Generals in Cyberspace: Military Insights for Defending Cyberspace

February 20, 2018

By Peter Campbell

Peter Campbell is an Assistant Professor of Political Science at Baylor University, Waco, TX. He conducts research and teaches in international relations and international security.

Abstract: *Recently, there have been calls for the United States to unleash the offensive power of cyberspace. Advocates contend that offense has the advantage in cyberspace. This article argues that cyberspace does not favor the offensive at either the tactical or the strategic level. In fact, a defensive doctrine has clear advantages over an offensive one. Support for this argument can be found in two unexpected sources: official statements of U.S. Army doctrine and Carl von Clausewitz's* On War. *This is surprising, given that scholars consider both the U.S. Army and Clausewitz diehard apostles of the cult of the offensive. This essay seeks to import their insights about the advantages of the defense into the virtual realm. When read carefully, U.S. Army doctrine and Clausewitz's classic text support the claim that defense is the stronger approach in the cyber realm.*

Policymakers, scholars, and the general public are trying to understand how conflict in the cyber realm will shape international relations. Will cyber warfare lead to a revolution in strategy similar to the advent of the steam engine, the airplane, or nuclear weapons?[1] Are cyber capabilities the new "absolute weapon"?[2] Does the new terrain of cyberspace alter the balance of power?[3] As in the past, political leaders have begun to formulate policy and strategy in response to these questions. Among the questions they are wrestling with is: Is it better to be on the *offensive* or the *defensive* in cyberspace?

This article contends that, contrary to the fears of many, cyberspace is not inherently the realm of offensive doctrine at the tactical, strategic, or the political level. In fact, a defensive doctrine has clear advantages over an offensive one. Moreover, two unexpected sources—official statements of U.S. Army doctrine and

[1] Joseph S. Nye, *Cyber Power* (Cambridge: MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010), p. 4.
[2] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, June 2012, pp. 401–428.
[3] The cost of entry into cyberspace is much lower than it would be, for instance, to develop sea or air power. The latter are within the reach of only a few major powers. With this low cost of entry, it is conceivable that the balance of power could shift, at least in the cyber realm. "Dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non-state actors," Nye, *Cyber Power*, pp. 4, 9, 11.

© 2018 Published for the Foreign Policy Research Institute by Elsevier Ltd.

doi: 10.1016/j.orbis.2018.02.006

Carl von Clausewitz's *On War*—support these claims may appear surprising. After all, many experts consider both the U.S. Army and the Prussian military theorist diehard apostles of the cult of the offensive.[4] Yet, when read carefully, U.S. Army doctrine and Clausewitz's classic text support these claims. This essay seeks to import their insights about the advantages of defense into the virtual realm. Such insights could help the United States develop a cyber strategy that does not rely too heavily on offensive cyber capabilities and their concomitant dangers. These defensive tactics and strategy have numerous advantages for the United States as it wrestles with cyber threats and prepares for future cyber crises.

Inevitably, the U.S. military became involved in responding to the dangers and opportunities in cyberspace. Between 2009 and 2010, the U.S. government created the United States Cyber Command and the Air Force, Navy, and Army all established their own cyber units.[5] And, in some cases, commanders are seeking greater latitude to conduct offensive cyber operation.[6] However, giving the military a prominent role in the cyber realm has raised alarms in the media and among cyber experts.[7] Among their concerns is that military officers subscribe to the old adage: "the best defense is a good offense."[8] Some fear that they will import their aggressive outlook into the cyber realm, militarize cyberspace, and use cyber weapons preemptively.[9] However, this narrow view of the military mindset overlooks important contributions that military thinking can make, especially regarding the advantages of *defensive* cyber operations.[10] While military officers do highlight the virtues of offensive action, they also have a deep appreciation for the advantages of the *defense*. This appreciation is especially important now that the offense is seen as preeminent in cyberspace. It is important for offensive capabilities to have a place in U.S. cyber strategy. However, a focus on the offense underestimates the advantages

[4] Jack Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, NY: Cornell University Press, 1984); Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security*, Spring 1998, pp. 5–43; and Stephen Van Evera, "The Cult of the Offensive and the Origins of the First World War," *International Security*, Summer 1984, pp. 58–107.

[5] The Air Force stood up the new 24th Air Force at Lackland Air Force Base in San Antonio, Texas, in 2009 while the US Navy activated a new 10th Fleet based at Fort Meade, Maryland in 2010. Nye, *Cyber Power*, p. 10; and W. Alexander Vacca, "Military Culture and Cyber Security," *Survival*, vol. 53, no. 6, 2011, p. 159.

[6] Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment," *International Security*, Winter 2016/2017, p. 73.

[7] David E. Sanger, John Markoff, Thom Shanker, "U.S. Plans Attack and Defense in Web Warfare," *New York Times*, Apr. 28, 2009; Thom Shanker, "U.S. Weighs Its Strategy on Warfare in Cyberspace," *New York Times*, Oct. 19, 2011.

[8] See footnote 4 above for scholars who argue that a "cult of the offensive" exists among military officers.

[9] Vacca, "Military Culture and Cyber Security," p. 165.

[10] This paper builds on but is distinct from other efforts to assess the "Cyber Offense-Defense Balance," Keir Lieber, "The Offense-Defense Balance and Cyber Warfare," in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2015), pp. 96–107; and in Slayton, "What Is the Cyber Offense-Defense Balance?" p. 73.

of the defense, as well as the dangers of attack. Leaving military officers out of cyber strategy, fearing their aggressive instincts, would preclude their perspectives about the power of cyber defense. It is hoped that this essay can be a corrective for both those who are enamored with the cyber offense and those who fear generals in cyberspace.

The essay begins by noting that one of the dangers emanating from cyberspace is conflict escalation resulting from offensive cyber operations. These dangers will persist because many experts think offense has the advantage in cyberspace. Moreover, cyberattacks are a particularly attractive form of covert action. Therefore, there is a need to set out the advantages of the defense in cyberspace. The essay then turns to a discussion of the power of the defense as rediscovered by the U.S. Army in the depths of the Cold War. In this period, the army thought innovatively about the advantages of defense. The article then applies these defensive concepts to cyber capabilities. It also unpacks Clausewitz's insights about the power of the defense and applies them to the cyber realm, too. The conclusion summarizes the main argument and discusses its policy implications, especially for U.S. cyber strategy.

Conflict Escalation, the Attraction of Covert Action, and the Necessity of Cyber Defense

Scholars and practitioners already have compiled ominous lists of the threats from cyberspace.[11] However, some scholars have argued that different groups are exaggerating the cyber threat. In some cases, they contend that the culprit is bureaucracies inflating cyber threats to garner more resources.[12] Thomas Ridd has argued, "cyberwar will not take place." Cyber capabilities are not like military

[11] Recently, a U.S. Department of Homeland Security report stated that hackers had breached a dozen nuclear power plants in the United States. "Hackers breached a dozen US nuclear plants, reports say," *BBC News*, July 7, 2017, http://www.bbc.com/news/world-us-canada-4053806. Alexander Klimburg discusses the dangers of "logic bombs," one of which threatened to shut down all the servers of U.S. mortgage giant Fannie Mae, while another may have been used during the Reagan administration to detonate a gas pipeline in the Soviet Union. Klimburg, "Mobilising Cyber Power," *Survival*, vol. 53, no. 1, p. 42. Hackers could also use malicious software to infiltrate the computer systems of major industries and utilities and, for example, to shut off the heat in a major city in the dead of winter, possibly leading to many deaths. As Nye further points out, "Computer networks essential to the American military are attacked hundreds of thousands of times every day." Nye, *Cyber Power*, p. 9. Also, see, Richard A. Clarke and Robert K. Knake, *Cyberwar* (New York: Harper Collins, 2010); and John Arquilla, "Cyberwar Is Already upon Us," *Foreign Policy*, Feb. 27, 2012, http://foreignpolicy.com/2012/02/27/cyberwar-is-alreadyupon-us/; and Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007).

[12] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," Security Studies, 2016, p. 345; and Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics*, vol. 10, no. 1, (2013), pp. 86–103.

capabilities, Ridd writes, because the damage they produce is only temporary and severe only when coupled with kinetic military operations.[13] Nevertheless, while there may never be a war of bits and bytes that decides the fate of nations, actions and reactions in cyberspace will affect international policy conflicts. Most concerning, cyberattacks could be an intermediate step in conflict escalation leading to limited or major wars.[14]

Although we think of the cyber realm as existing in the ether, it has a number of physical conduits and locations.[15] Conceivably, a state could target this physical infrastructure with missiles or saboteurs in response to a particularly severe cyber-attack. In addition, powerful states are not the only targets of cyber-attacks that might choose to escalate. Weaker powers subjected to a sophisticated cyber-attack could lack the capacity to respond in kind. However, they might respond with a terrorist attack against the perpetrator or one of its allies. Indeed, one of the most prominent cyberattacks yet, Stuxnet, targeted the nuclear program of Iran, a notorious supporter of international terrorism.[16] Therefore, a terrorist campaign in response to a cyberattack, as part of a broader international policy conflict, is conceivable. These progressive escalations could lead to direct military conflict. Cyber conflicts could also lead to accidental or uncontrolled escalation. A number of the actors that states employ in the cyber realm are only partly under their control.[17]

[13] Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies*, Feb. 2012, pp. 5–32.

[14] "A key strategic risk in cyber attack, finally, lies in potential escalatory responses." James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, vol. 53, no. 1 (2011), p. 35; and Lawrence J. Cavaiola, David C. Gompert, and Martin Libicki, "Cyber House Rules: On War, Retaliation and Escalation," *Survival: Global Politics and Strategy*, vol. 57, no. 1, (2015), pp. 81-104; and Martin C. Libicki, *Cyberdeterrence and Cyberwar* (CA: Rand Project Air Force, 2009).

[15] Nye, *Cyber Power*, p. 6, "physical routers and servers and the fiber optic cables that carry the electrons of the internet have geographical locations within governmental jurisdictions."

[16] Iran may have responded to Stuxnet with cyber-attacks on the U.S. banking system and cyber-attacks on the Saudi Aramco Corporation. Nye, "Deterrence and Dissuasion in Cyberspace," p. 48; James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, vol. 53, no. 1 (2001), pp. 24-25; and Nye, *Cyber Power*, p. 14. However, the United States is not the only country using cyber capabilities to hit out at its enemies. Israel, Russia, and China have used cyber capabilities as an adjunct to military operations or a stand-alone means of targeting states and groups. Israel may have used cyber capabilities to blind Syrian air defenses as part of its raid to destroy a secret Syrian nuclear reactor in 2007. Russia attacked Georgian government websites during its war with that country. China has conducted or acquiesced in cyber-attacks on the Tibetan leadership in exile. Nye, *Cyber Power*, p. 11; and Clarke and Knake, *Cyberwar*, ch. 1.

[17] China and Russia have both employed decentralized networks of hackers that they fund, but do not control. Klimburg sets out this relationship nicely in the case of China and describes the career path of one of China's best hackers. Klimburg, "Mobilising Cyber Power," *Survival*, vol. 53, no. 1, pp. 43-4, 46-7, 50-51. On an alleged Russian link to apparent patriotic hackers' attack on anti-doping and other athletic organizations through the Fancy Bears hacking team, see, "Fancy Bears: IAAF hacked and fears athletes' information compromised," *BBC News*, April 3, 2017, http://www.bbc.co.uk/sport/athletics/39477302;

As Borghard and Lonergan point out, cyber proxies are unpredictable and could drag their state sponsors into an escalating conflict.[18] Although war in cyberspace may never occur, cyberattacks will play a part in ongoing policy conflicts and threaten to burst out of the ether and into the world of bombs and bullets. The offensive or defensive character of national cyber strategy can contribute to or diminish the potential for conflict escalation. Recommendations to go on the offense in the cyber realm must consider the dangers of escalation and the advantages of a more defensive approach.

Even if the effects of cyber-attacks are temporary, as Ridd contends, they will remain a tempting tool for political leaders. By definition, covert actions seek to hide the identity of the perpetrator. Anonymity is a protection against retaliation and subsequent escalation. Because of the difficulty of attribution in the cyber realm, cyber-attacks are a very attractive form of covert action. In some cases, the cyber attackers can erase their cyber-footprints as they withdraw from an infiltrated network.[19] Moreover, cyber-attacks do not require the deployment of even small Special Forces units, greatly reducing the political risks.

As Jimmy Carter's Desert One raid showed, failed covert actions can have devastating political consequences. If a cyber-operation fails, however, the attribution problem produces a highly robust deniability, reducing the political consequences. Unlike Desert One, if a cyber-attack fails, there will be no burnt hulks of helicopters in the desert as an ignominious sign of that failure.

Cyber-attacks look even more attractive when leaders are advised that the offense has the advantage in the cyber realm and that enemies will exploit those advantages if they do not.[20] Calls for U.S. policymakers to unleash the cyber offense exist. As one official noted, "In cyberspace, the offense has the upper hand" and the United States cannot "retreat behind a Maginot Line of firewalls or it will risk being overrun."[21] The offense is dominant in cyber space because of the lack of friction and the openness of an Internet built to be user friendly rather than secure.[22] This argument has some merits. Going on the offense has numerous advantages in

and "What we know about Fancy Bears hack team," *BBC News*, Sept. 15, 2016, http://www.bbc.co.uk/newsbeat/articles/37374053.

[18] Erica D. Borghard and Shawn W. Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?" *Orbis*, Summer 2016, pp. 395-416.

[19] Clarke and Knake, *Cyber Warfare*.

[20] This argument derives from the logic of the offense, defense balance. Robert Jervis published the foundational work in contemporary offense-defense theory, Jervis, "Cooperation under the Security Dilemma," *World Politics*, Jan. 1978, pp. 167–214.

[21] U.S. Assistant Secretary of Defense, William J Lynn III quoted in Gartzke and Lindsay, "Weaving Tangled Webs," pp. 320-321. See also William J. Lynn III, "Defending a New Domain: The Pentagon's Cyber strategy," *Foreign* Affairs, Sept./Oct. 2010, p. 98; Jack Goldsmith, "Can we stop the global cyber arms race?" *Washington Post*, Feb. 1, 2010; James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, vol. 53, no. 1, (2011), pp. 30-31.

[22] Nye, *Cyber Power*, p. 5.

warfare, and those advantages could be transferable to the cyber realm. To name only a few, offensive action enjoys the initiative in conflicts between reactive opponents. Basically, if you are on the offense and your opponent is responding to your actions, he cannot be planning to attack you at the same time. Moreover, your offensive action changes the conditions on which your opponent based previous plans, requiring a reassessment of those plans and the loss of precious time. In this way, the cyber attacker can enjoy the initiative. However, advocates of the cyber offense underestimate the potential of a cyberattack to escalate to more kinetic uses of force. Moreover, an adversary could misinterpret reconnaissance in preparation for a cyberattack as the attack itself and begin retaliating.[23]

However, while the cyber offense may enjoy significant advantages, for the United States it does not replace the need for a cyber defense.[24] The United States must protect the cyber lines of communication in the same way that it secures the sea and air lines of communication, and for the same reasons. These lines of communication are part of the backbone of international commerce and communications—key elements of U.S. prosperity and power.[25] In short, in the cyber realm, the United States is a status quo power, perhaps *the* status quo power. Thus, setting out the advantages of cyber-defense is essential because the United States has little choice but to prepare a cyber-doctrine with a heavily defensive component. This analysis attempts to make a virtue out of necessity and to frame some of the tactical, strategic, and political advantages of such a cyber defense.

The Power of the Defense and U.S. Army Doctrine in the Cold War

The U.S. Army during the Cold War is one of the last places we might expect to find insights about the power of the defense.[26] Certainly, several scholars have argued that U.S. Army doctrine in this period predominantly focused on the

[23] Lawrence J. Cavaiola, David C. Gompert, and Martin Libicki, "Cyber House Rules: On War, Retaliation and Escalation," *Survival: Global Politics and Strategy*, vol. 57, no. 1, (2015), pp. 81-104.

[24] There are those who argue that the cyber realm is in fact defense dominant. However, they employ the espionage analogy and less the military analogy that I use here. According to Gartzke and Lindsay, the internet is actually defense dominant not offense dominant. They argue that the key is that the defender in cyber space can deceive the attacker. Gartzke and Lindsay, "Weaving Tangled Webs," pp. 316-348. I will argue that this is true but that the authors do not fully appreciate the defensive analogy from warfare.

[25] James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," Senate Armed Services Committee, 114th Cong., 2nd sess., Feb. 9, 2016, https://www.dni.gov/index.php/newsroom/testimonies/217-congressional-testimonies-2016/1313-statement-for-the-record-worldwide-threat-assessment-of-the-u-s-ic-before-the-senate-armedservices-committee-2016.

[26] I am not the first to use military doctrine to produce insights for cyber security. See, Dorothy E. Denning and Bradley J. Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain," in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2015), pp. 64-75.

offense.[27] The superiority of offense over defense was enshrined in the Principles of War, a central part of U.S. Army doctrine and thinking since the 1920s. According to these Principles, *decisive results in war are only achieved through offensive action,* and *the defensive is only a temporary expedient until offense is possible*.[28] On the contrary, upon close examination, the U.S. Army doctrine in the Cold War is a font of insight into the advantages of *defensive* operations. These insights can help us see the virtues of the defense in the cyber realm.

Consider that from the 1960s until the end of the Cold War, the U.S. Army had to develop a doctrine for fighting a foe with numerous numerical and material advantages. For instance, in the 1960s, the Soviets had 50 percent more tanks than the Atlantic Alliance in Europe.[29] These armored units were the backbone of a Soviet military doctrine based on rapid armored thrusts.[30] In addition, unlike the United States, Soviet reinforcements did not need to cross the Atlantic Ocean in case of another European war. Despite its traditional focus on decisive offensive operations, the situation facing the U.S. Army in Europe at the height of the Cold War forced its leaders to reconsider their affinity for attack. The situation worsened after 1967, as U.S. leaders reduced forces in Europe while the Soviets modernized and expanded their forces. During the 1960s, army leaders realized that they needed to draw on the inherent advantages of the defense to have a fighting chance in Europe.[31]

Military officers have long appreciated the inherent advantages of the defense. They encapsulate this appreciation in the tactical rule of thumb that an

[27] Ingo Trauschweizer, *The Cold War U.S. Army: Building Deterrence for Limited War* (Lawrence, KS: University Press of Kansas, 2008), p. 163; Walter E., Kretchik, *U.S. Army Doctrine: From the American Revolution to the War on Terror* (Lawrence, KS: University Press of Kansas, 2011); and Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore, MD: Johns Hopkins University Press, 1989).

[28] See, War Department Training Regulation 10-5 (1921); John I. Alger, *The Quest for Victory: The History of the Principles of War* (Westport, CT: Greenwood Press, 1982).

[29] The U.S. Department of Defense arrived at this figure after Robert McNamara updated and downgraded estimates of Soviet superiority. Alain Enthoven and K. Wayne Smith, *How Much Is Enough?: Shaping the Defense Program, 1961-1969* (Santa Monica, CA: RAND Corporation, 2005), ch. 4. Enthoven later acknowledged that there were major disparities between NATO and Soviet conventional forces in Europe. See, W.S. Bennett, R. R. Sandoval, R. G. Shreffler and Alain C. Enthoven, "Correspondence," *Foreign Affairs*, July 1975, p. 776.

[30] Col. S. Kozlov, "Soviet Military Art and Science in Walter Darnell Jacobs, tr., *Military Review*, Sept. 1959; Raymond L. Garthoff, "Soviet Doctrine on the Decisive Factors in Modern War," *Military Review*, July 1959; Anonymous American Officer, "Offensive Doctrines of the Soviet Army," *Military Review*, Sept. 1962; and Lt. Col. Truman R. Boman, "Current Soviet Tactics," *Military Review*, March 1962.

[31] See, U.S. Army, *Field Manual 100-5, Operations 1962*, pp. 73-74; Mitchel Goldenthal, "Corps in the Mobile Defense," *Military Review*, Sept. 1957, p. 14; and Robert A, Doughty, "The Evolution of U.S. Army Tactical Doctrine, 1946-76," Leavenworth Papers (Ft. Leavenworth, KS: Combat Studies Institute, 1979), pp. 23-25.

attacker requires a 3 to 1 superiority to overcome a defender.[32] This superiority is necessary because the attackers must break cover and expose themselves to the defender's fire in order to dislodge them. This exposure leads to greater casualties on the side of the attacker, hence the required superiority.[33] Therefore, if a force is outnumbered, one option is to exploit the inherent advantages of the defender to blunt the attacker's superiority and to even the playing field.

This reasoning about defense was incorporated into U.S. Army doctrine in the early 1960s. Up until then, *Field Manual 100-5, Operations*, the U.S. Army's main warfighting manual, drew its understanding of the relationship between attack and defense from the Principles of War. Ideally, a commander would seize the initiative with the attack. Thereby, the attacking force would dictate the tempo of operations and undermine the adversary's plans by forcing it to react to the initiator's actions. However, such a concept of operations was not an option for an outnumbered and outgunned force. Bowing to tradition, the 1960s manual included the Principles of War, but immediately placed significant caveats on them and warned that blind adherence to the Principles risked defeat. Moreover, the Principles did not appreciate the advantages of defensive operations. Contrary to previous army doctrine, *Operations 1962* and *1968* argued that the defender could actually enjoy the initiative. A commander could possess the initiative in the defense by compelling the attacker to respond to the defender's plan. For instance, the attacker must traverse ground prepared by the defender. The defender can exploit the terrain to canalize the attacker into areas where the defender enjoys advantages. The defender then withdraws rearward when the attacker concentrates to destroy it. Through such a defense in depth, the defender gains the initiative and wears down the attacker.

In his 2004 work *Military Power*, Stephen Biddle corroborates this insight and argues that the defense in depth is an extremely powerful military tactic that has shaped modern warfare.[34] U.S. Army doctrine in the 1960s also argued that such a defense could *destroy* the attacker and eject it from the defender's prepared position. This was an important change because, according to the Principles of War and previous army doctrine, destruction was the decisive means to victory and was reserved for the attacker alone. The defender, it was now revealed, could also engage in decisive action.

A defense organized in depth also helped the defender gather intelligence about the attacker and his intentions. This insight was a key element of the Active Defense, the post-Vietnam doctrine of the U.S. Army. Here, a covering force initially would resist the attacker to determine where its main effort was concentrated. A mobile reserve would then place itself in the path of the main effort and employ a

[32] John J. Mearsheimer, "Assessing the Conventional Balance: the 3:1 and Its Critics," *International Security*, Spring 1989, pp.54-89; and T.N. Dupuy, "Combat Data and the 3:1 Rule," *International Security*, Summer 1989, pp. 195-201.

[33] For a recent treatment of these ideas, see, B.A. Friedman, "Chapter 13: The Offense, the Defense, and the Initiative," *On Tactics: A Theory of Victory in Battle* (Annapolis, MD: Naval Institute Press, 2017).

[34] Stephen D. Biddle, *Military Power: Explaining Victory and Defeat in Modern Warfare* (Princeton, NJ: Princeton University Press, 2004).

defensive doctrine to slow and destroy the attacker as he advanced into terrain known and prepared by the defender.[35]

However, a purely defensive scheme was unlikely to defeat a Soviet attack on Europe. To defeat Soviet forces in local engagements, Army doctrine writers realized that commanders would need to make use of local counterattacks. Here, they invoked Clausewitz's understudied wisdom on the power of the defense. A defense is not completely passive, Clausewitz argued, but is a shield made up of carefully directed blows.[36] The key for the army was to organize local counterattacks to defeat segments of the enemy force but avoid a general counteroffensive, which would fail given the balance of forces. A general counterattack, which defense intellectuals suggested as an alternative doctrine,[37] would be too risky and lead to the destruction of NATO's outnumbered force.[38] Local counterattacks were the answer.

The perilous conditions of the U.S. Army in Europe inspired its leaders to enumerate the advantages of defense. We can profit from their insights to develop components of an effective cyber-defense and counter claims that the offense enjoys all the advantages on virtual battlefields.

Insights from Cold War Army Doctrine and the Cyber Realm

In cyberspace, as in military tactics and strategy, the defender can know the terrain better than the attacker and can design its network security to constitute a defense in depth. Interestingly, Microsoft is already drawing on this doctrinal insight when it recommends a "defense in depth" to its security clients.[39] The defender can prepare the cyber terrain in a number of ways. In combat, the defender can make a position appear vulnerable by leaving the first few defensive positions empty to lull the attacker into a false sense of security and draw it deeper into the prepared position. Similarly, in the cyber realm, the defender could leave certain obvious vulnerabilities in parts of the network to draw in hackers seeking the path of least resistance. As the attacker is drawn deeper into the defensive position, the defender can observe it.[40] In the same way, as the cyber defender draws the hacker into the designated part of the network, the defender gathers intelligence on the hacker's

[35] U.S. Army, *Field Manual 100-5, Operations* 1976, pp. 3-6, 3-3, 4-10 to 4-11, 5-2, 5-7, 5-10; and Benjamin M. Jensen, *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford, CA: Stanford University Press, 2016), pp. 40-41.

[36] Clausewitz, *On War*, p. 357

[37] William S. Lind, "Some Doctrinal Questions for the United States Army," *Military Review*, March 1977, pp. 54-65; and Edward N. Luttwak "The American Style of Warfare and the Military Balance," *Survival*, March/April 1979, pp. 57-60.

[38] Richard Lock-Pullan, "Civilian Ideas and Military Innovation: Manoeuvre Warfare and Organisational Change in the US Army," *War and Society*, vol. 20, no. 1 (2002), pp. 125-147.

[39] Microsoft, "Security Content Overview," https://msdn.microsoft.com/en-us/library/cc767969.aspx#XSLTsection121121120120.

[40] Gartzke and Lindsay, "Weaving Tangled Webs," pp. 320-321.

behavior, capabilities, and possible origin. All the while, the defender can remain concealed.

As Gartzke and Lindsay point out, such methods are not just speculative. In 1986, after detecting an intrusion attempt in the Berkeley Laboratory network, Clifford Stoll created pretend systems and documents, which he then used to assess the hacker's methods and objectives. Stoll fabricated classified documents, the opening of which triggered alarms. The authorities eventually apprehended the hacker who turned out to be a West German citizen selling secrets to the KGB. More recently, cyber defenders have used "honeypots," fake systems with fake databases and logs, to gather intelligence on and apprehend hackers.[41]

Relatedly, in 2017, a cyber wargame hosted by NATO's Cooperative Cyber Defense Center of Excellence (CCD COE), "Crossed Swords," also demonstrated the power of defensive cyber capabilities. NATO tasked its highly skilled "red team" of hackers with infiltrating a network protected by the cyber security firm *Cymmetria*. The cyber defender used multiple detection tools to discover the presence of the attacker. They set up decoy machines and "breadcrumb" files to discover when and how the attack happened. At one point, the red team infiltrated a decoy machine that the cyber defender had made to look like a human resources database. On this database, the attackers found credentials to another database that was being run by yet another of the defender's decoy machine. As the attacker mapped this network, it discovered more decoys. The attacker used valuable time exploiting this fictitious network. The attackers thought they had the initiative when in fact they were responding to the defender's plan. As one participant later wrote: "Few things are as satisfying as seeing attackers write: 'We got the creds for the relay machine on workstation 6, infect,' when it's exactly where you want them to go."[42] Even when the defenders showed the attackers how they were caught on the first day, the attackers "still didn't pinpoint any of the decoys, including the machine they were running on during the first day." Dean Sysman summed up the results of the exercise in a way that highlights the advantages of the defense in cyberspace:

> The web hacking team spent a lot of time trying to crack the first decoy that they had encountered, the HR database. We saw them trying to authenticate using all the credentials they had collected, and then run a lot of different queries and GET requests to try to hack the decoy. Throughout the exercise, they did not give up. This would prove very valuable for defenders in a real-world scenario, as we not only gained clear intel from the attacker's actions, it also wasted their time and resources throughout the week.[43]

[41] There are even more complex networked collections of honeypots called "honeynets." See, Gartzke and Lindsay "Weaving Tangled Webs," pp. 340-41; and Kristin E. Heckman et al., "Active Cyber Defense with Denial and Deception: A Cyber-Wargame Experiment," *Computers & Security,* Sept. 2013. pp. 72–77.

[42] Dean Sysman, "The Crossed Swords Wargame: Catching NATO Red Teams with Cyber Deception," *Cymmetria*, 2017, http://blog.cymmetria.com/nato-crossed-swords-exercise.

[43] Sysman, "The Crossed Swords Wargame, http://blog.cymmetria.com/nato-crossed-swords-exercise.

The cyber defender made the attacker respond to its defensive plan and gathered intelligence on the attacker as it tried to work its way through a fictitious network. Here again, real-world cyber defenders exploit the advantages of the cyber defense.

Such defensive tactics can also help overcome one of the main issues in cyberspace: attribution. An in-depth defense using such preparations can provide time to identify the attacker and prepare an accurate and proportionate response. The defending state or group can thereby name the attacker and expose its activities to the international community.

In its battle with a hacker, the Georgian government allowed the perpetrator to infect a government computer. The government hid malicious code on the computer that took control of the camera on the hacker's computer. As a result, Georgia was able to expose the hacker, an agent of the Russian government.[44] The longer a hacker engages with this screen of fictitious vulnerabilities, the more information the cyber defender can gather on the hacker's intentions, capabilities, and origins. All the while, the attacker believes that it possesses the initiative because it is attacking. In reality, however, as Cold War U.S. Army doctrine points out, the defender is drawing the attacker into its defensive plan, so the initiative lies with the defender.

Thus, whether they recognize its origin in military tactics or not, cyber defenders have already begun to exploit the advantages of the defense that the Cold War U.S. Army rediscovered. Military insights for the cyber realm are not just of the offensive variety.

Clausewitz's Insights for the Cyber Defender

B.H. Liddle Hart argues that Clausewitz's unremitting promotion of the attack in *On War* helped fuel the mindless offensives and slaughter of World War I.[45] What Liddle Hart and others overlook is Clausewitz's deep appreciation for the power of the defense at the tactical, strategic, and political level. In *On War*, Clausewitz argues that defense is the strongest form of warfare.[46] Within tactics, or during the engagement, Clausewitz argues that the defense has three main advantages: surprise, terrain, and concentric attack. The attacker enjoys surprise at only a single point within the engagement, at the start. The defender, on the other hand, through unexpected counterattacks, enjoys the advantage of surprise all along the line with the attacking force. Moreover, while the defender might be at a disadvantage on a specific piece of terrain in an engagement, overall the defender knows the terrain better than the attacker does. In addition, Clausewitz contends that because the attacking force is pushing into the defender's territory, he is

[44] Denning and Strawser, "Active Cyber Defense," p. 67.
[45] Basil Liddle Hart, *The Ghost of Napoleon* (London, UK: Faber & Faber, 1933), p. 122; and Hew Strachan, *Clausewitz's On War: A Biography* (New York, NY: Grove Press, 2007), p. 16.
[46] Carl von Clausewitz, *On War*, pp. 357-359.

constantly in danger and in fear of encirclement and of being cut off.[47] The attacker also rarely knows the defender's position in full, but the attacker's tactical disposition is often under the observation of the defender before the engagement.[48] Earlier, we saw how the Cold War U.S. Army appreciated this advantage and that cyber defenders are already employing it to significant effect.

These advantages notwithstanding, Clausewitz argues that, although defense is the stronger form of fighting, its object—resistance—is a negative one. To achieve any kind of significant tactical victory, the defender must transition to the attack. However, it is in this transition from defense to attack that the defense finds one of its greatest advantages. For the attacker, all the natural elements of friction are acting on it as it approaches the defender's position. The very act of moving his forces, even in the absence of the defender's fire, wear them down physically and mechanically. While the defender waits for the attacker, he experiences much less wear. When we appreciate the effects of friction, it is clear that the attacker will suffer more losses than the defender. Again, this reality inspired the rule of thumb that the attacker must enjoy a 3 to 1 superiority. The counterattack is a far less dangerous maneuver than the attack against prepared positions. The attacker will not be expecting the surprise and will not have time to prepare defensive positions. When the attacker becomes the attacked, therefore, it enjoys none of the advantages of defense, and its offensive exertions have already worn it out. In this way, a *counter*attack is more effective than an initial attack. Therefore, if a party to conflict wants its attacking forces to be most effective, it is best to begin on the defensive, preferably one organized in depth, and then to transition to the attack.

Attack is the weaker form of fighting, for Clausewitz, but it has the positive objective of victory rather than resistance. Thus, *if the defender seeks to impose a decision by force on the attacker*, defense is a prelude to attack.[49] However, the defender may not seek a decision and instead prefers to wear out the attacker as it runs aground on the shoals of a well-established defense. In such circumstances, the attack ends when the attacker despairs of achieving its object and withdraws.

Regarding strategy, Clausewitz also sees the defense as having important advantages. When an army attacks into a country's territory, the strategic defense retains the three advantages of the tactical defense, and for the same reasons. However, the defender also enjoys at least one further advantage. The use of offensive tactical engagements allows the strategic defender to win victories and redress the balance of power within the theater of war. Once these defensive victories have shifted the balance in the defender's favor, it can move to the strategic offensive to defeat the attacker and recapture lost territory. Like the tactical defense of a position, the strategic defense of a country is only an expedient prelude to a move to the strategic offensive. However, any country that wishes to defend itself at the lowest possible cost uses the advantages of the defense to wear its opponent down before shifting to the offense—assuming, of course, that the defender seeks to

[47] Clausewitz, *On War*, Book 6, Ch. 1, p. 360.

[48] Clausewitz, *On War,* p. 361

[49] Clausewitz, *On War*, p. 358.

impose a decision on the attacker by force rather than the attacker withdrawing out of frustration.

We can apply Clausewitz's insights about the defense and surprise up to this point to the cyber realm. While the defender observes the attacker entering the defender's prepared network, the defender is concealed. When the defender launches its counterattack, local or general, it will likely achieve surprise. Additionally, the most effective way to enable the cyber offense may be to begin on the defensive and then, once defensive tactics have gathered information about the attacker's capabilities, intentions, and origins, transition to the offense. The defender then enjoys surprise and can act before the cyber attacker has an opportunity to prepare its cyber defense. Consequently, even if we want our national cyber strategy to have a powerful offensive element, it will be most effective if a powerful cyber defense precedes a major counterattack.

However, as in war, a transition to the cyber offense is not always necessary. The cyber defense can so frustrate the attacker that it temporarily halts its attack. Here, the defender does not seek a decision, but rather frustrates the attacker with a powerful defensive front. For example, the cyber defender can stop attacks coming from specific IP addresses with the proper legal authorities and cooperation with other governments and private companies.[50] With the importance of such cyber allies in mind, we turn to Clausewitz's final insight about the power of the defense.

The final advantage of Clausewitz's strategic defense is of particular interest to scholars of international relations who are concerned about shifts in the international status quo. In an often overlooked section of *On War*, Clausewitz argues that there is a "tendency" among states in the international system towards promotion of the *status quo* and stability, and away from revision and instability. Clausewitz employs the word *tendency* because he argues that when a single state is sufficiently strong it can override the general tendency of the system. However, he argues, this does not disprove the tendency.[51]

> This we suggest is how the balance of power should be interpreted; and this kind of balance is bound to emerge spontaneously whenever a number of civilized countries are in multilateral relations.[52]

Clausewitz is arguing that the states in the international system seek stability. States seeking to upset the balance of interests in the international system, therefore, will experience friction from the whole. The defender often has the strategic advantage of representing the maintenance of that stability, the *status quo*. Consequently, the defender "will find that it has more friends than enemies."[53] Countervailing coalitions of status quo powers will balance against states that seek to upset the *status*

[50] Denning and Strawser, "Active Cyber Defense," p. 72.
[51] Clausewitz, *On War*, p. 373.
[52] Clausewitz, *On War*, Book 6, Ch. 1, p. 373.
[53] Clausewitz, *On War*, pp. 373-374.

quo.[54] Clausewitz writes, moreover, that the more vigorous a state's defense of the status quo against aggression, the more likely other states in the system will come to its aid.

By employing defensive tactics and strategy properly, a state can bring forth the defensive tendency in the international system. In the present international system, the United States is a status quo power, and the majority of countries are not seeking to revise the current international order.[55] As noted earlier, in the cyber realm, too, the United States is a status quo power. If the United States can mount a powerful defense of cyberspace, it can expose the origin of attacks and make itself the champion of the cyber status quo. In theory, a robust defense will attract cyber allies to the United States. Like the United States, many states depend on free and open virtual lines of communication for international commerce and communications. Hence, the majority of countries prefer the cyber status quo and are likely to come to the aid of its defender. They are also more likely to share information critical to tracing the origins of cyber threats and cutting them off upstream from their targets.[56] Such a defense might not only attract state support, but also private industry and other non-state actors in the cyber realm. An effective cyber defense, therefore, could facilitate the kind of virtual cooperation that is most difficult—that between states and the private companies that manage things like key infrastructure. Conversely, an overly aggressive U.S. cyber strategy could lead other states to see the United States as a disturber of the cyber peace. A strong U.S. cyber defense will solidify its status quo role and promote cooperation with other states and actors in the cyber realm. A firm defense also buys time for the United States to identify the attacker and bolster international support for a response. Clausewitz's insights about the advantages of the strategic defensive, therefore, could have powerful analogs in the cyber realm and show important advantages in a more defensive cyber strategy, especially for the United States.

Possible Objections

I should address two possible objections. First, experts in the hardware and software of cyberspace might dismiss some of the defensive advantages set out here because the technology to execute them does not yet exist. However, this article not only examines how we might use existing capabilities but what future capabilities are desirable. Interestingly, recent research into key technologies developed for the U.S. Army over the past five decades shows that the Army imagined concepts of

[54] This is not the same understanding that Waltz or Mearsheimer have of the balance of power, but Waltz, at least, identifies a similar tendency. See, Kenneth Waltz, *Theory of International Politics* (New York: McGraw-Hill), p. 127: and John Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton & Co., 2001), p. 20

[55] See, Stephen G. Brooks and William C. Wohlforth, *World Out of Balance: International Relations and the Challenge of American Primacy* (Princeton, NJ: Princeton University Press, 2008).

[56] Denning and Strawser, "Active Cyber Defense," pp. 66 and 68.

operations and then industry developed the technologies to enact those concepts.[57] Therefore, this essay may help develop concepts of operations for the cyber defense that can guide the development of defensive cyber capabilities. Second, some might object that transferring concepts from other forms of warfare to the cyber realm will either fail or hinder the policy process.[58] However, whether we like it or not that transfer has already taken place, and the result has been an emphasis on a cyber offensive with some dangerous implications. The goal here is to show that we can also use insights from conventional warfare to promote a robust cyber defense. In addition, even if we cannot apply arguments about the power of the defense directly to the cyber realm, we can use them to counter those who import arguments about the superiority of offensive warfare into the cyber strategy debates. Because several of the arguments come from Clausewitz, considered one of the greatest military minds of all time, the arguments about the defense will have added force. Thus, the arguments presented here can head off calls for a highly offensive cyber doctrine, with all its dangerous implications.

Cyber Defense Going Forward

Military doctrine and thinking can be an important source of insight into the advantages of defensive operations in cyberspace. Calls for the United States to develop the offensive side of its cyber strategy have their merits. Moreover, leaders will be attracted to cyber-attacks as a low-cost covert action. However, the cyber offense risks conflict escalation and could undermine the image of the United States as the defender of the internet status quo. The promotion of offensive cyber operations overlooks the real and potential advantages of the cyber defense. A number of these advantages, like defense in depth and surprise, can be adapted to the cyber realm. In addition, awareness of the virtues of cyber defense, some of which cyber defenders already use, can help guide the development of new cyber capabilities. These defensive insights can help to shape concepts of operations, which often drive technological innovation, rather than vice versa. For instance, this analysis shows the importance of developing better capabilities for observing hackers after they infiltrate a network and in developing better "honeypots" and false networks to buy more time to identify the attacker and its intentions. In addition, for those who insist on a cyber offense, a robust cyber defense is actually the most effective prelude to an offensive cyber counterattack.

This scenario leads to two requirements for cyber capabilities. The first requirement is that further development of capabilities for limited cyber counterattacks should let the adversary know that the response is limited. Second,

[57] Jensen. *Forging the Sword: Doctrinal Changes in the U.S. Army* (Stanford, CA: Stanford University Press, 2016), pp. 74, 123.

[58] Recently Joseph Nye examined the ways in which the traditional concepts of deterrence and dissuasion are analogous to deterrence and dissuasion in the cyber realm. Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Winter 2016/2017; and Martin C. Libicki, *Cyberdeterrence and Cyberwarface* (Santa Monica, CA: RAND, 2009), p. xiii.

and less limited, is the development of cyber capabilities that can shift from defense to offense rapidly to exploit the powerful transition from defense to counterattack highlighted here. In the end, the best offense actually begins with a strong defense.

Some experts argue that the biggest hindrance to cyber defense is its high cost, though Slayton argues convincingly against this contention.[59] However, even if the cyber defense is more costly than offense, we must weigh the resource investment against the costs of inadvertent escalation produced by a more offensive cyber strategy. We also need to consider the strategic and political costs. A strong cyber defense makes it clear that the United States is the protector of the cyber status quo, while an offensive strategy paints the country as the disruptor of that status quo. The benefits of this image are not superficial. Maintaining the internet status quo is in the interests of many countries, as well as private companies, and U.S. cyber strategy should encourage them to ally with the United States to pursue their common goal of a stable cyberspace.

[59] Eneken Tikk, "Ten Rules for Cyber Security," *Survival*, vol. 53, no. 3 (2011), p. 129; and Slayton, "What Is the Cyber Offense-Defense Balance?"