Protectors without Prerogative
The Challenge of Military Defense against Information Warfare

Christopher Whyte, PhD

Abstract: This article considers the unique threat of information warfare and the challenges posed to defense establishments in democratic states that are typically legally limited in their ability to operate in domestic affairs. This author argues that military strategy on information warfare must be informed by understanding the systems of social and political function being targeted by foreign adversaries. Looking to theories of political communication, the author locates such understanding in describing democracies as information systems whose functionality resides in the countervailing operation of key social forces. Defense establishments would do well to develop greater analytic capacity for prediction of attack based on such societal—rather than strategic—factors and incorporate these predictions into efforts to shape adversary behavior in cyberspace, the primary medium via which information warfare is prosecuted today.

Keywords: information warfare, cyber, democracy, persistent engagement, subversion

In following professional conversations and punditry on national security in recent years, it would be hard to escape the conclusion that information warfare and political interference—often enabled and augmented by offensive

Dr. Christopher Whyte is an assistant professor in the program on homeland security and emergency preparedness at the L. Douglas Wilder School of Government and Public Affairs at Virginia Commonwealth University in Richmond. His research and teaching focus on the dynamics of global cyber conflict, the execution of information warfare campaigns, and the impact of emergent information technologies on the national security enterprise. His work has been published in numerous journals and media outlets. Dr. Whyte is coauthor of a volume on cyber warfare, lead editor of a book on information warfare in the age of the internet, and coauthor of a forthcoming monograph that contextualizes military efforts to employ artificial intelligence toward battlefield innovation.

Journal of Advanced Military Studies vol. 11, no. 1
Spring 2020
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.2020110108

cyber operations—has rapidly become one of the most pressing threats facing Western democracies. Since at least 2013, nearly two dozen countries across the West and the former Soviet sphere have been victims of interference operations conducted by the Russian Federation.[1] These campaigns, substantially prosecuted via the manipulative use of social media platforms, troll farms, and fabricated news content, have targeted all manner of sociopolitical process—from preelection and referenda debates to issue-specific political marketing efforts—and have often included the application of other elements of state power, including cyber operations, human espionage, dark money, and limited military force.[2] The Russian Federation is not the only world power to have turned to political warfare augmented by sophisticated digital methods with such gusto. The People's Republic of China, the Islamic Republic of Iran, Syria, and the so-called Islamic State have all prosecuted political warfare principally via digital platforms and often augmented by cyber means against Western polities with increasing intensity and sophistication during just the past few years.[3]

Beyond simply the rising tide of information operations enabled by the internet, interference operations wherein information is weaponized to disrupt democratic social and political processes are concerning because near-term developments promise to make them both more robust and accessible. Machine learning techniques used to create deepfake media content, where fabrication is immensely difficult to distinguish from reality, for instance, is not only worrying because of the fidelity of the fake news product.[4] The underlying algorithms involved are adversarial, which means that attempts to make better tools for analyzing the authenticity of video or imagery—even utilizing machine learning approaches to do so—will simply strengthen the fabricated production over time.[5] Moreover, the software needed to create deepfakes is becoming more widespread, with applications to produce reasonable quality fake productions even now available for little to no cost in easy-to-access web stores. In short, information warfare is, by the very nature of the technologies that now enable it within the modern global media environment, likely to become a *more* common feature of international affairs even as Western states take steps to defend against and deter unwanted foreign interference.

This article considers the unique threat of information warfare and the singular challenges posed to defense establishments in democratic states that, while tasked to secure national interests and ensure the integrity of the polity, are typically legally limited in their ability to operate in domestic affairs. Even more so than has been true with the pivot toward greater effectiveness in defining the mission of national militaries that are increasingly operating in the cyber domain, the specter of broad-scoped influence operations dictates an expansion of the national security enterprise that can be difficult to onboard. For example, the term *information warfare* is often used by military practitioners to simply refer to the range of security actions—from military deception efforts to electronic warfare and sensor manipulation—that involve the employment of information as the principal tool of active engagement.[6] In the digital age, many practitioners have written of information warfare and cyberspace explicitly in terms of countercommand/control warfare, wherein the value of offensive use of the internet is in those distinct opportunities for disruption or manipulation of the military control cycle.[7] By contrast with such usage, the references to information warfare made in the remainder of this article reflect a colloquial pivot toward the description of broad-scoped psychological operations (psyops) that blend the use of different elements together to influence information systems less tangible than servers and computers—those of democratic process.

For state militaries, this shift in the form of information warfare threats is problematic. Arguably the most significant obstacle for defense planners lies in the fact that most democracies legally distinguish between the role and responsibilities of military forces versus law enforcement, intelligence entities, and other elements of civilian government. Given the manner in which the attack surface of a country inevitably encompasses diverse elements of civil society, private industry, and civilian government with influence operations, such constraints can be limiting.[8] Hardening of the attack surface of democracies must inevitably emerge in large part from partnerships between civil society and civilian government, with militaries operating in support. And yet, militaries cannot simply take points from civilian authorities. After all, interference operations often portend direct consequences for military power and often take the form of hybrid strategies that involve the blended use of military force alongside other activities.[9] How then should defense establishments strategize to deter such malicious foreign behavior?

Even as they consider their posture and strategy for dealing with information warfare threats, most military analysts remain woefully unclear on the nature of the threat being faced.[10] Simply thinking of information warfare as being leveraged in influence operations to disrupt democratic discourse and cause instability awards no explanatory capacity for strategists that are interested in understanding what kind of punitive measures and defensive actions might impose greater cost on foreign adversaries than others. In short, if the specter of information warfare seen in recent years is not paired with an appropriate understanding of the function of the systems being targeted, then defense officials cannot effectively design deterrent plans that effectively reduce the promise of continued interference from abroad. This is especially the case given those characteristics of modern influence operations that make them such an appealing strategy to begin with, namely that they are cheap, deniable, and exist below the threshold of violence. As such, this article addresses the notion that militaries in democratic states are both constitutionally and operationally limited in their ability to address the threat of information warfare from belligerent foreign powers, offering both theoretical context and subsequent recommendations for military planning.

The remaining sections of this article offer insights to help alleviate this gap in thinking on information warfare in the context of prospective military strategies for defense and deterrence in democratic societies. In the first section, the author offers a perspective on the form and function of such operations informed by literature in the political communications field of studies, describing democracies as information systems that have discrete information assurance processes that information warfare campaigns aim to disrupt. The article then describes the evolving threat of such campaigns in the context of a dynamic game often used by computer scientists to describe information security within complex information systems. Finally, the article addresses the question of defense strategy in an age of advancing techniques for interference and uses the foregoing analysis to suggest opportunities for when military force might be successfully applied to shape adversarial behavior below the threshold of armed conflict in this form. Specifically, recent developments in cyber conflict doctrine in the United States are offered as context for the discussion.

Understanding "Democracy Hacking": A Communications Perspective

Information warfare is the manipulation of information to gain strategic or battlefield advantage over opponents.[11] The term *information warfare* is often used interchangeably with others such as *political warfare*. Though there are some differentiations one might make between the terms, both invite thought of activities that fall outside the realm of declared hostilities between states. Indeed, political warfare involves the full range of mechanisms of state power *other* than—though sometimes inclusive of—military power to secure national interests in international affairs. George F. Kennan called political warfare "the logical application of Clausewitz's doctrine in time of peace . . . the employment of all means at a nation's command, short of war, to achieve its national objectives." This includes operations that "range from such covert actions as political alliances, economic measures, and white propaganda to such covert operations as clandestine support to friendly foreign elements, black psychological warfare and even encouragement of underground resistance in hostile states." The purpose of political warfare is to augment state positioning and capabilities in the forum of high level international engagement by, among other things, enhancing the credibility of threats, exerting lateral pressures, and addressing the micro-foundations of state power.[12]

In the digital age, information warfare has thus far generally been viewed—rightly so—in terms of the attack surface of network-enabled information and communications systems.[13] In the past, this has made substantial sense because the ability of adversaries to manipulate the value of information, alter informational conditions, disrupt or subvert communications channels, and generate uncertainty in victims has substantially emerged from considerations of design and usage of those underlying platforms. Whether the decision-making target is a military or civilian political one and that decision making largely relies on the function of internet-enabled infrastructure—from sensors employed on the battlefield to data stored in computers and code that makes them work—that infrastructure becomes singularly significant insofar as most potential attack vectors can be found.

With recent campaigns aimed at "election hacking" or "democracy hacking" that have so fully captured the attention of Western security establishments in recent years, the significance of such systems' security features and mechanisms is secondary.[14] After all, the attack surface of political systems emerges from the processes that allow the normal operation thereof.[15] Conceptually, this realization does not imply a fundamental shift away from assessing vulnerabilities to information warfare on informational grounds for analysts. It simply implies a different set of empirical criteria that pertain to the relative effectiveness of strategies aimed more generally at societal processes than at specific organizational or battlefield communications systems.

The Strategic Logic of Digital Age Disinformation Operations

Democracies are information systems.[16] As an extensive literature in political communication and international relations holds, democracies variably employ mechanisms that move popular discourse—and, subsequently, public and foreign policy—toward moderate outcomes.[17] To be clear, democratic discourse does not naturally lead toward truth or fact. The process of debating significant issues that are handled and interpreted across a wide array of perspectives does, however, tend to moderate participant views and allow for the emergence of prudent undertones that thereafter influence policy.

Mechanically, democracies rely on a series of countervailing institutions that assure the proper function of the information environment.[18] In traditional treatments of the marketplace of ideas in democracies, these institutions include state leaders; elected officials and representatives; experts; other popular influential voices; the statements of official intelligence sources; and a robust, independent watchdog media ecosystem.[19] Taken together, these elements ensure that information pertinent to any particular issue under debate is sufficiently handled, dissected, and framed so as to allow for Bayesian updating, or updating the process by which someone updates the probability that a hypothesis is accurate as more information becomes available to them (i.e., when individuals reconsider their position or beliefs based on new evidence), and decision making among the broader population. The system only breaks down when one of these mechanisms fails to behave normally, which is what occurred during the debate leading up to the 2003 Iraq War, where the George W. Bush administration inflated the threat of Iraqi weapons of mass destruction and elected legislators were too unwilling to go against the patriotic feeling of the nation in the year and a half following the 11 September 2001 attacks to push back against uncertain facts.

In reality, these institutions are only themselves significant to the function of democracies as information systems insofar as they assure the handling and integrity of information four distinct ways. Whereas much classical literature in the political communications field assesses that democratic functionality is substantially about ensuring diversity of voices in a given environment, this is only one element of the challenge. Certainly, the quality of information provided to broader debate processes matters a great deal. Democracies thrive and observe prudent discursive and policy outcomes, particularly when accurate and extensive information is available to the public and to interpreters thereof. For this reason, even "spin" media that politicizes facts for one or another perspective to aid an agenda is not undesirable in democracies; under normal conditions, such information handling should ultimately contribute to the overall health of debate as citizens encounter more diverse perspectives on established information.

However, the function of the system also requires handling of information in ways that allow for attribution of the information's origins. For democracies to work, it has to be reasonably easy to figure out whose voice is actually behind the publication of information, at least within reason. Even where corporations or political action entities sponsor advocacy or advertisements, there should be restrictions on the use of capital for political activity sufficient to ensure that the median voter could discover the source of information via a reasonable amount of additional information search. This requirement parallels information assurance requirements commonly applied in design science for computer systems in that democracies do not have to be free from any form of manipulation, such as political spin or special interests' influence; rather, it simply has to be possible for such tampering to be discoverable or exposable. If this is not the case, then it becomes difficult to fundamentally assure the quality of underlying information being handled in popular debates.

The function of democratic information systems also relies on effective safeguards of the credibility of information. This manifests in two ways. First, and clearly related to the attribution requirement above, it is necessary that democratic populations trust that discourse *is* discourse. In other words, it is critical that citizens believe their speech is not artificially being manipulated. Here, the best way to think about this requirement may be to consider the case of vibrant civil society discourse around significant issues in China, wherein much popular debate emerges as the result of astroturfing.[20] In that case, the aim of Chinese authorities is simple—to simulate a relatively free civil society landscape so as to dissuade social forces from unrest.[21] In democratic systems, it is critical that broad-scoped discourse remain credibly free from outside control, lest policy not reflect popular sentiment. And, second, it is similarly necessary that citizenry believe that all points of view—with exceptions only at the extreme fringes of societal norms and beliefs be allowed. If trust in the freedom of citizens to express themselves cannot be sufficiently maintained, then voices required to help moderate discussion may cease normal operation and skew the outputs of democratic processes.

The weak points of democratic societies are the sum of those mechanisms whose operation is critical to ensure the quality, origination, credibility, and freedom of information. Sophisticated disinformation and propaganda campaigns target those mechanisms of functionality so as to prevent both social and political processes from functioning normally. When those processes *do* cease to function normally, one might expect discursive outcomes to differ significantly from what would be seen under "normal" operating conditions. Naturally, with any individual campaign, there is context in the parochial machinations of the adversary. Vladimir Putin's vendetta against the candidacy of Hillary R. Clinton clearly flavored the effort of the Internet Research Agency (IRA) and affiliated cyber threat actors in interference efforts targeting the 2016 American election season. However, the best way to understand the different tactics developed and strategies employed is by understanding the landscape of vulnerabilities of the system under attack, in this case the democracy of the United States.

Given that framework, the element of the information revolution that has up until recently been placed front and center in analyses of information warfare upgraded by the internet—the development of infrastructure that underwrites core functions of global society but that is fundamentally insecure—becomes a secondary consideration. Of greater relevance to the conduct and prospects for influence operations in the digital age is the construction of new systems of information generation, which allows the presentation and dissemination of information that today allows for easy distribution without traditional media gatekeepers.

For prosecutors of information warfare, the implication herein is twofold. First, diffusion of the mechanical function of democratic information environments means new attack vectors for disinformation efforts. This is particularly relevant given that the potential for such interference has been until recently—and arguably remains so up to the point of writing—dramatically unrealized, even given the construction of an entire command structure for combating cyber threats and the promulgation of a new strategic posture in cyberspace, which is discussed below. Second, the coupling of new media systems that offer users direct access to a diverse ecosystem with the rise of commercial owners of such mediums of discourse means unique opportunities for the subversion of the process. In recent experiences with so-called democracy hacking across Europe and North America, this reality has played out in the sophisticated manipulation of new media functions aimed at influencing discourse in national populations. As recent work has concluded, fake content deployed in platforms such as Facebook were targeted to specific audiences using in-built advertiser tools provided by the company.[22] Moreover, directed influence efforts on Twitter, Instagram, and YouTube were designed with the function of redistribution algorithms in mind. Tweets were optimized so as to stand a greater chance of appearing as a suggested result for users with certain social or political inclinations. Fake new content would be published with clickbait titles and, at least sometimes, benefited from click fraud that raised the chances of broader viewership.[23] In these ways, armed in some instances with the stolen data products of cyber intrusions, the IRA and other entities were able to attempt interference and to sell disinformation to democratic polities writ large.[24]

Byzantine Failures of Democracy

Why is disinformation enabled by the internet such a seemingly intractable problem for Western states to deal with? From one perspective, of course, one might argue that the diverse smorgasbord of relevant actors that must coordinate to defend against such threats is the problem, one that authoritarian states do not have in as meaningful ways. This article argues that such issues are preceded by another, however. Simply put, from technology companies to numerous media entities, those stakeholders whose collaboration would ensure an ability to combat sophisticated foreign information warfare efforts are not themselves—at least, not all—necessarily aware of the role they play as mechanical elements of democratic process. Though a company such as Google is certainly aware that manipulation of search algorithm fundamentals by malicious parties to seed sensational content is broadly problematic, it is likely that there is no direct acknowledgment that such problems are most directly rooted in the company's role in assuring normal democratic discourse. The result is a dissonance wherein corrective policies on the part of the company, such as those efforts made by Google to deweight websites in search results based on low traffic, PageRank scores, and more since 2018 reflect an interest in the removal of disruptive content rather than removal of content that aids the subversion of marketplace mechanisms.[25] Left unaddressed, this dynamic makes the national security interests and coercive mechanisms within a state secondary to the interests of business, political advocacy, and other social causes. The challenge for Western states is, as this section illustrates via reference to a seminal game theoretic model employed by information security experts, to better design information assurance mechanisms that limit the likelihood that such dissonance will manifest.

As noted above, democracies are complex systems wherein functionality is determined by mechanisms for assuring information. The role and importance of these mechanisms differs depending on how a democracy is structurally designed and works in practice. Given a parliamentary system of government, for instance, the voice of significant cabinet members may constitute a more relevant reference point for the general public than might be the case with presidential or hybrid majoritarian systems. Likewise, where regulatory power is deeply embedded in bureaucratic establishments—such as in the immense federal institutions in democratic states such as Brazil that have been labeled a form of "bureaucratic authoritarianism"—such figures might similarly play a role as a countervailing mechanism of democratic discourse that might be considered unusual elsewhere.

More than simply understanding which people, organizations, and institutions matter in any one given system, however, it is important to remember that these mechanisms—bureaucrats, experts, executives, media entities, etc.—enable certain functional conditions that allow for this structuring of democratic society to work as intended. As described above, the moderating function of democracies emerges from the reasonable provision of capacity to ensure the origination, credibility, quality, and freedom of information in the environment. We might generalize these requirements of proper system function as consensus on what information, in a functional sense, is. The traditional mechanisms described by the classical theory of the "marketplace of ideas" are merely the corollaries of such provision.

This article has laid out the function of democracies as information systems because it is insufficient to simply work from past examinations of information warfare as an activity that disrupts discourse or is constructed around situation-specific goals (e.g., favoring one candidate over others). Those works have laid a valuable groundwork but do fail in being flexible insofar as they often overgeneralize about the static significance of certain people or institutions, such as American presidents. Some studies have acknowledged that changes to the information environment due to exogenous shocks like war or technological innovation can change the behavior of particular countervailing institutions of democratic process.[26] Remarkably little work, however, has thought to emphasize the notion that democratic functionality rests on the underlying conditions of information assurance in democracies, which mechanically present in the actions of certain social and political forces. Subversion of the interests and motivations of such forces, which is traditionally thought of only where war or some other outside context is encountered, endangers the normal operation of the political system as a whole. Modern digitally enabled information warfare threats constitute such a prospective subversion but do not manifest in such obvious fashion as the exogenous concerns typically written about by scholars.

This theoretical clarification is critical to unpack the nature of risks involved in democracy hacking such that a better perspective on relevant military strategy might be obtained. Though the direct outcomes of Russian efforts to interfere in the United States during the 2016 presidential election remain unclear at the time of writing, the dynamics of the broader effort are evidence enough that new internet-enabled services and methods for communicating impact the ability of the system to reach consensus on the integrity and functional utility of information. In the past half-decade in the United States and elsewhere, the design and management of new media service platforms created a new space in which the system could be hacked. Specifically, these conditions created a recently underrealized space wherein interfering with the mechanical elements of democratic information assurance that ensure a reasonable consensus on the underlying nature of information is more possible than it has ever been. Because pre-internet communications mediums concentrated control of information presentation in the hands of certain institutional gatekeepers, potential failure of the marketplace could reasonably be said to come down to one of a few deviant outcomes, including the blatant dereliction of duty of the watchdog media or executive threat inflation. These new information conditions—meaning not only the now-decades-old appearance of the internet, but the more recent revolution in social media services and platforms built to work on the internet—change that calculus.

Perhaps the best illustration of how they have changed the dynamics of communication platforms is the paradigmatic example of the Byzantine Generals Problem game that is used by computer scientists and others to describe the security challenges inherent in designing fault-tolerant systems. In the game's scenario, multiple generals lead armies that must work together to successfully attack a city. If all armies attack simultaneously, their assault will succeed; if not, the fraction that attacks will fail and the remainder will not be able to succeed in the future. The critical task before the general of each army is one of communication. They must guarantee the integrity of the message they send to their counterparts so as to be sure that their own attack will not end in failure. In part, the challenge is one of developing the means to communicate effectively—using codes, trusted couriers, or novel methods of transmission, for instance, to better secure messages. More broadly, however, the challenge is the same socio-psychological issue identified by realists in the problem of other minds. How can one ensure that there are not traitors of one kind or another among the other generals? Such an individual might lie about their intended action, may tamper with messaging being forwarded to other commanders, or may lie because they themselves believe another actor is untrustworthy. If that problem cannot be overcome, then the entire enterprise is vulnerable to what is known as a "Byzantine" fault, wherein the system breaks down but in ways that are not easily detectable and seem arbitrary to the victim.

The Byzantine General's Problem, at least in the terms of the on-paper representation of the scenario facing the different armies' commanders, is unsolvable. Within the confines of the game, there is simply no way to guarantee the integrity and privacy of messages in such a way as to satisfy the suspicious (by necessity) minds of each general. Moreover, there is no way to guarantee knowledge of where the system has failed. Much like the bargaining theory of war, however, the point of the game is to emphasize the difficulties and subsequent implemental requirements for those seeking to design well-functioning information systems. A Byzantine fault-tolerant system is one that remains dependable during some system failure even where there is uncertainty about where or how the failure has manifested.[27]

Traditionally, democratic information systems—idealized classically in the concept of the marketplace of ideas—are remarkably resilient. Above almost anything else, subversion of the proper information functions of democratic societies is difficult at scale. This is because of the manner in which broad-scoped, diverse popular participation and contestation is traditionally directed through limited channels over time in the form of a relatively small constellation of media outlets reporting the words of important political voices, celebrities, and experts. In particular, because the function of democracy does not require perfect information but rather a reasonable enough consensus understanding of the value of information to spur moderating effects, defense against Byzantine failure is generally possible as electorates observe, dissect, and update their understanding. As a resultant, the only failures that democracies are commonly prone to are those wherein a prominent mechanism of information assurance ceases to function, such as when executives falsify or sensationalize information.

In the recent experience of the United States with foreign-based, cyber-enabled information warfare, the important role of quiet countervailing institutions and an executive proxy in then-presidential candidate Donald J. Trump, whose rhetorical approach to politics embraced sensationalism cannot be overlooked. Nevertheless, it seems clear that the design and use of modern internet-enabled media platforms, coupled with a limited ability by relevant stakeholders and citizenry to attribute and validate information consumed thereon, are the critical factors that make the threat of information warfare in the digital age novel.

The ability of meddling foreign threat actors to covertly enter domestic conversations via use of fake accounts, to spread false narratives and facts in a manner that is generally hard to track for the average citizen, and to strategically inject information to counter the moderating effect of time on national deliberations create an attribution challenge for the marketplace of ideas that opens space for Byzantine failures of the system. Moreover, regardless of whether or not such failures took place as a result of Russian information warfare from 2014 onward, it seems clear that a lack of oversight on the manner in which design characteristics of new information dissemination platforms and the unfamiliarity of elites and media actors with discourse channeled through such mediums particularly magnify the potential for their occurrence. Simply put, though the failure of traditional marketplace mechanisms is still substantially needed for major disruptions to democratic process to occur, the confluence of circumstances brought about by new environmental conditions clearly create new space within which information attribution and subsequent assurance is unprecedentedly difficult.

Countering Information Warfare: The Defense Establishment Perspective

This short article has made two simple arguments. First, the targeting strategies of sophisticated information warfare campaign should not be understood in terms of the specific platforms, voices, or issues that are victimized. Rather, they should be informed and contextualized by understanding of the democratic process. This argument is not a controversial one. After all, the first step in any threat mitigation effort is to understand how the force being employed impacts the function of the targeted system, whether that system is a computer, a military organization, or an entire national political apparatus. Here, it is simply the case that scholars and practitioners have largely avoided—surprisingly—the immense body of knowledge generated within the communications and political science fields of study that offer perspective on how democracies handle and use information to reach prudent deliberative outcomes.[28] By understanding the potential vulnerabilities of Western democracies as mechanisms that are more or less significant to the task of assuring the quality, origination, credibility, and freedom of information, defense planners are better situated to develop both defensive and deterrent solutions to the threat of information warfare.

Second, the article has argued that the unique threat posed by counterpopulation information warfare (i.e., the integrity of societal information processes are being targeted) is not only a function of novel attack vectors and a diffuse attack surface, but of the dissonance that organically emerges among actors in civil society and private industry when there is no recognition of the link between their interests and their functional position within the marketplace of ideas. In other words, such circumstances, which are more readily brought about given new internet-enabled dynamics of societal interaction, make it hard to see failures of the system actually *are* failures of the system. This, of course, adds to the challenge of national defenders insofar as the case-specific challenges of modern information warfare are not simply complex but also sometimes undetectable.

These dynamics suggest two distinct operating criteria for military forces interested in deterring threats of information warfare from organized foreign adversaries such as the Russian Federation, Islamic State, and the People's Republic of China. Naturally, as mentioned in the introduction, most Western states face a challenge in meeting the requirements of such an imperative that is not shared by counterpart institutions in authoritarian countries in that national law tends to limit the ability of militaries to take those domestic actions that would be of use in this particular case. Instead, military forces must be employed to aid domestic law enforcement and intelligence entities in their missions insomuch as national statutes permit. In many cases, this will involve resource sharing that does not violate the requirement of most national constitutions across North America and Western Europe that armed forces cannot operate offensively in the homeland.[29]

In other cases, this might involve joint training with civilian government agencies, the sponsorship of education programming, and more—some of which already exists. Indeed, military institutions that have often led in developing new educational curricula and methods of training large populations stand to be effective as standard-bearers for national efforts to further make Western populations resilient to the effects of information warfare. If information war is not simply a set of new tricks and tactics practiced by belligerent foreign powers, but rather the manifestation of an entrenched commitment by malicious actors to manipulate as a pillar of modern great power conflict, then the institutions of national security must lead by example even where they cannot directly specific elements of the national defense. Moreover, another distinct opportunity for greater military involvement in defensive efforts vis-à-vis information warfare would be in cases where new platforms and infrastructure—perhaps even some currently in private hands—are designated as critical assets for national security purposes, thus opening the doorway for the direct provision of technical and operational expertise. These actions, however, fall beyond the scope of the following suggestions.

First, efforts to deter digital threats using cyber operations and related instruments of state power would do well to incorporate an understanding of the information assurance mechanisms of democratic process described in brief above into targeting strategies.[30] As of 2018, the United States' approach to combating digital threats changed in a significant fashion with the promulgation of a strategy for cyberspace that calls for "defending forward."[31] The strategy, which many democratic partner nations are now adopting in some fashion, defines *cyberspace* as a domain of persistent engagement where adversaries are constantly interacting.[32] Given this dynamic, the traditional trappings of deterrence theory do not seem to strictly apply. Restraint and a strong notion of sovereign territory are concepts ill-suited to threats that manifest via the internet, necessitating a domain-specific alternative. By defending forward, the United States now aims to shape adversary behavior by consistently engaging digital threats wherever they are found, particularly when they can be engaged beyond American networks. The idea, not indistinct from the strategy of deterrence by punishment with cyber-specific characteristics, is to force and reinforce preferred modes of digital interaction with adversaries such that other threat mitigation efforts—such as the diplomatic construction of norms of nonaggression in online conflict—are considered instead of an ever-expanding information warfare race in the cyber realm.

Naturally, given the manner in which modern information warfare emerges mainly from the spread of the internet and the possibilities of web technologies, it has been suggested that a strategy of deterrence similar to that now being practiced with cyber conflict should apply. Indeed, it seems obvious that the line between the two is substantially blurred given the degree to which cyber operations are sometimes used to augment influence campaigns.

The analysis in the sections above imply, perhaps more than anything else, that an effective military posture on information warfare should reference analytics on what specific actions most threaten the several information-assuring mechanisms of the marketplace of ideas. Counteroffensive cyber operations intended to set behavioral red lines on whether acceptable information warfare practices, for instance, might be employed where a bot campaign is employed rapidly and at scale to stoke doubts about the statements made by national political candidates for executive office, but not when those same bots attempt to spread clickbait malware to their follower base. The idea of such a strategy is not to eliminate the practice of interference operations, but to shape the behavior of foreign adversaries such that their efforts are unlikely to be effective. By imposing costs specifically around actions linked to core functional mechanisms of the system under attack (i.e., the democracy itself) militaries can effectively enhance the potential of other defensive efforts, such as industry attempts to harden social media platforms against fake news infiltration or diplomatic attempts to build constraining norms against political warfare.

Second, the above analysis suggests that the response tempo of Western efforts to deter hybrid threats—particularly those encountered in cyberspace—should be governed by analysis of how foreign adversaries use cyberspace for information warfare, irrespective of detectability of specific operations underway. A significant fear of strategic planners who supported a more defensive posture for the United States in cyberspace through 2018 was that cyber aggression might lead to escalation in hostilities with other countries across other domains.

The logic behind defending forward holds that escalation is not particularly concerning, particularly because tactical actions can be designed so as to leverage strategic gains.[33] Counteroffensive cyber operations that are not determined by incidence of foreign aggression but rather by probabilistic analysis of the likelihood that cyber power is being employed in aid of information warfare should be embraced as an acceptable and expected outcome of the prevailing line of thinking. Not only does such punitive action—employed clearly against targets linked to information warfare efforts—help mitigate the challenge of Byzantine failure as an inevitable condition of being targeted for interference by foreign adversaries, but it also reinforces disapproval of certain approaches over and above incident-specific reactions.

Conclusions

Few threats to national security loom as large in the eyes of defense strategists and scholars as the specter of political warfare augmented by advancing information technologies. In recent years, cyber operations have enhanced deft manipulation of the algorithmic underpinnings of modern media platforms to reinforce and project attempts to sell prejudice, skew opinion, and coerce and distract democratic populations. In the future, it is a certainty that information warfare will continue to prove a significant challenge. Undoubtedly, recent manifestations of political warfare appear to have caused such widespread alarm in part because the space was previously underrealized. Going forward, however, it seems likely that advancing smart systems for producing fabricated content and for shaping the informational inputs made available to democratic populations will widen that space and invite further foreign interference in Western sociopolitical processes.

For defense establishments, addressing the threat of modern information warfare aimed at entire populations is a daunting one, not least because the expanded attack surface of democratic states does not align with the statutory limitations placed on many military institutions vis-à-vis their defensive mandate. Nevertheless, addressing such challenges is possible. This article has argued that the analytic foundation on which military perspectives on hybrid threats are formed must diversify to combat emerging threats. Understanding information warfare aimed at entire populations demands greater in-depth understanding of the function of those political and social systems being targeted. Such understanding then lends itself to an ability to more effectively gauge the categories of threat and types of incidents that can be targeted under the auspices of deterrent strategies to impose costs and reduce—if not the actual incidence of information warfare efforts by multiform foreign threat actors—the potential for *meaningful* interference in the process of democratic governance.

Endnotes

1. Way and Casey document nearly two dozen such operations undertaken by the Russian Federation since 2014. Additionally, Martin, Shapiro, and Nedashkovskaya similarly code 53 distinct influence campaigns undertaken by several countries across 24 target nations between 2013 and 2018. See Lucan Ahmad Way and Adam Casey, “Russia Has Been Meddling in Foreign Elections for Decades. Has It Made a Difference?,” *Washington Post*, 5 January 2018; and Diego A. Martin, Jacob N. Shapiro, and Michelle Nedashkovskaya, “Recent Trends in Online Foreign Influence Efforts,” *Journal of Information Warfare* 18, no. 3 (2019): 15–48.
2. Franziska B. Keller et al., “Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign,” *Political Communication* 37, no. 2 (2020): 1–25, https://doi.org/10.1080/10584609.2019.1661888; Brandon C. Boatwright, Darren L. Linvill, and Patrick L. Warren, *Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building* (Leipzig, Germany: Resource Centre on Media Freedom in Europe, 2018); Sandor Fabian, “The Russian Hybrid Warfare Strategy—Neither Russian nor Strategy,” *Defense & Security Analysis* 35, no. 3 (2019): 30825, https://doi.org/10.1080/14751798.2019.1640424; and David Filipov, “The Notorious Kremlin-linked ‘Troll Farm’ and the Russians Trying to Take It Down,” *Washington Post*, 6 October 2017.
3. For more on the broad landscape of such threats in the modern era, see Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: Rand, 2018), https://doi.org/10.7249/RR1772; Mark Stokes and Russell Hsiao, *The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics* (Arlington, VA: Project 2049 Institute, 2013); Antonios Nestoras, “Political Warfare: Competition in the Cyber Era,” *European View* 18, no. 2 (2019): https://doi.org/10.1177/1781685819885318; and Levin H. Dov, “Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset,” *Conflict Management and Peace Science* 36, no. 1 (2019): 88–106, https://doi.org/10.1177/0738894216661190.
4. For the purposes of this discussion, deepfake generally refers to videos where the face and/or voice of a person, usually a public figure, has been manipulated using artificial intelligence software in a way that makes the altered video look authentic.
5. James Vincent, “Deepfake Detection Algorithms Will Never Be Enough,” Verge, 27 June 2019.
6. Martin C. Libicki, *What Is Information Warfare?*, Strategic Forum No. 28 (Washington, DC: Institute for National Strategic Studies, National Defense University, 1995).
7. For instance, Martin C. Libicki, *Information Dominance* (Washington, DC: Institute for National Strategic Studies,National Defense University, 1997).
8. *Attack surface* refers to the sum of vulnerable points of a given target system.
9. See Andrew Monaghan, “The ‘War’ in Russia's ‘Hybrid Warfare’,” *Parameters* 45, no. 4 (Winter 2015): 65; Alexander Lanoszka, “Russian Hybrid Warfare and Extended Deterrence in Eastern Europe,” *International affairs* 92, no. 1 (2016): 175–95, https://doi.org/10.1111/1468-2346.12509; Bettina Renz, “Russia and ‘Hybrid Warfare’,” *Contemporary Politics* 22, no. 3 (2016): 283–300, https://doi.org/10.1080/13569775.2016.1201316; and Christopher S. Chivvis, *Understanding Russian “Hybrid Warfare” and What Can Be Done About It* (Santa Monica, CA: Rand, 2017), 2–4, https://doi.org/10.7249/CT468.
10. As argued, for instance, in Peter Pomerantsev, *This Is Not Propaganda: Adventures in the War Against Reality* (New York: Hachette Book Group, 2019). Pomerantsev argues that the notion of Russian “information war” is commonly put on a pedestal by strategic thinkers and military operators, particularly during the past several years, as a set of tactics and methods rooted in Cold War-era thinking about media manipulation and tricks. And yet, what is clear in much scholarship and in many developments since at least 2016 is that information warfare is remarkably deeply ingrained in Russian (and other states') efforts to secure national interests and export favorable worldviews, to the

point where defensive efforts demand the strategic countering of such efforts rather than the operational mitigation of irritating interference.

11. For seminal descriptions of information warfare, see Dorothy E. Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999); Roger C. Molander, Andrew Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: Rand, 1996), https://doi.org/10.7249/MR661; and Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), https://doi.org/10.1017/CBO9780511804250.

12. See "Policy Planning Staff Memorandum," 4 May 1948, *Foreign Relations of the United States, 1945–1950, Emergence of the Intelligence Establishment* (Washington, DC: Government Printing Office, 1948), document 269.

13. It is important to note here that the author in no way claims that political interference or information warfare aimed at population-level manipulation is a new phenomenon. Foreign-induced political subversion is a strategy found in history as far back as Louis XIV's influence campaigns prosecuted in central Europe ahead of his military conquests. In the modern era, both the People's Republic of China and the Russian Federation have extensively sought to export their models of political process or otherwise favorably shape foreign societal dynamics in line with national interests with influence operations.

14. David E. Sanger, "Obama Strikes Back at Russia for Election Hacking," *New York* Times, 29 December 2016; and Thomas Rid and Ben Buchanan, "Hacking democracy," *SAIS Review of International Affairs* 38, no. 1 (2018): 3–16, https://doi.org/10.1353/sais.2018.0001. Also see Isabella Hansen and Darren J. Lim, "Doxing Democracy: Influencing Elections Via Cyber Voter Interference," *Contemporary Politics* 25, no. 2 (2018): 1–22, https://doi.org/10.1080/13569775.2018.1493629.

15. Herbet Lin and Jaclyn Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation," in *Oxford Handbook of Cyber Security*, ed. Paul Cornish (New York: Oxford University Press, 2018).

16. Henry Farrell and Bruce Schneier, *Common-Knowledge Attacks on Democracy*, Berkman Klein Center Research Publication no. 2018-7 (Cambridge, MA: Berkman Klein Center for Internet & Society; Harvard University, 2018), http://dx.doi.org/10.2139/ssrn.3273111.

17. For seminal examples, see Anthony Downs, *An Economic Theory of Democracy* (New York: Harper, 1957); Jack Snyder, *Myths of Empire: Domestic Politics and Political Ambition* (Ithaca, NY: Cornell University Press, 1991); Bruce Russett, *Grasping the Democratic Peace: Principles for a Post–Cold War World* (Princeton, NJ: Princeton University Press, 1993); Stephen Van Evera, *The Causes of War: Power and the Roots of Conflict* (Ithaca, NY: Cornell University Press, 1999); and Dan Reiter and Allan C. Stam, *Democracies at War* (Princeton, NJ: Princeton University Press, 2002).

18. Perhaps the best description is in Chaim Kaufmann and Ronald Krebs, "Selling the Market Short?: The Marketplace of Ideas and the Iraq War," *International Security* 29, no. 4 (Spring 2005): 196–207, https://doi.org/10.1162/isec.2005.29.4.196. Also see Tim Dunne, "Liberalism, International Terrorism, and Democratic Wars," *International Relations* 23, no. 1 (2009): 107–14, https://doi.org/10.1177/0047117808104156; and Jane K. Cramer and A. Trevor Thrall, "Introduction: Understanding Threat Inflation," in *American Foreign Policy and the Politics of Fear: Threat Inflation since 9/11*, ed. A. Trevor Thrall and Jane K. Kramer (New York: Routledge, 2009), 19–33.

19. See, for instance, A. Trevor Thrall, "A Bear in the Woods?: Threat Framing and the Marketplace of Values," *Security Studies* 16, no. 3 (2007): 452–88, https://doi.org/10.1080/09636410701547915; and A. Trevor Thrall, "Framing Iraq: Threat Inflation in the Marketplace of Values," in *American Foreign Policy and the Politics of Fear*, 192–209.

20. For the purposes of this discussion, astroturfing refers to organized activity intended to create a false impression of a widespread, spontaneously arising, grassroots movement in support of or in opposition to something (e.g., political policy) but in reality, was initiated and controlled by a concealed group or organization (e.g., corporation).

21. Jonathan Hassid, "Safety Valve or Pressure Cooker?: Blogs in Chinese Political Life," *Journal of Communication* 62, no. 2 (2012): 212–30, https://doi.org/10.1111/j.1460-2466.2012.01634.x; and Rebecca MacKinnon, "Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom" (paper, Liberation Technology in Authoritarian Regimes, Stanford University, 11–12 October 2010).
22. Karoun Demirjian et al., "Russian Ads, Now Publicly Released, Show Sophistication of Influence Campaign," *Washington Post*, 1 November 2017.
23. Mark Carman, et al., "Manipulating Visibility of Political and Apolitical Threads on Reddit via Score Boosting" (paper, 17th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, New York, 1–3 August 2018), 184–90, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00037.
24. Perhaps the most prominent popular work detailing such efforts is Kathleen Hall Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know* (New York: Oxford University Press, 2018); Michael Isikoff and David Corn, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump* (New York: Twelve, 2018); and Malcolm Nance, *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election* (New York: Simon and Schuster, 2016). More detailed empirical explorations of Russia and other nations' efforts include Savvas Zannettou et al., "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web" (paper, WWW '19: Companion Proceedings of the 2019 World Wide Web Conference, May 2018); Adam Badawy, Emilio Ferrara, and Kristina Lerman, "Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign" (paper, 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Barcelona, Spain, 2018); Yuriy Gorodnichenko, Tho Pham, Oleksandr Talavera, "Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #USElection," NBER Working Paper No. 24631 (Cambridge, MA: National Bureau of Economic Research, 2018): https://doi.org/10.3386/w24631; Massimo Stella, Emilio Ferrara, and Manlio De Domenico, "Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems," *Proceedings of the National Academy of Sciences* 115, no. 49 (2018): 12435–40, https://doi.org/10.1073/pnas.1803470115; Pik-Mai Hui et al., "BotSlayer: Real-Time Detection of Bot Amplification on Twitter," *Journal of Open Source Software* 4, no. 42 (2019): 1706, https://doi.org/10.21105/joss.01706; Michael Bossetta, "A Simulated Cyberattack on Twitter: Assessing Partisan Vulnerability to Spear Phishing and Disinformation Ahead of the 2018 US Midterm Elections," *First Monday* 23, no. 12 (2018): https://doi.org/10.5210/fm.v23i12.9540; Marco Bastos and Johan Farkas, " 'Donald Trump Is My President!': The Internet Research Agency Propaganda Machine," *Social Media + Society* 5, no. 3 (2019): https://doi.org/10.1177/2056305119865466; and Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 3 (August 2017): 1–18, https://doi.org/10.1017/S0003055417000144.
25. See Stacie Hoffmann, Emily Taylor, and Samantha Bradshaw, *The Market of Disinformation* (Oxford, UK: University of Oxford, 2019), 13–14.
26. For instance, those in the tradition that developed the notion of the CNN effect. See Piers Robinson, *The CNN Effect: The Myth of News, Foreign Policy and Intervention* (New York: Routledge, 2005); and Eytan Gilboa, "The CNN Effect: The Search for a Communication Theory of International Relations," *Political Communication* 22, no. 1 (2005): 27–44, https://doi.org/10.1080/10584600590908429.
27. Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems* 4, no. 3 (July 1982): https://doi.org/10.1145/357172.357176.
28. Though there are, naturally, noteworthy recent exceptions to this trend. The paradigm example of this is the report of Special Prosecutor Robert S. Mueller III, submitted in

April 2019. See Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vols. I and II, redacted version of 18 March 2019 (Washington, DC: Department of Justice, 2019). In addition, the effort of scholars—including several linked to the Oxford Series in Digital Politics—stand out in this regard. See Farrell and Schneier, *Common-Knowledge Attacks on Democracy*; Harold Feld, *The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms* (New York: Roosevelt Institute, 2019); Catherine Frost, "The Power of Voice: Bots, Democracy and the Problem of Political Ventriloquism," *Journal of Political Power* 13, no. 1 (2019): 1–16, https://doi.org/10.1080/2158379X.2019.1701831; Samuel C. Woolley and Philip N. Howard, eds., *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (New York: Oxford University Press, 2018), https://doi.org/10.1093/oso/9780190931407.001.0001; Nigel Shadbolt et al., *The Theory and Practice of Social Machines* (Cham, Switzerland: Springer, 2019), https://doi.org/10.1007/978-3-030-10889-2; and Ciarán McMahon, *The Psychology of Social Media* (New York: Routledge, 2019).

29. In the United States, the relevant statute in this regard is the Posse Comitatus Act of 1878 that prohibits the use of active duty military personnel to "execute the laws" passed by Congress to regulate domestic society. Though there is some argument about what the restriction entails in terms of prospective advising capacities of the national military, there have historically been remarkably few exceptions to the prohibition on domestic operation. Two incidents that stand out are the use of military personnel for law enforcement duties in Louisiana following Hurricane Katrina (2005) and in the Los Angeles riots (1992), both of which were allowed for under the Insurrection Act of 1807. The Posse Comitatus Act also exempts the Coast Guard, the use of military assets for drug trade interdiction, the deployment of National Guard units by state authorities, and the execution of surveillance missions for national security purposes. Though this final point might be prospectively a basis for more elaborate military operation within domestic networks for national security purposes, no such argument has yet been advanced either in prose or practice to date. See Charles Doyle, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law* (Washington, DC: Congressional Research Service, 2000); William C. Banks, "Providing 'Supplemental Security'—The Insurrection Act and the Military Role in Responding to Domestic Crises," *Journal of National Security Law & Policy* 3, no. 1 (2009): 39–94; and Shane McGrane, "Katrina, Federalism, and Military Law Enforcement: A New Exception to the Posse Comitatus Act," *Michigan Law Review* 108, no. 7 (2010): 1309–40.

30. For more on the debate around the potential for cyber deterrence, see Aaron F. Brantly, "The Cyber Deterrence Problem" (paper, 2018 10th International Conference on Cyber Conflict [CyCon], Tallinn, Estonia, 29 May–June 2018); Damien Van Puyvelde and Aaron F. Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Hoboken, NJ: Wiley, 2019); and Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 44–71, https://doi.org/10.1162/ISEC_a_00266.

31. Donald J. Trump, *National Cyber Strategy of the United States of America, September 2018* (Washington, DC: White House, 2018).

32. Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017): 381–93, https://doi.org/10.1016/j.orbis.2017.05.003.

33. Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," 381–93.