

# MANEUVER AND MANIPULATION: ON THE MILITARY STRATEGY OF ONLINE INFORMATION WARFARE

Tim Hwang



ADVANCING  
STRATEGIC THOUGHT  
SERIES



# The United States Army War College

---

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a “think factory” for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.



The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.



The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.



The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.



The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.



The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.



# STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.



**Strategic Studies Institute  
and  
U.S. Army War College Press**

**MANEUVER AND MANIPULATION:  
ON THE MILITARY STRATEGY OF ONLINE  
INFORMATION WARFARE**

**Tim Hwang**

**May 2019**

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This report is cleared for public release; distribution is unlimited.

\*\*\*\*\*

This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

\*\*\*\*\*

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5238.

\*\*\*\*\*

All Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications may be downloaded free of charge from the SSI website. Hard copies of certain reports may also be obtained through the U.S. Government Bookstore's website at <https://bookstore.gpo.gov>. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: <https://ssi.armywarcollege.edu/>.

\*\*\*\*\*

The Strategic Studies Institute (SSI) is the U.S. Army's institute for geostrategic and national research and analysis. SSI supports the U.S. Army War College (USAWC) curricula, provides direct analysis for Army and Department of Defense leadership, and serves as a bridge to the wider strategic community. SSI studies are published by the USAWC Press and distributed to key strategic leaders in the Army and Department of Defense, the military educational system, Congress, the media, other think tanks and defense institutes, and major colleges and universities.

ISBN 1-58487-815-0



## FOREWORD

Ongoing revelations about Russian meddling in the 2016 U.S. Presidential election leave policymakers and the defense community with a set of challenging questions. How should the United States best counter and deter these types of activities going forward? How much of a threat do these types of tactics pose to democracy? What interventions are consistent with our national values and the proper role of the military?

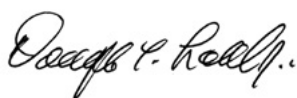
Approaches that myopically focus on the latest headlines will miss the bigger picture. The Strategic Studies Institute (SSI) believes that these developments demonstrate that the continued growth and evolution of the cyber domain has reshaped the fundamental nature of information warfare. We must develop a broader strategic concept that organizes defense efforts into a cohesive, effective whole. On this count, *Maneuver and Manipulation*—authored by researcher Tim Hwang—is a key contribution to the discussion as the defense community develops its approach to the information warfare of the present day and beyond. Grounding his analysis in a careful look at how the Internet has transformed persuasion, he builds a framework that provides important insight into the nature, goals, conduct, and defense strategies of modern information warfare.

*Maneuver and Manipulation* is also a valuable resource for examining existing thought on online persuasive conflict and its limitations. Mr. Hwang provides a useful analysis that examines and compares strategic concepts for information warfare among nation states, focusing on the United States, China, and Russia. He also reviews the strategic approaches taken by some of the nonstate actors which have proven to

be some of the most prolific practitioners of this new breed of informational conflict—the Islamic State in Iraq and Syria and WikiLeaks.

This monograph is particularly unique because of the pioneering work of Mr. Hwang in this domain. As early as 2010, Mr. Hwang was one of the first to demonstrate that swarms of bots could shape online discourse and relationships between users on social media. His subsequent research has tracked the use of these techniques among state and nonstate actors and experimented with potential countermeasures in the space. In this respect, Mr. Hwang writes not just as a theorist, but with the hard-won experience of a practitioner of modern information warfare.

SSI believes that this monograph will be a useful resource as the broader U.S. strategic community continues to develop, debate, and decide the shape of informational conflict in the 21st century.



DOUGLAS C. LOVELACE, JR.  
Director  
Strategic Studies Institute and  
U.S. Army War College Press

## ABOUT THE AUTHOR

TIM HWANG currently serves as director of the Harvard-Massachusetts Institute of Technology (MIT) Ethics and Governance of Artificial Intelligence (AI) Initiative, a philanthropic project working to ensure that machine learning and autonomous technologies are researched, developed, and deployed in the public interest. Previously, he was at Google, where he was the company's global public policy lead on AI, leading outreach to government and civil society on issues surrounding the social impact of the technology. Mr. Hwang is a researcher focusing on the strategy of modern information warfare and the geopolitical aspects of computational power and machine learning. His experiments in using bot swarms to shape online discourse in 2011 were some of the first to demonstrate the potential risks posed by these technologies. Since then, he has tracked the use of fake, automated identities by state and nonstate actors as a means of shaping group behavior on social media. Dubbed "The Busiest Man on the Internet" by *Forbes*, his work has appeared in *The New York Times*, *The Washington Post*, *Wired*, *The Atlantic*, and *The Wall Street Journal*, among others.



## SUMMARY

Ongoing discussion around the Russian development of hybrid warfare and the revelations about meddling in the 2016 U.S. Presidential election have focused the public's attention on the threats posed by coordinated campaigns of propaganda and disinformation. These recent events have also raised concerns around the broader challenge posed by the emergence of a "post-fact society," the notion that the weakening ability for civil society and the public to analyze truth and falsity is creating a threat to the health and sustainability of democratic institutions.

Technology and the Internet, in particular, play a key role in shaping the flow of information through society. Not surprisingly, the role of these systems in enabling new types of information warfare has figured prominently in the discussion as policymakers and scholars begin to develop their thinking about the appropriate response to these issues. Platforms such as Facebook and Google have been seen as having had a significant role in facilitating Russian propaganda efforts, incentivizing the distribution of false information, and encouraging the creation of extremist "filter bubbles."

As the defense community develops its approach to countering present-day online propaganda and disinformation techniques, it will need to place concerns around immediate threats into a broader understanding of the nature of the challenge. It will require, in short, an articulation of a broad and flexible, unified, strategic concept that encompasses the aspects of military, diplomatic, economic, informational, and other matters regarding the strategic situation. This monograph offers an initial sketch of such a concept,

proposing one approach to characterizing the strategic situation in the current information space and, based on that, some conjectures about the effective conduct of online information warfare.

The threat and use of operations that aim to shape perceptions, beliefs, and behaviors are, of course, not new to the theory or practice of warfare. Whether directed at the public or adversaries on a battlefield, these activities—to a greater or lesser extent—have long been part of the discussion of psychological operations, information operations (IO), military operations other than war, counterinsurgency, and public diplomacy, among others. In the context of the Internet and technology more broadly, more recent concepts of computational propaganda and, less recently, netwar, also offer a precedent.

This monograph draws on and adapts this lineage of thinking and others to the current technological and informational environment. Specifically, it argues the following:

- Modern information warfare falls somewhere between topics in the defense space. On the one hand, online disinformation efforts continue a long lineage of thinking and tactical innovation around the use of persuasion and influence in conflict. On the other, these topics are a salient, novel form of threat online that introduces a new set of themes into the discussion of cybersecurity and cyberwarfare strategy. In developing an effective, strategic concept which captures the nature of modern information warfare and the manner in which it is best conducted, the former needs to be married with the latter.
- Reviewing published strategic works on online information warfare in the United States,

Russia, and China, as well as among nonstate actors, suggests that the theoretical frameworks in the space remain frustratingly incomplete and vague. These texts are mostly silent on the nature of modern information warfare, the conduct of modern information warfare, and the effective means of defending against campaigns of information warfare.

- Modern information warfare is characterized by a cartographic shift: social behavior is now directly observable at many different scales at remarkably low cost. One can observe social reactions to a stimulus as it occurs and compare these reactions across both time and space. These developments and the concentration of this data in a small set of platforms change the nature of information flow and open new possibilities for the strategic development of information warfare.
- This cartographic shift influences the aims of information warfare. Conflicts shift from contests over the adoption or rejection of certain ideas and points of view to contests over the network structure of relationships and strength of ties within a population. Victory in these conditions entails capturing the ability to shape these networks toward desired ends, while defeat entails the inability to deny this influence to an adversary.
- Liberal democracies face special challenges in this environment because they must defend the aggregate amount of social capital or trust within society. Liberal democracies must also defend a particular arrangement of social capital—one that gives independent civil society and

public institutions a primary role. This requirement forces liberal democracies to construct defensible publics. This effort requires the creation of public systems of detection, support for robust social networks within society, and clear policies around the conditions for state intervention in the information space.



# MANEUVER AND MANIPULATION: ON THE MILITARY STRATEGY OF ONLINE INFORMATION WARFARE

## INTRODUCTION

Ongoing discussion around the Russian development of hybrid warfare and the revelations about meddling in the 2016 U.S. Presidential election has focused the public's attention on the threats posed by coordinated campaigns of propaganda and disinformation. These recent events have also raised concerns around the broader challenge posed by the emergence of a "post-fact society," the notion that the weakening ability for civil society and the public to analyze truth and falsity is creating a threat to the health and sustainability of democratic institutions.<sup>1</sup>

Technology and the Internet, in particular, play a key role in shaping the flow of information through a society. Not surprisingly, the role of these systems in enabling new types of information warfare has figured prominently in the discussion as policymakers and scholars begin to develop their thinking about the appropriate response to these issues.<sup>2</sup> Platforms such as Facebook and Google have been seen as having had a significant role in facilitating Russian propaganda efforts, incentivizing the distribution of false information, and encouraging the creation of extremist "filter bubbles."<sup>3</sup>

As the defense community develops its approach to countering present-day online propaganda and disinformation techniques, it will need to consider concerns of immediate threats with a broader understanding of the nature of the challenge. It will require, in short, an articulation of a unified, strategic concept:

The course of action accepted as the result of the estimate of the strategic situation . . . a statement of what is to be done in broad terms sufficiently flexible to permit its use in framing the military, diplomatic, economic, informational, and other measures which stem from it.<sup>4</sup>

This monograph offers an initial sketch of such a concept, proposing one approach to characterizing the strategic situation in the current information space and, based on that, some conjectures about the effective conduct of online information warfare.

The threat and use of operations that aim to shape perceptions, beliefs, and behaviors are, of course, not new to the theory or practice of warfare. Whether directed at the public or adversaries on a battlefield, these activities—to a greater or lesser extent—have long been part of the discussion of psychological operations, information operations (IO), military operations other than war, counterinsurgency, and public diplomacy, among others. In the context of the Internet and technology more broadly, more recent concepts of computational propaganda and, less recently, netwar, also offer a precedent.

This monograph draws on and adapts this lineage of thinking and others to the current technological and informational environment. Part I will frame the discussion, examining the structure of online disinformation and propaganda campaigns and the extent to which they fall into existing notions of “information warfare.” Part II will examine parallel lines of strategic thinking that have addressed the question of information warfare and the changing technological landscape. Part III will evaluate these precedents, arguing that the changing nature of the web offers a sharper and more nuanced strategic concept. Part IV then sketches out the parameters of this approach.

## **PART I: THE STATE OF PLAY**

Though Russian interference in the 2016 U.S. Presidential election triggered the present wave of interest in online propaganda campaigns, this most recent effort is far from unprecedented. Instead, these actions should be seen as only one particularly dramatic culmination of a range of activities pursued by Russia and other actors on the web over the past decade.

Developing an effective, strategic approach requires a characterization of the current environment. As a means of assessing the current state of play, this section reviews what is currently known about these efforts, explores the potential future routes for their development, and asks whether existing categories of “information warfare” in the defense literature adequately capture the phenomena.

### **The Triad of Online Disinformation—Media, Advertising, and Hacking**

While it may not have been the first, the 2016 campaign serves as a useful representative of the range of techniques that are being used to spread disinformation and manipulate discourse online. Three core components appeared in the Russian effort which are characteristic of campaigns seen elsewhere.

First was the use of formal and informal media outlets to shape public narratives and spread disinformation. Most prominently, the Russian campaign leveraged state-run media outlets such as Russia Today (RT) and Sputnik to distribute disinformation and support then-candidate Donald Trump.<sup>5</sup> These more obvious channels were accompanied by a range of less visible efforts. This included the recruitment of paid

online trolls and automated fake identities—“bots”—to amplify scandals and spread disinformation on a grassroots level.<sup>6</sup> This included promoting claims around biased or unfair news coverage as well as the propagation of a series of conspiracy narratives such as “Pizzagate,” which claimed that candidate Hillary Clinton and members of her staff were involved in an underground child sex trafficking ring.<sup>7</sup> This use of automation to “spam” disinformation alongside human agent provocateurs has been dubbed by researchers Sam Woolley and Phil Howard as “computational propaganda.”<sup>8</sup> Similar patterns have been seen in campaigns throughout the world, including Syria, England, Mexico, Ukraine, and Finland.<sup>9</sup>

Second, the “organic” spread of disinformation was accelerated through online channels of advertising. Advertising played a role in two aspects. In the first, Russian operatives leveraged the advertising platforms offered by platforms like Google and Facebook.<sup>10</sup> This allowed the highly targeted spread of false information about the candidates and facilitated messaging efforts attempting to create a polarization between opposing political advocacy groups within society more generally.<sup>11</sup> These state-driven efforts were also supported by a global ecosystem of profit-driven actors who benefited from the spread of widely shared disinformation. From teenage bloggers in Macedonia to entrepreneurs in Los Angeles, “fake news” was also supported by independent businesses seeking to drive traffic to their sites to generate advertising revenue.<sup>12</sup> The influence of advertising is not isolated to the Russian case: Chinese state-run media have also been experimenting with Facebook advertising as a way of driving their propaganda efforts.<sup>13</sup>

Third, the Russian campaign also incorporated the use of hacking to compromise the networks of the U.S. Democratic National Committee and leak information discrediting the Clinton campaign and staff.<sup>14</sup> This served as a means of disrupting the operations of campaign targets as well as a way of building the credibility of outlets that could later assist in the spread of doctored “leaks” to spread disinformation. This use of cyberattacks as a complement to information warfare operations was also observed during the 2017 French Presidential election and in the blockade of the United Arab Emirates later that year.<sup>15</sup>

These building blocks of social manipulation—media, advertising, and hacking—are widely available and can be deployed at a low cost. This allows both well-resourced state actors and more informal groups to take advantage of them. Terrorist networks have been particularly prolific users of these techniques. Groups such as al-Qaeda and the Islamic State of Iraq and Syria (ISIS) have leveraged the power of online communication as a means of increasing their prominence, recruiting collaborators, and maximizing the emotional impact of their efforts.<sup>16</sup> Researchers have also documented the use of these techniques by the loosely connected coalition of far-right and less radical “alt-right” communities that spread conspiracy theories during the 2016 U.S. Presidential campaign and have continued to remain active beyond the election.<sup>17</sup>

## **The Future**

The tactics of online propaganda are constantly evolving as state and nonstate actors continue to invest in and experiment with these techniques. Two

major technological trends seem poised to augment the impact of these campaigns going forward.

First, recent breakthroughs in artificial intelligence—specifically in the subfield of machine learning—seem likely to make it increasingly easy to fabricate realistic imitations of real-world video and audio.<sup>18</sup> One recent demonstration from researchers at Stanford, Face2Face, demonstrates how machine learning can create a believable representation of the face of a public figure from open source video.<sup>19</sup> These can be used in turn to “puppet” the face as desired.<sup>20</sup> In the demonstration, this technique is used to create believable “interviews” with Barack Obama, Donald Trump, and Vladimir Putin.<sup>21</sup> Similarly, WaveNet software, released in 2016, leverages machine learning to synthesize voices and other sounds to make them much more believable than in the past.<sup>22</sup>

As the computational cost of these types of techniques continues to decline, they become more available to actors interested in using these techniques to supplement campaigns of disinformation. A disinformation effort might have an increased ability to create believable videos of political leaders and celebrities that can be widely shared and more challenging to refute. These technologies might also be integrated to provide swarms of bots with more realistic “personalities” and behaviors that evade the detection systems of social media platforms and are difficult for users to discern easily as fakes. To that end, machine learning may expand the potential scope of these campaigns, enabling automated systems to better substitute for human agents in spreading disinformation.

Second, in the past 2 decades, the field of quantitative social science has grown considerably, aided by the availability of large, rich datasets about social

behavior enabled by the Internet.<sup>23</sup> Dubbed by one researcher to be a new field of “social physics,” data abundance has allowed researchers to gain a deeper understanding of a range of social behaviors, from how information spreads through groups and becomes “viral” to what leads certain groups to be robust against or vulnerable to false information.<sup>24</sup>

It is possible that these research findings will be used by malicious actors seeking to enhance the impact of their disinformation campaigns. Future perpetrators of these efforts may be able to tailor more accurately and target messaging for maximal persuasive or behavioral impact. These efforts may also allow these actors to better assess “vulnerabilities” in a social network—individuals who may be both susceptible to a messaging campaign and able to influence others. Beyond simply increasing the potential efficacy of disinformation efforts, more accurate targeting may also enable adversaries to achieve their aim without the extensive blanketing of a population with messaging. This may make campaigns more subtle and challenging to detect going forward.

### **The State of Play: Causal Ambiguity and Strategic Relevance**

While at the time of this writing it is clear that many actors are investing in and experimenting with online propaganda, it is important to note that empirical support for the causal impact of these campaigns remains unclear. Due to the opaque nature of the campaigns conducted by Russia and others, it is challenging to assess accurately whether these efforts have a relevant impact on behaviors like voting. This situational fog-giness also extends to potential countermeasures and

interventions that might be implemented. It is ambiguous, for example, whether interventions such as labeling content for information quality can lower the perceived credibility of “fake news.”<sup>25</sup> More generally, it is even unclear if the default state of the Internet exacerbates or reduces issues such as polarization.<sup>26</sup> Research continues to expand our understanding of these campaigns and their impact, but there remains much that is not known.<sup>27</sup>

Even in light of this ambiguity, these online techniques and campaigns of social manipulation should be a source of genuine concern to the national security and defense communities for a number of reasons. For one, the immediate case of 2016 may not be a useful guide to the effectiveness of these campaigns in general. The continued investment in these techniques by actors like Russia and China and a range of nonstate actors warrants observation and holds the possibility that continued research and development may make these methods more impactful going forward.

Second, the impact of these campaigns may not depend on their actual ability to shape concrete behaviors like voting. Even the suggestion or intentional revelation of interference may cast doubt on the legitimacy of the electoral process and democratic institutions. The numerous investigations and hearings following the 2016 election season attest to the ability of these efforts to create mistrust, drive polarization, and distract from governance.

Third, even in the absence of active adversarial efforts, the potential emergence of a “post-fact society” presents questions about the ability of policymakers and society at large to make accurate determinations about national security and the use of military force. Insofar as the “home front” and public opinion are



critical aspects of military operations in a democratic society, a reduction in the value of truthful information is a national security matter.<sup>28</sup> At the very least, such considerations make an accurate and nuanced assessment of risks a high priority.

### **The More Things Change, the More They Stay the Same**

From the perspective of the defense community, these online disinformation activities both are a reaffirmation of the past and serve as a novel provocation. In one sense, this present generation of influence campaigns is a natural extension of the history of IO and information warfare. The Joint Staff defines IO broadly as “Actions taken to affect adversary information and information systems while defending one’s own information and information systems.”<sup>29</sup> These disinformation campaigns are rightly categorized as merely the latest in the evolution of psychological operations, often categorized as a subset of IO. Like other psychological operations, the primary objective of these activities is to:

convey selected information and indicators to foreign audiences to influence the emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.<sup>30</sup>

To that end, our existing conceptions of IO are capacious enough to describe and contextualize the new tactics enabled by the web and technology more broadly. We should not treat campaigns like the one executed during the 2016 U.S. Presidential election as unprecedented. Indeed, to do so would ignore the long history of leafleting, radio broadcasts, and other

IO efforts taken in earlier generations of conflict.<sup>31</sup> While the tactics and strategy of these efforts may change as the dynamics of information flow through social change, we can and should see these efforts in the context of earlier techniques used to achieve the same end.

These disinformation activities are novel since they expand the existing frame of discussion around cybersecurity. Literature around cyberwarfare and “cyber” strategy has tended to focus on the threats arising from the compromising of systems. One common definition put forth by Richard Clarke defines cyberwar as “actions . . . to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”<sup>32</sup> Technical vulnerability and the extent to which malicious actors can access and control computers have been the “prevailing focus” of the “global cyber security community.”<sup>33</sup>

The use of these networks for the purposes of conducting influence campaigns has been less frequently seen in the spotlight. “Social engineering” has often been the center of gravity of the security discussion around topics of influence and persuasion, but this term fails to capture the online disinformation campaigns being described here.<sup>34</sup> The threats often described in the social engineering context are ones in which technical compromise remains the ultimate objective, and where the deception often takes place on an individual level.<sup>35</sup> In contrast, the information warfare efforts typified by the 2016 Russian campaign may aim to influence social behavior as an end in and of itself. These efforts target large groups—if not societies—rather than individuals.

In that respect, the present generation of online information warfare falls somewhere between topics

in the defense space. On the one hand, online disinformation efforts continue a long lineage of thinking and tactical innovation around the use of persuasion and influence in conflict. On the other hand, these topics are a salient, novel form of threat online that introduces a new set of themes into the discussion of cybersecurity and cyberwarfare strategy. To develop an effective, strategic concept that captures the nature of modern information warfare and how it is best conducted, one needs to marry the former with the latter. It is key that existing understandings around strategic influence be informed by the unique dynamics that information technology introduces into the space.

To inform this analysis, we look to a set of strategic sources that have attempted in some respects to do precisely this: consider how techniques of influence and persuasion are relevant and different in the present technological context.

## **PART II: PARALLEL CONCEPTS OF INFORMATION WARFARE**

Strategic thinking about the nature of information warfare is not new, and neither is thinking about the ways in which the Internet and technology more generally shape conflict. As one seeks to articulate a common, strategic concept that will guide military activity in the current information environment, it is important to draw on these sources—both contemporaneous and historical—for guidance.

This section reviews the existing, precedential thinking around information warfare, with emphasis on work that has considered the ways in which the Internet has shaped the landscape in which these activities take place. It examines work within the U.S.

defense context as well as parallel thinking among Russian and Chinese thinkers. Of course, persuasion and the targeted use of influence are not simply a state affair, as this section also looks at strategic frames adopted by nonstate actors, such as WikiLeaks and ISIS. This section will then assess these parallel concepts, arguing that they are limited in characterizing the present-day nature of informational conflict online.

We exclude here a discussion of strategic thinking emerging from the advertising and marketing space, though numerous historical roots connecting this field to the work of information warfare exist.<sup>36</sup> While these sources do provide valuable insight into the nature of persuasion in the present technological environment, they are less helpful in the context of thinking about broader defense or military strategy. For one, strategic concepts are specific to the context of an organization. Commercial actors operate in a significantly different landscape of opportunities and restraints than information warfare actors. Legal restrictions, for instance, may act as a significant limitation to the kinds of techniques in which most commercial actors are willing to engage. Actors in the advertising space may generally refrain from hacking as a means of achieving their ends, but those in the information warfare space are not so limited.<sup>37</sup>

Second, the objectives of marketing actors and information warfare actors may give rise to very different kinds of campaigns. One objective of an information warfare campaign may be simply to produce conflict and confusion between groups within a society.<sup>38</sup> While the use of invented controversy may be a means of attempting to build attention around a product or a service in the marketing space, the ultimate

target is less likely to be simply greater polarization for its own sake.<sup>39</sup>

Finally, marketing and commercial actors may also be attempting to shape very different kinds of motivations. Whereas marketing may attempt to influence purchase behavior, information warfare may attempt to motivate targets to make significantly costlier choices, such as joining an insurgent group, leaking information, or harassing others online. Behavioral science suggests that these decisions—both of a greater personal magnitude and often existing beyond a strictly “commercial” context—may take place in a different behavioral calculus than a simple purchase does.<sup>40</sup> This means that the optimal tactics, time frame, and overall strategic outlook may differ significantly between domains.

To that end, while elements of the world of advertising overlap somewhat with the kinds of activities and techniques used in the information warfare context, these broader differences make it more valuable to focus on precedents which correspond more with the defense context.

### **“Netwar” and U.S. Defense Theory**

Within the context of U.S. national security thinking, the work of John Arquilla and David Ronfeldt is perhaps the closest natural precedent for thinking about the intersection between information technology and information warfare. During the mid-1990s, these theorists put forth a framework that drew distinctions between the pure compromises of systems technically and their use as a means of persuasion and influence.

In their words, the information revolution enabled cyberwar—“conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying . . . information and communications systems.”<sup>41</sup> On the other hand, these technologies also opened the possibility of what the authors called “netwar”—“information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population ‘knows’ or thinks it knows about itself and the world around it.”<sup>42</sup> Richard Szafranski, one contributor to a 1997 collection of essays on netwar entitled, *In Athena’s Camp*, characterizes this conflict as a kind of “epistemological” warfare, targeting “everything a human organism—an individual or a group—holds to be true or real, no matter whether that which is held as true or real was acquired as knowledge or as a belief.”<sup>43</sup>

The predictions of Arquilla and Ronfeldt have proven to be particularly prescient in characterizing the information warfare of recent years. They capture the challenges of attribution in the online environment, writing:

it is difficult to ascertain who, if anyone in particular, lies behind a netwar. This may be particularly the case where a network configured for netwar is transnational and able to maneuver adroitly and quietly across increasingly permeable nation-state borders.<sup>44</sup>

Arquilla and Ronfeldt also successfully predict the often ambiguous nature of online information warfare, writing, “it may not be clear when a netwar has started, or how and when it ends. A netwar actor may engage in long cycles of quietly watching and waiting, and then swell and swarm rapidly into action.”<sup>45</sup>

Beyond merely characterizing the nature of conflict in modern information warfare, Arquilla's and Ronfeldt's key strategic contribution is a set of arguments around how actors most effectively wage and defend against netwar. The two authors argue that organizational structure is critical, focusing on "web[s] (or network[s]) of dispersed, interconnected 'nodes' (or activity centers)" with "no single central leader or commander."<sup>46</sup> These "network forms of organization" are seen to gain major advantages in the conduct of netwar as they are able to systematically outmaneuver hierarchical organizations.<sup>47</sup> To that end, the strategic crux of modern persuasive or influence warfare is a race to master an organizational form that enables the most agile leveraging of the affordances of the technology.<sup>48</sup>

This prediction has played out in part. Loosely organized networks of commercial and ideological actors indeed took an active role in attempting to spread disinformation during the 2016 U.S. election and in a number of other recent cases.<sup>49</sup> At the same time, hierarchical state actors have not been forced to overhaul their organizational structures to take advantage of the opportunities created by the Internet for waging netwar. Instead, states have become parts of networks to achieve their aims without necessarily having to become networks themselves. Russia's role in commissioning and orchestrating components of the 2016 campaign suggests the central role that a government can continue to play in the planning and execution of these efforts.

Interestingly, this parallels the development of strategic thinking in Russia and China on the topic of information warfare. While theorists in those countries are in agreement with Arquilla and Ronfeldt on

the tactical opportunities made possible by the Internet as a tool, they do not appear to have been so quick in adopting similar prescriptions around an organizational form.

### **State Actors: Russia**

Arquilla and Ronfeldt were not the only ones attempting to clarify and develop a framework for thinking about military strategy in the modern information environment. Theorists in the Russian and Chinese national security community have also considered these issues, often coming to parallel conclusions with their counterparts in the United States.

Most discussed in the Russian context is the so-called “Gerasimov Doctrine,” which originates from a 2013 article entitled, “The Value of Science is in the Foresight” by Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces.<sup>50</sup> The piece tackles “a tendency toward blurring the lines between the states of war and peace” in the conflicts of the 21st century.<sup>51</sup> Tactically, the article focuses on the fact that the “role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.”<sup>52</sup>

Within Gerasimov’s framework, propaganda and information warfare appear as only one of a number of “asymmetric actions” which enable the “nullification of an enemy’s advantages in armed conflict.”<sup>53</sup> Warfare in the information space runs alongside robotic systems, “initiations of military operations by groupings of line-units (forces) in peacetime,” and the “mass use of high-precision weaponry.”<sup>54</sup> Gerasimov highlights the importance of these agile tools in creating “a



permanently operating front through the entire territory of the enemy state.”<sup>55</sup>

Particularly in light of Russian meddling in the 2016 U.S. Presidential election, Gerasimov’s article has seen coverage in the mainstream press.<sup>56</sup> However, the degree to which a “Gerasimov Doctrine,” and the “hybrid warfare” it describes actually guide Russian military strategy remains an open question of debate.<sup>57</sup> One domain expert has written, “there is a general consensus in Russian military circles that hybrid war is a completely Western concept. . . . The Russian military has been adamant that they do not practice a hybrid-war strategy.”<sup>58</sup> Another observer has noted that a more recent 2016 article by Gerasimov “entirely contradicts the widely held interpretation of his February 2013 article and implies his earlier article was being misread and misinterpreted outside Russia.”<sup>59</sup> “The Value of Science” is also less a complete strategic concept and more a call to action. Gerasimov writes that “[Russia has] only a superficial understanding of asymmetrical forms and means. . . . the importance of military science, which must create a comprehensive theory of such actions, is growing.”<sup>60</sup>

Even in spite of this ambiguity, it is still valuable to examine “The Value of Science” as a point of reference for thinking about how military officials beyond the United States have contextualized information warfare and its importance in modern conflict. On the one hand, “The Value of Science” is consonant in part with much of the thinking of Arquilla and Ronfeldt. Both highlight the ambiguous space between war and peace that information warfare occupies.<sup>61</sup> Both note the permeable nature of national borders and the ability to project a contested “front” through many parts of a target society.<sup>62</sup> Both argue that nonmilitary means

have expanded in importance and that “information operations (indirect actions) have reached a point in development where they can take on strategic tasks.”<sup>63</sup>

Gerasimov and netwar theory diverge in one important respect. Hybrid warfare still frames state actors as the primary protagonists in the strategic landscape of information warfare. Indeed, “The Value of Science” opens with a consideration of the “color revolutions” of the Middle East and North Africa during the 2010s.<sup>64</sup> Events like the Arab Spring are understood to be a manifestation of a new hybrid warfare of regime change driven primarily by Western governments.<sup>65</sup>

In that respect, Gerasimov characterizes new technologies as primarily opening up new opportunities and tools that are leveraged by state actors. Netwar takes a different tack, arguing that the technologies themselves enable new types of actors that will be systematically more nimble and effective than “hierarchical” government counterparts.<sup>66</sup> These actors include a range of diffuse, decentralized organizations, from transnational criminal networks to loosely joined terrorist cells.<sup>67</sup> In Arquilla’s and Ronfeldt’s writings, these new networks become the primary antagonist in modern information warfare and require fundamental organizational changes to enable traditional institutions to compete with them.<sup>68</sup>

As discussed earlier, these dynamics have not played out in an absolute sense: network actors have indeed come to be prominent protagonists in driving online information warfare, but state actors have continued to play a significant role without being forced to fully become networks themselves. This contrast between U.S. and Russian strategic sources characterizes a similar contrast across U.S. and Chinese literature as well.

## State Actors: China

Paralleling U.S. netwar and Russian hybrid warfare is the Chinese strategic framework around the “Three Warfares,” which trifurcates the broad, sprawling category of information warfare into psychological warfare, media warfare, and legal warfare.<sup>69</sup> The first category, encompassing efforts which “undermine an enemy’s ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations,” falls into the “classic” definitions which focus on the use of psychological operations in support of military operations.<sup>70</sup>

The other two warfares are arguably more unique. One, “media warfare,” is aimed at “influencing domestic and international public opinion to build support for China’s military actions and dissuade an adversary from pursuing actions contrary to China’s interests.”<sup>71</sup> The second, “legal warfare,” “uses international and domestic law to claim the legal high ground or assert Chinese interests.”<sup>72</sup>

In 2003, the People’s Liberation Army’s (PLA’s) highest military policymaking body—the Central Military Commission (CMC)—endorsed this framework. One 2011 report by the U.S. Secretary of Defense to Congress concluded that this endorsement “[reflects] China’s recognition that as a global actor, it will benefit from learning to effectively utilize the tools of public opinion, messaging, and influence.”<sup>73</sup> One 2014 PLA analysis called this framework a “major innovation” in the political work of the Chinese military. The PLA has integrated training on these topics into its organization.<sup>74</sup>

The Three Warfares should be viewed in light of *The Science of Military Strategy*, the “apex of the PLA’s professional military literature on the study of war.”<sup>75</sup> The 2013 edition of this text highlights the concept of huayuquan—essentially, “the capability to control the narrative in a given scenario . . . [or] discursive power.”<sup>76</sup> Contesting and controlling huayuquan become the essential objective of information warfare, requiring the effective integration of the Three Warfares.<sup>77</sup> This corresponds to *The Science of Military Strategy’s* views on the changing nature of warfare, which emphasizes that future conflict will incorporate conflicts of “political, economic, social, and legal” systems, and will be increasingly “Unmanned, invisible, and inaudible.”<sup>78</sup>

As with hybrid warfare, dispute exists around the extent to which these strategic approaches have shaped specific activities on the ground. Some U.S. analyses link the Three Warfares to a range of actions taken by the PLA in the past decade.<sup>79</sup> For their part, Chinese researchers—like their Russian counterparts—have criticized Western analyses of China’s persuasive efforts, arguing that a “[tendency] to confuse the personal views of Chinese government officials with comprehensive national strategy and policies” has led to “an obfuscated understanding of China’s strategic motivation[s].”<sup>80</sup> *Unrestricted Warfare*, a 1999 monograph by Qiao Liang and Wang Xiangsui—at the time, two senior colonels in the PLA—is often cited in this context.<sup>81</sup>

Nevertheless, these texts serve as a useful jumping-off point for thinking about the many approaches to managing information warfare in the contemporary online ecosystem. On that count, what is openly available about Chinese thinking indicates a synthesis of

sorts, combining themes from writings on both netwar and hybrid warfare.

Chinese military thinking sees “information warfare” from the same vantage point that Arquilla and Ronfeldt adopt. The objective of information warfare may not be simply to complement or substitute military operations, but to aim to control the “epistemological” dimension of a society. This is in contrast to the framing given by Gerasimov in “The Value of Science,” which sees information warfare as only one of a set of asymmetric tactics used to nullify military advantages. At the same time, these strategic frameworks still exist within the existing, top-down, command-and-control architecture of the PLA; in that respect, Chinese military thinking borrows from a Gerasimov-style approach which eschews the broader organizational changes advocated for in the netwar literature.

### **Nonstate Actors: WikiLeaks and ISIS**

The Internet and the democratization of computing power have expanded the field of actors which are able to engage effectively in information warfare. Indeed, some of the most nimble practitioners of modern information warfare are arguably not well-resourced states but nonstate actors. To that end, a review of the strategic approaches in the space must include some of the thinking emerging from these groups. Two case studies provide a useful sampling of strategic concepts emerging beyond the formal military context: WikiLeaks and ISIS.

## *WikiLeaks*

Launched in 2006, WikiLeaks is, by its own description, an international “media organization” which is focused on acquiring and releasing large caches of data and information that has been classified or censored and that deals with the subjects of war, intelligence operations, and “corruption.”<sup>82</sup> An outlet for leaked materials, the site played a notable role in the 2010 “Cablegate” by releasing hundreds of thousands of classified cables sent by the U.S. State Department.<sup>83</sup> In 2016, the site published a set of leaked emails from the U.S. Democratic National Committee which the intelligence community claims was supplied to the organization by Russian hackers.<sup>84</sup> The organization also played a role in helping to promote conspiracy theories about candidate Clinton during the campaign.<sup>85</sup>

While not articulating a cohesive strategic concept in the military sense, founder Julian Assange’s writings and public comments do suggest a particular model for thinking about modern information warfare. One 2006 essay, *Conspiracy as Governance*, suggests thinking of authoritarian regimes as connected graphs: networks of more or less important players with more or less important ties with one another.<sup>86</sup> For Assange, these individual units form a single, cohesive organism described as “a system of interacting organs, a beast with arteries and veins . . . [but] unable to comprehend and control the forces in its environment.”<sup>87</sup>

Technology plays a major role in the strategic narrative of WikiLeaks and Assange. Since the strength of such a “conspiratorial” network is based on the number and strength of the links between its members, the Internet plays a role in “increasing the speed

of accuracy of the [sic] their interactions” and expanding the “maximum size a conspiracy may achieve before it breaks down.”<sup>88</sup>

Given such a framing, effective information warfare relies on an ability to take actions that erode the viability of the links between participants in the conspiracy.<sup>89</sup> Assange suggests a strategy which “*deceive[s]* or *blind[s]* a conspiracy by distorting or restricting the information available to it [or] unstructured attacks on links or through *throttling* and *separating* [italics in original].”<sup>90</sup> One powerful technique is the use of leaks, which “induce[s] fear and paranoia in its leadership and planning coterie” and “result[s] in minimization of efficient internal communications mechanisms (an increase in cognitive ‘secrecy tax’).”<sup>91</sup> This inhibition of effective group activity, the essay argues, slows the action of a targeted conspiracy until it is unable to adapt effectively to the environment around it.<sup>92</sup>

Networks also play a significant role in the strategic thinking of WikiLeaks, not just in its offensive approach, but in its internal organizational doctrines as well.

The WikiLeaks approach toward information warfare overlaps in part with the strategic thinking emerging in the national security context. As in netwar, hybrid warfare, and the Three Warfares, WikiLeaks implicitly recognizes the potency of tools beyond traditional munitions to impair and destroy institutions. Paralleling netwar, WikiLeaks also highlights the competition between organizational forms, with smaller, more concentrated hierarchies on one side, and diffuse, nimble networks on the other. As with Arquilla and Ronfeldt, one tension is the extent to which the recent decade bears out the prediction that networks on their own would gain a systematic advantage

against hierarchies. To the extent that WikiLeaks itself collaborated with the Russian Government to achieve mutual ends during the 2016 U.S. election, the practical operation of WikiLeaks may be more complicated than suggested by its doctrinal theory.

There are also two nuances worth noting. Though concepts of netwar and the strategic concepts guiding WikiLeaks share a common agreement that technology empowers networked actors, they disagree as to whether the technology also enforces openness. For Arquilla and Ronfeldt, some of the most prolific and successful practitioners of netwar are secretive terrorist and criminal networks.<sup>93</sup> In contrast, Assange asserts that “in a world where leaking is easy, secretive or unjust systems are nonlinearly hit relative to open, just systems.”<sup>94</sup> Secretive systems are “exquisitely vulnerable” to mass leaking.<sup>95</sup>

Second, the specific details of network structure play an important role in the information warfare of WikiLeaks. Leaks are a primary tool in part because they erode the trust necessary for target networks to communicate and coordinate their actions effectively. For Assange, this depends very much on the topology of relationships between supporters and the actions necessary for modifying that pattern of connections at scale. This is somewhat unique among the precedents reviewed earlier. What is publicly available about hybrid warfare and the Three Warfares does not dwell on the network structure of mass movements, in part because they are written from the perspective of militaries which do not rely on those movements. Arquilla and Ronfeldt do examine matters of specific network structure, although they credit dense networks for their operational agility, rather than their “computational” capacity.<sup>96</sup>



## ISIS

ISIS also serves as a useful source of parallel concepts in evaluating nonstate or proto-state thinking around modern information warfare. As has been noted by numerous commentators elsewhere, the use of IO has been core to the growth of ISIS.<sup>97</sup> The organization maintains an elaborate structure for producing and localizing media, with a formal Ministry of Media accompanying regional media bureaus and grassroots supporters.<sup>98</sup> As one researcher describes it:

the media proficiency of the [Islamic State] exists because of an extensive media infrastructure that allows it to produce high-quality, timely products in different languages to different audiences that fit the narrative that the group wishes to convey.<sup>99</sup>

One official publication from ISIS, entitled, *Media Man, You Are a Mujāhid Too*, serves as a point of entry in thinking about the strategic approach underlying these information warfare efforts.<sup>100</sup> Published in April 2016, *Media Man* is a short, motivational pamphlet written for a broad set of “media operatives”—a term which applies to “frontline cameramen [as much] as it does to self-appointed social media disseminators.”<sup>101</sup> The pamphlet attempts to frame propaganda activity as core to the religious jihad, arguing that, in certain cases, “verbal jihad is more important than jihad of the sword,” and that “media rockets exceed in their ferocity and danger the flames of bombs dropped from airplanes.”<sup>102</sup>

Importantly, *Media Man* articulates an approach to the conduct of information warfare. Researcher Charlie Winter frames this as a tripartite set of strategies: framing ISIS as a positive alternative to sympathetic

audiences, engaging in counter-speech to refute claims made by the United States and its allies, and creating media “weapons” which reduce the morale and effectiveness of ISIS’s adversaries.<sup>103</sup>

These three pillars are not novel concepts in the history of strategic thought around information warfare. However, *Media Man* does emphasize one element that seems to apply with particular force in the current technological environment of information warfare: that polarization can generate salient benefits as much as persuasive efforts can. The pamphlet notes that well-targeted media weapons are able to “make adversaries act irrationally by ‘infuriating them’ and ensnaring policymakers into ill-conceived knee-jerk politics.”<sup>104</sup>

Researcher Haroro J. Ingram has called this tactic “baiting,” observing that ISIS information warfare frequently is “not about winning over ‘undecided’ viewers, but unambiguously reinforcing the perceptions and polarizing the support of friends and foes alike.”<sup>105</sup> Polarization renders a number of useful benefits to ISIS. It potentially provokes a disproportionate response from adversaries that creates real-world crises of which ISIS can take advantage.<sup>106</sup> Polarization can produce notoriety among sympathetic audiences and create the opportunity to recruit the like-minded.<sup>107</sup> Polarization also serves to puncture the media “halo” suggesting that “America is this unconquerable nation that is undivided, undefeated, and can never be thwarted.”<sup>108</sup>

It is important to note that this strategic approach is based on a set of understandings about the proclivities of the present-day media ecosystem. *The Management of Savagery*—a jihadi text published in 2004 which would become the “blueprint” of the Islamic State—advises readers to “study the West’s media so they

could understand how best to mimic its methods of persuasion."<sup>109</sup> Ingram also reports an interview with one senior producer from a Syrian opposition radio station that stated, "[ISIS] made a media trap and all of the Western media fell in it. They know the fears and images that the Western media is hungry for, so [ISIS] give it and the media spreads it."<sup>110</sup>

This approach to information warfare has also been shared by others. As researcher Whitney Phillips has documented, the long-standing online culture of "trolls" has existed in a symbiotic relationship with the mass media.<sup>111</sup> Trolls generate shocking and polarizing incidents, which traditional and social media spotlights in turn.<sup>112</sup> This attention incentivizes further action by the trolls and acts as a recruiting medium for others attracted by this activity. Others have documented a similar dynamic in the activities and tactics of the alt-right in their manipulation of the media ecosystem.<sup>113</sup>

As in the WikiLeaks case, the information warfare strategy of ISIS both parallels and diverges from the defense thinking emerging from the military domain. *Media Man* and the activities of ISIS in practice evince an understanding of the role that information plays as a significant asymmetric tool. In this sense, the strategic concept of information warfare in the ISIS context parallels the recognition of a changing battlefield articulated in Gerasimov's "The Value of Science" article. Structurally, the elaborate media operation established by ISIS also seems to follow the approach taken in China and Russia which attempts to fit existing command-and-control structures into the evolving conflict environment, rather than adopt the more diffuse, crowd-driven strategy seen in netwar or the WikiLeaks case.

## Assessing Existing Precedents

Strategic thinking on influence and persuasion has not remained static. Many state and nonstate actors have considered the evolving strategy and tactics of waging information warfare against the backdrop of the significant technological change of the past 2 decades. This allows us to assess the current state of military thinking on the topic and where it might require revision or renovation.

On one level, these precedents appear to do a good job of capturing some of the unique aspects of information warfare in the current technological environment. Strategists in the United States, Russia, and China consistently underscore the growing relevance of information warfare as an asymmetric technique. They agree on the extent to which technology and the changing nature of warfare result in an environment where influence and persuasion become significant means, sometimes equivalent means, of achieving military ends. Multiple theorists—from Arquilla and Ronfeldt to Assange and the PLA—have refocused the goals of information warfare; whereas simply supporting troops on a battlefield was once the goal, now, shaping the social landscape has become a potential end in and of itself. Both the writings and information warfare practices of ISIS and WikiLeaks highlight the tactical gambits of polarization and leaking that have proven to be a potent means of manipulating discourse in the current online environment.

Existing work on the strategy of online information warfare is useful in these respects. This literature does characterize core elements of what is potentially destabilizing about the 2016 disinformation effort in the United States and the techniques that are likely

to see further development going forward. However, there is much that remains missing from these strategic concepts—or at least what is publicly available about them.

Existing theory is limited in its thinking about the essential nature of information warfare and how it is changed by technology. What precisely is being targeted in an informational conflict? How is information warfare won or lost? “Influenc[ing] the emotions, motives, [and] objective reasoning” of a target population may be the objective, but the literature is vague about how this happens, and how technology may create a new environment for accomplishing this task.

The literature is also mostly silent as to the optimal conduct of information warfare. How should operations be launched, and what do they look like? What are the tools of modern information warfare, and how are they integrated into operations? Many theorists seem to assume implicitly that information warfare can be comfortably waged within the existing military hierarchy, though the success of nonstate actors suggests that alternative models may be equally or more successful. The strategic thinking of netwar and WikiLeaks advocate for these different organizational forms, although they perhaps underestimate the continuing effectiveness of state actors in the space. An approach is needed which joins these two views.

These precedential works also overwhelmingly focus on the projection of force, rather than examining the question of defensive approach. Frequently, theorists adopt the frame of how the Internet and related technologies open new opportunities to attack and undermine targets. What is left unsaid is how a military should tackle the question of defending society against online campaigns of propaganda and manipulation.

The existing literature on the military strategy of information warfare and how technology shapes it may, therefore, articulate aspects of strategy without fully cohering into a broader strategic concept per se. Three missing components are needed: a more thorough account of the nature of the conflict, an examination of how information warfare is best conducted, and an extension of the thinking to the questions of defense. Can a more complete strategic concept for the current technological environment be articulated?

### **PART III: TOWARD A NEW STRATEGIC CONCEPT**

This section offers one potential sketch of what a strategic concept for influence and persuasion might look like in the present information environment. In particular, it focuses on the impact that increased visibility of social behavior produces in the nature and conduct of, and defensive approaches to, information warfare.

One important caveat is warranted. In “Why cyber war will not and should not have its grand strategist,” Martin Libicki puts forth a provocative thesis that casts doubt on the idea that “a classic strategic treatment of cyber war is possible, or, even if it were, it would be particularly beneficial.”<sup>114</sup> One key argument he advances is that cyberspace is “ill-suited for grand strategic theories,” in part because it is rapidly changing in many important respects.<sup>115</sup> As an illustration, he points out how the core nature of the threat in the cyber domain has shifted over time, from individual, “rough-and-ready” hackers with manually deployed exploits to teams that build large-scale, remotely controlled malware tools.<sup>116</sup>

Libicki's critique highlights a relevant point for this topic as well. Regardless of whether an enduring grand strategy is possible, the rapid change of the underlying technology implies that strategic concepts may go quickly out of date. This applies in the classic cyberwarfare context as well as in the context of online information and disinformation efforts. In the mid-1990s, Arquilla's and Ronfeldt's netwar theories described an Internet that predated the mass adoption of smartphones and which had only begun to see the impact of the search engine. Writing in 2006, Julian Assange described an Internet prior to the mass adoption of social networks like Facebook and Twitter. These products and services change the nature of information flow through the web, and so change the conduct of strategic persuasion and influence.

On this count, it is worth setting aside the effort to articulate a "grand," permanent strategy in the space and, instead, ask the more pragmatic question of what strategic concept should guide information warfare for the Internet as it exists in the late 2010s. Doing so requires a characterization of how technology shapes the broader persuasive landscape beyond the narrow military and national security context.

### **Strategic Situation: The Cartographic Shift in Information Warfare**

Articulating a strategic concept requires an "estimate of the strategic situation."<sup>117</sup> One place to begin may simply be to ask why existing literature and doctrinal thinking have been vague on questions of the nature of information warfare, its conduct, and the proper approaches toward defense.

One potential explanation is that the environment of strategic persuasion has traditionally existed in a dense fog of war. The moods and opinions of a target population could only be sampled through intermittent, expensive polling, and the topology of links connecting individuals within a society could only be speculated about or discussed in a general way.<sup>118</sup> Actors engaging in information warfare were limited in how they might target their campaigns, the scope of the tactics they could undertake, and their ability to evaluate the effectiveness of a given technique. Such an environment inhibits the articulation of crisp strategies and concrete doctrines.

The evolution of the Internet has shifted this landscape in a dramatic way. The social interactions of many publics around the world now take place through a digital medium. This medium is capturing an extraordinarily detailed and nuanced record of individual and group behaviors.

This has been facilitated by a few developments that have shaped the web in the past 2 decades. Social media's rise and wide acceptance make it the primary source of the Internet-enabled mass collection of social data.<sup>119</sup> The adoption of mobile devices has enabled this collection to persist throughout the course of an entire day, allowing an ever-richer temporal understanding of group social behavior.<sup>120</sup> The establishment of advertising as the core business model of the web created incentives to store and organize Internet users' behavioral data and make it available to third parties.<sup>121</sup>

The result is that social behavior is now directly observable at many different levels at remarkably low cost. It is possible to peer into small communities of niche interest and zoom out to examine the entire



landscape of social activity. This record also grants a time series perspective that was previously costly to acquire. One can observe social reactions to a stimulus as they occur and compare these reactions across both time and space. These developments and the concentration of data in a small set of platforms change the nature of information flow and so open new possibilities for the strategic development of information warfare.

Even in light of these shifts, it is important to keep in mind that the Internet is just a medium through which social activity takes place. While it has come to dominate some aspects of social life, the map is still not the territory. The Internet only captures a part of the behaviors, large and small, within a society. What is publicly available may also represent only one particular lens on social activity within a public. The types of interactions posted to open, public platforms like Twitter and Facebook will contrast with the data flowing through trusted, private communication networks on services like Signal and Whatsapp.

The social data of the Internet is not representative in that sense—and may be particularly unrepresentative in regions with low Internet penetration or where access to the network is only permitted to particular segments of a society. The analysis below may apply with less force in these contexts.

However, as with the introduction of radar during World War II, the increased ability to see—even in a limited set of contexts—can produce concrete changes in the strategic approaches which succeed in the battlefield.<sup>122</sup> This “cartographic shift” in our ability to visualize and understand social behavior has produced significant and parallel changes in the fields of economics, advertising, and sociology, and will also shape the conduct of information warfare.

## The Nature of Modern Information Warfare

This cartographic shift changes the nature of information warfare. It does so on two fronts, shaping not only the focus of what is targeted in information warfare but also the aims of conflict in the space as well.

### *From Targeting Beliefs to Targeting Networks*

Earlier campaigns of influence attempted to shape particular beliefs or opinions held by a population writ large and conflicts between actors centered on contesting whether a given idea would predominate within a target audience. The Internet makes practicable operations which are aimed at influencing a new dimension—not on contesting particular ideas per se, but on the granular manipulation of underlying relationships and networks of trust among individuals. Whereas earlier campaigns may have aimed to influence the beliefs that an individual had about the strength or effectiveness of his or her government, the contemporary technological environment enables campaigns to aim to alter whom that individual communicates and socializes with and those whom the person considers credible.

Granted, targeting the connections between groups within a society has long been a stated objective of information warfare campaigns. However, limited by the capacity to see and understand social behavior at scale, these tactics and strategic thinking have typically been forced to rely on crude pictures of society and the relationships between institutions. Campaigns, for instance, might work to attack the trust between a government and its people or erode the sympathy of a population for the military.<sup>123</sup>

However, “government,” “people,” and “military” are simplifications of a more complex reality. Masses of individuals and the connections among them make up these groups and the hierarchies within them. Rather than talking about media outlets, we might talk about the editors of these companies and the circles of connections they rely on for story leads. Rather than talking about readers as an undifferentiated mass, we might talk about the specific clusters of individuals that regularly consume content from a particular outlet and the relationships between them. This is a kind of “social wiring,” formed by the complex web of formal relationships, friendships, acquaintanceships, and other connections which exist between people and which enable institutions and social groups to function on a day-to-day basis.

The Internet as a medium exposes this detailed social wiring within large institutions and reveals smaller groups that may have been practically impossible to identify in the past. The ability to map these connections and activities allows the targeting of those relationships in a manner and scale that was previously impossible or prohibitively expensive. Modern information warfare can think less about rough categories of demographic segments, groups, and institutions, and more about individuals, specific networks of relationships, and the flow of information between clusters of people.

To illustrate, consider an IO aimed at encouraging a mass movement to mobilize and take action against a target government. In an earlier era, those conducting such a persuasive campaign would have been limited by the scope of what was practically knowable. While some prominent dissidents might be publicly known to the mainstream press, it might be challenging to

identify quickly influential but more low-key figures in a movement. Importantly, it would be difficult to rapidly and cheaply ascertain which members of the public are sympathetic to anti-government sentiment. Strategy in such an environment would require the planner of this hypothetical IO to simply attempt to rally “dissident elements” broadly writ or identify known groups such as student activist organizations as a way of targeting messaging.

The Internet creates an environment where these key facts about individuals are more easily acquired. The public organizing activity of activists on social media platforms provides a means by which to compile rosters quickly of the relevant actors in an anti-government movement. It becomes possible to assess which citizens are sympathetic to this movement by monitoring the public response to dissident messaging online and measuring the degree to which specific activists are able to rally the public toward certain actions. One might also be able to map the connections between specific dissident leaders and the audiences that they are most able to engage with and motivate to action. This detailed data reduces dependence on the targeting of broadly defined segments of the population and enables a focus on individual dissidents and their connections to others.

This visibility translates into an increased capacity to manipulate. The Internet not only provides the means by which to see and understand social behavior in a way that was previously extremely expensive, but it also allows for targeting and intervention. It is now possible to identify a community of interest, listen in on a conversation, and then take an action which intervenes in that community from a global distance. This might look like an effort to grow bonds of trust and

norms between key clusters of individuals or, simply, to encourage a pattern of relationships between individuals in a society.

To return to our example, a mapping of the social media environment might identify clusters of influential individuals who are sympathetic to anti-government sentiment but not yet mobilized to action. One campaign might focus on cultivating social ties between these promising clusters and active dissidents who have proven successful in mobilizing similar individuals in the past. This effort might, therefore, aim to grow the number of participants in a mass movement and spark action among a broader cluster of citizens.

The capacity to target these social ties is important because experimental evidence suggests that the structure of social connections exerts a deep, causal influence on beliefs and behavior.<sup>124</sup> Network structure shapes our political affiliations, health habits, and even the likelihood of divorce.<sup>125</sup> Manipulating this network of relationships can, therefore, influence the entire structure of beliefs and behaviors within a society or a target group.

Consider our hypothetical campaign once more. Mapping the web of social connections might reveal that our dissident groups—and those sympathetic to them—are largely in their own social universe. These individuals might only socialize with one another and lack substantial connections to the rest of the population. However, this analysis might show that these dissident elements share a range of common interests with the broader society. These might be entirely non-political: a favorite sports team, a common set of recreational activities, or institutional affiliations with a school or workplace. Such an analysis might reveal

promising areas where the intentional launching of social activities targeted at bridging certain clusters of individuals might serve to bring these dissident elements more in contact with the broader population. Where an unmobilized individual begins to have multiple connections to individuals in the dissident group, peer influence may play a significant role in increasing the individual's anti-government sympathies.

In this respect, the cartographic shift in information warfare may work to augment the effectiveness of existing approaches that focus on contesting a specific belief or opinion. Rather than simply attempting to win the argument by spreading certain messages, influence campaigns can also attempt to manipulate peer behaviors to accelerate the adoption or rejection of certain ideas en masse.

But this is not all. The capacity to manipulate social ties also expands the potential targets of information warfare. For one, this capacity suggests an expanded ability to attack and degrade social cohesion writ large. The shift from altering a targeted belief to shaping underlying networks is important because these relationships are the source of social capital within a society.<sup>126</sup> Social capital is the "connections among individuals—social networks and the norms of reciprocity and trustworthiness that arise from them."<sup>127</sup> As Francis Fukuyama observes, social capital is critical as it lowers transactional costs in the economic sphere and "promot[es] the associational life which is necessary for the success of limited government and modern democracy."<sup>128</sup> From individuals and groups to institutions and governments, a society—particularly liberal democracies—must be able to create and conserve pools of social capital to function.

Second, the capacity to target social ties accurately also allows the manipulation of what we might call the “metabolism” of knowledge—the creation, spread, and updating of accepted facts through a society. Social ties define what sources are trusted, what processes of checking information are considered legitimate, and the groups and institutions that define the social criteria under which information is discarded.<sup>129</sup> Information shared by one’s established friends may be considered more credible or trustworthy than information shared by a stranger. These peers may also play a role in establishing norms around what sources are acceptable and which are to be rejected out of hand. Having multiple trusted associates react incredulously to information published by a given news outlet might erode the willingness of an individual to believe or distribute information from that source going forward. Manipulating these micro-level dynamics at scale across a society opens the possibility of influencing the overall practice of knowledge generation and dissemination.

### *The Aims of Information Warfare*

The terms of what is contestable define the terms of victory and defeat. In a world of limited or high-cost visibility into social behavior, information warfare focuses on contests over the specific beliefs and points of view held by a population. Victory entails the adoption of a belief desired by a contestant and defeat entails the inability to deny the adoption of an adversary belief by a population.

However, these terms of victory may become hollow as the strategic environment itself changes. An actor with aims that center on shaping a specific

belief may be at the mercy of an actor who focuses on obtaining the capacity to shape the underlying social ties of a society. Even if the former succeeds in spreading a belief, the adoption of that belief may be fragile or temporary if the social structure of a population is rendered unsupportive or if the sources of this belief are considered categorically false by the population at large. Consider an effort launched by a government to persuade the public that its military is succeeding in a war. This effort might be supported by state-run mass media channels which give the government the capacity to blanket the public with messaging. However, this persuasive campaign may nonetheless fail if an adversary can erode public trust in the mass media generally and build social ties between alternative online media outlets and groups of influential citizens within a society.

Similarly, a singular focus on changing a target set of beliefs may be blind to the damage of campaigns which attempt to erode social cohesion broadly through the manipulation of underlying social ties. These campaigns may not attempt to promote a particular belief but, instead, introduce multiple, even conflicting, ideas to fragment relationships between groups in a society. In our example, a government overly focused on bolstering the credibility of its military and fending off criticisms that it is not effective may not be alert to the damage produced by a persuasive campaign that simply seeks to maximize controversy around the issue and drive the polarization of supporters and detractors. Such an adversary may at times actually work to promote certain individuals and groups aligned with the government position, insofar as it helps to prolong an internal conflict.



To this end, the cartographic shift in information warfare also shapes the terms of success or failure in the space. What is contested is not superiority in the ability to control specific beliefs or options, but the capacity to control the topology of relationships within a society. Spreading a belief may become an instrument in achieving this aim, but doing so may no longer in and of itself be the primary end of information warfare. Victory entails the capture of this structural influence, while defeat entails the inability to deny this influence to adversaries.

### **The Conduct of Modern Information Warfare: From Attrition to Maneuver**

The cartographic shift also helps us to articulate more concretely shifts in the effective conduct of information warfare. Borrowing from a distinction made by the U.S. Marine Corps (USMC) in its core strategic doctrine, persuasive warfare has been traditionally a **war of attrition**.<sup>130</sup> “Warfare by attrition pursues victory through the cumulative destruction of the enemy’s material assets by superior firepower.”<sup>131</sup> From leafletting to radio broadcasts, information warfare by attrition has characterized many of the “classic” tactics deployed by state and nonstate actors. These tactics attempt to blanket an entire social ecosystem, hoping to change opinions or otherwise reduce morale. This is a natural application of strategic persuasion in a world of limited knowledge about the architecture of connections and beliefs that make up a target group or society.

Information warfare waged as “warfare by maneuver” has been traditionally less common. This is a kind of information warfare where, “Rather than

pursuing the cumulative destruction of every component in the enemy arsenal, the goal is to attack the enemy 'system'—to incapacitate the enemy *systemically* [italics in original]."<sup>132</sup> This operational mode emphasizes the identification and targeting of vulnerabilities that render an adversary unable to "function as part of a cohesive whole."<sup>133</sup> Where this has taken place through more focused tactics, such as the subversion of adversary groups or the targeting of particular communities, the scope of operations has been relatively narrow and expensive.<sup>134</sup> These efforts, which have been difficult to use effectively, have only infrequently attempted to manipulate the flow of information through an entire society broadly writ. However, the rich and up-to-date data around social behavior significantly augments opportunities for conducting information warfare by maneuver and suggests that the coming decades will see more offensives that leverage these opportunities.<sup>135</sup>

Framing the evolution of information warfare as a transition from attrition combat to maneuver combat also helps to reconcile the apparent failure of netwar and WikiLeaks to predict the continued strength and even dominance of centralized actors like governments in this space. Arquilla, Ronfeldt, and Assange championed the ability of diffuse, "leaderless" networks of actors to systematically outcompete hierarchical organizational structures. In retrospect, it may not have been strategic advantages inherent to a particular organizational form, but, instead, that these types of diffuse organizations—criminal networks, terrorist organizations, international transparency movements—were simply the first to adopt techniques which nimbly leveraged the targeting and iteration made possible by the web. As it turns out, a diverse

variety of actors can take advantage of warfare by maneuver, as Russia's activities in the space demonstrate. The correct strategic characterization, in the end, may not have been combat between different organizational forms—hierarchies vs. networks—but combat between different styles of information warfare—attrition vs. maneuver.

So, what does information warfare by maneuver look like in practice? The successful conduct of these more targeted campaigns requires operations that combine three attributes: effective obfuscation, effective iteration, and effective automation.

### *Effective Obfuscation*

Information warfare by maneuver is most effective when it maintains a low profile and is challenging to detect. This enables operations to proceed and influence the social landscape long before they are noticed and reacted to by an adversary. This is possible because of three factors, two of which parallel aspects of operations in the broader domain of cybersecurity. First, definitively attributing a given threat online to a particular person or entity in the real world can be difficult.<sup>136</sup> Second, the potential attack surface for these operations—all sites of social activity online—is expansive and not easily tracked in a comprehensive way by those likely to be the targets of these campaigns. Beyond more public social media platforms like Facebook and Twitter, influence campaigns might also take place through less-visible private channels like Whatsapp and Signal, where it is less straightforward to obtain data.

The cartographic shift in information warfare is a third important factor. Rather than blanketing an

entire target population with a message, operations focus on identifying and influencing smaller key constituencies. Moreover, a focus on shaping networks and relationships rather than promoting a given idea enables persuasive efforts that might appear to have no direct relationship to promoting a consistent ideology or point of view. Efforts to expand the audience of radical elements within a society, for instance, might focus on bridging hard-core supporters with other groups through an innocuous common interest.<sup>137</sup> This hinders efforts to ascertain the ultimate intent of a given set of persuasive actions observed online, or even to identify it as part of a larger campaign.

It is worth contrasting this environment with earlier information warfare techniques. Operations such as leafletting and radio broadcasts are highly distinct from the types of persuasive efforts which are possible online. For one, the distribution medium—hand-bills dropped from a plane or a broadcast that anyone can tune into—can make it extremely apparent that a persuasive effort is taking place. These efforts are also considerably more attributable than online operations, given the physical requirements for distributing these messages. Planes must take off and refuel from a given location, and a sufficiently powerful radio transmitter is needed for a blanket broadcast. In short, the operational profile of these earlier techniques is “noisier”; adversaries are more likely to be alerted to the presence of these techniques. This makes the possibility of encountering dedicated and effective counter-messaging and countermeasures more likely than in the online context, where detection may take a long time or never occur at all.

Successful obfuscation also buttresses a second operational need for effective information warfare by

maneuver—that of iteration. Since influence can be low profile, operations can be conducted in an agile and iterative fashion, which is needed to assess what persuasive techniques will be most effective in a specific context.

### *Effective Iteration*

Information warfare by maneuver is most effective when it is agile and highly iterative. The visibility that the Internet provides into social activity enables both attackers and defenders to contest each other on a highly granular, targeted level. However, seeing and mastery are not the same: the ecosystem of influence and persuasion remains an extremely noisy one. There is a vast range of intervening factors, and modeling social behavior remains an inexact science at present.<sup>138</sup> The success of one persuasive tactic does not necessarily guarantee the success of the next, and causal relationships between action and result are frequently challenging to assess.

This chaotic environment is exacerbated by a continually shifting set of targets, obscuring which to aim at that would produce the biggest impact on a target society. Clausewitz speaks of a “center of gravity” in military maneuver—“sources of moral or physical strength, power and resistance.”<sup>139</sup> The optimal target of military operations in that classic treatment is the center of gravity.<sup>140</sup> However, in the information warfare context, the center of gravity is frequently in motion in a society—there may be different centers of gravity that exist across different domains and arenas of belief. These centers of gravity may shift across individuals and institutions as influence waxes and wanes, guided by the changing relationships between actors in a society.

What applies on the physical battlefield may also apply in the information space. USMC doctrine could be describing the persuasive conditions of the modern web when it writes:

past battlefields could be described as linear formations and uninterrupted linear fronts, we cannot think of today's battlefield in linear terms. . . . modern weapons have increased dispersion. . . . the natural result of dispersion is unoccupied areas, gaps, and exposed flanks which can and will be exploited, blurring the distinction between front and rear and friendly- and enemy-controlled areas.<sup>141</sup>

For the USMC, the key factor for success in such an environment is agility—"rapid, flexible, opportunistic maneuver."<sup>142</sup> The same may be true in the contemporary online information warfare space, where a highly iterative and improvisational cadence of activity is required to be effective. This is made particularly possible given the relative low cost and low profile of these operations, which enables continuous experimentation and multiple attempts at exerting influence. Speed becomes a particularly key operational necessity, allowing attackers to recognize opportunities and exploit them before a target has the chance to react.<sup>143</sup> This strategic picture is one that matches with reality: what is known of the 2016 Russian effort was that it operated on a highly decentralized, fast-moving, improvisational basis.<sup>144</sup>

### *Effective Automation*

Information warfare by maneuver is most effective when it leverages automation, both as a means of expanding operational capacity and as a target of operations. The sheer scale and complexity of social

activity online—a factor enabling obfuscation and necessitating rapid iteration—presents another challenge to the successful execution of information warfare by maneuver. How is an operation able to identify the correct targets from such a broad field of potential targets? How is it able to engage with all potential targets simultaneously? Automation plays an important, if not necessary, role in being able to project influence in a targeted way across the scale of the persuasive terrain online.

One dimension of this is in the expansion of operational capacity. For one, social data and analytics play a major role in identifying potential targets and assessing the relative success or failure of a persuasive tactic. Automating this assessment augments the maneuver capacity of a persuasive effort: it becomes more possible to understand the “system” of a target population and the dynamics that might cause it to shift to a desired state. Bots—automated accounts purporting to be real users on a platform—also have emerged in some recent online influence campaigns, a means by which to expand the ability for a small team to engage on a direct basis with many users and shape the conversation.<sup>145</sup>

Second, automation itself can also be a target of operations. By and large, online social platforms filter and recommend content and social interactions to users autonomously through algorithms. These algorithms play a major role in shaping the flow of information through a society and the social behavior of the public.<sup>146</sup> The algorithms can also shape the relative influence and financial strength of key groups that contribute to the definition of the flow of information through a society. For instance, journalists, and the press more generally, have had their fortunes

shaped by the algorithmic specifics of platforms like Facebook and Google.<sup>147</sup> By manipulating the algorithms of a service or the incentives of the companies that run them, an attacker or defender can shape the persuasive landscape to his or her advantage.<sup>148</sup> YouTube's recommendation system, which links users to relevant videos based on the video just watched, has seen precisely this kind of manipulation. During the 2016 election, bots and false "sock puppet" accounts were deployed to nudge the system toward recommending a range of conspiracy theories around the Clinton campaign.<sup>149</sup>

This assessment of the operational features of online information warfare begs the question of defense. If effective obfuscation, effective iteration, and effective automation are necessary for conducting successful operations in this space, what is necessary for mounting a successful defense against these kinds of campaigns? The increased visibility of group social behavior made possible by the Internet again provides a way forward.

## **Defense in Modern Information Warfare**

At the time of this writing, current approaches to defending or countering campaigns of online disinformation like the ones seen in the 2016 U.S. election are quite limited in their specificity. Some analyses suggest changes in messaging, concluding that the United States should engage in counter-propaganda to fight these campaigns.<sup>150</sup> These include "coordinated effort[s] to saturate contested IO realms with images and messages of American prosperity and freedom."<sup>151</sup> This could also take the form of a coalition, a:



United Front, as it were, of truth-seeking nations, soberly facing their opponents, willing to accept the airing of one's own imperfection for the sake of improvement, and committed to the norm that there is an objective reality that matters.<sup>152</sup>

Others believe that "the antidote to Netwar poison is active transparency" and call for "a new vision and purpose for the military based on preservation of credibility and trust."<sup>153</sup> There is also occasionally resignation, with one analysis suggesting that the hybrid warfare approaches adopted by Russia allow its information warfare capabilities to "gain degrees of speed and agility that U.S. joint doctrine and policy cannot hope to match."<sup>154</sup>

While these prescriptions may advise particular actions that might be useful in part, the overriding weakness of many existing analyses is the vagueness of their proposals. While it may be helpful to respond to propaganda with "messages of American prosperity and freedom," it is unclear what such messages look like, how they would be deployed, and whether they would be effective against campaigns directed toward manipulating underlying social ties and relationships.<sup>155</sup>

This in part reflects the fog of war that has traditionally characterized information warfare operations and the level of abstraction that its strategic thinking has been historically forced to resolve. Even the suggestion that such messaging should be "saturated" reflects earlier information wars of attrition rather than the wars of maneuver that may now be possible.<sup>156</sup> Countering "firehose of falsehood" strategies might not rely on the development of a reciprocal "firehose of truth" but, instead, require a more targeted approach.<sup>157</sup> The increased visibility of social

data enables us to articulate what such an effective defense strategy would look like with a significantly higher level of specificity.

### *Defense in the Context of Liberal Democracy*

Liberal democracies face distinct vulnerabilities and constraints in developing an effective defense against the current generation of information warfare. As earlier, the nature of modern persuasive warfare is shaped by the ability to observe social interaction and behavior at a highly granular level. Conflicts shift from contests over the adoption or rejection of certain ideas and points of view to contests over the network structure of relationships and strength of ties within a population. Victory in these conditions entails capturing the ability to shape these networks toward desired ends, while defeat entails the inability to deny this influence to an adversary.

Liberal democracies face an additional challenge. The relationships among individuals and groups within a society are important not only because they influence behavior at a deep level but also because they produce social capital, “the norms of reciprocity and trustworthiness that arise from [social networks].”<sup>158</sup> Social capital is key to the effective functioning of liberal democracies.<sup>159</sup> Nevertheless, liberal democracies must also defend more than their social capital. Societies that lack trust in all institutions beyond a single leader or an institution such as the military are not liberal democracies. At best, they are illiberal democracies or democracies in name only.<sup>160</sup>

To that end, liberal democracies must not only defend the aggregate amount of social capital or trust within a society. They must also defend a particular

arrangement of social capital—one which gives independent civil society and public institutions a primary role.<sup>161</sup> Trust in independent journalistic entities, for instance, is one critical component which ensures that liberal democracies function appropriately.<sup>162</sup> In this view, liberal democracies may face defeat in the arena of information warfare in two ways: either by an inability to resist the influence of an adversary in the landscape of connections within a society or in the depletion of social capital and trust held by civil society. This may make liberal democracies acutely vulnerable to the high-precision targeting available to modern offensive IO. Because liberal democracies rely on a diffuse ecosystem of actors to generate and maintain trust within a society, there exists a broad potential attack surface of organizations that an adversary might choose to manipulate or disrupt.

This dual commitment to securing a society's social capital and securing a particular distribution of social capital also proscribes the set of tactics that a military specifically, or the government generally, might deploy in defending this ecosystem. A liberal democracy which implements a government-run command-and-control regime to filter truth from falsity, for instance, surrenders a key priority in a rush to defend against disinformation threats, though it may protect some absolute quantity of trust within a society. State intervention might seek to protect or strengthen a public against manipulation, but to the extent that they attempt to replace or supplant a robust ecosystem of civil society, these interventions violate democratic commitments.<sup>163</sup>

## *Architecture of a Defensible Public*

In light of these vulnerabilities and constraints, liberal democracies must work to construct defensible publics, an ecosystem of nongovernmental organizations and institutions that are themselves robust against attempts to manipulate and disrupt their capacity for creating and accumulating social capital. The trick is to facilitate and support this robustness without supplanting the independent function that these groups play within the context of a liberal democracy. Three essential building blocks appear to be necessary to lay the foundation for an effective defense.

### **Construct Public Systems of Detection**

Obfuscation is a core element of effective online IO. It enables adversaries to pursue their efforts without resistance or counter-messaging. It facilitates ongoing iteration and multiple attempts to develop the set of persuasive techniques most fitted to a specific goal and context. It permits widespread use of bots and automation to scale the impact and scope of persuasive operations. Exposing that these techniques are in use, particularly by foreign adversaries, can help to rally further scrutiny, support the development of countermeasures by civil society, and pressure the platforms hosting this activity to take action. This limits the options of those engaging in these campaigns and makes a public defensible.

However, civil society itself may lack the resources to perform this detection effectively and credibly. It may also lack the cohesiveness and capacity to compel major online platforms to expose information around

these campaigns promptly. The government could take a role in ensuring a regular stream of verified analytics about the social state of the web in the same manner that it already does around public health, weather, and the economy. Such a move would leverage a cartographic shift in support of defense. The same degree of social visibility that permits an enhanced level of accuracy in the targeting of influence efforts can, given adequate resources, simultaneously make it more straightforward to detect these efforts in progress.

Note that the military and government need not make determinations around the truthfulness of a given message and become “arbiters of truth” in order to execute on this priority. Indeed, such an effort would intrude on the role of civil society and risk democratic commitments. The triad of elements that make up contemporary online information warfare campaigns—the use of state-run media and informal infiltration of groups online, the manipulation of channels of advertising, and leveraging hacking to disrupt targets—can be monitored and exposed without necessarily speaking to the truth value of the messages being spread. These analytics might also focus on exposing the occurrence of specific techniques; for example, they could detect the use of swarms of bots to spread messages on social media.

### **Support Robust Network Topologies**

One way to view a defensible public is through the lens of its network structure. Are there certain patterns of relationships between individuals that are systematically more robust against manipulation and enable an effective flow of trustworthy information? Why are some networks of individuals better at detecting and rooting out disinformation than others?<sup>164</sup>

Research into these questions is ongoing, with a range of results drawing on the rich social data now available through social networks and other platforms.<sup>165</sup> Literature points to a number of testable hypotheses about the network features that facilitate or inhibit the spread of rumors within a network. Elements such as the level of segregation within a network, the degree of the transience of the information being spread, and the distribution of influential users all play a role.<sup>166</sup> Algorithms may also point the way to identifying specific individuals who will be most effective in helping to contain the spread of disinformation.<sup>167</sup>

These results naturally lead to the question of intervention. Once it is understood what topologies are more resistant to manipulation than others, the next important step is to understand the types of forces which can generate these configurations of people and norms. This may take Assange's notions of "simulated annealing" for the purpose of defense.<sup>168</sup> Incentives and pressures might be introduced to encourage the network structure of civil society and the public at large to align in ways that are more able to contend with campaigns of active manipulation. This might manifest in a range of different ways. For instance, changes to the way major social platforms recommend new users to "friend" and distribute content could encourage new network topologies between users and communities online. Third-party tools might be used to assist committed groups of users in injecting counter-messaging into key networks and identifying manipulative techniques in use.

The military and government can play a role in facilitating the development of these techniques and their transition into applied usage in two ways. First,

the government might substantially expand its existing role in funding basic research on these topics, helping to advance state-of-the-art technology and provide promising practicable options for civil society to adopt. Second, the government might play a role in launching viable testbeds for assessing these approaches and hosting wargame simulations that enable better preparedness and coordination among a network of key institutions.

### **Clearly Define Policies of Intervention**

Civil society may not always be able to serve as an effective bulwark against a state-sponsored, well-resourced, information warfare effort. The resources of states remain substantial, and a diffuse civil society of journalistic organizations and activist groups may not have the tools, or even the legal authorities needed to combat a dedicated influence effort effectively. Given the resources needed to execute these types of advanced campaigns, we might expect their occurrence to not be the norm—though, to the extent that they do emerge, they present a salient threat. In these cases, the ability for the military and government to act forcefully in the space may be critical to shielding the ecosystem of civil society from major threats or balancing the power of platforms that may be abetting significant disinformation campaigns.

Again, such an intervention requires striking a delicate balance. While the authority and capabilities of the military are significant, the commitments of liberal democracy prevent it from deep interventions or efforts to supplant entirely the role that civil society plays in facilitating information flow and managing social capital. Doing so would erode trust and harm

the independent ecosystem of information key to maintaining the system itself.

In collaboration with civil society, the government should work to develop a set of agreed-upon “red lines” which would specify the conditions and manner under which a nation’s military would act to mitigate the harm from major campaigns of information warfare. Reflecting on the netwar literature of the 1990s, one scholar has written, “defense by the government of the targeted population is appropriate and called for” in the event of state-actor manipulation of the social sphere.<sup>169</sup> This project envisions the creation and evolution of protocols for escalation and retaliation, advocating for “careful work . . . to limn what falls on what side of a line, so as to neither be provoked too readily, raising the specter of mutual or even accidental escalation.”<sup>170</sup> Enforcing the terms of these protocols would again require the leveraging of the increased social visibility made possible through the Internet to determine when an agreed-upon set of emergency conditions have been met.

To avoid overreach, it will be necessary to define the terms of this policy with specificity. Merely designating “influence by a foreign power” as sufficient for triggering intervention would invite abuse. It is necessary to define a scope of the institutions or networks that are considered out of bounds and a definition of the kinds of influence techniques that would necessitate action. If disseminated in a public manner, these declared boundaries could play an important role in shaping the international norms of engaging in these information warfare activities as various states consider the value and consequences of using these types of techniques going forward.



## CONCLUSION

The disinformation campaigns of 2016 should not be seen in isolation. Russian activities during the U.S. election were intimately linked to the history of information warfare and act as one dramatic exemplar of how the Internet has changed, and will continue to change, the nature of strategic influence and persuasion. As always, the challenge is to design a response that will not just counter the specifics of a particular threat, but tackle the emerging class of challenges as well. The Russian example should provoke a deeper exploration of the underlying dynamics that enabled that campaign and will enable others going forward.

As the flow of information through a society continues to change under the influence of a rapidly changing technological ecosystem, so too must our strategic concept of information warfare evolve to keep up. Without granular access to and detailed understanding of large-scale social behavior, defense thinking around information warfare and the impact of technology on it have been lacking in several important respects. In particular, strategic literature has been largely limited in its characterization of the essential nature of information warfare, the optimal conduct of that conflict, and the articulation of a clear approach toward defense in the space.

Technological change allows us to expand and sharpen these to-date missing or vaguely articulated pillars of information warfare strategy. One salient shift argued here is the extent to which the

contemporary Internet facilitates a dramatic transition in the ability of actors to perceive and understand the social behavior of large groups within a society. This shift, which has been facilitated by the rise of social networking platforms, significantly changes the operational context of information warfare. Access to data enables a highly granular approach to influence, enabling the identification and low-cost targeting of specific individuals and communities of interest. This enables a precision attack on the network structure and social capital of a community in a way that shifts information warfare from a combat of attrition to a combat of maneuver.

Rich data about social activity also enables the construction of a strategy for defense in the online environment. In liberal democracies, the military and government must walk a tightrope: defend and support an independent civil society which is endogenously robust against these campaigns, while avoiding actions which would themselves supplant and undermine these institutions. This advocates for a role that the military can play in using this data to expose these campaigns and support basic research, reserving its most forceful interventions for actions by adversaries which present the most significant threats.

The Internet and information technology have lowered the costs and expanded the set of adversaries that can launch information warfare campaigns, and these campaigns seem poised to become more effective with time. Executing a successful strategic concept for the online environment will require real investment in technologies and techniques which take into account the modern online context of persuasive warfare, rather than falling back on the strategies that were designed for an earlier generation of informational conflict.

## ENDNOTES

1. See e.g., William Davies, "The Age of Post-Truth Politics," *The New York Times*, August 24, 2016, available from <https://www.nytimes.com/2016/08/24/opinion/campaign-stops/the-age-of-post-truth-politics.html>, accessed January 18, 2018.

2. See e.g., "Tech Executives Testify in Senate Hearing on Russian Election Activity—Live Coverage," *The Wall Street Journal*, available from <https://www.wsj.com/livecoverage/senate-judiciary-hearing-tech-executives-russia-campaign>, accessed January 18, 2018.

3. See e.g., Jasper Jackson, "Eli Pariser: activist whose filter bubble warnings presaged Trump and Brexit," *The Guardian*, January 8, 2017, available from <http://www.theguardian.com/media/2017/jan/08/eli-pariser-activist-whose-filter-bubble-warnings-presaged-trump-and-brexit>, accessed January 18, 2018.

4. Joint Chiefs of Staff, *Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02, Washington, DC: Department of Defense, 2005.

5. National Intelligence Council, Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, ICA 2017-01D, Washington, DC: The Government Printing Office, January 6, 2017, pp. 3-4; Adrian Chen, "The Agency," *The New York Times*, June 2, 2015, available from <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>, accessed October 11, 2017.

6. Chen.

7. Amanda Robb, "Anatomy of a Fake News Scandal," *Rolling Stone*, November 16, 2017, available from <http://www.rollingstone.com/politics/news/pizzagate-anatomy-of-a-fake-news-scandal-w511904>, accessed November 20, 2017.

8. Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," Working Paper 2017.11, Oxford, UK: Project on Computational Propaganda, 2017, available from <http://comprop.oii.ox.ac.uk/publishing/working-papers/computational-propaganda-worldwide-executive-summary/>.

9. See e.g., Jillian C. York, "Syria's Twitter spambots," *The Guardian*, April 21, 2011, available from <http://www.theguardian.com/commentisfree/2011/apr/21/syria-twitter-spambots-pro-revolution>, accessed January 18, 2018; Natasha Lomas, "Study: Russian Twitter bots sent 45k Brexit tweets close to vote," *TechCrunch*, November 15, 2017, available from <http://social.techcrunch.com/2017/11/15/study-russian-twitter-bots-sent-45k-brexit-tweets-close-to-vote/>, accessed January 18, 2018; Klint Finley, "Pro-Government Twitter Bots Try to Hush Mexican Activists," *Wired*, August 23, 2015, available from <https://www.wired.com/2015/08/pro-government-twitter-bots-try-hush-mexican-activists/>, accessed January 18, 2018; Bettina Renz and Hanna Smith, "Russia and Hybrid Warfare-Going Beyond The Label," *Aleksanteri Papers*, No. 1/2016, Helsinki, Finland: University of Helsinki, 2016, p. 40, available from [http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap\\_1\\_2016.pdf](http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf); Jessikka Aro, "The cyberspace war: propaganda and trolling as warfare tools," *European View*, Vol. 15, Iss. 1, 2016, pp. 121-132.

10. Jen Weedon, William Nuland, and Alex Stamos, *Information Operations and Facebook*, ver. 1.0, Menlo Park, CA: Facebook, April 27, 2017, p. 27.

11. See e.g., Yamiche Alcindor, "Black Lawmakers Pressure Facebook Over Racially Divisive Russian Ads," *The New York Times*, September 28, 2017, available from <https://www.nytimes.com/2017/09/28/us/politics/facebook-russia-race-congressional-black-caucus.html>, accessed November 20, 2017; Deepa Seetharaman, "Russian-Backed Facebook Accounts Staged Events Around Divisive Issues," *The Wall Street Journal*, October 30, 2017, available from <https://www.wsj.com/articles/russian-backed-facebook-accounts-organized-events-on-all-sides-of-polarizing-issues-1509355801>, accessed November 14, 2017.

12. Samantha Subramanian, "Inside the Macedonian Fake-News Complex," *Wired*, February 15, 2017, available from <https://www.wired.com/2017/02/veles-macedonia-fake-news/>, accessed October 11, 2017; Dan Tynan, "How Facebook powers money machines for obscure political 'news' sites," *The Guardian*, August 24, 2016, available from <http://www.theguardian.com/technology/2016/aug/24/facebook-clickbait-political-news-sites-us-election-trump>, accessed November 21, 2017.

13. Paul Mozur, "China Spreads Propaganda to U.S. on Facebook, a Platform It Bans at Home," *The New York Times*, November 8, 2017, available from <https://www.nytimes.com/2017/11/08/technology/china-facebook.html>, accessed November 21, 2017.

14. National Intelligence Council, pp. 2-3.

15. Patrick Wintour, "Russian hackers to blame for sparking Qatar crisis, FBI inquiry finds," *The Guardian*, June 7, 2017, available from <http://www.theguardian.com/world/2017/jun/07/russian-hackers-qatar-crisis-fbi-inquiry-saudi-arabia-uae>, accessed November 21, 2017; Kim Willsher and Jon Henley, "Emmanuel Macron's campaign hacked on eve of French election," *The Guardian*, May 6, 2017, available from <http://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election>, accessed January 18, 2018.

16. See e.g., Muhammad al-'Ubaydi, Nelly Lahoud, Daniel Milton, and Bryan Price, *The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State*, West Point, NY: The Combating Terrorism Center at West Point, December 2014, pp. 46-56, available from <https://ctc.usma.edu/app/uploads/2014/12/CTC-The-Group-That-Calls-Itself-A-State-December20141.pdf>.

17. See e.g., Alice Marwick and Rebecca Lewis, *Media manipulation and disinformation online*, New York: Data & Society Research Institute, 2017; Ben Schreckinger, "World War Meme," *POLITICO Magazine*, March/April 2017, available from <https://www.politico.com/magazine/story/2017/03/memes-4chan-trump-supporters-trolls-internet-214856>, accessed November 21, 2017.

18. Cade Metz and Keith Collins, "How an A.I. 'Cat-and-Mouse Game' Generates Believable Fake Photos," *The New York Times*, January 2, 2018, available from <https://www.nytimes.com/interactive/2018/01/02/technology/ai-generated-photos.html>, accessed January 18, 2018.

19. Matthias Niessner, "Face2Face: Real-time Face Capture and Reenactment of RGB Videos (CVPR 2016 Oral)," YouTube video, 6:35, March 17, 2016, available from <https://www.youtube.com/watch?v=ohmajJTcpNk>, accessed January 18, 2018; see also Kevin Roose, "Here Come the Fake Videos, Too," *The New*

York Times, March 4, 2018, available from <https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html>, accessed April 4, 2018.

20. Emma Grey Ellis, "People Can Put Your Face on Porn—and the Law Can't Help You," *Wired*, January 26, 2018, available from <https://www.wired.com/story/face-swap-porn-legal-limbo/>, accessed January 30, 2018.

21. *Ibid.*

22. Aäron van den Oord and Sander Dieleman, "WaveNet: A Generative Model for Raw Audio," DeepMind, September 8, 2016, available from <https://deepmind.com/blog/wavenet-generative-model-raw-audio/>, accessed January 18, 2018.

23. See e.g., Nicholas A. Christakis and James H. Fowler, *Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives*, New York: Little, Brown, and Company, 2009.

24. Alex Pentland, *Social Physics: How Social Networks Can Make Us Smarter*, Reissue Ed., London, UK: Penguin Books, 2015.

25. Gordon Pennycook, Adam Bear, Evan T. Collins, and David G. Rand, *The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Stories Increases Perceived Accuracy of Stories Without Warnings*, SSRN, last revised March 22, 2019, available from <https://papers.ssrn.com/abstract=3035384>, accessed May 1, 2019.

26. Levi Boxell, Matthew Gentzkow, and Jesse M. Shapiro, "Greater Internet use is not associated with faster growth in political polarization among US demographic groups," *Proceedings of the National Academy of Sciences*, October 2017, Vol. 114, No. 40, pp. 10612-10617, available from <https://doi.org/10.1073/pnas.1706588114>.

27. See e.g., Robert Faris, Hal Roberts, Bruce Etling, Nikki Bourassa, Ethan Zuckerman, and Yochai Benkler, *Partisanship, Propaganda, and Disinformation: Online Media and the 2016 US Presidential Election*, Research Publication 2017-6, Cambridge, MA: Berkman Klein Center for Internet & Society at Harvard

University, August 2017, for an evaluation of the 2016 media landscape and discussion on the limitations of these studies.

28. Jennifer Kavanagh and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica, CA: RAND Corporation, 2018, available from [https://www.rand.org/pubs/research\\_reports/RR2314.html](https://www.rand.org/pubs/research_reports/RR2314.html).

29. Joint Chiefs of Staff, *Information Operations*, JP 3-13, Washington, DC: U.S. Department of Defense, updated 2014, available from [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_13.pdf](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf).

30. Joint Chiefs of Staff, *Doctrine for Joint Psychological Operations*, JP 3-53, Washington, DC: U.S. Department of Defense, 2003, available from [https://nsarchive2.gwu.edu//NSAEBB/NSAEBB177/02\\_psyop-jp-3-53.pdf](https://nsarchive2.gwu.edu//NSAEBB/NSAEBB177/02_psyop-jp-3-53.pdf).

31. For a brief review of these activities, see Philip M. Taylor, "‘Munitions of the mind’: A brief history of military psychological operations," *Place Branding and Public Diplomacy*, Vol. 3, No. 3, 2007, pp. 196-204.

32. Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: HarperCollins, 2010. Also see Oona A. Hathaway, Rebecca Crotof, William Perdue, and Philip Levitz, "The Law of Cyber-Attack," *California Law Review*, Vol. 100, Iss. 4, 2012, pp. 817-885, for a review of the definitional controversies around the term "cyberwarfare."

33. Robert Brose, "Cyberwar, Netwar, and the Future of Cyberdefense," 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 2015, pp. 25-38.

34. See e.g., Kevin D. Mitnick and William L. Simon, *The Art of Deception: Controlling the Human Element of Security*, 1st Ed., Indianapolis, IN: Wiley Publishing, Incorporated, 2002.

35. Ibid.

36. See e.g., Larry Tye, *The Father of Spin: Edward L. Bernays and the Birth of Public Relations*, Reprint Ed., New York: Owl Books,

2002, for early public relations efforts applied to World War I and in post-war marketing.

37. See e.g., Chen regarding hacking during the 2016 U.S. Presidential election.

38. See e.g., Alcindor; Seetharaman. Both discuss advertising used to polarize groups during the 2016 U.S. Presidential election.

39. See e.g., Ryan Holiday, *Trust Me, I'm Lying: Confessions of a Media Manipulator*, New York: Penguin Random House, 2013.

40. See Dan Ariely, *Predictably Irrational: The Hidden Forces That Shape Our Decisions*, Rev. and Enlarged Ed., New York: HarperCollins Publishers, 2009, chs. 4-5, 10, which reviews results in behavioral economics that show differing behavior in “non-commercial” settings.

41. John Arquilla and David Ronfeldt, “Cyberwar is Coming!” in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, CA: RAND Corporation, 1997.

42. Ibid.

43. Richard Szafranski, “A Theory of Information Warfare: Preparing for 2020,” *Airpower Journal*, Spring 1995, available from <http://www.iwar.org.uk/iwar/resources/airchronicles/szfran.htm>.

44. See John Arquilla and David Ronfeldt, “The Advent of Netwar,” in Arquilla and Ronfeldt, eds., *In Athena's Camp*, p. 283.

45. Ibid., p. 283.

46. Ibid., p. 280.

47. Ibid., p. 290.

48. Ibid.

49. See Robb; Marwick and Lewis.

50. Valery Gerasimov, “The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and



Methods of Carrying out Combat Operations,” Robert Coalson, trans., *Military Review*, Vol. 96, No. 1, January-February 2016, p. 23.

51. Ibid., p. 24.

52. Ibid., p. 25.

53. Ibid.

54. Ibid.

55. Ibid.

56. See e.g., Molly K. Mckew, “The Gerasimov Doctrine,” *POLITICO Magazine*, September/October 2017, available from <https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538>, accessed November 25, 2017; “Valery Gerasimov, the general with a doctrine for Russia,” *Financial Times*, September 15, 2017, available from <https://www.ft.com/content/7e14a438-989b-11e7-a652-cde3f882dd7b>, accessed January 18, 2018.

57. Andrew Monaghan, “The ‘War’ in Russia’s ‘Hybrid Warfare’,” *Parameters*, Vol. 45, No. 4, Winter 2015-16, p. 45, summarizes these debates.

58. Charles K. Bartles, “Getting Gerasimov Right,” *Military Review*, Vol. 96, No. 1, January-February 2016, p. 30.

59. Roger N. McDermott, “Does Russia Have a Gerasimov Doctrine?” *Parameters*, Spring 2016, Vol. 46, No. 1, available from [https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring\\_2016/12\\_McDermott.pdf](https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2016/12_McDermott.pdf).

60. See Gerasimov, “The Value of Science is in the Foresight,” p. 25.

61. Compare with John Arquilla and David Ronfeldt, *The Advent of Netwar*, Santa Monica, CA: RAND Corporation, 1996, pp. 13-14.

62. Ibid.

63. See S. G. Chekinov and S. A. Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security," *Military Thought*, 2010, Iss. 3, p. 1, for contemporary Russian military strategy writing that is consonant with Gerasimov.

64. See Gerasimov, "The Value of Science is in the Foresight," p. 24.

65. Ibid.

66. See Arquilla and Ronfeldt, "The Advent of Netwar," in Arquilla and Ronfeldt, eds., *In Athena's Camp*, p. 290.

67. See generally, John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, CA: RAND Corporation, 2001, available from [https://www.rand.org/pubs/monograph\\_reports/MR1382.html](https://www.rand.org/pubs/monograph_reports/MR1382.html), accessed November 29, 2017.

68. Ibid.

69. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, Washington, DC: The Government Printing Office, 2011, p. 26.

70. Ibid.

71. Ibid.

72. Ibid.

73. Ibid.

74. Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," CIMSEC, August 25, 2016, available from <http://cimsec.org/plas-latest-strategic-thinking-three-warfares/27468>, accessed January 3, 2018.

75. M. Taylor Fravel, "Chapter 2: China's Changing Approach to Military Strategy: The Science of Military Strategy from 2001 and 2013," in Joe McReynolds, ed., *China's Evolving Military Strategy*, Washington, DC: The Jamestown Foundation, 2016.

76. See Ibid.

77. Ibid.

78. Mingda Qiu, "China's Science of Military Strategy: Cross-Domain Concepts in the 2013 Edition," Cross-Domain Deterrence Project (CDD) Working Paper, La Jolla, CA: University of California San Diego, September 2015.

79. See e.g., Stefan Halper, ed., *China: The Three Warfares*, Washington, DC: Department of Defense, Office of Net Assessments, 2013, available from <https://cryptome.org/2014/06/prc-three-wars.pdf>; Laura Jackson, "Revisions of Reality: The Three Warfares—China's New Way of War," in *Information at War: From China's Three Warfares to NATO's Narratives*, Beyond Propaganda Series, London, UK: Legatum Institute, September 2015, available from <https://lif.blob.core.windows.net/lif/docs/default-source/publications/information-at-war-from-china-s-three-warfares-to-nato-s-narratives-pdf.pdf?sforsn=2>.

80. Kejin Zhao, "The Motivation Behind China's Public Diplomacy," *Chinese Journal of International Politics*, Vol. 8, Iss. 2, Summer 2015, pp. 167-196.

81. See Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Beijing, China: PLA Literature and Arts Publishing House, February 1999; see also Qiu, p. 1.

82. Alexis C. Madrigal, "How to Think About Wikileaks," *The Atlantic*, December 13, 2010.

83. Bill Keller, "Dealing with Assange and the Wikileaks Secrets," *The New York Times*, January 26, 2011, available from <http://www.nytimes.com/2011/01/30/magazine/30Wikileaks-t.html>.

84. See National Intelligence Council, pp. 2-3.

85. See e.g., Jeremy Stahl, "WikiLeaks is fanning a Conspiracy Theory That Hillary Murdered a DNC Staffer," *Slate*, August 9, 2016, available from [http://www.slate.com/blogs/the\\_slate/2016/08/09/wikileaks\\_is\\_fanning\\_a\\_conspiracy\\_theory\\_that\\_hillary\\_murdered\\_a\\_dnc\\_staffer.html](http://www.slate.com/blogs/the_slate/2016/08/09/wikileaks_is_fanning_a_conspiracy_theory_that_hillary_murdered_a_dnc_staffer.html), accessed January 18, 2018.

86. Julian Assange, "Conspiracy as Governance," December 3, 2006, available from <http://web.archive.org/web/20070110200827/http://iq.org:80/conspiracies.pdf>.

87. Ibid., p. 5.

88. Ibid.

89. Ibid.

90. Ibid.

91. Julian Assange, "Sun 31 Dec 2006: The non linear effects of leaks on unjust systems of governance," IQ.org, December 31, 2006, available from <http://web.archive.org/web/20070110200827/http://iq.org/#Thenonlineareffectsofleaksonunjustsystemsofgovernance>.

92. Ibid.

93. Arquilla and Ronfeldt, *Networks and Netwars*.

94. See Assange, "Sun 31 Dec 2006: The non linear effects of leaks on unjust systems of governance."

95. Ibid.

96. See Arquilla and David Ronfeldt, *Networks and Netwars*, pp. 7-10.

97. Charlie Winter, *Documenting the Virtual 'Caliphate'*, London, UK: Quilliam Foundation, 2015, available from <https://www.quilliaminternational.com/documenting-the-virtual-caliphate/>.

98. See al-'Ubaydi, Lahoud, Milton, and Price, pp.46-56.

99. Ibid., p. 47.

100. Islamic State, *Media Man, You Are a Mujāhid Too*, 2nd Ed., n.p.: Islamic State, April 6, 2016, available from <https://jihadology.net/2016/04/06/new-book-from-the-islamic-state-media-man-you-are-a-mujahid-too-second-edition/>.

101. Charlie Winter, *Media Jihad: The Islamic State's Doctrine for Information Warfare*, Vol. 9, London, UK: International Centre

for the Study of Radicalisation and Political Violence, Department of War Studies, King's College, 2017, available from <http://ficsr.info/2017/02/ficsr-report-media-jihad-islamic-states-doctrine-information-warfare/>.

102. Marwan M. Kraidy, "The projectilic image: Islamic State's digital visual warfare and global networked affect," *Media, Culture & Society*, Vol. 39, Iss. 8, November 2017, pp. 1194-1209, quoting *Media Man, You Are a Mujāhid Too*.

103. See Winter, *Media Jihad*, pp. 17-18.

104. *Ibid.*, p. 18.

105. Haroro J. Ingram, "The Strategic Logic of Islamic State Information Operations," *Australian Journal of International Affairs*, Vol. 69, Iss. 6, 2015, pp. 744-745.

106. *Ibid.*

107. Brendan I. Koerner, "Why ISIS Is Winning the Social Media War," *Wired*, April 2016, available from <https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/>, accessed January 11, 2018.

108. *Ibid.*

109. *Ibid.*

110. See Ingram, p. 746.

111. Whitney Phillips, *This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture*, Cambridge, MA: Massachusetts Institute of Technology Press, 2015.

112. *Ibid.*

113. Marwick and Lewis.

114. Martin C. Libicki, "Why cyber war will not and should not have its grand strategist," *Strategic Studies Quarterly*, Vol. 23, 2014.

115. *Ibid.*, p. 33.

116. *Ibid.*, pp. 33-34.

117. See Joint Chiefs of Staff, *Dictionary of Military and Associated Terms*.

118. See e.g., Orjar Oyen and Melvin L. De Fleur, "The Spatial Diffusion of an Airborne Leaflet Message," *American Journal of Sociology*, Vol. 59, No. 2, September 1953, pp. 144-149.

119. See Erez Shmueli, Vivek K. Singh, Bruno Lepri, and Alex Pentland, "Sensing, understanding, and shaping social behavior," (*IEEE*) *Transactions on Computational Social Systems*, Vol. 1, Iss. 1, March 2014, pp. 22-34, for a review of research results leveraging these technological changes.

120. *Ibid.*

121. Zeynep Tufekci, "We're building a dystopia just to make people click on ads," TED Talks, available from [https://www.ted.com/talks/zeynep\\_tufekci\\_we\\_re\\_building\\_a\\_dystopia\\_just\\_to\\_make\\_people\\_click\\_on\\_ads](https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads), accessed January 18, 2018; Nicholas Thompson, "Our Minds Have Been Hijacked by Our Phones. Tristan Harris Wants to Rescue Them," *Wired*, July 26, 2017, available from <https://www.wired.com/story/our-minds-have-been-hijacked-by-our-phones-tristan-harris-wants-to-rescue-them/>, accessed January 18, 2018.

122. Louis Brown, *A Radar History of World War II: Technical and Military Imperatives*, Bristol, UK, and Philadelphia, PA: Institute of Physics Publishing, 1999.

123. See e.g., Jeffrey B. Jones and Jack N. Summe, "Psychological Operations in Desert Shield, Desert Storm, and Urban Freedom," *Landpower Essay Series*, No. 97-3, Arlington, VA: Institute of Land Warfare, Association of the United States Army, August 1997, available from <https://www.ansa.org/sites/default/files/LPE-97-3-Psychological-Operations-in-Desert-Shield-Desert-Storm-and-Urban-Freedom.pdf>, detailing messaging operations during Operation DESERT STORM and pamphlets with the theme of "peace not war" and "Saddam has betrayed you."

124. Regarding political beliefs, see David Lazer, Brian Rubineau, Carol Chetkovich, Nancy Katz, and Michael Neblo, "The Coevolution of Networks and Political Attitudes," *Political Communication*, Vol. 27, Iss. 3, 2010, pp. 248-274; regarding obesity, see Nicholas A. Christakis and James H. Fowler, "The Spread of Obesity in a Large Social Network over 32 Years," *New England Journal of Medicine*, Vol. 357, No. 4, July 26, 2007, pp. 370-379; regarding divorce, see Rose McDermott, James H. Fowler, and Nicholas A. Christakis, "Breaking Up Is Hard to Do, Unless Everyone Else Is Doing It Too: Social Network Effects on Divorce in a Longitudinal Sample," *Soc Forces*, Vol. 92, No. 2, 2013, pp. 491-519.

125. Lazer et al.; Christakis and Fowler; McDermott et al.

126. For a classic review of the argument bridging network structure with social capital, see Ronald S. Burt, "The Contingent Value of Social Capital," *Administrative Science Quarterly*, Vol. 42, No. 2, June 1997, pp. 339-365.

127. Robert D. Putnam, *Bowling Alone: The Collapse And Revival Of American Community*, New York: Simon & Schuster, 2000, p. 19.

128. Francis Fukuyama, "Social Capital, Civil Society and Development," *Third World Quarterly*, Vol. 22, No. 1, February 2001, pp. 7-20.

129. See Paul S. Adler and Seok-Woo Kwon, "Social Capital: Prospects for a New Concept," *Academy of Management Review*, Vol. 27, No. 1, 2002, pp. 17-40 (reviewing literature on the relationship between social capital and information flow); Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity*, New York: Free Press, 1995.

130. U.S. Marine Corps, *Warfighting*, U.S. Marine Corps Doctrine Pamphlet (MCDP) 1, Washington, DC: Department of Defense, 1997, p. 36, hereafter MCDP-1.

131. *Ibid.*

132. *Ibid.*, p. 37.

133. *Ibid.*

134. See e.g., Tim Weiner, *Legacy of Ashes: The History of the CIA*, New York: Doubleday, 2007, ch. 16, detailing Central Intelligence Agency (CIA) propaganda and recruitment efforts in Cuba and eventually culminating in the conclusion that the agency knew “next to nothing about the anti-Castro forces inside Cuba.”

135. Compare to Vincent Stewart, “The Age of Cognitive War,” Keynote Address, Department of Defense Intelligence Information Systems Worldwide Conference, August 14, 2017, in which the Director of the Defense Intelligence Agency drew links between maneuver and information warfare.

136. See e.g., FireEye, Inc., “APT28: A Window into Russia’s Cyber Espionage Operations?” FireEye, October 27, 2014, available from <https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html>, accessed February 27, 2019, which examines two advanced, persistent threats observed in the Russian campaign.

137. See e.g., Emanuel Maiberg, “Under Trump, Gamergate Can Stop Pretending It Was About Games,” Vice Motherboard, available from [https://motherboard.vice.com/en\\_us/article/bm5wd4/under-trump-gamergate-can-stop-pretending-it-was-about-games](https://motherboard.vice.com/en_us/article/bm5wd4/under-trump-gamergate-can-stop-pretending-it-was-about-games), accessed April 5, 2018, discussing the relationship between the alt-right and video gaming communities.

138. See Eytan Bakshy, Jake M. Hofman, Winter A. Mason, and Duncan J. Watts, “Everyone’s an Influencer: Quantifying Influence on Twitter,” in *Proceedings of the Fourth ACM International Conference on Web Search and Data Mining*, New York: Association for Computing Machinery, 2011, pp. 65-74, available from <http://doi.acm.org/10.1145/1935826.1935845>, accessed February 1, 2018, which notes that the prediction of “influencers” is “relatively unreliable.”

139. Joe Strange, “Centers of Gravity and Critical Vulnerabilities,” *Perspectives on Warfighting*, No. 4, Quantico, VA: Marine Corps University, 1996, p. ix, provides this definition and describes some of the doctrinal debates about its meaning.

140. See MCDP-1, pp. 45-47.

141. *Ibid.*, p. 11.



142. *Ibid.*, p. 72.

143. Sasha Issenberg, "How Obama's Team Used Big Data to Rally Voters," *MIT Technology Review*, December 19, 2012, available from <https://www.technologyreview.com/s/509026/how-obamas-team-used-big-data-to-rally-voters/>, accessed April 23, 2018, discusses the advantages of speed and data in a political campaign context.

144. See e.g., Shaun Walker, "The Russian troll factory at the heart of the meddling allegations," *The Guardian*, April 2, 2015, available from <https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house>, accessed February 27, 2019.

145. See e.g., Woolley and Howard; Finley.

146. See generally, Eli Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, Reprint Ed., New York: Penguin Books, 2012.

147. See e.g., Joshua Benton, "Facebook is making its News Feed a little bit more about your friends and a little less about publishers," NiemanLab, June 29, 2016, available from <http://www.niemanlab.org/2016/06/facebook-is-making-its-news-feed-a-little-bit-more-about-your-friends-and-a-little-less-about-publishers/>, accessed January 18, 2018.

148. "U.S. built secret 'Cuban Twitter' to stir unrest: AP," Reuters, April 3, 2014, available from <https://www.reuters.com/article/us-usa-cuba-twitter/u-s-built-secret-cuban-twitter-to-stir-unrest-ap-idUSBREA321F920140403>, accessed January 18, 2018, describes one such approach.

149. See Paul Lewis, "'Fiction is outperforming reality': how YouTube's algorithm distorts truth," *The Guardian*, February 2, 2018, available from <http://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth>, accessed April 23, 2018.

150. Jesse McIntyre III, "To Respond or Not to Respond: Addressing Adversarial Propaganda," *Military Review*, Vol. 96, No. 3, May-June 2016, p. 62.

151. Major Scott J. Harr, "Expanding Tolstoy and Shrinking Dostoyevsky: How Russian Actions in the Information Space Are Inverting Doctrinal Paradigms of Warfare," *Military Review*, Vol. 97, No. 5, September-October 2017, p. 39.

152. Brose, p. 38.

153. Cliff W. Gilmore and Richard R. Osial, "The Fourth Estate is dead, long live the Fourth Estate: A new military mindset for a rapidly evolving communication environment," *Public Relations Review*, Vol. 38, Iss. 2, June 2012, pp. 208-213.

154. Harr, p. 44.

155. *Ibid.*, p. 47.

156. *Ibid.*

157. See Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, Santa Monica, CA: RAND Corporation, 2016, available from [https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND\\_PE198.pdf](https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf), accessed April 23, 2018, which casts doubt on the notion of counter-propaganda.

158. See Putnam, p. 19.

159. See e.g., Fukuyama, "Social Capital, Civil Society and Development," p. 11: "An abundant stock of social capital is presumably what produces a dense civil society, which in turn has been almost universally seen as a necessary condition for modern liberal democracy."

160. See Wolfgang Merkel, "Embedded and defective democracies," *Democratization*, Vol. 11, Iss. 5, 2004, pp. 33-58, which argues that uneven patterns of social capital can create the emergence of an illiberal democracy.

161. See Simone Chambers and Jeffrey Kopstein, "Bad Civil Society," *Political Theory*, Vol. 29, Iss. 6, December 2001, p. 837, which notes that there are "so many proponents of versions of this argument that it would be difficult to list them all."

162. Brian McNair, *Journalism and Democracy: An Evaluation of the Political Public Sphere*, London, UK: Routledge, 2012, ch. 1, reviews the arguments linking media to the public sphere and liberal democracy.

163. Francis Fukuyama, *Social Capital: The Tanner Lectures on Human Values Delivered at Brasenose College, Oxford, May 12, 14, and 15, 1997*, Salt Lake City, UT: University of Utah, 1998, pp. 475-476, available from [https://tannerlectures.utah.edu/\\_documents/a-to-z/ff/Fukuyama98.pdf](https://tannerlectures.utah.edu/_documents/a-to-z/ff/Fukuyama98.pdf), discusses the potential for government intervention to deplete the ability of civil society to act.

164. Jacob Rogers, "Wikipedia and Intermediary Immunity: Supporting Sturdy Crowd Systems for Producing Reliable Information," *Yale Law Journal Forum*, Vol. 127, October 9, 2017, pp. 360-362, reviews some of the literature on why Wikipedia has proven robust against disinformation.

165. For a sampling of the research currently ongoing on this topic, see the reading material and resources from "MIS2: Misinformation and Misbehavior Mining on the Web," workshop held February 9, 2018, in Los Angeles, CA, available from <http://snap.stanford.edu/mis2/>, accessed January 18, 2018.

166. See e.g., Daron Acemoglu, Asuman Ozdaglar, and Ali ParandehGheibi, "Spread of Misinformation in Social Networks," arXiv, Vol. 0906.5007, June 26, 2009, available from <http://arxiv.org/abs/0906.5007>, accessed April 6, 2018, about modeling the influence of "forceful" users who shape beliefs without updating their own; Marcella Tambuscio, Diego F. M. Oliveira, Giovanni Luca Ciampaglia, and Giancarlo Ruffo, "Network segregation in a model of misinformation and fact checking," version 2, arXiv, Vol. 1610.04170, updated January 17, 2018, available from <http://arxiv.org/abs/1610.04170>, accessed April 6, 2018, which examines the role of network sparsity and "forgetting" in the spread of misinformation.

167. See e.g., Ceren Budak, Divyakant Agrawal, and Amr El Abbadi, "Limiting the spread of misinformation in social networks," in *Proceedings of the 20th international conference on World wide web*, New York: Association for Computing Machinery, 2011, p. 665, available from <http://portal.acm.org/citation.cfm?doid=1963405.1963499>, accessed April 6, 2018; Nam P.

Nguyen, Guanhua Yan, and My T. Thai, "Analysis of misinformation containment in online social networks," *Computer Networks*, Vol. 57, Iss. 10, July 5, 2013, pp. 2133-2146.

168. See "Transcript of secret meeting between Julian Assange and Google CEO Eric Schmidt."

169. Jonathan Zittrain, "'Netwar': The unwelcome militarization of the Internet has arrived," *Bulletin of the Atomic Scientists*, Vol. 73, Iss. 5, September 2017, pp. 300-304, especially p. 304.

170. *Ibid.*

**U.S. ARMY WAR COLLEGE**

**Major General John S. Kem  
Commandant**

\*\*\*\*\*

**STRATEGIC STUDIES INSTITUTE  
AND  
U.S. ARMY WAR COLLEGE PRESS**

**Director  
Professor Douglas C. Lovelace, Jr.**

**Director of Research  
Dr. Steven K. Metz**

**Author  
Tim Hwang**

**Publications Assistant  
Ms. Denise J. Kersting**

\*\*\*\*\*

**Composition  
Mrs. Jennifer E. Nevil**





U.S. ARMY



FOR THIS AND OTHER PUBLICATIONS, VISIT

US AT

<https://www.armywarcollege.edu/>

ISBN 1-58487-815-0



9



This Publication



SSI Website



USAWC Website