The US Army War College Quarterly: Parameters

Volume 50
Number 3 *Parameters Autumn 2020*

Article 13

8-14-2020

On “Social Media Warriors: Leveraging a New Battlespace”

Jason W. Warren

Recommended Citation
Jason W. Warren, "On “Social Media Warriors: Leveraging a New Battlespace”," *Parameters* 50, no. 3 (2020), doi:10.55540/0031-1723.2680.

On "Social Media Warriors: Leveraging a New Battlespace"

Jason W. Warren

This commentary responds to the article by Buddhika B. Jayamaha and Jahara Matisek entitled "Social Media Warriors: Leveraging a New Battlespace" published in the Winter 2018–19 issue of Parameters (vol. 48, no. 4).

The Army was all but defeated. Concentrated across the Delaware River from the advancing Redcoats and their mercenary German allies, General George Washington's Continental Army was hemorrhaging personnel after successive defeats during the 1776 campaign. The Army, indeed the entire patriot cause, was in danger of annihilation and a bloody conclusion to the war if an opportunity had not presented itself. Information warfare (IWar) provided that strategic opportunity, altering not only the fate of the Continental Army, but also the prospects for the new nation.[1]

The case of 1776 was not unique in the history of IWar as it likely has been employed in some fashion since man walked the earth in hunting groups, and certainly since the advent of recorded history in the West, with both Herodotus and Thucydides describing the use of information warfare. Today, almost 250 years after the Revolutionary War, IWar has grabbed center stage again with Russian and Chinese information warfare campaigns worldwide; it is now vitally important for the United States to redefine this concept and tie it to a larger strategic framework.

While IWar has always existed, the updated version includes the combination of modern technologically driven fields such as cyber operations and electronic warfare. The US Army War College's Conrad Crane recently traced the origins and evolution of IWar in the Army, focusing on its influence on decision making, while demonstrating the concept is far from novel.[2] Yet the IWar concept is the "new" kid on the block in security circles given shorter-term institutional memories about victories back in 1776, and there is momentum to enact this concept with a transitioned US Army Cyber Command to US Army Information Warfare Command. Lingering concern over Russian interference in US elections and the continuing Chinese threat over stealing technologies contributes impetus for this effort. Buddhika B. Jayamaha and Jahara Matisek, in "Social Media Warriors: Leveraging a New Battlespace," call for new strategies to combat this information operations threat as it exists on social media platforms.

Absent from Jayamaha and Matisek's argument, however, is the idea that the central facet of an adversary's attempt to undermine democracy

Dr. Jason W. Warren, a retired US Army lieutenant colonel, is a lead associate for Booz Allen Hamilton, supporting information and cyber defense and security policy. His latest publication is *Landpower in the Long War: Projecting Force After 9/11* (University Press of Kentucky, 2019).

1. David Hackett Fischer, *Washington's Crossing* (New York: Oxford University Press, 2004), 201–3.

2. Conrad Crane, "The United States Needs an Information Warfare Command: A Historical Examination," War on the Rocks, June 14, 2019, https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/.

is disinformation, which can be ameliorated by generating a more compelling narrative. Calls for more government intervention through the expansion of the Posse Comitatus Act of 1878 and more efficient domestic regulations on freedom of speech miss the point that these too will undermine democracy—and perhaps more so than Russian bots.[3] Plentiful historical examples of IWar undercut the idea that it is a new concept, while the refocused efforts of the US military to converge existing information-related fields demonstrate this an issue larger than political narratives and military decision making alone.

In its vision for transformation, the Army converges and develops capabilities to identify, defend, and dominate information in the operational environment to achieve objectives and aid in winning the nation's wars. Information warfare would provide national security leaders meaningful and timely information for decisional advantage over adversaries.[4] It is a critical element in achieving strategic landpower. Without it, the use of strategic force becomes unmoored from its political and policy antecedents. IWar bridges the military's employment of force from the realm of policy and politics, as Clausewitz described war as the latter's continuation by other means. It does so with softer informational power to influence and persuade relevant actors, while employing harder power with cyber or electronic warfare through operations in the information environment and as a means to enhance traditional combat power in other domains.

IWar provided Washington an asymmetrical opportunity. As British and Hessian units went into winter quarters local patriots undertook IWar to discredit the legitimacy of the occupying forces in New York and New Jersey. This narrative, somewhat accurate but embellished, portrayed the occupying army as committing depredations against the local inhabitants. It also highlighted the botched British effort in what practitioners now consider civil affairs and psychological operations (types of operations included in the IWar concept), failing to sustain the narrative of colonial reconciliation with the British Crown.

While Washington did not orchestrate this IWar campaign, his regular army benefited from the intelligence the campaign generated, namely that supporting forces had left Hessian General Johann Rall temporarily isolated at Trenton. IWar ultimately guided and determined Washington's successful use of force against a vulnerable adversary. The Trenton example is the American version of the type of information warfare the ancient Greeks and Persians, and modern Chinese and Russians, have used to great effect.

IWar hence creates economies of force in the traditional domains, establishing a framework to task organize by identifying adversary vulnerabilities. It allows for an economy of force mission, channeling military power toward an achievable objective. This economy of force is especially critical in the case such as Washington's strategic situation, where the adversary maintains superiority; there is similarity today with near-peer adversaries' advantages in their near abroad for the United

3. Buddhika B. Jayamaha and Jahara Matisek, "Social Media Warriors: Leveraging a New Battlespace" *Parameters* 48, no. 4 (Winter 2018–9).

4. Author's personal experience drafting "Information Warfare Transformation" plans and strategies, during spring 2020 at US Army Cyber Command, US Department of the Army.

States. The United States and its allies may face local disadvantage, which the proper employment of IWar could ameliorate.

IWar includes as a critical component an information narrative that helps commanders to burnish the why of mission accomplishment. During the Trenton-Princeton winter campaign, the patriot narrative of harsh British and German treatment ultimately caused the militia to retake the field and led to the delivery of timely and accurate intelligence to Washington's headquarters for operations against Rall. IWar thus allows for commanders to sense, understand, act, and assess, and allows combatants to focus on information key terrain to the advantage of their operations vis á vis the enemy.

IWar consists of more than maneuver forces capitalizing on advantages and tailoring forces as a result of information narratives and related intelligence. It also includes electronic warfare and cyber operations in the information environment, generating effects for the operational environment. These operations act to disable physically or logically the command and control capabilities of an adversary or even the adversary's materiel itself. Electronic warfare attempts to control the electromagnetic spectrum, attacking an adversary or impeding his electronic warfare assaults. Cyber operations proceed along physical, logical, or persona avenues of approach into a network either to defend friendly mission-relevant terrain—cyber and/or key terrain—cyber or hold that of the enemy at risk. Electronic warfare and cyber support the maneuver force in all military domains through independent action in the information environment, which reinforces both the information narrative and the operations, actions, and activities of other maneuver forces.

By focusing on social media platforms, current IWar literature misses the critical capabilities of electronic warfare and cyber focused on more than decision making and actually seeking to disable and destroy enemy materiel. Armies since the beginning of time have had the capability to raid headquarters and ambush couriers, thus the targeting of command and control nodes was still a possibility even without advanced technology, as well as focusing on information key terrain as it pertained to their historical contexts. It is worth remembering there are more traditional means to disrupt command and control—should an adversary cyberattack in the contemporary environment achieve transitory superiority on friendly networks.

The key functions embodied in IWar include the existing military operational specialties of information operations (including military deception and operational security), as well as psychological and cyber operations, civil and public affairs, electronic warfare, signals (and other) intelligence, and space.[5] The concept is larger than its individual components, however, seeking synergy between them and is more encompassing in its relation to maneuver. It enables strategic landpower by undergirding the maneuver operational framework which links tactical operations, actions, and activities to strategic objectives.

Thus IWar incorporates information aspects that shape the friendly narrative and direct force, but also with inherent capability to act

5. Author's personal experience drafting "Information War Transformation" plans and strategies, spring 2020 at US Army Cyber Command, US Department of the Army.

independently as with electronic warfare and cyber operations inside the information environment. Friendly forces often employ cyber, electronic warfare, and information operations to target the decision-making ability and cycle of an adversary through disinformation and damage to systems that provide a conduit for communications and data. Security and defensive forces also protect the decision-making capabilities of friendly commanders through mission assurance of data, information, and communication. Given the interconnectedness of software, hardware, and information on all military platforms, and as a shaper and enabler of operations in the operating environment, IWar is integral to every aspect of warfare.

IWar ultimately assists in achieving strategic objectives by better focusing operations and lessening risk. Instead of conducting a general operation to reverse the patriot's flagging cause, the information narrative, and the intelligence it generated, provided Washington with a way to pinpoint Rall's garrison as a vulnerable target and economize his own limited capabilities. This directing of maneuver force to an achievable operational objective, redounded to success at both the strategy and policy tiers, as the colonials were able to extend the war effort with successful limited operations. New recruits and reenlistments were additional policy benefits from Trenton and Princeton as was confidence from a new information narrative that the colonials could wage conventional war against a superior enemy.

Whether strategy is defined as the balancing of ends, ways, and means or the relationship of risk and resources to political goals, IWar aligns operations to achieve strategic results. Proper employment of IWar lessened risk in the overall patriot war effort because Washington's choice of an exposed garrison reduced danger to the Continentals' main field army and Congress was better able to align resources in the dwindling war effort. With the ends, ways, means paradigm, IWar allowed Washington to fashion his ends of preserving the Army and the war effort with the ways of the Trenton-Princeton campaign at the operational level of war, as well as the tactical means of the Continental Army targeting Rall's isolated regiments and later the British supply base at Princeton. IWar hence can establish a framework for strategic results.

IWar interrelates not only to the strategic level of war, but with all levels of war and indeed every aspect of warfare as part of the national instruments of power. The information narrative, for instance, helps to fashion diplomatic overtures that inform actions across the Competition Continuum. By converging functions and tasks related to information, IWar harnesses informational power in part for decision-making advantage and to limit the decision-making capabilities of competitors and adversaries. IWar enables economic power, especially during competition with adversaries, assisting in freedom of navigation activities and protecting cyber critical infrastructure.

In the military realm, IWar undergirds all the other domains, acting to direct and focus force utilizing an information narrative (and supported by other IWar components like cyber operations) against an objective, whether in space, land, air, sea, or cyberspace. The activities of nonexclusive military entities, such as the Interagency and civilian partners, intersect with IWar as well and include the fashioning of information narratives and supporting operations such as cyber

defensive of non-DoD networks. Civilian infrastructure supports most of the military power grid at home and abroad and therefore demands partnerships for integrated security and defense. The overlap of civilian infrastructure and military operations creates potential legal pitfalls such as with Posse Comitatus and legal teams must carefully monitor these.

All of the components of IWar—information, intelligence, cyber, and electronic warfare operations—compose functions in the information environment. It is important to note the information environment is not disparate but intersects with the operational environment.[6] While IWar acts outwardly to direct and tailor maneuver in the other domains, it also encompasses cyber and electronic warfare operations in the information environment, which generate their own objectives and effects. The components of IWar, however, do not orient toward independent objectives but should be planned as supporting a larger scheme of operational maneuver or strategic effects at the national level. Thus IWar is far more than simply dominating media messaging to influence audiences.

IWar complements the Army's new multi-domain operations construct and its concentration on competition below the threshold of armed conflict, while supporting its operational focus for penetrating and exploiting near-peer adversary's anti-access/area-denial capabilities.[7] IWar as part of multi-domain operations enables the persistent engagement of foes by informing both host nation and friendly populations as to the purposes of friendly operations and shaping the battlefield in the competition portion of the warfare continuum.

IWar is adversary focused and occurs through persistent engagement of competitors and adversaries across the Competition Continuum by ensuring the delivery, reception, assessment, and protection of proactive messaging. This further develops information resiliency across the force. In the course of persistent engagement, operations in the information environment provide commanders at echelon with continuous identification of key terrain, opportunity, and risk.

Likewise, commands produce feedback to influence future operations at echelon, providing local, regional, and global input to operations in the information environment. IWar supports multi-domain operations with a calibrated force posture: mission-specific integrated information formations at echelon; reach-back operations and intelligence capabilities; and forward deployed IWar teams. With convergence, commanders will possess information capabilities to employ in the operational environment. Persistent engagement and analysis throughout the competition continuum provides commanders with the ability to posture for conflict.

IWar incorporates psychological operations to shape the perceptions of targeted audiences and creates effects through military deception and cyber operations. During high intensity combat, IWar focuses combat power on the weak links of the enemy's anti-access/area-denial capabilities to support a penetration followed by rapid exploitation

6. Joint Chiefs of Staff (JCS), *Joint Operations*, Joint Publication 3-0, chg. 1 (Washington, DC: JCS, 2018).

7. US Army Training and Doctrine Command (TRADOC), *The U.S. Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1 (Washington, DC: US Army TRADOC, 2018).

and freedom of maneuver. IWar may identify and disable a portion of the enemy's anti-access/area-denial defenses allowing for economy of force missions, where the enemy has had local superiority of fires and maneuver elements. IWar allows for the targeting of precise areas in the enemy defenses that assets from all military domains can penetrate and exploit, with follow-on forces gaining freedom of maneuver.

Not every corner of the West's security sector is as enamored of IWar as some Army cyber operators. Discounting the ability of IWar operations, actions, and activities to produce casualties, some Israeli scholars believe the qualification for warfare is predicated on traditional forms of combat, and hence IWar does not apply in their worldview.[8] The US Intelligence Community tends to view IWar-related capabilities as national-strategic assets meant for extremely targeted and controlled employment, and only authorized at the highest levels of government.[9] The Army's internal and traditional branch parochialisms also are at play, as various communities of interest fight to retain siloes of authorities and power within the institution at the expense of the IWar concept. Various key players in the Army institutional power structure dislike IWar and are skeptical of its prospects if applied at echelon to Army formations.[10]

Then there is the problem of scale and scope in defining the battlefield. The government network—the DoD Information Network—is so large, it has proven impossible to defend.[11] This is just the defensive portion of cyber operations, not accounting for the complexity of offense in the cyber domain. The IWar concept will expand the scope of operations even further by accounting for all of the other information-related capabilities and their functions.

This idea of scope and scale in this new battlespace for IWar seems lost on many observers as a recent *Strategy Bridge* article demonstrated.[12] There will have to be a reckoning between the desired functionality of IWar and the budgeting of scarce resources (exacerbated by political combat between branch interests), the aversion to new command and control structures like headquarters, and the very size of this new enterprise. Even with these concerns, the fact the nation is at risk from foreign adversaries, who have meddled in US national political discourse and launched cyberattacks of all kinds, while vying for an asymmetrical advantage, will be enough to push IWar development into operation.

From the earliest times, the functions of IWar and resulting economies of force, regardless of technical capabilities over the intervening years, have acted as a guiding light for forces to achieve objectives. Whether in Washington's time with the information narrative of British and German despoliations that generated intelligence for the Trenton-Princeton campaign, or in fashioning a counternarrative

8. Email exchanges with author after a conference at St. Andrews, Scotland, April–May 2016.

9. Author's experience as Future Plans Chief, Joint Force Headquarters, DoD Information Network.

10. Author's experience as lead planner for US Army Cyber Command for transformation to Information Warfare Command effort. (As of summer 2020, the effort has been placed on hold.)

11. Author's experience as Future Plans Chief Joint Force Headquarters, DoD Information Network.

12. Jeff Edmonds and Samuel Bendett, "Russian Battlefield Awareness and Information Dominance: Improved Capabilities and Future Challenges," *Strategy Bridge*, February 26, 2019, https://thestrategybridge.org/the-bridge/2019/2/26/russian-battlefield-awareness-and-information-dominance-improved-capabilities-and-future-challenges.

for Russian incursions into Eastern Europe, IWar serves as a basis for operations in all domains.

Although social media messaging and IWar effects on decision making are important, these do not represent the totality of these converged capabilities. During competition, IWar combines with ways and means enacted in other domains to deter potential adversaries and prevent conflict. With the outbreak of conflict, IWar operations actions and activities in the information environment create effects used by maneuver forces to penetrate, exploit, and regain freedom of maneuver during multi-domain operations. IWar then refocuses for the recompete stage of the competition continuum to consolidate gains and prevent future policy discord. IWar is nothing short of a crucial part of warfare spanning military history and is especially critical for the information-dominated battlefields of the twenty-first century.

The Authors Reply

Buddhika B. Jayamaha and Jahara Matisek

A fundamental axiom that the nature of war remains the same while the character of war keeps evolving overtime is increasingly under scrutiny. For several millennia, land and sea were the domains in which the fortunes of armies were decided. We know industrialization transformed the way wars were fought in World War I and World War II and further advances such as nuclear weapons altered the way wars were waged in various battlespaces throughout the Cold War. In this context, scholars such as Weigley in 1973 believed the American way of war—predicated on combined arms maneuver and a preponderance of force—was becoming antiquated.[13] Admiral J. C. Wylie wrote in 1967 about a new vision for effective military strategy, specifically that all military tools and domains should be used to support landpower in pursuit of *control*.[14] Weigley and Wylie were correct in identifying an emerging problem, but their paradigms were still predicated on land as the defining domain of warfare.

America and its allies are returning to an era of Great Power competition, as expressed in all national security documents from the current administration. Space is identified as an autonomous domain of warfare, requiring us to imagine what constitutes space power and what role the new US Space Force should play in defending American vulnerabilities. Still, while autonomous, space is just as intertwined with the day-to-day realities and joint warfighting principles as the other domains.

But the advent of cyber is something fundamentally different from the military domains of land, sea, air, and space, specifically owing to

13. Russel F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (New York: Macmillan Co., 1973).

14. J. C. Wylie, *Military Strategy: A General Theory of Power Control* (New Brunswick, NJ: Rutgers University Press, 1967).

cyberspace's intangibility and the inability to apply to it Clausewitzian ideas of *mass* and *maneuver* in a conventional sense. Thus, scholars and practitioners face conceptual and analytical challenges in attempting to analyze cyber domain threats, especially in terms of whether this domain has changed the nature and/or character of warfare. In many ways, Dr. Jason Warren's thoughts about information warfare (IWar) are on point, aligning closely with the conventional warfare thoughts espoused by Weigley and Wylie. Warren's conception of IWar is wedded to supporting strategic landpower where information plays an auxiliary shaping function and kinetic missions—the main effort—are expected to generate the desired end state.

He is correct that the United States constantly utilizes information warfare in overall campaign plans—from 1775 to Operation Inherent Resolve. The challenge we identified is the way civil society is organized and functions in liberal democracies. The unique nature of cyber as its own domain and the sinews connecting people in that domain make both cyber and civil society undefended attack surfaces state and nonstate adversaries could leverage into new battlespaces effectively with very little cost, in comparison to elaborate Cold War information warfare campaigns.

Though we are far from it, America's adversaries are increasingly realizing if things we take for granted can be weaponized by hijacking them—voluntary surveillance equipment that tracks movement, heartbeats, vehicles we drive, televisions, thermostats, and anything with the prefix "smart." Of course, "smart electronic device" is merely a euphemism—it is linked to a third party and can be hijacked by an unauthorized third party. This is the really terrifying part—where reality can be warped. It just might be landpower, which used to be the main effort, may end up playing an auxiliary role to the main thrust of military power—cyber weapons and information-political warfare.

Civil Society and Cyberspace: Distilling into a New Battlespace

Cyber domain in its totality consists of the sinews connecting the warfighters, machines, widgets, societies, economies, governments, and people. These sinews have created a humanly devised domain integral to everything we do, just as it remains its own autonomous domain. While people are an important element of any domain of warfare, the shift of the battlespace to civil society is an existential threat due to the fact that cyberspace is increasingly embedded within the constructs of civil society, informing what reality *is* and *how* reality is socially constructed and interpreted. Influencing a civil society—people—is always part of any military campaign, as is targeting the government and army, encapsulating Clausewitz's trinity.[15] Influencing civil society involves efforts to alter people's behaviors with the use (or threat) of violence, or with the use of disinformation campaigns, prior to, during, or after a military campaign.

There is a conceptual disconnect in Warren's view that current campaigns by state, state-affiliated proxies, and nonstate actors to sow discord in civil societies are nothing more than old-school

15. Carl Von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989 [1832]).

disinformation campaigns which can be ameliorated with more compelling counternarratives. Yes, the Soviet Union, China, and other adversaries actively executed disinformation campaigns against the United States and her allies during the Cold War. The world of information warfare Warren describes, however, pertains to a pre-Internet era where the traditional means of waging a dis/misinformation campaign were qualitatively different. Those Cold War-era campaigns were broad based and ideational (with multiple barriers to entry and high risk) as opposed to the targeted, individualized attacks made possible with today's technology. As a result, information-political operations were part of elaborate covert campaigns.

The emergence of the cyber domain and its real-time fidelity and linkages to what we perceive as reality in terms of daily interactions, be it with humans, news, social media, bots, foreign actors with malicious intent, etc., fundamentally changes Warren's notions of IWar on multiple levels. Social media warriors can inflict damage by relying on the power of social movements to either create or fuel new and radical politically aware groups in civil society that polarize and/or create new policy outcomes undermining state power. This influence of social media warriors over social movements has tremendous implications for liberal democracies worldwide due to the great asymmetry in power between them and their authoritarian and illiberal adversaries.

Cognitive Hacking: Weaponizing Reality

The AK-47 democratized violence and became the great equalizer during the myriad civil wars that proliferated in the twentieth century, allowing the weak to fight with some degree of comparable firepower. The cyber domain is similar in its low barriers to entry requiring only a rudimentary knowledge of networks and code, making it the AK-47 of the twenty-first century. Cyber versions of this weapon are affordable, portable, can be hidden in plain sight, and are deployable from an unsuspecting table in a peaceful café with Wi-Fi. The greatest differences, however, are the intensity, precision, and capabilities afforded in targeting and attacking, at low cost and little to no risk. Taking up physical arms against the state in the pre-Internet era was a high-risk activity with minimal payoffs; the cyber era has flipped this calculus upside down.

Cyber power in the hands of many, buttressed by state power, has only further democratized the ability of adversarial states and nonstate actors to wage political-information warfare in civil societies ostensibly not at war. Today, foreign adversaries can reach out and touch an individual in any number of platforms with targeted information, based on easy, unclassified data collection techniques that resonate with the subject's inherent cognitive biases in ways previously unimagined. This targeting, combined with big data and increasing levels of knowledge about human behavior and other elements of social science, has brought an unfathomable level of scale to information warfare.

Individual decisions are shaped by the context of information; when a hostile actor can control this context (made very specific and limited by the way we are connected) generating a cognitive hack, the result

is reinforcing ideational "echo chambers."[16] Such echo chambers pass the threshold of the imaginary and become real when individuals make decisions in terms of it.

The advent of artificial intelligence, blockchain and bitcoin technologies, quantum computing, and deepfakes, while still in their adolescence, will only further amplify the weaponization of cyberspace and targeting of civil society and individuals. These actions could deepen existing social cleavages or generate new ones where none may have existed, providing America's adversaries multiple points of entry and empowering the "Social Media Warriors" we described in our original *Parameters* article to wreak havoc on civil society through the process of *schismogenesis*.[17] Meanwhile China, as the quintessential example of an authoritarian adversary, can gerrymander their population through social credit scores, with heightened surveillance technologies ensuring any belief, idea, or value that does not fit the company line of the dear glorious Chinese Communist Party (CCP) is locked away deep in the cerebellum of Chinese citizens (for the short term at least!).

These CCP activities also highlight the asymmetry between liberal democracies and authoritarian regimes in their abilities to inoculate their respective societies. By exploiting the freedoms espoused in liberal democracies that give rise to vibrant civil societies, adversaries can gain access to those societies and use information platforms to exploit societal cleavages. Authoritarian regimes such as China socially engineer their citizens, finding innumerable ways to "sanitize" corruptive Western thought. By generating the narrative that Western ideals are dangerous, the CCP creates an information echo chamber for over a billion people.

The dear CCP official can screen all movies, music, art, poetry, history books, and any other form of information and entertainment. All of these actions of course seem abhorrent and over-controlling to those in the West. Yet the Chinese Communist Party can easily and transparently advise their citizenry that they block some Western content because it perverts Chinese values and could cause chaos, which would hurt Chinese prosperity. This relatively explicit social contract by the CCP appears readily accepted except in Hong Kong, precisely because Hong Kong natives are only now becoming exposed to Chinese censorship. The demonstrations are a reaction to the enforcement of the new CCP normal.

And while a Chinese citizen cannot use the social media platform Twitter, Chinese-based TikTok has access to American citizens, providing them biased reporting of protests in Hong Kong. In other words, the unit of analysis is the civil society at home. We cannot limit our liberties to counter our adversaries—this would mean handing our adversaries an inadvertent victory. We cannot, as Warren suggests, counter the weaponization of civil society in liberal democracies with more compelling counternarratives.

16. Elanor Colleoni, Alessandro Rozza, and Adam Arvidsson, "Echo Chamber or Public Sphere? Predicting Political Orientation and Measuring Political Homophily in Twitter Using Big Data," *Journal of Communication* 64, no. 2 (2014): 317–32.

17. Buddhika Jayamaha and Jahara Matisek, "Social Media Warriors: Leveraging a New Battlespace," *Parameters* 48, no. 4 (Winter 2018–19): 11–24.

Governments and state authorities in liberal democracies are not in the business of waging information operations in their own societies no matter how well intentioned. This is precisely what authoritarian regimes do, with China being the exceptional example. And counternarratives have additional dangers. As Benedict Anderson noted, the ability of a state and nation to construct an "Imagined Community" creates the most cross-cleavage unity and alliances across elites in support of the desired nation-state identity.[18] China and Russia have increasingly put a stranglehold on the free exchange of ideas in order to ensure their imagined community fits the worldview of their political leadership. Simultaneously they are attempting to fracture overarching national identities in the United States and across Europe, precisely because it is easier to do in liberal democracies with myriad crisscrossing and crosscutting social cleavages.

Conclusion

The more salient puzzle of Warren's concerns about the 1878 Posse Comitatus Act requires significant reflection on what actually made America so great to begin with. We cannot allow our security and intelligence agencies to wage information operations on home soil. Our only contention, however, is such policing of the cyber domain and defending against foreign social media warriors should include new levels of engagement by national security institutions to protect against subversion and other acts attempting to sow panic and/or undermine security.

As emerging data are already showing, the COVID-19 pandemic has given China and Russia yet another entry point to sow confusion and fear in Western civil society, such as their attempts at advertising how much better their countries are handling the crisis. This enables them to push anti-Western news and narratives on unsuspecting and concerned social media users in the West. These users, in turn, share the misleading information, conspiracies, and memes, only contributing more to the crisis and shortages, like the "Great Toilet Paper Panic of 2020." Moreover, we contend there is tremendous information-political warfare value in referring to COVID-19 as the Chinese flu, as the Trump administration is attempting to do, precisely because it ups the counternarrative ante on China.

Finally, we do agree with Warren's broader point that what is required is a more compelling counternarrative but one aimed at our adversaries—again—as we used to do and were exceptionally effective in doing during the Cold War. Alas, that required a consensus among national security and political elites on the nature of the threat and the desired effects such a campaign was meant to generate—people who espouse liberal democratic ideals, buttressed by a faith in free markets. Unfortunately, such a consensus is far removed at a time when a vocal minority question both liberal democracy and capitalism. Perhaps such growing skepticism is partially a function of the effective weaponization of civil society as a new battlespace.

18. Benedict Anderson, *Imagined Communities: Reflections on the Origin and Spread of Nationalism* (New York: Verso, 2006 [1983]).

All we know is from Pearl Harbor to 9/11, threats to the United States have brought Americans together across the political spectrum for consensus, making the country more powerful and unified in policy decisions. But if we correctly assume the Chinese and Russians (and others) have studied the social processes of what makes America great, then they have every reason to invest in *schismogenesis* attacks against civil society, ensuring a divided and polarized America once the dust settles from the current Chinese flu pandemic and basic scientific facts pertaining to wearing a mask.