Winning the Digital War: Cyber Ideology and the Spectrum of Conflict

Matthew Flynn

Marine Corps University, mflynn92@gmail.com

Follow this and additional works at: <https://digitalcommons.usf.edu/jss>
pp. 87-102

Recommended Citation

Flynn, Matthew. "Winning the Digital War: Cyber Ideology and the Spectrum of Conflict." *Journal of Strategic Security* 14, no. 4 (2021) : 87-102.

DOI: <https://doi.org/10.5038/1944-0472.14.4.1968>

Available at: <https://digitalcommons.usf.edu/jss/vol14/iss4/6>

This Article is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in Journal of Strategic Security by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.

Winning the Digital War: Cyber Ideology and the Spectrum of Conflict

Abstract

Cyberspace allows ideology to dictate who wins a war. That technological medium has marginalized violence to such an extent that a belligerent must make a cognitive effort a priority. That focus means humanity has at last reached a coveted threshold where ideas determine a war's outcome. This article traces that evolution along the "spectrum of conflict," a military categorization encompassing all of war. This act of reductionism must confront cyber realities that alter an understanding of war as one driven by acts of violence. This feat means a digital peace finds an equal footing with war arising from a cyber ideological conflict. That conflict rests on cyber rebellions derived from an online interface contested in content but able to withstand the pull of government oversight. Stripped of violence as an absolute defining war, cognitive war becomes of paramount importance as a broad intellectualism compels a state of war. Ideology comes less from a meaning shaped by political context and more from online access impacting political norms. This contest in cyberspace means winning the digital war requires an open interface to pressure authoritarian regimes into reform, all the while allowing for much of this same friction that arises in states favoring democracy. Finding that balance arrests the endless process of war as the chief means of human interaction.

Introduction

Cyber ideology best captures the primary means of warfare in the cyber domain. Any conflict in cyberspace relegates violence to a secondary even tertiary effect, paving the way for a cognitive battle online. This confrontation overwhelmingly favors nations supporting “openness,” that is, the free exchange of information online. In this mix lies a clash over values stemming from a social interaction as a needed interchange given human disposition and in offering the means to improve the human condition. This online quality tests political systems as those seeking centralized control look to contain openness, while those favoring democratic government attempt to ensure unfettered access online all the while shoring up their own vulnerabilities. Technology may allow a plethora of options when online, and it stands to enrich social interaction as a result, but other realities strive to curtail this connectivity. Hence, the ideological struggle online emerges as ideas determine the validity of user access.

The cyber war over ideological consensus forces those so engaged both to preserve the digital medium on which the war is waged and to control it. Such sparring raises issues of what constitutes the natural state of online use and how this standing corresponds to human activity. But what that struggle looks like requires explication seeking a measure of war along what the U.S. military calls the “spectrum of conflict.” That continuum presently exists without a measure of the impact of cyberspace on that axis. This article takes that step leaving war looking different from a measure of physical harm imposed by one party on another; rather, a cyber war exists on a cognitive plane devoid of physical violence. With violence marginalized, this article’s thesis is that the online battlefield allows belligerents to resolve tensions short of armed conflict producing an ideological confrontation across an open Internet.

That battlefield in cyberspace means popular uprisings against authority have received a new lease on life.¹ Social media has fostered online activism to such a point as to bolster the means of organization and objection to oppressive rulers. Thousands upon thousands of people use these channels to help marshal that opposition. They also risk persecution at the hands of repressive regimes looking to crush internal dissent. Worse, nations cherishing the openness of the Internet may act in similar

fashion as authoritarian states and restrict online access. The United States currently weighs the pros and cons of increased controls to counter the growing threat of political violence at home propelled by online forums, best exemplified by the recent storming of the U.S. Capitol by a mob unleashed by the Trump administration's false claims of election fraud. That shocking spectacle may register in many ways, but it best serves to remind the United States to safeguard an open Internet to compel an ideological showdown online. Winning the cyber war means accepting the friction this technology introduces into the governing process to pressure authoritarian regimes to reform. That tradeoff forces Americans to live up to the ideals that established the nation, chief among them that citizens do not meet differing views with acts of violence. Cyber realities could break the nation or lead it to rekindle its global mission of defending democracy, a mission that starts at home.

The Nature of War

To assess the experience of war starts with a consensus in military circles that the nature of war is unchanging, only its character changes. The nature of war consists of several constants including friction, chance, and genius. Friction ensures that once a military action unfolds, plans will go astray, and consequences will arise producing unwanted and unintended effects. Chance explains those things that contribute to friction and are often out of human control or arise inadvertently because of human activity. Genius speaks to the ability of certain individuals to overcome these issues, not to prevent them, but to overcome them. These aspects of the nature of war, in this case coming from Carl von Clausewitz's study, *On War*, and any other aspects one may add, are select and limited.² For this reason, attention quickly pivots to defining the changing character of war.

The character of war is ever expanding given new weapons and tactics introduced to the battlefield. Change appears endemic to the definition, upending the construct that the nature of war never changes. Many uphold the new in the name of modernity as each age announces its weapons as revolutionary and promising to reshape the battlefield. Examples include the flourishing of military innovation prior to the Second World War.³ "Effects based operations" arose in the 1980s-1990s, followed by "netcentric" warfare.⁴ Frequently these modern developments do bring change. However, a closer look acknowledges that the new weapons may

well change the character of war, but not the nature of war, meaning friction, chance, and genius. No weapon system has overcome or disavowed these constants.

The unchanging nature of war but its expansive character makes for a striking continuum, a small constant comprising the nature of war, and an ever-expanding set of factors accounting for its changing character (see Figure 1):

Figure 1

Source: This figure and the following figures created by the author.

The construct's chief importance lies in the quest of military personnel to seek timeless principles of war. No matter the age, certain things will always be present and found in the unchanging nature of war. For the U.S. military, should one grasp such basic tasks as mass and maneuver, deception, leadership, and the will to fight, they stand to be the more capable warfighters. The Marine Corps calls this goal "maneuver warfare," a mandate repeated in Joint doctrine.⁵ The U.S. Army stresses four "tenets of unified land operations" consisting of simultaneity, depth, synchronization, flexibility.⁶ These capabilities can surmount friction and survive chance due to an almost learned genius. To gain this skill requires an intensive study of war. Finding something quantifiable in the long history of war brings comfort to military personnel. Seeing patterns and continuity across time identifies the means one can point to and rely on to excel at warfighting to master the ugly reality of war.

Cyberspace may well upset this calculation. That new space may have changed the nature of war making principles harder to determine. Former U.S. Defense Secretary James Mattis appears one of few voices open to this change when he pointed to the advent of AI as possibly changing the nature of war.⁷ At a minimum, increased complexity due to expanding war into the cyber domain means new patterns or possibly the invalidation of

past patterns defining the character of war. Either way, having to recalibrate the principles of war places an unwelcomed burden on the warfighter. The student of war must thoughtfully conduct this analysis or risk losing the next war. Given the stakes, one can understand the apprehension among military professionals as they take a measure of cyberspace as a warzone.

The Spectrum of Conflict

The trepidation of having to learn new, key aspects of war appears valid because cyber realities prompt one to ask if war must include acts of physical violence via combat arms producing death and destruction as a measure of force. This common view of war looks like the following along the spectrum of conflict (see Figure 2):

Figure 2

Army uses of this construct vary a bit, from a U.S. Army graphic depicting a “spectrum of combat” and a “spectrum of peace” in Army Vision 2010, a document the Army released in 2005 to take ownership of its contribution to joint operations in pursuit of “full spectrum dominance” across a “spectrum of crisis.” By 2008, “spectrum of conflict” was in place as a backdrop for Army Operations.⁸ The Marine Corps was more consistent. In two documents spanning eight years, from 1989 to 1997, the spectrum of conflict refers to actions meriting restraint of military force and those where restraint is absent given a state of general war.⁹

Regardless of the depiction, violence stands as the foremost indicator of where one sits on this continuum. One gets closer to peace with the absence of violence. The reality of war grows clear with the onset of violence. Cyber appears to have changed the nature of war by stripping that measure of violence from war. But war never rested on only military arms dispensing violence. Its dimensions always grew bigger than this. One must contemplate the use of force without combat, or a state of war without violence. An actor can apply force via instruments of power short of physical violence. A broader understanding of force absent physical acts of violence creates room for the cognitive struggle defining war. Still, the

nature of war does not change. Rather, with cyber, war now includes the primacy of intellectual acts.

In making this intellectual side of war paramount, cyber gets us back to what war is supposed to be, or can be, and that is conflict as an argument. This end achieves Plato's 'political man' in *The Republic*, where humanity seeks rationalization through philosophical inquiry to attain the "good life" via argumentation rather than force. To engage argumentation as an act of war leaves one with a broad understanding of war, but another simple continuum charts this sensible conclusion (see Figure 3):

Figure 3

Stressing this intellectual parameter leads one to the view that there will always be war. The oldest military maxim asserts that humans will fight and there will always be war because of that fact. But physical violence is not its foremost measure. Chinese military theorist Sun Tzu got at this distinction long ago. In his famed, *The Art of War*, when seeking to defeat an enemy short of the use of military arms, he wrote, "To subdue the enemy without fighting is the acme of skill."¹⁰ War does, in fact, remain a constant, but the means of war clearly hinge on intellectual confrontation rather than meting out physical violence.

As sure as there is war, less certain is peace; just as war will always take place, peace can never be at hand. Even the complete elimination of the enemy means no matter who survives, conflict, and, therefore, war, is the result. Allies will fray and one of them will assume the role of adversary leaving once unified victors to clash among themselves. One way or another, war will reoccur.

This reality presents one measure of absolute war, promising that war will always happen and not end. Cyber adds to this reality, meaning that the advent of cyberspace has not changed the nature of war. Rather, cyber realities suggest that war looks different from war resting solely on violence via use of force. Acts of physical violence certainly help define war, but those acts highlight conflict featuring the cognitive struggle defining argumentation.

No Peace on the Spectrum of Conflict

The idea of always facing war via intellectual threats and at times facing threats of physical violence soon encounters a nature of war that offers another measure of war as delivering complete destruction. One exists along an axis offering degrees of war. To stay far left limits war, but does not deliver peace. A move right invites total war. An escalation to the right renders wars more physical and feared and therefore restricted, if possible, all the while accepting war as a perpetual condition of existence.

Consequently, the continuum now defines war as a spectrum of conflict within two parameters as follows (see Figure 4):

Figure 4

One should fear total war since nuclear weapons have indeed meant an absolute as the complete destruction of humanity. A total war now has a face. Limited war acts as a good since it curbs this threat of complete destruction. Now war assumes a second reason for an absolute. Not only is it always present as part of human existence, but obliteration of humanity as an absolute exists as well. On the continuum, an absolute peace fades further from view, peace meaning no outright hostilities but always preparing for war or being on-guard from a horrible end. That preparation accepts the absolute of war, even total war. There is now one absolute, but not another. An absolute war exists but not an absolute peace prompting a need to correct the illogic of the continuum: If absolute war is possible, so too is absolute peace.

Unfortunately, things do not improve as the continuum gains more items. Genocide presents another absolute defining total war. That alarming end registers fear with no optimism or hope of something better other than lesser acts of war. Here, kinds of war surface and these take many labels: Small, irregular, unconventional, people's war, all existing along the spectrum of conflict. The labels abound but the concept dictates a linear progression. A move from left to right takes one from unconventional to conventional war (see Figure 5):

Figure 5

 Unconventional War

Conventional War

In this way, an absolute war again surfaces as a norm since conventional war will equate with total war and the goal to destroy an enemy. Conventional use of force refers to those armies enjoying a tremendous advantage in combat arms, and therefore seeking the obliteration of the enemy, or total war. Its place on the far right is clear. Unconventional refers to those contesting that overwhelming military power and having to do so well short of any ability to stand up and face the enemy in combat. The continuum does not measure peace as again war is the norm, only war's manifestation is in doubt.

The more useful message with plotting unconventional and conventional war along a continuum is that to sit on the far-left means seeking other means of contesting enemy strength, offering more of an intellectual challenge. The trajectory looks like this (see Figure 6):

Figure 6

 Unconventional War
Intellectual Challenge
Conventional War
Physical Brawn

Violence is present on either end, but the violence goes mute on the left. On the right, a reliance on physical force of arms remains the norm. This view shows that one likely does more thinking when in a position of inferiority of combat arms and does less thinking when enjoying a preponderance of strength and seeking a conventional fight. The issue becomes one of asking how much intellectualism impacts war, and should be in war.

Any continuum at this point looks like following (see Figure 7):

Figure 7

Cyber uproots this view because of the difficulty of classifying a cyber war. With no violence, war becomes a lost sighting. Cyber expert Thomas Rid casts this need for violence firmly in the tradition of Clausewitz when he paraphrases the master: “All war, pretty simply, is violent.”¹¹ War seeks out physical force to break an opponent’s will and net a political gain. Without the violence, the strife in cyberspace presents sabotage, espionage, and subversion as the mainstay of conflict in that domain. In Rid’s estimation, this reality is different from war.

In that case, a continuum with cyber suggests only a cognitive means of warfare, and therefore an intellectual showdown as war. Stealing data, interdicting connectivity mixes with outright subterfuge via messaging and looks like the following (see Figure 8):

Figure 8

Gravitating toward messaging certainly shapes a cognitive battlefield and takes one away from any physical measure that might be found at the opposite end of this continuum. No matter the intellectual strife, one could say peace triumphs across the flow of information merely impacted by a means of warfare bereft of violence.

While this cyber battlefield may lack violence, the prospect of war looms large. Many experts reject the view that no war occurs in the domain because violence does not lurk there. Some declare a war is afoot even without physical conflict. Coercion due to use of force remains prominent, even if violence does not kill people. For instance, John Stone writes, “Acts of war involve the application of force to produce violent effects. These

violent effects need not be lethal in character.”¹² Force defines war, not the cost in lives. Timothy J. Junio essentially agrees, writing that, “if cyber war happens, it will be extremely costly even if not lethal.”¹³

Given the assumed stakes of the struggle there, a war is the best determination. Certainly, Plato’s classification of war as argumentation comes back to the forefront of things. Beyond cognitive realities, to fully account for digital hacks, intrusions, and attacks, the physical does matter a great deal in terms of the potential to cripple a power grid or some other critical infrastructure of a nation via online attack. While this possibility is extreme, it is still possible. Conversely, on the purely cognitive end stands the ability to impart political change based on a sharing of information alone fostering “cyber rebellions.”¹⁴ In other words, connectivity shapes the following battlefield, positioning war as the chief concern in cyberspace (see Figure 9):

Figure 9

One is purely cognitive, the other physical. In between comes a struggle over the openness of the Internet functioning in cyberspace. On the left sits a struggle over ideology, on the right a need to prevent an overt, online attack.

A Cyber Cognitive War

The cyber lens underscores that war is primarily a clash over ideas. If an enemy cannot be destroyed, and if peace is impossible, and the various continuums say this is so, then the war continues albeit on a much more cognitive basis. In short, military action, no matter how violent, cannot wipe out the thinking that helped foster the war. To break the enemy’s will (mentality) may be the main goal of any war, but that end comes with an understanding that physical violence only gets one part of the way there.¹⁵ In this context, the violence at the hands of armies is supposed to push the conflict into the cognitive realm on terms most favorable to the side enjoying a preponderance of physical strength. Of course, the vanquished can look to the other extreme, and along this axis see mental defiance as

the final place of resistance, and the best means of doing so for how does one defeat the mind?

Cyberspace presents an answer. In the rampaging of cyber ideology lays a struggle in that domain completely in favor of states embracing openness. The push for an unfettered exchange of information as empowering a community sparks a cognitive challenge to all those opposing this norm. This axis places openness on one end, surveillance on the other (see Figure 10):

Figure 10

The contested space in between amounts to a cognitive war, a struggle to convince users of the dangers of being online if one seeks to overturn openness as a norm, and an online struggle to welcome users to engage in discourse, not just free of government oversight, but as a means of defying that idea of control, if one supports openness. No violence marks this confrontation, but the struggle over ideas in cyberspace defines war itself. The inability of conventional force to achieve a 'decisive' end drives conflict into this intellectual arena where war assumes its true nature, a cognitive struggle to determine victory. This cyber battle ensures that the intellectual imperative that always defined war has overcome violence along the spectrum of conflict producing a state of war without physical violence.

The cyber war as ideological struggle does not mean an end of conflict, only a war on favorable terms to those states embracing openness. At last, a combatant can team a physical domination with a mental assault as well that speaks to achieving victory and seeing peace as a real possibility, even if remaining at cognitive war. Peace gains meaning as the absence of purposely violent acts seeking physical destruction and loss of life. For this reason, war becomes an intellectual act first. In other words, resorting to violence constitutes an admission of inferior ideas, that one has lost the intellectual battle.

Once free of violence, warfare now becomes a means of cognitive struggle, the battlefield the cyber domain. Here, any combatant at tremendous

disadvantage in a physical confrontation will find another application of war that may yield better results. This thinking means the range of war acts moves from primarily a physical embrace of violence to a shunning of violence altogether in favor of a strictly cognitive battle. The cognitive showdown in cyberspace is as genuine as any war witnessing the use of violence, making the strife there something far greater than crime or espionage. In the ideological implications of cyberspace rests a struggle to advance the democratic process and to deny it. The good news for cultures supposedly tied to that democratic tradition becomes their ability to pursue this kind of representative government by defending the openness of the cyber domain, always shorn of violence as the chief measure of war. While strife besets this virtual world as much as the physical one, the trajectory along the spectrum of conflict speaks to finding virtue in a supremacy of arms predicated on an elevation of ideas as the primary means of conflict in war. The measure of this dynamic remains a focus on cyber ideology, and one can find much encouragement in this now bloodless pursuit.

In this view, war always spoke to hopefully mitigating violence, and therefore sparing life and property. This result came from embracing the use of force to such a point that war would be so horrible that actors would refuse to take this step. This belief came after a long period of trial and error where use of force represented a means of quick victory, shielding all combatants from the worst impact of war, if one could prosecute the war successfully. Still, even in the few instances of such military success, another war followed, and another after that. The recourse to physical destruction of the enemy no matter how contrived proved incapable of netting an end to war.

A Digital Peace

Technology has all but delivered this result of ending war, forcing those less prepared to wage a conventional fight to seek out other ways of challenging a militarily imposed supremacy. Violent acts continue, but the desired brevity of war due to the threat of death and destruction, the desire to limit war to avoid that same end, speaks to getting past violence as the primary means of conflict. Cyber has helped make this aim possible.

A closer look at the rise of cyber realities and their impact on conflict in terms of the ideological struggle in this domain reveals that one has reached a point exposing the inadequacy of measuring war as mainly a contest of violence. Instead, victory as a measure of peace comes into view. Here cyber makes its definitive contribution to war. War consists of the standalone, intellectual confrontation in cyberspace, warfare the effort to enjoy superiority in that cognitive fight in the cyber domain. War continues, but that war does indeed, can indeed, assume a purely intellectual dimension. With no physical and material destruction, a spectrum of conflict yields to a continuum of peace, or where Rid suggested things should stand (see Figure 11):

Figure 11

In between the two extremes comes a series or stages of peace, not kinds of wars along a spectrum of conflict. One could see peaceful coexistence, an alliance, or mutual standoff all existing on a continuum of peace.

Reintroducing peace perhaps represents the most useful element of the continuum, except for again clashing with absolutes. There cannot be an absolute peace or total peace; but a total war is possible if not desirable. The impossibility of peace as an absolute yields to ways of war that match a combatant's preferences of battle. Ways of war are tied to conventional strength of arms, a concession to conventional arms as the best kind of war and as the "American" way of war.¹⁶ Some question this characterization as too ridged given numerous American instances of waging protracted war as something well short of decisive battle.¹⁷ Still, the ideal matters most here, a western way of war pursued by more actors than the United States and always as one of seeking a quick victory by killing the enemy to account for battlefield supremacy and thereby garner a political windfall.¹⁸ Should one enjoy a preponderance of strength in terms of physical arms, many deem that kind of war best and pursue it. If one considers themselves weak in terms of conventional strength, they pursue a cognitive challenge. In either case, the belligerents assume that conventional force of arms predicated on a physical strength of arms works best. That disposition nets political gain from the sheer helplessness of the opponent, now unable to defend themselves and survive and so they

sue for peace, or just capitulate, or have that decree forced upon them by the victor.

That result means so much to military thinking about war that in the eyes of those charged with fighting the next war, cyber's ability to replace such a framework cannot stand as the new reality. But the context to change one's mind, the true aim of war, has become overt in purpose and means in cyberspace, an intellectual exchange online meaning that combatants achieve an absolute—war without violence. That such an absolute has found its way into cyberspace spells an end of militarism. Cognitive warfare there means no war in terms of a measure of violence, and this advancement seemingly deprives military professionals of their foremost reason for being.

Consequently, military retrenchment came in the face of the tremendous success of cyber rendering war a cognitive clash and therefore one of morality and values determining the winner. The clash of wills requires a clash over the ideas shaping both qualities, or cyber ideology. The obvious refrain broke out among those so marginalized and added to the chorus of doubters that Internet realities had added anything dynamic and positive to the human condition. For even if war had assumed cognitive parameters, those on the losing end of this conflict would resort to military force that did produce acts of violence. Moreover, the certainty of violence was not humanity faltering before achievement. War always constituted a physical state of competition, a clash netting violent outcomes. Cyber war poses as no more than a breeding ground for that inevitable contest of arms as a material confrontation. The intellect bowed before brawn, or, as is a constant refrain, the pen is mightier than the sword but no match for a gun.

Because of cyber, one could no longer merely recognize what amount of physical force a military actor might need to find their place on the continuum. The purely cognitive struggle now unleashed in the cyber domain spoke less to force of arms and more to a bloodless contest that spoke to the best of the human condition. Taken together, conflict certainly would remain a human blight, but the virtue of nonviolence now defined this cognitive war online.

A cyber spectrum of conflict looks like this, or where things started (see Figure 12):

Figure 12

Cyber tensions abound but dictate engagement short of violence across the spectrum. This limited reach meant a standalone, cognitive struggle in cyberspace. In drawing this conclusion, one must not fall victim to the artificially linear thinking a continuum invites. Naturally cross-domain interaction allows cyber actions to impact the other domains. But one can distinguish the frequency and composition of actions unfolding only in cyberspace from those in other domains by the lack of physical force involved in any such attacks. That separation renders conflict there a fundamentally standalone confrontation over the openness of that domain. Physical connectedness remains, while belligerents contest logical access. An ideological struggle to preserve that quality of openness ensues, and those operating in cyberspace, as one expert put it, must recognize that the cyber war means the domains of land, sea, air, and space serve cyberspace rather than the cyber domain merely augmenting these other domains via cyber warfare:

...cyber warfare will have a strategic effect by acting as [the] primary means to achieve conventional ends, hence will induce a paradigm shift from the conventional notion of cyber warfare as a tactical force multiplier to the notion of strategic cyber warfare acting as [the] primary means of achieving grand strategic objectives in the contemporary world order.¹⁹

Embracing the old meant losing sight of the new. And it was true that embracing war as a physical contest netting acts of violence to dictate a winner meant little had changed. For war gives up on intellect as a means of settling disputes. In fact, physical brute force meant an admission of a bankruptcy of ideas, a paucity of intellect that one could only overcome via acts of violence. Even noble acts or justified causes could not survive this test since that mandate of virtue rested on the beholder and spoke again to division among humans; they could not agree on a single principle of right

and wrong, that is, until cyberspace. Here intellectualism spoke to humanness plain and simple, a desire to get past bloodshed as an arbiter of war. And best of all, the nation that wielded the physical brawn so tied to war as an act of violence had produced the medium that challenged that thinking. The United States could use its military reach to force conflict into the cyber domain, into an intellectual space where its values and societal norms of shared communication and knowledge to self-improvement could reign supreme. The distinction represents a thin line but a clear line. Physical violence defining war remains a reality, but the strongest nation engaged in such acts only to compel a cognitive war in cyberspace. The spectrum of conflict in the hands of the U.S. military has achieved its foremost purpose. Far from eclipse, the threat of military force proves essential to waging the cyber war.

Pursuing this other view makes cyberspace a monumental moment and achievement. Cyberspace can turn technology into an unquestioned good, can overcome the human schemes to always be at war, and can at last serve as a testimony to human intellectual achievement. That domain can do so without contemplating a future pointing to an idealized end promising a harmony that saddens the triumph of connectivity. This domain embraces a full expression of the human condition and its ability to seek out connections to make this self-actualization happen while having to contend with pitfalls and resistance. It remains a marvelous triumph speaking well of humanity, the United States, and of an optimistic future. Far from becoming vulnerable because of an inability to better place the cyber domain in a familiar context of military conflict as an act of violence, this impossibility speaks well of the outcome of waging war there. Any conflict in this domain features one of ideology. That clash reveals that those embracing openness stand to reap an ideological advantage and profit from online existence muting violence along the spectrum of conflict. This needed goal requires the United States quell the instability at home born of Internet conspiracy theories, all the while preserving an Internet minimizing government controls. To find that balance will model how democracy can function in an Internet age and allow the United States to win the digital war by continuing to advance democratic principles globally.

Endnotes

- ¹ The National Intelligence Council, *Global Trends 2040: A More Contested World* (Washington, DC: Office of the Director of National Intelligence, 2021), 76, https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.
- ² Carl von Clausewitz, *On War*, trans. Peter Paret (Princeton, NJ: Princeton University Press, 1976), 100-122.
- ³ Williamson Murray and Allan R. Millett, eds., *Military Innovation in the Interwar Period* (New York: Cambridge University Press, 1996), 3-4.
- ⁴ Matt M. Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth: Combat Studies Institute Press Long War Paper 26, 2008), 3; David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. (DoD C4ISR Cooperative Research Program, 2000), 1.
- ⁵ Department of the Navy, *Warfighting*, MCDP 1 (Washington, DC: Headquarters United States Marine Corps, 1997), 72-76, <https://www.marines.mil/Portals/1/Publications/MCDP%201%20Warfighting.pdf>.
- ⁶ Department of the Army, *Operations*, ADP 3-0 (Washington, DC: Headquarters, Department of the Army, 2019), 3-12, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf.
- ⁷ Aaron Mehta, "AI Makes Mattis Question 'Fundamental' Beliefs About War," C4ISRNET, last modified February 17, 2018, <https://www.c4isrnet.com/intel-geoint/2018/02/17/ai-makes-mattis-question-fundamental-beliefs-about-war/>.
- ⁸ Department of the Army, *Army Vision 2010* (Washington DC: Department of the Army, 2005), 1, 5, 10; Department of the Army, *Operations*, Field Manual 3-0 (Washington DC: Department of the Army, 2008), 2-1.
- ⁹ Department of the Navy, *Warfighting*, FMFM1 (Washington, DC: Headquarters United States Marine Corps, 1989), 21, <https://www.globalsecurity.org/military/library/policy/usmc/fmfm/1/fmfm1.pdf>; and *Warfighting*, MCDP 1, 26.
- ¹⁰ Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 77.
- ¹¹ Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University, 2013), 1-2, xiv.
- ¹² John Stone, "Cyber War Will Take Place!" *Journal of Strategic Studies*, 36, no. 1 (2013): 107, <http://dx.doi.org/10.1080/01402390.2012.730485>.
- ¹³ Timothy J. Junio, "How Probable is Cyber War?: Bringing IR Theory Back in to the Cyber Conflict Debate," *Journal of Strategic Studies*, 36, no. 1 (2013): 132, <http://dx.doi.org/10.1080/01402390.2012.739561>.
- ¹⁴ Matthew J. Flynn, "Cyber Rebellions: The Online Struggle for Openness," *Journal of International Affairs*, 71, no. 1.5 (Special Issue 2018): 2, 7, <https://jia.sipa.columbia.edu/cyber-rebellions-online-struggle-openness>.
- ¹⁵ Clausewitz, *On War*, 75, 90, 94.
- ¹⁶ Russell Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (Bloomington, IN: Indiana University, 1977), xxii.
- ¹⁷ Brian Linn, *The Echo of Battle: The Army's War of War* (Cambridge, MA: Harvard University, 2007), 5.
- ¹⁸ Victor Davis Hanson, *Carnage and Culture: Landmark Battles in the Rise to Western Power* (New York: Doubleday, 2001), 7.
- ¹⁹ Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009), 4.