Shoot, Move, Communicate

Thinking Through Cyber's Role in Ground Combat

Frank J. Cilluffo and Joseph R. Clark, Ph.D.

Mr. Cilluffo is an Associate Vice President at The George Washington University where he directs the Center for Cyber and Homeland Security. He previously served as Special Assistant to President George W. Bush for Homeland Security.

Dr. Clark is an Assistant Professor of Political Science at Towson University. He previously served as a Psychological Operations Sergeant in the U.S. Army.

FOREWORD: The phrase 'cyber components and capabilities' is used as a catch-all phrase. It is imprecise. Given that the argument presented here is about the need to further develop offensive and defensive cyber operations, it was important not to truncate the concept on the basis of current (and potentially transitory) definitions. For the purposes of this essay, the phrase can be understood as including any and all computer network attacks (CNA), computer network exploits (CNE), or computer network operations (CNO), that facilitate or resist offensive or defensive land operations and tactical air support.

Shoot, move, communicate. Ground combat can be distilled to these three tasks. Regardless of any weapon's degree of sophistication or the complexity of any scheme of maneuver — battlefield victory is a product of how well individuals, units, and armies shoot, move, and communicate. These actions underpin a military's ability to destroy enemy formations, secure objectives, and set the conditions for peace. As cyber components and capabilities[1] gain potential to affect how land forces shoot, move, and communicate, the Army — as a whole — must think through, plan for, and rehearse how cyber will affect military missions at the operational and tactical levels of war (and in turn shape strategic outcomes).

National security debates and discussions increasingly focus on the potential effects of cyber. The emphasis has been on strategic level threats or opportunities. These debates are important. Yet they often overlook a basic truth — strategic effect is a product of operational and tactical capability. It is at the operational level where cyber components and capabilities are most likely to have decisive effects. While cyber is a domain unto itself, it will be those military forces that best integrate cyber into operations carried out across the physical domains of air, land, sea, and space, which will gain significant advantage.

To ensure cyber becomes fully and properly integrated into the full spectrum of land operations, discussions about cyber's operational and tactical level effects are needed. To maintain focus on land operations writ large and avoid becoming a parochial debate about how cyber may affect the tasks or roles of a given branch, these conversations must be Army wide. They must also include technical, academic, and policy experts from outside the service. These discussions should strive to answer three interwoven questions. First, how does (or will) cyberspace influence combat, combat support, and service support operations to project, deploy, and deliver force? Second, how does (or will) cyber components and capabilities affect the ability of US forces to conduct opposed forcible entry operations? Third, how does (or will) cyber components and capabilities affect the ability of US forces to deny or oppose the forcible entry operations of enemy forces? These are not the only important questions about the effects of cyber on land operations. But these three questions allow the Army to start evaluating the magnitude of cyber's effect on its core missions.

In some ways, these discussions have already begun. In February, FM 3-38 Cyber Electromagnetic Activities was released. The field manual outlines the cyber (and electronic warfare) tactics and procedures commanders must consider in support of unified land operations. It provides a cyber-electromagnetic activities appendix for operations plans and orders. Last September, US Cyber Command activated the headquarters for its Cyber Mission Force. It has established joint force headquarters-cyber to support the combatant commands. Cyber Command is now in the process of building, training, and certifying one hundred and thirty-three national missions team, combat mission teams, and cyber protection teams — including those of US Army Cyber Command. Furthermore, articles addressing the utility and effects of cyber are increasingly prevalent in military journals. These events are welcome developments. Yet, they run the risk of partitioning cyber off as something distinct and separate from how the Army as a whole shoots, moves, and communicates in the twenty first century. Piecemeal consideration of how cyber components and capabilities affect targeting, operations or signals security, network-centric warfare, or even the utility of cyber components as weapons themselves are important topics. Yet, cyber requirements and capabilities cannot be relegated to a specific appendix, a specific task, or given command. Their consideration must be Army-wide and explicit. Discussions about the operational effects of cyber components and capabilities on strategic land power are needed.

What follows is offered as a thinking exercise to highlight the importance of an Army wide, operational level approach to the role of cyber. It is not gospel. It is inevitably flawed. Still, it is an important step in fueling discussions about how cyber will influence the Army's ability to shoot, move, and communicate to ensure tactical, operational, and strategic success and superiority.

Operational Opportunities and New Instruments

Georgian hackers felt it first. They were among the first targets of the Russian attack. Late on 07 August 2008, distributed denial of service (DDoS) and structured query language (SQL) database injection attacks were used to suppress the capabilities of pro-Georgian hackers. These attacks significantly reduced Georgia's ability respond to or retaliate against follow-on attacks in both the cyber and physical domains. In quick succession, DDoS and SQL attacks were used to bring down fifty-four Georgian government, communications, and financial websites. The attacks slowed intra-government communication, isolated the Georgian government from its citizens, halted electronic banking services, and silenced news agencies just as Russia launched combat operations into Georgia. These cyber-attacks interwove a range of effects normally produced via electronic warfare or conceptualized as information operations. Although there is no definitive public evidence of an official command and control link between Russian forces and these cyber-attacks, the level of synchronization between cyber and conventional actions was impressive.[2] It suggests a high degree of coordination. "Many of the most serious attacks began just as the tanks began to roll… the choice of targets is especially telling. Official sites in Gori, along with local news sites, were shut down by denial-of-service attacks before the Russian planes got there."[3] If the objective was to slow Georgia's response and complicate the counter-concentration of Georgian forces — it worked. Cyber-attacks degraded the ability of Georgian forces to shoot, move, and communicate. Cyber components and capabilities provided pivotal support to the Russian ground offensive that stripped South Ossetia and Abkhazia from Georgia.

The Georgian example represents an early and dramatic case in a growing universe of cases in which cyber components and capabilities have been employed at the operational and tactical level. That universe includes Israel's 2007 take down of Syria's air defenses in coordination with strikes against a suspected nuclear materials cite.[4] It includes the Syrian Electronic Army's ongoing efforts to spread pro-Assad propaganda and steal data for use in targeting anti-Assad forces.[5] Most recently, it includes Russia's seizure of Crimea. As Russian forces moved to take control of airports and other objectives, Russian hackers attacked Ukrainian websites and telecommunications facilities. The attacks against Ukraine included a DDoS assault thirty-two times larger than that launched against Georgia and the use of a cyber-espionage system called "Snake."[6] Once again, Russian forces used physical and cyber-attacks — this time, to isolate Crimea from the rest of Ukraine. These cases suggest a new reality. Regardless of asymmetries in other capabilities, cyber components and capabilities are now part of how armies shoot, move, and communicate, whether carried out directly or via proxies that provides impetus for all military forces, from those of powerful nation-states to those of weak insurgent movements, to acquire cyber components and capabilities.

The acquisition of new components and capabilities does not necessarily led to the acquisition of new techniques or tactics. More importantly, new technological components and capabilities alone are not enough to produce victory. It is the employment of technology that matters. It is how the new instrument affect a military's ability to shoot, move, and communicate that matters. Four quick illustrations make the point.

In 1415, the longbow decided the Battle of Agincourt not because of its four hundred yard range, but because of its employment. Positioned on slightly elevated sloping ground, to the left and right of King Henry's men-at-arms, against a numerically superior enemy whose ability to maneuver was constrained by mud and wooded terrain — the new technology devastated the opposing French forces.[7] If Henry's archers had been used without consideration of terrain, or without a fixing force to slow the French, the outcome would have been different.

The same can be said of Major General John Buford's use of breach loading carbines at Gettysburg in 1863. Their technological advantages, the ability to reload rapidly and fire without standing, only became significant because of how they were employed. Buford's decision to have his cavalry fight dismounted and his use of terrain shaped a successful covering force battle that positioned the Army for victory at Gettysburg, and forced General Robert Lee to withdraw out of Pennsylvania back into Virginia.[8]Against numerically superior Confederate force possessing much greater firepower, the technology alone would not have been decisive.

Early tank warfare provides a counter-example. Despite the emergence of subsequent myths about their effectiveness, in 1918 tanks did not play a decisive role in the battles that broke the stalemate of World War I. At Amiens, the Allies had some 414 tanks — four days later, 6 were operational. As a new technology the tank was mechanically unreliable. Yet, it was employment that undermine their effectiveness. At Amiens the tanks advanced ahead of infantry. No reserve force was kept. The machines faltered in the face of Germany's elastic defense. As a result of poor force employment, by November 1918, there were only 37 operable tanks in the entire British army.[9] The tank had no effect on how (or how well) the armies of World War I fought.

Similarly, because of poor force employment at the operational level, the first operational combat jet had no beneficial effect on how the

Luftwaffe performed. Adolf Hitler's insistence that the Me262 program be used to develop a Blitz bomber, nullified the potential effect of the aircraft's speed. If the Me262 had been developed solely as a fighter and employed to blunt Allied bombing, it could have swarmed American and British air forces and inflicted significantly higher losses — producing tactical, operational, and perhaps even strategic effects. Hitler's decision to overrule the force employment preferences of Hermann Göring prevented this.[10]

As these illustrations make clear, raw capability is not enough. Success is a function of application, integration, and execution. Whether or not, and how, a new instrument or technology matters depends on how it is employed. That is the impetus behind the need to discuss how cyber components and capabilities will affect how the Army (and its adversaries) shoot, move, and communicate.

Cyber & Force Employment

Stephen Biddle argues that technology magnifies the effects of force employment.[11] Technology makes capable forces, more capable. If integrated properly, technology enhances how military units execute or react to actions born out of the principles of war: mass, maneuver, surprise, security, simplicity, objective, offensive, economy of force, and unity of command. Technology is not a substitute for good force employment. It will not make a 'bad' force better. It can, however, allow commanders to concentrate the application of effort upon the most decisive elements of a given operation. Of course, the opposite is also true. The failure to effectively employ a technology mastered by an adversary leaves a force less capable. It may result in missed opportunities or expose friendly forces. This gets to the heart of why the Army as a whole must consider cyber's effects on land operations.

In combat, cyber components are likely to affect how adversaries detect and respond to attacks — hasty and deliberate. Cyber is likely to shift the culminating point for victory. Depending on the strategic objective and the characteristics of the adversaries, cyber may affect the combatants' center of gravity. Cyber technologies will affect force employment. Whether or not they enhance or degrade the Army's ability to shoot, move, and communicate depends on how well officers and non-commissioned officers think through the effects of cyber components and capabilities on mission, enemy, terrain, troops, time (METT-T), and even civilians (METT-TC). Consider how cyber components and capabilities can affect intelligence, covert, and conventional mission sets.

In regard to intelligence missions, cyber offers a more effective means for collecting, processing, pooling, and analyzing information from traditional and non-traditional sources. Data from forward observers, spot reports, aircraft, country studies, and intelligence reports can be merged and accessed more quickly and efficiently than before. Cyber has the potential to simultaneously draw information emanating from neutral sources as well as those of the adversary. Battlefield relevant data from news media and social media can be quickly obtained and analyzed. Enemy systems can be hacked and monitored, allowing data to be gathered about the concentration of forces, the placement or replacement rates of material resources, ciphers, or other intelligence requirements. The ability to pool data from a host of various sources at the operational level, would provide a richer picture of the area of operations. Furthermore, the ability of cyber components to collect from various streams — to observe targets from various vantage points, including the enemy's — would make intelligence, surveillance, and reconnaissance less transient, more constant, in nature.

If cyber components are fully integrated into intelligence missions at operational and tactical levels, they could allow commanders to forecast the primary, secondary, and tertiary effects of real or planned events. Sophisticated algorithms and models delivered via cloud computing could be used to carry out probabilistic analysis of enemy force concentrations, likely counter-concentrations in response to US actions, and the likely effects of battlefield damage to specific targets. The goal is not to replace the intelligence function with cyber. No one should seek to replace 'the 2-shop' with Arthur C. Clarke's HAL 9000. The goal is to use the speed and access grated by cyber to enable analysts to capture a more accurate and aggregate understanding of the situation, enemy capabilities, and the behavior of the adversary. Doing so would allow for better preparation of the battlefield, target acquisition, and battle damage assessments.

Imagine the effect if at the operational and tactical level US forces were able to confirm current or accurately predict future enemy positions by constantly triangulating data from friendly force observation, social media and other neutral sources, and the enemy's own networks. Better yet, imagine a scenario in which the same could be used to confirm current or accurately predict the location of enemy logistical elements. Such capability could give commanders the ability to operationalize General Omar Bradley's (perhaps apocryphal) adage that "amateurs study strategy, professionals study logistics."[12] Now, imagine if enemy forces were able to do this to American forces? To what degree are Army units capable of monitoring and reacting to the use of cyber components and capabilities to find and track them? To what degree are commands prepared monitor and react to the use of cyber to identify and track individual soldiers within their commands?

In regard to covert mission sets, cyber components can offer deep strike and irregular warfare capabilities to operational and tactical commanders via computer network exploits and computer network operations. Cyber techniques are proving capable of producing kinetic effects. At the operational and tactical levels, these emerging capabilities could be used to strike elements in the adversary's rear — without exposing friendly forces or physical avenues of approach. Cyber components could be used to falsely trigger enemy sensors, diverting enemy forces and attention. This capability could be used to harass and confuse enemy units, forcing them to expend time, energy, and resources — without exposing friendly forces. On the battlefield, this could support friendly action by altering force-to-force ratios or force-to-space ratios. Depending on the situation, covert cyber could be used to slow the response of enemy forces or undermine enemy command and control before the launch of operations without the enemy even being aware it was happening. As the 2008 Russian invasion of Georgia demonstrates, even if the effect is not covert, cyber-attacks can undermine command and control, slowing responses at critical moments. As before, this raises the question of the degree to which Army units are factoring such — on the part of friendly and enemy forces — into operations plans and orders.

Introducing digital mission command systems and supporting networks will continue to make the Command Post the center of a commander's universe Unified Land Operations (ULO). Despite this current concentration of critical information in the CP, commanders should not have to decide between staying in their CP, or moving to the front lines.

It is in regard to conventional missions where cyber components are likely to have the greatest effect. At the operational level, conventional operations will often include the intelligence, if not covert missions, described above. Cyber's effect on conventional missions, however, will extend beyond intelligence and irregular warfare. Cyber's ability to network communications and provide for information sharing will affect the speed of combat operations. This will affect synchronization and it will affect the time attackers and defenders have to make decisions. The ability of cyber components to produce kinetic effects will allow cyber to play a suppressive fire, and eventually indirect fire, function. The ability of cyber components to fool or flood enemy sensors and systems with noise will allow cyber to play an electronic warfare function and conceal friendly forces and actions and expose those of the enemy. The ability of cyber systems to monitor friendly supply chains will aid in just in time delivery of liquids, ammunition, equipment, and casualty support. Cyber components will affect how modern forces employ the principles of war; including, mass, maneuver, surprise, security, simplicity, objective, offensive, economy of force, and unity of command.

Cyber components and capabilities have the potential to dramatically affect a force's ability to breakthrough an adversary's defenses and exploit the ensuing gap. It is not hard to imagine a context in which the following occurs. Cyber components and capabilities have the potential to conceal massing forces, producing favorable force-to-force and force-to-space ratios. Cyber components and capabilities can potentially expand the penetration corridor by taking down enemy sensors and helping to move civilians out of the battlespace. Cyber components and capabilities can increase friendly force mobility through their effect on communication and coordination, allowing friendly forces to more effectively exploit terrain and the location of enemy forces. Cyber components and capabilities can produce more precise targeting, ensuring that attacks have maximum effect on the objective while reducing collateral damage. After breakthrough, cyber components and capabilities could reduce the enemy's ability to flank invading friendly forces by providing real time information about counter-concentrations to operational and tactical level commanders — allowing them to avoid or swarm enemy forces. Cyber does not stand to alter the basic premise of breakthrough and exploitation, but it stands to increase the likelihood that it can be carried out successfully and it stands to adjust the costs of such operations. One last historical reference reinforces this point.

In 1940, the spearhead Panzer units invading France were able to operate over long distances due to radio and a command organization that knew how best to exploit the new technology. The supreme commander of French forces opposing the German's sat in a headquarters with no radio and only a single telephone line — which was unavailable during the middle of day when the operator took lunch.[13] Today the question is, to what degree is the Army working through how the plans and operations necessary to understand how cyber will affect breakthrough and exploitation in the 21st century.

As with all the tasks and missions that make up modern force employment, the success of operations — and the fate of the strategic goals for which they are undertaken — are a product of the relative operational and tactical level skill of opposing forces. Cyber components and capabilities will play a role in how well the US Army conducts "combined arms maneuver to gain physical, temporal, and psychological advantages over an enemy."[14] To do so successfully, cyber cannot be left to a specific appendix or a given command. It must be integrated into how the Army shoots, moves, and communicates. The whole of the Army must integrate cyber into operational level force employment. Evidence suggests its adversaries are doing just that. ■

NOTES

1. D. Danchev, "Coordinated Russia vs Georgia cyber-attack in progress," ZDNet, (Aug. 2008): http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670. G. Keizer, "Russian hacker 'militia' mobilizes to attack Georgia," Network World, (Aug. 2008): http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html?page=1. B. Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," The Wash. Post, (Oct. 2008): http://voices.washingtonpost.com/security-fix/2008/10/report_russian_hacker_forums_f.html. E. Tikk, K. Kaska, K. Rünnimeri, M. Kert, A. Talihärm, L. Vihul, "Cyber Attacks Against Georgia: Legal Lessons Identified," Cooperative Cyber Defence Centre of Excellence, (Nov. 2008): http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

2. D. Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, (Jan. 2011): http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

3. "D. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis," Aviation Week, (Oct. 2007) http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog%3A27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3A2710d024-5eda-416c-b117-ae6d649146cd. S. Weinberger, "How Israel Spoofed Syria's Air Defense System," Wired, (Oct. 2007): http://www.wired.com/dangerroom/2007/10/how-israel-spoo/.

4. N. Hopkins and L. Harding, "Pro-Assad Syrian hackers launching cyber-attacks on western media," The Guardian, (Apr. 2013): http://www.theguardian.com/world/2013/apr/29/assad-syrian-hackers-cyber-attacks.

5. M. Clayton, "Major cyber-assaults on Ukraine, then Moscow, on eve of Crimea vote," The Christian Science Monitor, (Mar. 2014): http://www.csmonitor.com/World/Passcode/2014/0314/Major-cyber-assaults-on-Ukraine-then-Moscow-on-eve-of-Crimea-vote-video. P. Paganini, "Crimea — The Russian Cyber Strategy to Hit Ukraine," Infosec Institute, (March 2014): http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/.

6. P. Allen, "Thousands of arrows to rain down on Agincourt for the first time in 600 years as English and French historians plan to recreate famous battle," Daily Mail, (Oct. 2013): http://www.dailymail.co.uk/news/article-2476438/Thousands-arrows-rain-Agincourt-time-600-years-English-French-historians-plan-recreate-famous-battle.html. J. Barker, "Day of the Longbow," National Post, (Oct. 2006): http://search.proquest.com.proxygw.wrlc.org/docview/330618059. J. Glanz, "Historians Reassess Battle of Agincourt," The N.Y. Times, (Oct. 2009): http://www.nytimes.com/2009/10/25/world/europe/25agincourt.html?pagewanted=all&_r=0.

7. D. Devlin, "Buford at Gettysburg," US Army War College, (April 1992), www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA250501. R. Soodalter, "Buford Hold the High Ground," The N.Y. Times, (June 2013): http://opinionator.blogs.nytimes.com/2013/06/29/buford-hold-the-high-ground/?_r=0.

8. Stephen Biddle, Military Power: Explaining Victory and Defeat in Modern Battle (Princeton Univ. Press, 2004), 34-35. S. L. A. Marshall, World War I (Boston: Mariner Books, 2001), 412-418. T. Travers, "Could the Tanks of 1918 Have Been War-Winners for the British Expeditionary Force?,", Journal of Contemporary History, 27, no. 3 (1992): 309-486.

9. T. Junge, "A Questionable Political Decision," in The Me 262 Stormbird, ed. Colin D. Heaton and Anne-Marie Lewis (Zenith Press, 2012), 61-72

10. Biddle, 146.

11. C. Gray, Fighting Talk: Forty Maxims on War, Peace, and Strategy (Westport: Greenwood Publishing Group, 2007), 115.

13. E. Simpson, War from the Ground Up (Oxford University Press, 2013), 186-187.

14. Dept. of the Army, TRADOC, Pam 525-3-1 US Army Operating Concept, 2016-2028. (Washington D.C.: Govt. Printing Office, 2010), 11.