interdiction can also be described in terms akin to air superiority and air interdiction. Cyber superiority provides friendly forces with the ability to exploit cyber power for reconnaissance, communication (that is, information mobility), and attack—in addition to orientation (that is, information/computer processing) and command and control—without prohibitive interference by the enemy. Cyber interdiction interrupts, destroys, or otherwise neutralizes electronic information lines of communication and electronic information systems of supply (that is, cyberspace) used by enemy land, sea, air, and space forces for a sufficient length of time that they will immediately or in due course prove fatal to his continuance of effective operations. Unlike today, World War II bombers lacked the precision attack capability to substitute for the lethality of land forces to destroy an enemy army. Hence airpower's primary offensive contribution was air interdiction. Like air interdiction in Slessor's time, cyber interdiction is the principal contribution of cyber attack operations in joint warfare today.

In the air and cyberspace domains, offensive operations to destroy or neutralize the adversary's air and cyber forces are the primary means of establishing superiority within each domain. Cyber reconnaissance, however, plays a much greater role in gaining cyber superiority than aerial reconnaissance plays in establishing air superiority. At the tactical level in cyberspace, the speeds of action and of observation both approach the speed of light. In other words, cyber defenders do not have the benefit of the warning time that observation at the speed of light via radar gives air defenders. Consequently, tactical defenses are unlikely to have sufficient warning to react against a cyber attack and prevent significant negative effects. Tactical defense in cyberspace is more akin to battle damage repair, recovery, and reconstitution than to any analogous effort to parry a physical blow. Effectively defeating cyber attacks thus largely depends on fielding a set of defensive measures that one knows in advance an adversary cannot overcome. That is, the most effective way to achieve cyber superiority is to field cyber defense and cyber attack capabilities that render potential corresponding enemy cyber attacks and defenses impotent a priori. The critical requirement for neutering potential

Marines monitor aircraft and ground troops for information to pass to combat elements, Operation *Javelin Thrust* (U. S. Marine Corps/ Chelsea Flowers)

enemy cyber attacks and defenses without known precedents, and thus the key to cyber superiority, is technical intelligence about enemy cyber attack and defense capabilities, as well as tactics, techniques, and procedures. Although all-source intelligence contributes to developing this foreknowledge, the principal way of gathering the requisite intelligence is cyber reconnaissance. Unlike orders of battle, cyber capabilities only exist in cyberspace and cannot be observed except from within cyberspace. Thus, those who win the cyber reconnaissance competition in peacetime will likely win the battle for cyber superiority in wartime.

To gain and maintain cyber superiority, peacetime cyber reconnaissance operations should prioritize intelligence about enemy cyber reconnaissance and attack capabilities (for example, enemy malicious code development), followed by enemy cyber defense capabilities. With intelligence about these activities, one can develop and field cyber defenses that negate adversary cyber attacks prior to their use as well as develop cyber attack capabilities impervious to enemy cyber defenses. Possessing cyber attack capabilities that are relatively impervious to anticipated defenses is a critical requirement for cyber interdiction. The kinetic corollary to this set of cyber reconnaissance activities might be more commonly described as intelligence preparation of the battlespace. Therefore, it is during the intelligence preparation of cyberspace, which should be constantly ongoing during peacetime, when cyber superiority is won or lost.

Cyber interdiction is made possible by, and complements, cyber superiority. Interdiction in general is a network warfare concept applicable to any domain. An electronic information network is simply a transportation network, but rather than physical supplies, information is the commodity. The objective of any transportation network is to deliver accurate, relevant, and timely supplies (that is, the right stuff to the right place at the right time)—or information in the case of cyberspace.[6] Regardless of whether an interdiction campaign chooses to target a network's capability to deliver supplies with accuracy, relevancy, or timeliness, the objective is the same: to introduce friction and uncertainty into the decision cycle so it becomes increasingly difficult for the enemy to conduct effective operations in comparison to friendly forces. Interdiction is not about the impact of any one attack on an enemy network, but rather the cumulative effects of a stoppage.[7]

A successful interdiction campaign accounts for a network's capacity—how much (flow volume) and how fast (flow rate) supplies can travel through the network to meet user demand. In air interdiction campaigns, air attacks and land operations complement each other to overwhelm the enemy's supply network.

Air attacks destroy, disrupt, or degrade nodes and links in the enemy's land transportation/supply network (for example, rail and roads), reducing its capacity. Simultaneously, land combat operations create demand for a high volume of supplies to flow through the network at a high rate. Land combat operations place timeliness requirements on an enemy's supply network that air interdiction prevents the network from meeting. For example, when combat was at a fever pitch in the phase of the Korean War spanning the Inchon Landing to China's entry, both sides consumed supplies voraciously, demanding a high volume and a high rate flow from their respective networks. However, the North Korean army had to rely on a low capacity rail and road network to meet its tremendous needs. American air interdiction ensured that North Korean forces could never accumulate enough supplies or resources in sufficient time to mount a successful counterattack, and U.S. forces rapidly moved north to the Yalu River. At precisely the time when the enemy needs the most from its supply network, interdiction makes it capable of providing the least.

A cyber interdiction campaign—where cyber interdiction is the destruction, disruption, or degradation of nodes, links, and data in an enemy information network to interrupt it and reduce its capacity—functions similarly to an air interdiction campaign, with one critical exception. Unlike air interdiction, cyber interdiction can make portions of cyberspace inaccessible for other operations such as reconnaissance. Air attacks do not prevent the use of the air domain for mobility and reconnaissance. Because cyberspace is composed of information networks, cyber interdiction, which by definition will disrupt enemy information networks, will probably hinder the ability of cyber reconnaissance to gather intelligence data from targeted networks. As a result, tension exists between cyber interdiction and cyber reconnaissance.

If one anticipates a long conflict, or if use of a specific cyber attack in one conflict would significantly decrease one's cyber advantage in more vital potential contingencies, one should favor the decision advantage created by cyber reconnaissance over cyber interdiction. For example, the United States in World War II, in what it anticipated to be a long conflict, protected the information advantage it gained from breaking German and Japanese encryption rather than taking actions that might compromise this invaluable intelligence source. This critical intelligence advantage allowed U.S. forces to decimate Japanese convoys as well as choose the time and place of battle in a war that lasted more than 3 years.[8] Commanders going forward must weigh the costs and benefits of sacrificing intelligence gained from cyber reconnaissance over the long term against the effects created by cyber interdiction in the near term.

Cyber interdiction compels an enemy to make a mistake. Like the complementary relationship between air interdiction and land operations, high intensity kinetic operations create information demands that can overwhelm an information network whose useful capacity has been reduced by cyber interdiction. To limit the effects of cyber interdiction, an opponent could concentrate his information supplies, which would place them at greater risk for destruction from cyber or kinetic attack. Additionally, cyber attacks that alter, reroute, or delay data present a choice to an opponent. If a cyber attack alters or reroutes an enemy's data, he can act on the information he has, increasing the likelihood that he will make a mistake, or submit additional requests in an attempt to acquire the missing data, thus reducing his network's useful capacity and hindering timely information development. If he chooses the latter, he will compound the effects of cyber attacks that add extraneous data into the network, further impeding timely information development and potentially depriving him of new information altogether. Cyber interdiction thus compromises an enemy's decision cycle by placing him on the horns of a dilemma. Should he yield superiority in decision speed or yield superiority in decision quality? Either way the cumulative effect of yielding decision superiority over time will inevitably lead to mistakes.

Cyber Power in the 2008 Russia-Georgia War

The 2008 Russia-Georgia war helped focus attention on cyber power and its utility in war in a way that previous cyber power uses had not. That conflict's high profile caused it to become the subject of much study, so it is a rich source of information for analyzing the dynamics of cyber power in a joint military campaign.

Following Georgian independence in 1991, secessionists seeking to remain part of Russia seized control of the majority of Abkhazia and portions of South Ossetia before cease-fire agreements were reached in 1992 and 1994.[9] These conflicts remained unresolved and formed the roots for the 5-day war between Russia and Georgia in 2008.[10]

On the surface, cyber power would not appear to be particularly useful in a war with Georgia. Only 7 percent of the citizens used the Internet daily,[11] which might cause one to overlook Georgia's critical cyber vulnerability—more than half of 13 connections to the outside world via the Internet passed through Russia, and most of the Internet traffic to Web sites within Georgia was routed through Turkish or Azerbaijani Internet service providers, many of which were in turn routed through Russia.[12] Georgia's Internet infrastructure suffered from a dearth of internal connections known as Internet exchange points.[13] Consequently, a Georgian user's request for a Georgian Web site would likely be routed through Russia, analogous to having to travel through Mexico to get from Los Angeles to San Francisco.[14] As a result, pro-Russian forces could employ cyber power to affect a large percentage of Georgia's access to, and use of, the portion of cyberspace known as the Internet. Lacking control of the infrastructure required for external or internal Internet use, Georgia could neither disperse network traffic nor cut Internet connectivity from abroad as defensive measures without ceding the cyber advantages of Internet access if the state came under cyber attack.[15]

The Russia-Georgia war officially started on August 7, 2008, after

Georgian military forces responded to alleged Russian provocation with a massive artillery barrage on the town of Tskhinvali in South Ossetia.[16] Moscow seized the opportunity to further solidify South Ossetia's and Abkhazia's independence from Georgia. It immediately deployed troops to South Ossetia and initiated aerial bombing raids on Georgian territory. It also deployed its navy to blockade the Georgian coast and landed marines on the coast of Abkhazia. After Russian mechanized forces and South Ossetian militia defeated the lightly armed Georgian military around Tskhinvali, they invaded Georgian territory uncontested.[17] Georgia was not able to offer even a modicum of additional resistance because of the advantage cyber power created for the Russian forces.[18]

The concentration and advanced preparation of cyber attacks in the war suggest that cyber superiority and cyber interdiction operations against Georgia were the product of cyber reconnaissance and intelligence preparation of cyberspace well in advance of the conflict. The cyber interdiction campaign against Georgia included both Web site defacements and distributed denial of service (DDoS) attacks. The botnet assault was precise in scope and concentration, never exceeding 11 targets, and the same Web sites continued to be attacked throughout the war.[19] Most of the cyber attacks were customized for Georgian targets with at least one Web site defacement prepared more than 2 years prior to the conflict.[20] The cyber attacks were also sophisticated in their targeting. Government and news media Web sites were struck first, helping sow confusion by hindering Georgians and their officials from determining what was actually happening and delaying any international response. In addition to Georgia's two major banks, cyber attacks targeted commercial entities that could have been used to communicate or help coordinate a response to Russian forces writ large and the cyber attack specifically.[21] The concentration of botnet cyber attacks on 11 targets, the years-long cyber attack development, and the sophisticated appreciation of how Georgia would likely use the Internet to operationally respond all indicate that the cyber superiority the pro-Russian cyber forces held over Georgia was the product of excellent preconflict cyber reconnaissance and intelligence preparation of cyberspace.

To assert cyber superiority, pro-Russian cyber forces suppressed Georgia's cyber defenses through diversion and direct attack. Educational institutions devoted to science, technology, and medicine were among the initial 11 botnet cyber targets struck.[22] At the time, Computer Emergency Response Team Georgia (CERT Georgia) was chartered solely to provide cyber security for higher education institutions within the Georgian Research and Educational Networking Association (GRENA).[23] By attacking educational institutions, cyber attackers focused CERT Georgia on its charter mission of protecting GRENA's cyberspace and away from responding to the larger national crisis. By attacking what the opponent must succor—the GRENA—pro-Russian cyber forces used CERT Georgia's natural response against it to divert and suppress the state's best cyber defenses. Also, a popular Georgian Internet hacker forum was among the initial 11 cyber attack targets, impeding some of Georgia's more capable cyber experts from coordinating an organized response.[24] Pro-Russian forces achieved cyber superiority using the method Slessor described to gain command of the air—through disruption, dislocation, and disorganization of the opposing force.

Pro-Russian cyber power maintained cyber superiority throughout the conflict, and as a result Georgia never mounted a successful cyber defense or cyber counterattack. For example, Georgia attempted to maneuver around the cyber attacks by filtering them out based on their origin (that is, their originating Internet protocol [IP] address). However, the cyber attackers' intelligence preparation allowed them to easily defeat this tactic. Cyber attackers routed their assault through foreign servers to mask their real IP addresses and created false IP addresses to spoof Georgia's cyber defense filters.[25] Still, Georgia preserved the use of some government Web sites by moving them to U.S.-based servers.[26] Despite the failure of Georgia's cyber defense, it did attempt at least one major counterattack, but it also failed. Georgia posted cyber attack tools and instructions in Russian-language Internet forums to deceive pro-Russian cyber forces into unwittingly attacking Russian Web sites instead of Georgian sites.[27] This Georgian counterattack appears to have had a negligible effect on the Russian Web sites targeted.[28] Overall, the cyber defense efforts were too little too late.

With cyber superiority in hand, pro-Russian forces used cyber interdiction to choke Georgian communications by leveraging the generic properties of transportation networks. After the first wave of botnet cyber attacks on the initial 11 targets, an ad hoc cyber militia joined the assault. Cyber attack tools and a list of suggested targets were posted on Web sites for Russian supporters to launch their own strikes. The instructions were simple enough for people with limited computer skills to follow. This ad hoc cyber militia was so effective that it shut down or defaced 43 Web sites beyond the 11 original botnet targets.[29] In total, 54 Georgian Web sites related to communications, finance, and government were struck, and Georgians could not access these sites for information or instructions.[30] The cyber attacks thus denied Georgian forces access to a key portion of their information network, the Internet, reducing their overall information network's useful capacity.

As a result, the cyber attacks dislocated Georgian data flows, shunting data that normally would have traveled over the Internet into more traditional conduits such as telephone and radio communications. Additionally, land, sea, and air combat operations created a dramatic spike in the data volume and data rate demands on Georgia's overall information network. For example, in the town of Gori, government and news Web sites were disabled with DDoS attacks just prior to a Russian air attack, which would predictably drive information demands up.[31] A subsequent spike in information communication demands combined with the dislocation of Internet communications to more traditional

Marine F/A-18 Hornets escort F-35 Lightning II to Eglin Air Force Base, Florida (U.S. Air Force/Joely Santiago)

forms—such as cell and land phones—appear to have created a bottleneck.

Georgians were trying to transmit more data at a higher rate than the useful capacity of their information network could accommodate because a large proportion was being consumed by cyber attacks injecting extraneous data into the network. The cyber attacks effectively jammed Georgia's overall information network during the early stages of the war when rapid and organized action by Georgian defenses, cyber and kinetic, could have had the greatest impact.[32] Cyber interdiction created a Russian military advantage at the operational and tactical levels by hindering the Georgian military's ability to organize and conduct effective operations to thwart kinetic Russian military operations. Cyber interdiction created conditions such that Georgian forces could not help but to act mistakenly.

Furthermore, cyber interdiction likely multiplied the effectiveness of cyber attacks conducted to achieve cyber superiority by interfering with CERT Georgia's ability to gain situational awareness and orient itself to more effectively respond. Slessor describes the problem of air superiority as "how to deprive the enemy the ability to interfere effectively by the use of his own air forces."[33] Because all Georgian information communications were essentially jammed by the cyber interdiction attacks, CERT Georgia would have had an extremely difficult time simply gathering enough data to understand the cyber attacks' effects, much less mitigate them. By jamming all Georgian communications, cyber interdiction not only interrupted Georgia's traditional military response but also likely stifled Georgia's cyber defenses, prolonging pro-Russian cyber superiority.

In that war, cyber attacks for cyber superiority and cyber interdiction were mutually reinforcing. The result was a situation where Georgian communications—its system of information supply—were gummed up, preventing timely delivery of data and commands to Georgian forces. The Georgians had to choose whether to yield superiority in decision speed or decision quality. The effect with either option was an unqualified Russian military advantage that Georgia could not overcome.

Implications

As in the early days of airpower, cyber power today is critical to victory, but it probably cannot win wars alone if for no other reason than its inability to create much violence, although this shortcoming will likely fade in the future. Consequently, it is imperative to understand how best to employ cyber power in concert with land-, sea-, and airpower. Airpower theory suggests two principles to guide cyber power strategy at the operational level: securing the enemy's freedom of action, and confronting him with a choice between at least two bad options. Cyber superiority satisfies the first principle, while cyber interdiction satisfies the second. The example of the 2008 Russia-Georgia war demonstrates the truth of these principles, but how should one go about gaining and maintaining cyber superiority and conducting cyber interdiction?

With securing cyber superiority being the first priority for military cyber power, initially focusing on neutralizing the adversary's capability to prohibitively interfere with friendly operations via cyberspace seems most logical. Consequently, the enemy's cyber attack, cyber reconnaissance, and cyber defense capabilities should be among the highest priority targets for cyber reconnaissance and all-source intelligence preparation of cyberspace, as well as among the highest priority targets for suppression or destruction (via cyber or kinetic attack) once hostilities begin. Second, cyber attacks directed at those portions of cyberspace irrelevant to the war but which an opponent must succor, such as the cyber attack on the GRENA that diverted CERT Georgia from the larger conflict, are valuable in that they focus the enemy's cyber defense forces away from decisive points. Third, cyber attacks should be used to interdict data required by enemy cyber repair, recovery, and quick reaction defense forces to disrupt the adversary's ability to effectively parry cyber strikes. Together, these actions should neutralize, divert, and disorganize an opponent's cyber power to gain and maintain cyber superiority.

Cyber interdiction targets are the next most important cyber objectives in joint military operations, first at the operational level and then the tactical and strategic levels. At the operational level, analogous to the rail marshaling yards that were the primary air interdiction targets of World War II, data marshaling yards (also known as data fusion centers) are the logical focal points for cyber interdiction. Data fusion centers are few in number compared to the combat systems they support (for example, fighters, tanks, and submarines), and they are the nodes where raw materials (data) are marshaled and transformed into information, a coherent understanding of the situation to be shared across military forces. Data fusion centers are centers of gravity in cyberspace because they are where orientation happens. Fusion centers at the operational level include enemy command and control nodes and intelligence, surveillance, and reconnaissance processing, exploitation, and dissemination nodes. By destroying, degrading, or neutralizing these data marshaling yards, cyber interdiction caps an adversary's operational effectiveness by limiting his ability to orient and concentrate effects in time and/or space. Regardless of an enemy's camouflage, concealment, and deception capability to foil kinetic strikes, data fusion centers must advertise their location in cyberspace (for example, IP address) to some degree to receive data and distribute information. Data fusion centers are almost certain to be vulnerable to cyber attack because their utility heavily depends on their connectivity—the power of a network grows exponentially with the number of users.[34] If these nodes are not widely connected, they are irrelevant to the enemy's warfighting effort and can be ignored. Degrading data fusion capabilities creates greater uncertainty at the operational level and compels an adversary to rely more on his ability to adapt at the tactical level. In turn, an enemy's ability to adapt at the tactical level depends on the effectiveness of his tactical network and communication/data links. Thus, cyber interdiction at the operational level magnifies the significance and impact of cyber interdiction and electronic attacks to disrupt data links at the tactical level.

An opponent's tactical data links are the next most important cyber interdiction target set after data fusion centers. At the tactical level, each node (for example, fighter plane, platoon, and destroyer) on the tactical network has some level of data fusion capability, so information is rarely concentrated to the point that attacking those nodes in cyberspace will have widespread effects. However, tactical data is so perishable that even temporary disruptions to the data link network can have significant negative impacts on the ability of each tactical unit to derive information before the data are no longer a valid basis for decisions. As a result, disrupting tactical network data links, not disabling nodes, is the appropriate objective of cyber interdiction at the tactical level. Interrupting these links can cause brief but meaningful delays and misperceptions in an opponent's decision cycle to create or magnify a "first look-first shot-first kill" tactical advantage. By focusing military cyber power on gaining and maintaining cyber superiority and cyber interdiction at the operational and tactical levels, joint forces can maximize their capabilities and gain a significant decision advantage difficult for an opposing force to overcome.

In joint warfare, it is the air campaign that can benefit most from the effects of cyber superiority and cyber interdiction against enemy data fusion centers and tactical data links. Although cyber power supports land and sea operations, the air campaign is typically the leading effort in joint warfare. Beginning with World War II, airpower has formed the vanguard of every U.S. military operation whether based on land or sea. Additionally, the ability of modern air forces to conduct parallel warfare in the style first used during the 1991 Persian Gulf War critically depends on the exploitation of cyber power for situational awareness, communication, and reconnaissance. Furthermore, enemy capabilities to defeat stealth aircraft have at their heart data fusion to overcome stealth's ability to hide from air defense radars. Cyber power puts the *integrated* in integrated air defense. With cyber power knitting air defense sensors and shooters together, an opponent could generate an airspace picture with fewer weaknesses. However, without a data network to fuse multiple sensors, surface-to-air missile batteries become individual defenders in a one-on-one engagement, a scenario that stealth aircraft have proved they can dominate since 1991. Cyber interdiction applied in support of air forces can dramatically ease the dangerous task given to air forces—to penetrate the teeth of an enemy's defenses at the outset when the defenses are most lethal. The price of air warfare without a cyber advantage is steep. The last time U.S. airpower fought through an enemy air defense without the benefit of cyber superiority in World War II, American aircrews had a lower probability of survival than Marines fighting in the Pacific.[35] In addition, air operations can unfold much more rapidly than land or sea operations. Surface forces move at tens of miles per hour compared to air forces, which move at hundreds of miles per hour. Land and sea forces—much like the foot soldiers of World War I who were too slow to convert a breakthrough into a breakout—will in all likelihood be too slow to exploit the fleeting advantages created by cyber interdiction as effectively as air forces.

Conclusion

Cyber power is critically important in joint warfare. Military cyberspace operations should have as their priority the attainment and maintenance of cyber superiority and cyber interdiction in support of kinetic operations with a focus on supporting the air campaign. Additionally, operations to gain and maintain cyber superiority should concentrate on neutralizing enemy cyber attack and cyber reconnaissance capabilities, followed by suppressing enemy cyber defenses. Cyber interdiction attack operations should focus on the cyber equivalent of rail marshaling yards—data fusion centers—and tactical data links. Together, cyberspace superiority and cyber interdiction yield a powerful decisionmaking advantage in joint warfare, the cumulative effect of which is to compel an enemy to make mistakes that will likely prove fatal in due course. **JFQ**

Notes

[1] Daniel T. Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Washington, DC: NDU Press/Potomac Books, Inc., 2009); Joint Publication (JP) 1-02, *DOD Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through October 15, 2011), 92.

[2] Lee Kennett, *The First Air War: 1914–1918* (New York: The Free Press, 1991), 220.

[3] Mandiant, *APT 1: Exposing One of China's Cyber Espionage Units*, available at <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.

[4] JP 1-02, 16.

[5] John C. Slessor, *Air Power and Armies* (Tuscaloosa: The University of Alabama Press, 2009), 16–17.

[6] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed., rev. (Washington, DC: DOD C4ISR Cooperative Research Program, 1999), 32.

[7] Slessor, 122–123.

[8] Thomas E. Griffith, Jr., *MacArthur's Airman: General George C. Kenney and the War in the Southwest Pacific* (Lawrence: University of Kansas Press, 1998), 244–246.

[9] U.S. Department of State, "Background Note: Georgia," available at <www.state.gov/outofdate/bgn/georgia/index.htm>.

[10] Ibid.

[11] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallin, Estonia: Cooperative Cyber Defense Centre of Excellence, 2008), 5; Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs* 9, no. 1–2 (Winter/Spring 2008), available at <www.europeaninstitute.org/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html>.

[12] Tikk et al., 6.

[13] Ben Arnoldy, "Cyberspace: New Frontier in Conflicts," *The Christian Science Monitor*, August 13, 2008, available at <www.csmonitor.com/USA/Military/2008/0813/p01s05-usmi.htm>.

[14] Ibid.

[15] Tikk et al., 6.

[16] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, 1, available at <www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>.

[17] Ibid.

[18] John Bumgarner and Scott Borg, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," in *Cyberwar Resources Guide*, Item #138, 2–3, available at <www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

[19] Ibid.

[20] Ibid., 4–5.

[21] Ibid., 5.

[22] Ibid.

[23] Georgian Research and Educational Networking Association, available at <www.grena.ge/eng/cert.html>; Tikk et al., 14–15.

[24] Greg Keizer, "Russian Hacker 'Militia' Mobilizes to Attack Georgia," *NetworkWorld.com*, August 13, 2008, available at <www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html>; Tikk et al., 12.

[25] Bumgarner and Borg, 7.

[26] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (2008), 66–67.

[27] Bumgarner and Borg, 7.

[28] Ibid., 7.

[29] Ibid., 4.

[30] John Oltsik, "Russian Cyber Attack on Georgia: Lessons Learned?" *NetworkWorld.com*, August 9, 2009, available at <www.networkworld.com/community/node/44448>; Bumgarner and Borg, 2.

[31] Joseph Menn, "Expert: Cyber-attacks on Georgia Web sites Tied to Mob, Russian Government," *Los Angeles Times*, August 13, 2008, available at <http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html>.

[32] Tikk et al., 6.

[33] Slessor, 31.

[34] Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Cambridge: Harvard Business School Press, 1999), 184.

[35] W. Murray and A.R. Millett, quoted in Paul Kennedy, *Engineers of Victory: The Problem Solvers Who Turned the Tide in the Second World War* (New York: Random House, 2013), 142.