The Gray Legion: Information Warfare Within Our Gates

Jeffrey Baptist
acbapj@gmail.com

Julian Gluck

Follow this and additional works at: <https://digitalcommons.usf.edu/jss>
pp. 37-55

Recommended Citation

Baptist, Jeffrey and Gluck, Julian. "The Gray Legion: Information Warfare Within Our Gates." *Journal of Strategic Security* 14, no. 4 (2021) : 37-55.
DOI: <https://doi.org/10.5038/1944-0472.14.4.1928>
Available at: <https://digitalcommons.usf.edu/jss/vol14/iss4/3>

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

The Gray Legion: Information Warfare Within Our Gates

Abstract

The information environment, once viewed as an unassailed common for human knowledge, has revealed itself to be a vector for malicious narratives in the ongoing battle for global hegemony. Since 2014, the United States has been under siege from information attacks on multiple fronts, from cyber infrastructure and goods to the cognitive outlooks of its citizenry. Disinformation as a social media tool represents a novel and grave danger to democracy; it serves as a means for sowing unrest and influencing policy changes while enabling conventional conflict or—in the best case for those who would exploit and manipulate narratives—avoiding it entirely. In this article, we identify the harbinger of a dire threat that circles outside, and now inside, the United States' walls by exploring the theoretical dynamics of foreign, state-sponsored disinformation in democracies throughout the West. We examine the mechanisms through which this approach operates and why it is Russia's preferred course of action.

Introduction

Nearly two centuries before the World Wide Web emerged, a prominent Prussian military theorist interpreted warfare as the summation of will and means as elements of competition between belligerents.¹ In the time prior to General Clausewitz's observation and in the conflicts that followed, the determination of the onset of hostilities would involve an engagement with or meaningful attack on an adversary's will and means, such as the assassination of a royal figure or the sinking of a ship. Although kinetic approaches more straightforwardly define the onset of hostilities, soft acts may just as easily signal state-level conflict, particularly through an ever-increasing range of information-based methods. It is for this reason that the question of opening salvos in the next war may have already been answered.

Foreign, state sponsored disinformation has co-opted commons created to facilitate free communication and engagement. Whether focused on the internet or the preponderance of the tech industry which manages major social media platforms, the West finds its creations (Facebook, Twitter, Reddit) now being used to attack its own vital decision-making processes.² The targets of these attacks are leaders and citizens, with the former uniquely dependent upon the latter in representative democracy. The proliferation of technology and means of access allow millions to receive and send messages, while the effective anonymity of online involvement cloaks nefarious actors. The masterminds behind these online personas seek to avoid conventional confrontation, and the modern internet landscape provides them a vector to better their geopolitical position without provoking a dire military situation; their fake accounts represent a facet of their asymmetric approach.

By refusing to meaningfully acknowledge and address disinformation and social media manipulation (or even the attempted manipulation thereof to deceptively affect democracies), the United States fools itself into believing that hostilities are on the verge of initiation when they, in the minds of the adversaries, are a matter of ongoing operations. Even without ongoing interference, the population's perception of journalism and scientific analysis has eroded in recent years, an environment which may be amenable to disinformation due to favorable audience predispositions to already accepted narratives or ongoing degradation of faith in democratic

institutions.³ The Rubicon has long been crossed; the legion has already marched to the foot of Rome's hills.⁴

A growing trove of expert analysis suggests a dark side to the information age, one that threatens objective truth, collective understanding, and legitimate democratic functions.⁵ The effects of these new disinformation tactics suggest a critical failure in traditional news media's screening procedures, a new source of virulent narratives spread via social media, and the ultimate subversion of dialogue among subgroups in the information space. Phenomena such as echo chambers, vox populi media reporting, and two-step communication flow result in multiple vectors and venues used to seed the information landscape; these tactics—though their content originates with foreign, deceptive online personas—exploit the organic, U.S. audience in propagating disinformation, an act made easier through social media mechanics.⁶

The fallout from the infamous Russian-based Internet Research Agency (IRA) case is not entirely unique; organizations and networks like the IRA multiply each day and their tactics advance at a pace limited only by fiber-optic cables. Multiple datasets and newly identified disinformation networks, as well as accompanying warnings, emerge routinely from social media corporations, security think tanks, and government agencies; many of these highlight focused efforts against democratic nations, including the United States.⁷ The legion that democracies and governments now face is one of murky narratives, questionably sourced half-truths, and cleverly managed online personas managed by foreign firms. In previous articles about this topic, many scholars eschew provocative language in favor of more neutral discourse; this is a form of euphemism or understatement in which the authors of this article will not partake given the gravity of the situation.⁸

This nation and its allies have been under insidious assault for years, from Russian online influence in U.S. elections to military activities observed in Georgia and Crimea. The United States is beginning to see such actions in a more serious light, but such response does not address the false perception that all is well on the information front.⁹ If warfare is an attack on the will or means to conduct the basic functions of statecraft, then an attempt to covertly subvert (especially deceptively) another nation's decision-making ability (democracy, public sentiment) is as nefarious an

action as a blockade or skirmish. However, this approach, though unsettling, should be unsurprising: in the standard Diplomacy, Information, Military, and Economy (DIME) model for state power, information is the only meaningful field of competition for the West's rivals.¹⁰ In Russia's case, its leaders either desire further prestige and power in a perceived zero-sum situation or believe that the West represents an existential threat through the neo-liberal system; both perceptions make conflict (short of provoking outright martial engagement) a required course of action in a battle of diplomatic and economic attrition with accompanying military protection.¹¹

The answers to the following questions support the assertion that soft war is upon the United States: What is happening (with a focus on Russia)? Why is it important? What can be done to stop it? This article will illustrate that these gray zone operations are existential threats which are uniquely situated to erode Western sovereignty with a focus on how will and capability manifest in a democracy facing disinformation. It is the authors' hope that readers will find themselves mobilized to further analyze, communicate, and address this threat in effective ways so that they may more meaningfully counteract foreign, state-sponsored disinformation. Members of the citizenry must no longer allow hubris or embrace ignorance; "peace for our time" usually comes at great cost—one that the Melian dialogue suggests many would find uncomfortable.¹²

Background

In the past decade, experts have witnessed the rise of soft warfare (influence) facilitated through cyberspace and social media.¹³ Until the hearings and indictments regarding Russian interference in the 2016 election, the United States had not openly discussed such behavior; at the time of this writing, many could make the argument that the nation is only beginning to address it. Soft power in and of itself can be a crippling sword in the battle between states, but the United States has normally enjoyed the benefits of its favor rather than seeing that weapon turned upon itself. With the resurgence of Russia, the United States finds new tests in the arena of soft power. The West, with all its military might, is likely to succeed in any local military endeavors and many expeditionary ones. To varying degrees, the United States has also been quite successful in the economic and diplomatic realms. Foolishly, however, it has ceded the

information arena to those with malicious intent.¹⁴ Some may argue, with degrees of validity, against this assertion. However, one need only consider the vitriol of the 2020 presidential election, marked by narratives promoted by past IRA actors, and carried by multiple incensed groups. As a vector for social media virulence, this marks a Western response that falls far short of what many would call success.

The citizens of the United States live in a democratic republic that—as with other western nations—enjoys voting processes and general freedom of information and expression. Ultimately, elected officials (ostensibly) make decisions based on the choices of the voting populace, whether that be retribution or support at the ballot box or apathy at the same. In a diffuse and delayed fashion, one can sway democratic states merely by influencing the citizenry—or its officials—to vote (or not vote, as the case may be) in a specific way favorable to a foreign entity, as is feared with contemporaneous hacking threats and their accompanying social influence efforts.¹⁵ These approaches circumvent arenas in which the United States and the West have cultivated national strength: Military and economic, both levers which are subject to leadership’s analysis and decisions, unlike activity in the information space. In a military sense, there is a clear delineation between Clausewitzian will and means: The means—tanks, boats, planes, bombs, treasure—are either too powerful or too impractical to engage. The will—how much Americans wish to employ state means manifested by the electorate through its leaders—is not.

As a nation, the United States has for many years dabbled or specialized in expeditionary deployment and conflict. The projection of its armed forces has become so ubiquitous—the constant state of war another element of the 21st century military milieu—that politicians continuously campaign on platforms (or modify agendas) of “bringing the troops home.”¹⁶ Many Americans lack the will to continue hostilities or engage in new ones, and both the media and politicians frame and react to that stance. Gray zone operations rely on public and government will or the lack thereof; by pushing the threshold of intervention just short of requisite retaliation, an adversary can steadily make small gains. At the state-level, shorter offensive advancements make for a slow but sure strategy against an opponent determined to prevent more powerful (and provocative) maneuvers. Given the pervasive nature of information, a well-planned campaign can also affect diplomatic outcomes, either increasing costs to

maintain newly strained relationships between allies or forcing leadership to continuously convince their electorate of the need for such global institutions. Paired with stoking internal conflict, this practice stalls immediate confrontation heuristics while poisoning long term national outlooks via the voting populace.

To expand upon Clausewitz and situate the effects of influence efforts on democratic nations, one can look to sociologist Charles Tilly who identified that states must engage in certain activities as a form of homeostasis—war making, production, extraction, adjudication, state making, distribution, and protection. Of these forms, extraction is the most complex in democratic forms of government: “drawing from [the nation’s] subject population the means of state making, war making, and protection” in the exact dynamic addressed with the matter of will and means.¹⁷ If the state cannot extract from its people the will to ensure internal order (state making), exert force upon external rivals (war making), or check rivals to state power internally and externally (protection, analogous to counterterrorism), then the state may as well be defenseless throughout, if not entirely defunct.

To this point, attacking the extraction function results in the inability to decisively act against threats or the mistaken perception that allied individuals and organizations are threats themselves.¹⁸ This trend appears across current disinformation in social media; it relies on hostile action which falls below a commonly acceptable threshold for egregious hostility and, thus, chips away at the ability to see it for what it is without spurring due response. Without addressing such activity meaningfully, the result is a silent war that the West will have lost the moment its citizens deny the existence of Odysseus and his men inside the Trojan horse; social media provides the perfect cover for the legion’s entrance into the discourse, as well as its perceived legitimacy as a beneficent, honest participant.

Russian Actions

The 2016 elections illustrated that the United States is not disconnected from the realities of its European allies. Ongoing disinformation issues—more advanced than the ones the United States encountered in past years—show that this antagonistic behavior is still useful to the Russian disinformation export apparatus. In addition to fanning the flames of

political and social turmoil, what should be most concerning is Russia's employment of hybrid warfare. The invasion of Georgia in 2008 saw an initial, expansive Russian cyber-attack to disrupt Georgian internal, internet-based communication methods (including media) paired with a propaganda campaign to inundate audience members with fabricated information.¹⁹ The result of this information barrage was a softened target unable to resist physical engagement due to internal confusion and dissuasion. A similar play from the Russian team in 2014 manifested in Crimea: Facing increasing unrest over the Maidan protests and their puppet Ukrainian President, Russia began to sow disinformation online that tapped into specific narratives of conflicting Ukrainian ideological subgroups.²⁰

Over the past six years, foreign sources stoked U.S. societal ills and conducted cyber-espionage to seed domestic media with information supporting or amplifying cultural anxieties, such as race, immigration, and crime.²¹ The manipulative online personas and their activities oftentimes appeared so legitimate that they were retweeted by elected officials, featured in U.S. media, and followed by its people. The coordination between multiple organizations to conduct such harmonious activities suggests an intentional, highly prioritized effort to degrade U.S. decision-making abilities and standing.²² Experts continue to observe IRA-affiliated network creation, with one discovery occurring as recently as July 2021; this activity is ongoing.²³

The effects do not have to be specific or even have a definite end goal. Clausewitz' concept of will is generally linked to certain behaviors (the waging of war), but it is much more abstract in this sense. It is the will to do anything of consequence outside of political infighting that is conducive to successful external and international influence; the more society focuses inwardly on elections, riots, or questioning legitimate societal institutions, the less attention and consideration its members grant to the bear trampling through the European woods. This is the beginning, at a macro level via micro means, of the degradation of the United States' ability to resist Russian influence. Members of society become dissuaded from action because they are convinced—either through the electorate or through the leaders who pride themselves on more limited military involvement—that the problem is not worth prioritization, compared to the more pressing conflicts within the borders or discord with allies. This

plays perfectly into the desired, countervailing global power structure Russia seeks to cultivate; where they create a vacuum of Western leadership via distraction and dissuasion, they give themselves room to grow.²⁴

In a scenario where disinformation actors completely delude their audiences, the problem itself, to the misled, is nonexistent—a seemingly likely possibility given the authors’ discussions with acquaintances as to whether Russian social media bots engaged domestic audiences between 2014 and 2018. The cost incurred by U.S. adversaries in taking these opening shots? Minimal, except for the time to weaken psychological foundations and principles—a resource which is inconsequential outside of a four-to-eight-year election priority cycle, an irrelevant constraint in Russian politics and strategy.

In line with the increasingly complex and frequent attacks on collective democratic decision-making, Russian military theorists’ foreshadowed the same tactics and strategy. Russian military journals define their unique form of information-psychological conflict thusly:

The main aim ... is regime change in the adversary country (through destroying the organs of government); by means of mass influence on the military-political leadership of the adversary achieving as a minimum an increase in the amount of time available for taking command decisions and lengthening the operational cycle; by means of influence on the mass consciousness of the population—directing people so that the population of the victim country is induced to support the aggressor, acting against its own interests.²⁵

Within the idea of gray zone conflict, Russian efforts have evolved (or returned) to embrace (coily, if not always publicly) the clear intent to destabilize other nations’ governments without ethical caveat. In previous years, nations would see targeted political influence in the information realm primarily as an affront to the notion of Pax Democratica and the ongoing pacifying march of Liberalism (both neo and classical). However, the data indicate neither restraint nor sole focus on specific geopolitical outcomes. The IRA’s tweets and posts seek to cause chaos instrumentally: To turn citizen against citizen by attacking issues of race, religion, and

rule. They focus on internal U.S. wedge issues while trying to insincerely guide conversations toward foreign policy. They aim not only for discrete outcomes in the international field of competition, but, rather, shoot to (on an informational, narrative level) kill. Their target: The dialogue that makes democracy possible and enables the destabilization of Western governments.

Synthesis

The United States and the West have generally viewed war as a continuation of politics but has failed to consider the inverse mechanics: Politics as a continuation of war. This inversion not only allows for the perpetuation of myths regarding peace through increased tension, but it supports foes who understand the extreme cost of full, expeditionary conventional military operations. It allows military and national buildup that remains below the level of outright conflict (and the technical declaration of war) but still results in the loss of both tangible and intangible national capital for the target. If the end goal is destruction of an enemy, arms are not the only means; just as adversaries view nonmilitary means as hostile (sanctions, diplomacy), so too should Americans view asymmetric efforts against the United States and its citizenry as directed attacks.²⁶

Adversaries recognize they need not separate military goals from national strategic goals. The former is not an end unto itself; it is a means to the latter. Through whole-of-government efforts and multi-domain operations, online influence becomes a chief tool for countless adversary objectives. This assessment is not idle conjecture, but the Russian military's stated strategy. It is a playbook they used in Crimea and Ukraine:

In the 21st century we have seen the tendency toward blurring the lines between the states of war and peace. Wars are no longer declared ... The role of non-military means of achieving political and strategic goals has grown. ... the broad use of political, economic, informational, humanitarian, and other non-military measures—applied in coordination with the protest potential of the population [is the new focus of conflict]. All this is supplemented by

military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces. The open use of forces—often under the guise of peacekeeping and crisis regulation—is resorted to only at a certain stage, primarily for the achievement of final success in the conflict.²⁷

And one that they have used against other nations in the West:

Of great importance here is the use of the global internet network to exert a massive, dedicated impact on the consciousness of the citizens of states that are the targets of aggression. Information resources have become one of the most effective types of weapon. Their extensive employment enables the situation in a country to be destabilized from within in a matter of days... In this manner, indirect and asymmetric actions and methods of conducting hybrid wars enable the opposing side to be deprived of its actual sovereignty without the state's territory being seized.²⁸

In this model of required state functions, adversaries avoid the diplomatically and financially expensive war making and protection aspects of government (the military M of the DIME model) and rather attack the extraction via assumedly innocuous methods such as social media. These nations enjoy operating in the gray area before the United States would escalate to conflict, effectively employing soft methods against U.S. decision-making (extraction) apparatuses and all while furthering their national standing in both territory and prestige. Rather than influence and interference for the sake of simple, standard statecraft, these information efforts occur in concert with expansion and questionable state motives including the first invasion in Europe since World War II.²⁹

Near-peer adversaries are stalling and distracting to delay military response; should the trend continue, they will likely force the West to a level where military confrontation is either ill-advised or untenable. These opening shots have been occurring in plain view as pundits, politicians, and military professionals—and the people writ-large—debate their existence, meaning, and interrelation in meaningful but ultimately

frivolous models, given the inaction that has thus far resulted. The first shots were fired years ago. The question of whether the United States chooses to truly acknowledge and act upon them remains.

Conclusion

In democracy, the institution of the electoral process and the choice of the people must be sacred. U.S. and western stakeholders must recognize, duly and totally, the attacks upon this central decision-making aspect: “Beliefs are not idle because the decisions we make on their basis have real consequences. If you believe false things about the world, and you make decisions based on those beliefs, then those decisions are unlikely to yield the outcomes you desire.”³⁰ This notion that adversaries have altered beliefs to enable strategic and operational military expansion and action—coupled with the attempt to modify beliefs across the West—should be the harbinger of a dire threat that circles outside, and now inside, our walls.

There are many suggestions as to the proper response to these attacks ranging from disrupting the flow of information to informing the citizenry.³¹ However, even when disinformation is labeled as false, many citizens and decision-makers chose to believe what they see, not necessarily the disclaimers that accompany memes and information.³² Short of stalling the spread of information (a difficult task), a holistic effort would be most effective—one that is informed by national-level apparatuses and enabled through partnership with private organizations. A purely governmental approach is inadequate; bureaucracy moves too slowly to defeat the disinformation, requiring additional stakeholders and partnerships.³³

The military cannot influence the domestic information space, but it, along with national-level intelligence organizations, can identify foreign behavior and sources.³⁴ Armed with this information, social media, and traditional media companies—who have already made great strides since 2016—must be convinced to associate propaganda sources with overt knowledge of the source. Readers’ exposure to knowledge of a source’s foreign or insidious origin may temper emotional response to the information.³⁵ Although it is difficult—due to the speed and dynamics of the online information ecosystem—to aggregate and display the most recent and relevant misinformation and disinformation, a figurative

“smoking kills” equivalent on sources like RT could eventually saturate the information environment in a positive direction.³⁶

Many platforms have already begun to implement a labeling approach to counter mis- and disinformation; this effort must continue, increase in scope, and leverage whole-of-government coordination to aid in identification and analysis of larger networks and changing tactics—allowing collective awareness among all friendly stakeholders. There is also a question of how to address existing disinformation that resides among legitimate domestic audiences as well as its recirculation via social media mechanics; this topic is beyond the scope of this study but represents the enduring threat that externally sourced disinformation can pose once narratives gain purchase in the West’s collective consciousness.³⁷

If pervasive symbols become persuasive, calling actual fake news by its name, repeatedly, could stick in citizens’ minds. This inoculation, paired with real-time, widespread deceptive persona identification and deletion, would attack both deceitful online personas and their ersatz news media payloads.³⁸ While watching and learning about an adversary who clearly has some new tricks to teach, domestic and allied stakeholders can begin to make things right: Addressing this threat, as a nation, and giving it due attention.

Unfortunately, the new baseline for interstate conflict has been set: the information realm has almost limitless potential for disruption, disinformation, and narrative manipulation. The legion has rallied, and the stakes made known. The free flow of ideas, Western democracy’s civic bulwark, has become a wall both subverted and co-opted by actors veiled with plausible deniability. This possibility, the notion that adversaries can use information against a system which theoretically benefits from its free flow, is neither novel nor nuanced; scholars and experts continue to raise the alarm to no avail.³⁹ Interestingly enough, the klaxons have been sounding for many years; in 1995, Colonel Richard Szafranski, with near prescience, claimed:

The United States should expect that its information systems are vulnerable to attack. It should further expect that attacks, when they come, may come in advance of any formal

declaration of hostile intent by an adversary state. When they come, the attacks will be prosecuted against both knowledge systems and belief systems [via technological means], aimed at influencing leadership choices. The knowledge and beliefs of leaders will be attacked both directly and indirectly. Noncombatants, those upon whom leaders depend for support and action, will be targets. This is what we have to look forward to in 2020 or sooner.⁴⁰

The year 2020 has given way to a new decade and a new era in which the reality of democratic vulnerabilities has been laid bare. The fields of friendly strife have been warped, converted into battlefields by those who would see benefit from divide et impera.⁴¹ Regarding those who seek to turn citizen against citizen, perhaps it is time the West views the interlopers as information environment invaders rather than embracing a grand and intoxicating ignorance granted by nearly a century of dominance. *Alea iacta est*. The die has been cast. It is how we face the legions now at and within our gates that will determine the Republic's fate.

Endnotes

- ¹ Carl von Clausewitz, *On War*, trans. J. J. Graham (Digireads.com Publishing, 2018, original work published 1832); Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* 9, no. 1 (1995): 3, <https://www.hsdl.org/?view&did=439843>.
- ² United States of America, Department of Justice, "Case 1:18-Cr-00032-DLF; Internet Research Agency Indictment," February 16, 2018, U.S. Department of Justice (2018), <https://www.justice.gov/file/1035477/download>; U.S. House of Representatives Permanent Select Committee on Intelligence, "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements Permanent Select Committee on Intelligence," n.d. accessed May 11, 2020, <https://intelligence.house.gov/social-media-content/>; U.S. Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election," n.d. accessed September 12, 2020, <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>; U.S. Senate Select Committee on Intelligence, "Open Hearing: Social Media Influence in the 2016 U.S. Election," November 1, 2017, <https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections>.
- ³ Ethan Zuckerman, "Mistrust, Efficacy and the New Civics: Understanding the Deep Roots of the Crisis of Faith in Journalism," *Knight Commission Workshop on Trust, Media and American Democracy*; Aspen Institute (2017), <https://dspace.mit.edu/bitstream/handle/1721.1/110987/deeprootsofmistrust.pdf?sequence=1&isAllowed=y>; Cary Funk et al., "Trust and Mistrust in Americans' Views of Scientific Experts," *Pew Research Center* (August 2019):

- https://www.newswise.com/pdf_docs/156460235934074_Embargoed%20REPORT%20trust%20scientists%207-30-19.pdf.
- 4 Paul Nakasone, "A Cyber Force for Persistent Operations," National Defense University, *Press Joint Force Quarterly* 92 (Spring 2019): 11, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf. General Paul M. Nakasone, Commander, USCYBERCOM, states that cyber means allow states to "augment their power, degrade or usurp the power of others, and gain strategic advantage through competition *without triggering armed response*. Our adversaries have learned this and are leveraging it against us."
 - 5 U.S. Office of the Director of National Intelligence (ODNI), *Assessing Russian Activities and Intentions in Recent US Elections* (ODNI, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf; Shona Ghosh, "The UK's Election Watchdog Has Now Questioned Google over Russian Meddling in Brexit," *Business Insider*, November 28, 2017, <https://www.businessinsider.com/electoral-commission-probe-google-over-russian-meddling-in-brexit-2017-11?r=DE&IR=T>; Todd Helmus et al., "Russian social media influence: Understanding Russian propaganda in Eastern Europe," *RAND Corporation* (2018), https://www.rand.org/pubs/research_reports/RR2237.html; Elizabeth Bodine-Baron et al., "Countering Russian Social Media Influence," *RAND Corporation* (2018), https://www.rand.org/pubs/research_reports/RR2740.html; Linda Robinson et al., "Modern Political Warfare: Current Practices and Possible Responses," *RAND Corporation* (2018), https://www.rand.org/pubs/research_reports/RR1772.html; Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It," *RAND Corporation* (2016), <https://www.rand.org/pubs/perspectives/PE198.html>; Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (Winter 2017): https://www.airuniversity.af.edu/portals/10/ssq/documents/volume-11_issue-4/prier.pdf.
 - 6 "Information Operations Archive," Alliance for Securing Democracy (2019), retrieved from <https://www.io-archive.org/#/>; Adam Badawy et al., "Characterizing the 2016 Russian IRA influence campaign," *Social Network Analysis and Mining* 9 (2019): 31, <https://doi.org/10.1007/s13278-019-0578-6>; Christopher Bail et al., "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *Proceedings of the National Academy of Sciences* 117 (2020): 243-250, <https://doi.org/10.1073/pnas.1906420116>; Marco Bastos and Johan Farkas, "Donald Trump Is My President!': The Internet Research Agency Propaganda Machine," *Social Media + Society* 5, no. 3 (August 2019), <https://doi.org/10.1177/2056305119865466>; Todd Helmus et al., "Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions," *RAND Corporation* (2020), https://www.rand.org/pubs/research_reports/RRA704-3.html; Kathleen Hall Jamieson, *CyberWar: How Russian hackers and trolls helped elect a president* (New York: Oxford University Press, 2018); Darren Linvill et al., "The Russians are Hacking my Brain! Investigating Russia's Internet Research Agency Twitter Tactics During the 2016 United States Presidential Campaign," *Computers in Human Behavior* 99, (Summer 2019): 292-300, <https://doi.org/10.1016/j.chb.2019.05.027>; Darren Linvill and Patrick Warren, "Troll factories: Manufacturing Specialized Disinformation on Twitter," *Political Communication* 37, no. 4 (Spring 2020): 1-21, <https://doi.org/10.1080/10584609.2020.1718257>; Darren Linvill and Patrick Warren, "Engaging with others: How the IRA Coordinated Information Operation Made Friends," *Harvard Kennedy School Misinformation Review* (April 2020), <https://doi.org/10.37016/mr-2020-011>; Josephine Lukito, "Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017," *Political Communication* 37, no. 2 (Fall 2019): 1-18, <https://doi.org/10.1080/10584609.2019.1661889>; Josephine Lukito et al., "The Wolves in Sheep's Clothing: How Russia's Internet Research Agency Tweets Appeared

- in U.S. News as Vox Populi,” *The International Journal of Press/Politics* 25, no. 2 (Winter 2019): 196–216, <https://doi.org/10.1177/1940161219895215>; Josephine Lukito and Chris Wells, “Most Major Outlets Have Used Russian Tweets as Sources for Partisan Opinion,” *Columbia Journalism Review*, March 8, 2018, <https://www.cjr.org/analysis/tweets-russia-news.php>; Ben Nimmo et al., “IRA Again: Unlucky Thirteen,” *Graphika*, September 1, 2020, <https://graphika.com/reports/ira-again-unlucky-thirteen/>; Yiping Xia et al., “Disinformation, Performed: Self-Presentation of a Russian IRA Account on Twitter,” *Information, Communication & Society* 22, no. 11 (Summer 2019): 1646–1664, <https://doi.org/10.1080/1369118X.2019.1621921>; Savvas Zannettou et al., “Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web,” *Companion Proceedings of the 2019 World Wide Web Conference on - WWW '19*, (January 2018): 218–226, <https://doi.org/10.1145/3308560.3316495>.
- ⁷ Alliance for Securing Democracy, “Information Operations Archive”; Ben Nimmo et al., “IRA Again”; ODNI, “Assessing Russian Activities.”
- ⁸ Some have described this stance as unnecessarily hawkish. While talons and olive branches both have their due place in geopolitical intrigue, this article’s authors (Jeffrey Baptist and Julian Gluck) seek to address the dire need for meaningful counteraction by highlighting this behavior for what it is. This article should not be viewed as a call to arms as much as it is an alarm signaling the gathering of an information storm. RAND termed “Virtual Societal Warfare” as a “New Form of Conflict” in chapter one of their report which shares the same name. Graduates of the United States Air Force Academy would be well familiar with this quotation in *Contrails* from Italian general and military theorist, Giulio Douhet: “Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.” Wisdom, then, is the act of recognizing an attack for what it is and appropriately responding without bias toward inaction or hostility. In this sense, we need not be doves nor hawks, but owls. Note: The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government. Michael Mazarr et al., “The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment,” *RAND Corporation* (2019), <https://doi.org/10.7249/RR2714>.
- ⁹ According to General Nakasone, there have been many changes within that organization alone regarding how they view and respond to great power competition and adversarial activity within U.S. discourse and networks. The authors do not imply that nothing is being done in this realm, but that the defense community should devote more attention to this issue as both defenders of the republic as well as its citizens, especially given the alarming gains others have made (Georgia, Crimea, election confusion). Success is reached when foreign influence does not easily gain purchase within the discourse. Paul Nakasone and Michael Sulmeyer, “How to Compete in Cyberspace: Cyber Command’s New Approach,” *Foreign Affairs*, August 25, 2020, <https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity>; Nakasone, “A Cyber Force.”
- ¹⁰ Refers to the common model of instruments of national power: Diplomatic, Informational, Military, and Economic (DIME), the (general) levers which a nation can use in interaction with its peers.
- ¹¹ Andrew Radin and Clint Reach, “Russian Views of the International Order,” *RAND Corporation* (2017), https://www.rand.org/pubs/research_reports/RR1826.html; Sarah Gamberini, “Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns,” *Joint Force Quarterly* 99 (Winter 2020), https://wmdcenter.ndu.edu/Portals/68/Documents/jfq/jfq-99/jfq-99-4-13_Gamberini.pdf?ver=Yoes_BQSVex7rNRLXvIo8Q%3d%3d; Sara Fischer, “Facebook says U.S. is the top target of disinformation campaigns,” *Axios*, June 1, 2021, <https://www.axios.com/facebook-disinformation-campaigns-globally-8859f7a8-f846-4899-93cb-dab635461c87.html>.

- ¹² “Peace for our time” is an infamous phrase notably used twice in British history, the second of which immediately preceded the tragic rise of Nazi Germany and conflict throughout Europe and the world. In his history of the Peloponnesian War, Thucydides describes a dialogue between representatives of the small island nation of Melos—allied with the Spartans—and the emissaries of the far stronger Athenian city-state, who sailed to Melos with offers of submission or eradication. Resolved to maintain independence and vassalage by the Athenians, Melos resisted and lost. As the Athenians stated: “[To fight in vain without winnable odds is not] well advised, the contest not being an equal one, with honor as the prize and shame as the penalty, but a question of self-preservation and of not resisting those who are far stronger than you are” 5.101. See Christopher Klein, “Chamberlain Declares ‘Peace for Our Time,’” *History*, January 3, 2020, <https://www.history.com/news/chamberlain-declares-peace-for-our-time-75-years-ago>; Thucydides, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*, Robert Strassler, eds. and trans. Richard Crawley (New York: Free Press), 2008.
- ¹³ Here, the authors refer to the already well-established history of influence but with focus on the emerging technology of Web 2.0 as a vector for influence, along with the shift toward using it in a widespread and outward (with regards to the country of origin) manner; psychological warfare and manipulation (including either dis or misinformation) was present in the Russia-Georgia war, the annexation of Crimea, and the subsequent tensions with and manipulation of U.S. parties, as well as the ongoing threat of hybrid warfare in the Baltic states: Michael Kofman et al., “Lessons from Russia’s Operations in Crimea and Eastern Ukraine,” *RAND Corporation*, (2017), <https://doi.org/10.7249/RR1498>; Anna Kowalewski, “Disinformation and Reflexive Control: The New Cold War,” *Georgetown Security Studies Review*, February 1, 2017, <https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/>; Mazarr et al., “Emerging Risk of Virtual Societal Warfare”; Michael Mazarr et al., “Hostile Social Manipulation: Present Realities and Emerging Trends,” *RAND Corporation*, 2019, <https://doi.org/10.7249/RR2713>; Andrew Radin, “Hybrid Warfare in the Baltics: Threats and Potential Responses,” *RAND Corporation*, 2017, <https://doi.org/10.7249/RR1577>; Sarah White, “Understanding Cyberwarfare: Lessons from the Russia-Georgia War,” *Modern War Institute at West Point*, March 20, 2018, <https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/>.
- ¹⁴ Two pieces that adequately focus on the two main actors in this area—China and Russia—describe the United States as “ceding” or abdicating primacy in the information environment. While this may be a technical oversimplification, the authors speak in terms of influencing perceptions and narratives regarding the legitimacy of cause and narrative. There are arguments for and against U.S. dominance in the other arenas; the authors make the assumption that the United States still maintains economic, diplomatic, and military primacy despite indicators that these measures may also be shifting (such as GDP, raw manpower and military size, sway in neoliberal institutions and organizations): Gordon G. Chang, “China’s Propaganda: Ludicrous, Malicious, Extremely Effective,” *Strategika* 72, May 5, 2021, <https://www.hoover.org/research/chinas-propaganda-ludicrous-malicious-extremely-effective>; Will DuVal and Adam Maisel, “It’s Time to Bring Back This Cold War Agency and Stop Ceding the Propaganda War to Russia,” *Modern War Institute at West Point*, August 15, 2017, <https://mwi.usma.edu/time-bring-back-cold-war-agency-stop-ceding-propaganda-war-russia/>.
- ¹⁵ William Evanina, “Statement by NCSC Director William Evanina: Election threat update for the American public,” United States Office of the Director of National Intelligence, accessed February 20, 2021, <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>; Garth Jowett and Victoria O’Donnell, *Propaganda and Persuasion* (Sage Publications, 2019); Jamieson, *Cyberwar*; Radin, “Hybrid Warfare in the Baltics.” The confluence of hacking and social engineering is present in almost every case of Russian intervention,

likely related to Russian strategic emphasis on irregular warfare and political subversion (what many would term propaganda or psychological warfare). Russian doctrine seems uniquely angled to focus on a major vulnerability in nations that value freedom of information and rely on democratic functions; information operations and political manipulation can achieve vastly different effects in countries where the state does not actively and strictly control the flow of information, especially from external sources (controlling information flow described in Jowett and O'Donnell's book).

- ¹⁶ Every U.S. president (and some of their campaign opponents) since September 11, 2001, has either campaigned claiming they would decrease deployed troop levels or has vowed to do so in at least one of their terms: "Bush Boasts About Bringing Troops Home," *CBS News*, September 9, 2008: <https://www.cbsnews.com/news/bush-boasts-about-bringing-troops-home/>; Robin Toner, "The 2004 Campaign: The Massachusetts Senator; Kerry Redoubles His Attack Over the War," *The New York Times*, May 29, 2004, <https://www.nytimes.com/2004/05/29/us/2004-campaign-massachusetts-senator-kerry-redoubles-his-attack-over-war.html>; Brian Montopoli, "Obama Announces End of Iraq War, Troops to Return Home by Year End," *CBS News*, October 21, 2011, <https://www.cbsnews.com/news/obama-announces-end-of-iraq-war-troops-to-return-home-by-year-end/>; David Jackson, "McCain: Win War in Iraq First, Then Bring Troops Home," *ABC News*, August 18, 2008, <https://abcnews.go.com/Politics/story?id=5606016&page=1>; Jacob Pramuk, "What Trump Said About Afghanistan Before He Became President," *CNBC*, August 21, 2017, <https://www.cnbc.com/2017/08/21/what-trump-said-about-afghanistan-before-he-became-president.html>; A. Blake, "2 Big Problems with Hillary Clinton's No-Ground-Troops Pledge," *The Washington Post*, September 8, 2016, <https://www.washingtonpost.com/news/the-fix/wp/2016/09/08/the-two-biggest-problems-with-hillary-clintons-pledge-to-never-send-ground-troops-into-iraq-and-syria/>.
- ¹⁷ Tilly describes this on page 263 in the cited text. However, he focuses on states during the last thousand years (specifically, the centuries before modern day) and the evolution of states toward different roles (such as adjudication and material distribution which were previously left to other organizations, such as the Church). These terms vary between states and throughout time but the ability to extract the means of major requirements has remained constant as a definition. A state simply *must* be able to extract the resources needed to maintain borders and establish some level of control (external or internal); failure to do so would result in everything from the inability to field armies to the lack of producing infrastructure. Tilly describes the addition of these activities as compounding the others, leading to increased synergy overall. In this way (and in the authors' determination), the hyper-efficiency of rational megastates, which rose with industrialism, became possible and cemented the requirement of extraction within other state roles and vice versa: Charles Tilly, "Coercion, Capital, and European States," *Contemporary Sociological Theory*, eds. Craig Calhoun et al. (West Sussex, UK: John Wiley & Sons, Ltd, 2012), 251-265.
- ¹⁸ Extraction, in this sense and for democratic nations, is different from the coercive implications of the word itself. There are many ways in which all states extract resources and behaviors from their populations (e.g. taxes, conscription); democratic extraction is not simply a compulsion of the people from the state, but, rather, a compulsion of the people from the state which is of the people. This circular feedback in governance is an ideological pillar of U.S. culture and is specifically the type of extraction that disinformation can impact. Whereas authoritarian governments are not as limited by popular public sentiment (assuming they can provide for internal security and put down any grassroots unrest; this does not speak to mid-level sources of power like bureaucrats or the modern equivalent of "duchies"), the West is more sensitive to the will of its people, the voting populace, the observed target of disinformation attacks similar to those conducted by the Russian IRA.
- ¹⁹ White goes into detail on hybrid warfare and how cyber enabled joint operations and psychological manipulation, a combination which set the tone for integrated operations in Crimea; online enabled operations in Georgia have not been directly linked to the

Russian government technically or legally but “patriotic hackers” support, which aligned with Russian military operations, focused on psychological effects and aided conventional outcomes. Thus, the authors view these groups as, effectively, the same: White, *Understanding Cyberwarfare*.

- ²⁰ Kofman et al. suggest social media and psychological warfare were used to generate support for Russian activity in Crimea along with domestic Russian messaging. In this, the United States continues to see a theme of influence operations integrated in hybrid warfare, confusing or stalling any meaningful resistance from noncombatants or belligerents who also seek to mobilize popular support to counter conventional military activity. This determination of (then) Ukrainian President Yanukovich’s relationship with Russia is due to his refusal to sign the Association Agreement with the EU despite popular Ukrainian support, resulting brutal policies against protesters, and subsequent travel to Russia before his impeachment and Russian invasion of Crimea: Kofman et al., “Lessons from Russian Operations”; “Maidan Protest Movement,” Britannica, accessed November 4, 2020, <https://www.britannica.com/place/Ukraine/The-Maidan-protest-movement>.
- ²¹ U.S. Department of Justice, “Internet Research Agency Indictment”; U.S. House of Representatives, “Exposing Russia’s Effort”; ODNI, “Assessing Russian Activities”; U.S. Senate, “Russian Active Measures”; U.S. Senate, “Open Hearing”; Jamieson, *Cyberwar*.
- ²² Bail et al., “Assessing the Russian Internet Research Agency’s Impact,” 250; Linvill et al., “THE RUSSIANS ARE HACKING MY BRAIN,” 292-300; Linvill, and Warren, “Troll Factories,” 1-21; Linvill and Warren, “Engaging with Others”; Lukito, “Coordinating a Multi-Platform Disinformation Campaign,” 1-18; Lukito et al., “The Wolves in Sheep’s Clothing,” 196-216; Lukito and Wells, “Most Major Outlets”; Xia et al., “Disinformation Performed,” 1646-1664; Helmus et al., “Russian Propaganda Hits Its Mark.”
- ²³ Networks of varying complexity and with diverse tactics continue to operate within the information sphere. In 2020, Nimmo et al. discovered a sophisticated article creation and dissemination network using comparatively advanced tactics. Standard social media personas from around the world continue influence operations through coordinated inauthentic behavior as recently as July 2021 (Facebook). Nimmo et al., “IRA again”; Facebook, “July 2021 Coordinated Inauthentic Behavior Report,” August, 2021, <https://about.fb.com/wp-content/uploads/2021/08/July-2021-CIB-Report.pdf>.
- ²⁴ Radin and Reach, “Russian Views.”
- ²⁵ Keir Giles, “Handbook of Russian Information Warfare,” NATO Defense College (October 2018), <https://www.ndc.nato.int/news/news.php?icode=995>.
- ²⁶ The authors do not mean to imply here that sanctions or diplomatic activities should be considered a form of attack, though many other nations wrongfully claim that they are. Nations have no obligation to conduct trade with or diplomatically support any nation; however, this is not active intervention. The difference here is that informational attacks (especially those that affect government) are not merely the decision of inaction or appropriate censure; they are provocative in that they require active interference with the intent to corrupt decision-making.
- ²⁷ Robinson et al., “Modern Political Warfare,” 43; Radin, “Hybrid Warfare in the Baltics,” 9.
- ²⁸ Giles, “Handbook of Russian Information Warfare.”
- ²⁹ In this regard, the People’s Republic of China (PRC) has also engaged in worrisome disinformation practices. While this piece focuses primarily on Russian activities, the authors do not want to downplay the significant indicators of PRC disinformation and influence efforts across the globe. Sources point to PRC disinformation and propaganda outreach to support favorable narratives and counter unfavorable themes regarding South China Sea expansion and COVID response, Uighur policies, and other items of national prestige. Most recently, the U.S. Department of State released a statement (through remarks from their office of East Asian and Pacific affairs) claiming that “Influence and interference operations are fundamental to how the Chinese Communist Part engages the world... its strategy is aggressive and intrusive”: Chang, “China’s Propaganda”; Audrye Wong, “COVID-19 and China’s Information Diplomacy in

-
- Southeast Asia,” *Brookings Institution*, September 3, 2020, <https://www.brookings.edu/blog/order-from-chaos/2020/09/03/covid-19-and-chinas-information-diplomacy-in-southeast-asia/>; Peter Mattis, “China’s ‘Three Warfares’ in Perspective,” *War on the Rocks*, January 30, 2018, <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>; Mazarr et al., “Hostile Social Manipulation”; Greg Torode and Mike Collett-White, “Ahead of Key Court Ruling, Beijing in Propaganda Overdrive,” *Reuters*, July 3, 2016, <https://www.reuters.com/article/us-southchinasea-ruling/ahead-of-key-court-ruling-beijing-in-propaganda-overdrive-idUSKCN0ZJ117>; “Covert, Coercive, and Corrupting: Countering the Chinese Communist Party’s Malign Influence in Free Societies,” Hoover Institution, Stanford University, Asia Society Virtual, October 30, 2020, <https://www.hoover.org/research/covert-coercive-and-corrupt-countering-chinese-communist-party-malign-influence-free>.
- ³⁰ Cailin O’Connor and James Owen Weatherall, *Misinformation Age* (New Haven: Yale University Press, 2019): 6.
- ³¹ General Nakasone, Commander, USCYBERCOM, and Dr. Michael Sulmeyer discuss “proactive defense” and “forward defense.” They describe this method as including possible practices such as “...publicly releasing adversary malware” to facilitate detection and mitigation and “...cyber effects operations [which] allow Cyber Command to disrupt and degrade the capabilities our adversaries use to conduct attacks.” These methods are not unlike or unrelated to “disrupting the flow of information,” as they have been termed, but also address many of the cyber issues which do not focus on influence as a central pillar of their effects: Nakasone and Sulmeyer, “How to Compete in Cyberspace;” Nakasone, “A Cyber Force.”
- ³² Paul and Matthews, “The Russian ‘Firehose of Falsehood.’”
- ³³ Doowan Lee, “The United States Isn’t Doomed to Lose the Information Wars,” *Foreign Policy*, October 16, 2020, <https://foreignpolicy.com/2020/10/16/us-election-interference-disinformation-china-russia-information-warfare/?fbclid=IwAR3VJbcMWKyIUazFYUFA739zLBHsX8RgGAbNkhVHoxeC5Or5q7feHcoRzMY>; Paul Nakasone, *Statement of General Paul M. Nakasone, Commander, United States Cyber Command, Before the Senate Committee on Armed Services*, U.S. Senate Committee on Armed Services, February 14, 2019, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.
- ³⁴ Public affairs with the intent to inform is the primary method with which the military can interact with the domestic information environment; military influence efforts, in Joint Publication 3-13, do not engage with domestic U.S. audiences.
- ³⁵ Helmus et al., T. C., “Russian Propaganda Hits Its Mark.”
- ³⁶ Russia Today (RT), a Russian state-run media outlet implicated by multiple sources in the IRA/Russian disinformation apparatus: ODNI, “Assessing Russian Activities”; Bodine-Baron et al., “Countering Russian Social Media Influence”; Robinson et al., “Modern Political Warfare.”
- ³⁷ Yaël Eisenstat, “Facebook is Ripe for Manipulation and Viral Misinformation,” Interview by Ian Tucker, *The Guardian*, July 26, 2020, <https://www.theguardian.com/technology/2020/jul/26/yael-eisenstat-facebook-is-ripe-for-manipulation-and-viral-misinformation>; Yaël Eisenstat, “How to Hold Social Media Accountable for Undermining Democracy,” *Harvard Business Review*, January 11, 2021, <https://hbr.org/2021/01/how-to-hold-social-media-accountable-for-undermining-democracy>.
- ³⁸ At the time of writing, many social media companies and the ODNI seem to be making great strides in inoculating users and communicating issues; this must continue and expand in scope. Unfortunately, there are still many individuals (anecdotally, from the standpoint of the authors) who continue to consume and pass on disinformation; once this gets into domestic streams, it becomes near impossible to address and raises questions of First Amendment rights regarding its censure depending on the initiating agents (government or private industry).
- ³⁹ Gamberini, “Social Media Weaponization”; Eisenstat, “How to Hold Social Media Accountable”; Eisenstat, “Facebook is Ripe for Manipulation.”

⁴⁰ Szafranski, “A Theory of Information Warfare,” 10-11.

⁴¹ Here the authors reference a now commonly understood phenomena within groups of three or more. This concept was first explored sociologically at a micro, individual level; here, it references larger groups which, when reduced to common units of analysis (large groups interacting in a collective sense) allows it to maintain validity: Georg Simmel, “The Dyad and the Triad,” *Classical Sociological Theory*, eds. Craig Calhoun et al. (West Sussex, UK: John Wiley & Sons, Ltd, 2012): 382-395.