National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

RUSSIAN INFLUENCE OPERATIONS: 'HYBRID WARFARE' OR MODERN STATECRAFT, AND ITS IMPACT TO THE WEST

Major Nicholas Culver

JCSP 46

Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 46

Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

RUSSIAN INFLUENCE OPERATIONS: 'HYBRID WARFARE' OR MODERN STATECRAFT, AND ITS IMPACT TO THE WEST

By Major Nicholas Culver

Word Count: 4,950

Nombre de mots : 4.950

RUSSIAN INFLUENCE OPERATIONS: "HYBRID WARFARE" OR MODERN STATECRAFT, AND ITS IMPACT TO THE WEST

INTRODUCTION

Chief of the Russian General Staff General Valery Gerasimov's February 2013 article in *Military-Industrial Kurier* was an unexpected catalyst for change among Western strategists. Entitled, "The Value of Science Is in the Foresight", upended previously accepted theories and created no shortage of controversy amongst Western academics and tacticians.[1] One such point of contention surrounds the article's intent. Some theorists interpret Gerasimov's article as a warfare vision statement, that calls upon a convergence of conventional and unconventional means — 'hybrid warfare — to achieve Russia's strategic goals.'[2] This perception of Gerasimov's article led to a frenetic evolution of Western theories; these new theories explained Russian 'hybrid warfare' as a means of attacking the conventionally superior West. Yet, 'hybrid warfare' is just one of many terms given to similar but different interpretations of Russian influence operations. These varying and often disparate terms used to describe Russian influence — 'hybrid warfare', the 'Next Generation of Warfare' (NGW), or 'gray zone' operations to name a few — are used interchangeably, resulting in widely errant Western misconceptions and inaccurate explanations of Russian strategic methods and objectives.

Therefore, a more detailed analysis and examination of Russia's overall strategy, aims and intentions are necessary to alleviate contention and confusion amongst Western

---

[1] Charles K. Bartles, "(PDF) Getting Gerasimov Right," Research Gate. *Military Review*, (January 2016): 30, https://www.researchgate.net/publication/32-9933852_Getting_Gerasimov_Right; Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," trans. Robert Coalson, *Military-Industrial Kurier*, 27 February 2013, accessed 4 April 2020, https://jmc.msu.edu/50th/download/21-conflict.pdf.

[2] Bartles, "(PDF) Getting Gerasimov Right," 30.

strategists and adequately frame the problem — namely, that Russia employs statecraft vice 'hybrid warfare' to achieve their strategic objectives. However, without a coadunate understanding of how Russia exercises influence operations against the West, subsequent mitigating strategies may prove ineffectual. That is to say, is Russia purposefully employing 'hybrid warfare' against Western democracies and its allies or is it evoking influence through a combination of national capabilities and statecraft? Furthermore, if the US and its allies are unable to articulate Russian influence strategy, how are they to going to effectively and efficiently combat it?

Russia is clearly employing information and cyber operations in an attempt to weaken, discredit, and debilitate Western influence. Accordingly, this paper will argue that Russian actions must be further scrutinized by the US and its allies in order to mitigate Russia's influence and gain the advantage in the information and cyber domains. Initially, this paper will emphasize the need to adequately frame the problem by examining the controversy surrounding 'hybrid warfare' and other like-terms, vis-à-vis whether the Russians are using 'hybrid warfare' or a combination of national capabilities and statecraft influence. Next, it will delve into recent and relevant Russian influence activities in the information and cyber domains. Finally, it will conclude by discussing ways the US and its allies can mitigate Russian influence and gain a lasting advantage in this space.

WHAT'S IN A NAME: 'HYBRID WARFARE', 'GRAY ZONE' OPERATIONS, THE 'NEXT GENERATION OF WARFARE (NGW)', OR MODERN STATECRAFT?

'Hybrid warfare', 'gray zone' operations, and 'NGW'

Russian 'hybrid warfare' is often characterized as a type of warfare that

extensively uses "subversive instruments, many of which are non-military, to further Russian national interests."[3] The 'hybrid' concept of 'hybrid warfare' is an amalgamation of conventional, unconventional, political, and informational means whose sum supposedly far exceeds its parts.[4] Further, depending on who you read, the terms 'gray zone', 'hybrid warfare', or 'NGW' are often wrongly used interchangeably; yet, they commonly share three specific areas along the spectrum of conflict. The right side of the spectrum encompasses attributable aggressions aimed at US deterrence.[5] The left side of the spectrum houses "persistent actions" that either do not surpass the moderate or extreme levels of the spectrum of warfare, or are widely unattributable.[6] Last, the middle of the spectrum — where 'hybrid warfare' and its counterparts are believed to reside — which comprises actions that are difficult to articulate, define, and defend against.[7] Despite which terms are used to describe Russian warfare, they all have unifying characteristics.

One commonality among these terms is the optimization of resource usage versus reward. Moscow allocates their resources to maximize potential gain and minimize loss; Russia does this because they cannot compete with the West conventionally.[8] Ultimately, allowing Russia to gain strategic advantages "without overt use of military power if

---

[3] Christopher S. Chivvis, *Understanding Russian "Hybrid Warfare" And What Can Be Done About It* (Santa Monica, CA: RAND Corporation, 2017), 1.

[4] Michael Kofman, and Matthew Rojansky, "A Closer Look at Russia's 'Hybrid War (PDF),'" Wilson Center, (April 2015): 2, https://www.wilsoncen-ter.org/sites/default/files/7-KENNAN CABLE-ROJANSKY KOFMAN.pdf.

[5] Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND Corporation, 2019), xvi.

[6] *Ibid.*

[7] *Ibid.*

[8] Chivvis, *Understanding Russian "Hybrid Warfare"*…, 2.

possible" with low-cost, high gain tools like disinformation and cyber warfare.[9] Through these niche tools, Russia can compete effectively and bring their strengths to bear against the West. Secondly, Russia actively targets Western populations through information operations and statecraft; they leverage and manipulate already existing political and social frameworks to exact influence.[10] A key factor in Russia's success is the ambiguity of their operations and their profound ability to covertly influence large target populations.

By harnessing uncertainty and expertly applying unconventional tactics, Russia is able to incrementally ratchet up aggression against the US and its allies. These tactics often include cyber-attacks, disinformation campaigns, and political warfare; and are "conducted in ways that are meant to make proper attribution of the responsible party difficult to nail down."[11] Moscow applies these unconventional methods "to achieve [sic] gains without escalating to overt warfare, without crossing established red-lines, and thus without exposing the practitioner to the penalties and risks that such escalation might bring."[12] What are Russia's intentions? Their goals are quite clear; they intend to induce confusion and inflict damage below that of the "threshold of armed conflict" and blur the lines between peace and conventional war.[13]

Despite disagreement amongst academics as to what terms best describe Russian ambiguous operations, all are in resounding agreement of Russia's objective. The consensus is that Russia is using whatever capabilities are at their disposal to discredit the

---

[9] *Ibid.*

[10] *Ibid.*

[11] Hal Brands, "Paradoxes of the Gray Zone (PDF)," Foreign Policy Research Institute, (February 5, 2016): 2, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

[12] *Ibid.*

[13] Morris, *Gaining Competitive Advantage in the Gray Zone*…, iii.

US as a means of "expressing dissatisfaction with aspects of the regional power and territorial status quo."[14] By targeting the US through multiple domains and escaping attribution, Russia subversively erodes Western influence below the threshold of war.[15] However, the idea of influence operations below the spectrum of war is not a novel concept. Throughout history, various actors sought to balance their gain "without incurring the costs and risks of overt aggression" — akin to the sponsoring of terrorism by Iran in the 1980s.[16]

Many critics of 'hybrid warfare' recognize that the concept is far from new. Furthermore, it is not surprising that "indirect approaches and unconventional tactics, such as the use of proxy fighters, information warfare, psychological operations or sabotage, have been tools in the military arsenal" in most modern militaries for a number of years.[17] Notwithstanding, General Gerasimov's article brought about a resurgence of theories and terms to the contrary. These "new" theories appear strangely like the theories of old, but with flashy name changes and capabilities like cyber.[18] Nevertheless, if the West falls victim to expressing these complex activities in general terms like 'hybrid warfare', 'NGW', or 'gray zone' operations interchangeably, they do so at their own peril.

A disturbing commonality among all these terms is Russia's application of "multiple instruments of power and influence, with an emphasis on non-military tools, to pursue its national interests outside its borders — often at the expense of U.S. interests

---

[14] *Ibid.,* 14.
[15] *Ibid.*
[16] Brands, "Paradoxes of the Gray Zone (PDF)," 5.
[17] Bettina Renz, "Russia and 'Hybrid Warfare'," *Contemporary Politics* 22, no. 3 (2016): 284, https://doi.org/10.1080/13569775.2016.1201316.
[18] *Ibid.*

and those of U.S. allies."[19] Russia is actively targeting the US and its allies through subversive and undetectable means near continuously, as seen in recent election meddling. But, instead of taking a holistic approach toward Russia's strategy and recognizing their fluidity, strategists are all too quickly reducing it to a single buzzword concept like 'hybrid warfare'. This allure to categorize and oversimplify Russian strategy could potentially lead to flawed assumptions and failed counter-tactics.[20] Consequently, 'hybrid warfare' "has become [one of many] catchall phrase[s]" that has invariably "done more harm than good to our understanding of developments in Russian military and defence policy" because it errantly ignores Russian history and examines their policies devoid of context.[21] Which brings into question whether these terms are just statecraft with a trendy name.

Statecraft

For the purpose of granularity, it is best to begin with an explanation of what is meant by statecraft. Statecraft "is about managing reality, coupling ends and means in ways that advance a country's interests."[22] What it is not, is a pure military or pure diplomatic application; instead, statecraft is a confluence of the political, diplomatic, and military efforts to achieve the same ends.[23] Again, this is not new, as Russia has used combinations of political, diplomatic, military capabilities, and national strengths for influence well before the notion of 'hybrid warfare'.[24] In fact, Russia's roots are easily

---

[19] Chivvis, *Understanding Russian "Hybrid Warfare"*…, 1.

[20] Mark Galeotti, "The Mythical 'Gerasimov Doctrine' and the Language of Threat," *Critical Studies on Security* 7, no. 2 (27 February 2018): 158, https://doi.org/10.1080/21624887.2018.1441623.

[21] Renz, "Russia and 'Hybrid Warfare'," 296-297.

[22] Angelo M.Codevilla, "Tools of Statecraft: Diplomacy and War," Foreign Policy Research Institute, (15 January 2008): 1, https://www.fpri.org/article/2008/01/tools-of-statecraft-diplomacy-and-war/.

[23] *Ibid.*

[24] Kofman, "A Closer Look at Russia's 'Hybrid War (PDF)'," 2.

traceable to statecraft tactics applied by the former Soviet Union — such as subversion, espionage and the application of special forces which all culminate in influence by whatever means available.[25] Again, statecraft is far from neoteric.

What is comparatively new in the fight against the US, are the environments and mediums of influence; chiefly, Russia is using "low-cost and low-risk" methods in the ever-expanding cyber and information spaces.[26] Attacks in these mediums coincide with Russia's realization of their strengths and capabilities. These domains allow the Kremlin to "impose its political will, without traditional decisive battlefield victory" and gain an overwhelming strategic advantage through "a skillful orchestration of military and non-military (political, psychological, ideological, informational) means" instead of engaging in conventional warfighting against a stronger US.[27] Consequently, US influence strategies may be partially to blame for these changes in Russian strategy.

Potential US blame stems from the notion that Russian influence operations evolved through observation and emulation of Western tactics. By modeling their influence tactics after US statecraft, Russia can use these newly-learned skillsets against the West.[28] Thus, it follows that the US's application of statecraft may be partially culpable in shaping Russia's "asymmetrical and indirect actions of political, economic, informational, and technological" capabilities against the West.[29] Moreover, Russia's adroit use of statecraft provides a powerful mechanism for influence that minimizes risk,

---

[25] Chivvis, *Understanding Russian "Hybrid Warfare"*…, 7.

[26] Stacie L. Pettyjohn and Becca Wasser, *Competing in the Gray Zone: Russian Tactics and Western Responses* (Santa Monica, CA: RAND Corporation, 2020), 23.

[27] Dmitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy (PDF)," *IFRI Security Studies*, (November 2015): 34, https://www.ifri.org/sites/default-/files/atoms/files/pp54adamsky.pdf.

[28] *Ibid.,* 20.

[29] *Ibid.,* 24.

maximizes gain, and remains highly cost effective.[30]

Russian disinformation campaigns depend heavily on economical force multipliers like espionage operations, cyber hacking and information operations to disrupt international order and discredit the US.[31] Information operations and Russian military strategy are inextricably intertwined; despite their close relationship, these operations extend far beyond military application and permeate Russia's entire government. Their operations require autonomous functioning and mutual supportability. Whether functioning together or independently, they have distinct and necessary ties to the Russian government for their funding, "intelligence and espionage capabilities, criminal networks of cyberhackers", media outlets, and state-sponsored online trolls to discredit and degrade US global influence.[32]

Russia's levers of influence represent a confluence of mutually supportive, covert and overt means that construct and operate in, by, and through a "very complex and sophisticated disinformation system."[33] Their expert practice of coordinated statecraft recruits and enlists hackers, proxy actors, "oligarchs, civil society groups, cyber criminals, intelligence agencies, private companies, and political actors" to serve Russian strategic objectives.[34] Yet, terms like 'hybrid warfare', 'NGW' or 'gray zone' operations, used primarily by Western strategists, have done little to adequately frame the problem.

---

[30] Mary Ellen Connell and Ryan Evans, "Russia's 'Ambiguous Warfare' and Implications for the U.S Marine Corps (PDF)," CNA, (May 2015): 7, https://www.cna.org/CNA_files/PDF/DOP-2015-U-010447-Final.pdf.

[31] Max Bergmann and Carolyn Kenney, "War by Other Means: Russian Active Measures and the Weaponization of Information (PDF)," The Moscow Project, (6 June 2017): 2-3, https://themoscowproject.org/reports/war-means-russian-active-measures-weaponization-information/.

[32] *Ibid.,* 9.

[33] *Ibid.*

[34] Alina Polyakova and Spencer P. Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition (PDF)," Brookings Institute, (March 2018): 3. https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf.

By collectively understanding how Russia accomplishes influence operations, Western strategists can concurrently frame the problem and achieve unity of purpose. That is to say, failing to recognize Russian influence as a form of statecraft places the US and its allies in a precarious and disadvantageous position that inadvertently flaunts Russian strategy as revolutionary. By and large, Western strategists should view Russian activities through the lens of statecraft, instead of reintroducing and reclassifying already existent strategies; this is especially important if the US and its allies are to deter and defeat Russian influence in the information and cyber domains.

RUSSIAN INFLUENCE METHODS, ACTORS, AND RELEVANT ACTIVITIES IN THE INFORMATION AND CYBER DOMAIN

Make no mistake about it, Russia's aim is to degrade the Western population's trust and erode "the authenticity of information crucial to a healthy and lively democratic society" by any means available.[35] Russia accomplishes these objectives by shrewdly applying disinformation in "sophisticated and complex information operations", resulting in overwhelmingly powerful effects along "multiple and mutually reinforcing lines of effort — through cyber-hacking, the employment of cyber trolls, and overt propaganda outlets."[36] Russian information operations rely on communicating mass disinformation along multiple channels through text, video and audio; this disinformation is distributed through network operatives and "propagated via the Internet, social media, satellite television, and traditional radio and television broadcasting."[37] The success of Russian disinformation depends on volume vice precision and size of their cyber operative

[35] Bergmann, "War by Other Means…," 4.
[36] *Ibid.*
[37] Christopher Paul and Miriam Matthews, "Russia's 'Firehose of Falsehood' Propaganda Model," (RAND Corporation, 11 July 2016): 2, https://www.rand.org/pubs/ perspectives/PE198.html.

network footprint.

Information and cyber operatives, known as "trolls", are recruited through chat rooms and online discussion forums; the "trolls" are shell accounts supported by the Kremlin to disseminate disinformation and inject discord through social media.[38] Moreover, evidence suggests that these Russian trolls are purportedly directed by their handlers to post 135 comments daily for proficiency.[39] Russia is continuously improving their cyber hacking capabilities as a means of degrading, denying, and disrupting Western influence in the most economical manner possible.[40]

These strategic goals are accomplished by their Main Intelligence Directorate (GRU) who employ hackers like Fancy Bear, APT28, and STRONTIUM; these nefarious networks are able to operate with impunity and conduct data breaching, cyber attacks, and disinformation campaigns against a conventionally stronger West.[41] Further complicating matters, is Russia's adept use of Virtual Private Networks (VPNs) as a mean of spoofing and obfuscating their actual locations.[42] By masking their whereabouts, GRU sponsored trolls are able to spoof legitimate locations where news stories may be originating and inject disinformation — while giving the air of legitimacy.[43] Since 2014, the GRU has been steadily increasing their scope and magnitude of activities; they have expanded their tactics and diversified their operations, allowing for increased information theft and widened distribution.[44] These cyber operations were often conducted under the

---

[38] *Ibid.*
[39] *Ibid.*
[40] Bergmann, "War by Other Means…," 10.
[41] *Ibid.*, 10-11.
[42] Dave Lee, "The Tactics of a Russian Troll Farm", *BBC News*, 16 February 2018, https://www.bbc.com/news/technology-43093390.
[43] *Ibid.*
[44] The Select Committee on Intelligence of the United States Senate, *Disinformation: A Primer in Russian Active Measures and Influence Campaigns Panel II*, (Washington, DC: U.S. Government Printing

guise of shell personas used to, "obfuscate their true identity, provide plausible deniability, and to create the perception of credibility."[45] Ultimately, sowing the seeds of doubt in the general public.

To accomplish these objectives, hackers gain access to compromising information against prominent Western individuals and organizations and use their newly acquired knowledge to discredit and denigrate key institutions.[46] Russia's goal is to manipulate the narrative to best serve their national interests and create social disharmony within their target countries; this same framework was used during the 2016 elections by the Kremlin to create discord within the United States, France, and Germany.[47]

Russia creates and fosters dissonance through their networks of cyber hackers, also known as troll farms; they have specific lines of operation, and prioritized objectives tracked by the Kremlin.[48] These seedy networks control the narrative by inundating the space with massive amounts of disinformation, free of cumbersome chains of command or rules of engagement.[49] Furthermore, their cyber breaches are cleverly waged without encroaching on US national security. More importantly, by staying just below this threshold, Russia is able to avoid Western retaliation.[50] Russian influence operations actually work best in unregulated and lawless spaces because their actions, more often than not, overstep established legal limits.[51]

Office, 30 March 2017): 8, https:// www.intelligence.senate.gov/sites/default/-files/hearings/S Hrg 115-40 Pt 2.pdf.

[45] *Ibid.*

[46] Polyakova, "The Future of Political Warfare…," 13.

[47] *Ibid.*

[48] Bergmann, "War by Other Means…," 13.

[49] *Ibid.,* 14.

[50] Veronika Spalkova, "Influence of Russian Disinformation Operations: Specific Examples in Data and Numbers," (Kremlin Watch Report, 2018): 12, https://www.europeanvalues.net/wp-content/uploads/2019/02/Influence-of-Russian-Disinformation-Operations-Specific-examples-in-data-and-numbers.pdf.

[51] *Ibid.*

By capitalizing on cyberspace's lack of regulations, APT28 has repeatedly exploited, infiltrated, accessed, and stolen data from United States' networks.[52] Additionally, Russia's highly skilled cyber warriors are notoriously agile and capable of vanishing if there is any indication of monitoring. Often, their tactics and procedures are difficult to observe, except in extreme circumstances where the hackers want to display a capability.[53] Russian influence operations are occurring near-continuously against the US and its allies and represent a clear and persistent threat. Russia's focus is discrediting and disrupting the West by creating, manipulating, and propagating disinformation.

One such example of Russian disinformation occurred on 11 September 2014, "when the Office of Homeland Security received reports that there had been a chemical plant explosion in Centerville, Louisiana."[54] The purported explosion began to flood Twitter, YouTube, and Facebook; there were massive numbers of 'people' uploading eyewitness videos and reports of the explosion.[55] However, US investigators found that the entire explosion, fake videos, witness reports, and user accounts were part of an elaborate ruse conducted by Russia's Internet Research Agency (IRA); the hoax was a well-orchestrated campaign "designed to sow public distrust of the U.S. media and U.S. government institutions."[56] However, discord is just one of several strategic objectives of Russian influence operations; they have also used cyberspace as a means of demonstrating their capabilities and asserting dominance. As was the case in Estonia in 2007.

---

[52] The Select Committee on Intelligence of the United States Senate, *Disinformation: A Primer in Russian…*, 2.

[53] *Ibid.,* 4.

[54] Bergmann, "War by Other Means…," 21.

[55] *Ibid.*

[56] *Ibid.*

On 27 April 2007, the government of Estonia took down a bronze statue from the capital city of Tallinn; the decision to remove the statue was incredibly controversial because the monument was erected by the former Soviet Union as a memorial to their fallen soldiers lost in World War II.[57] Conversely, the Estonians associated the statue with former Soviet Union oppression and control which led to their eventual decision to remove the statue — despite vehement protest from the Russian government.[58] The Russian government promised stern reprisal if the statue was removed and such actions would be "disastrous for Estonians."[59] Nevertheless, the statue was removed and thus began the infamous digital assault on Estonians.[60] The attacks on Estonia occurred from the screens of "hundreds of thousands of individual computers from around the world that had been hijacked previously by hackers"; these computers, surreptitiously commandeered by bad actors, overloaded chosen Internet Protocol addresses with data in order to deny and disrupt Estonia's digital pattern of life.[61]

On May 8th, Estonia's servers and digital infrastructure were bombarded by over 4 million packets of data per second; their electronic systems were inundated by 1 million precisely aimed computers.[62] By the middle of May 2007, the digital attacks on Estonia's infrastructure ended just as abruptly as they began — the malicious scripts had been set

---

[57] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 5 June 2017, https://www.wired.com/2007/08/ff-estonia/; Damien McGuinness, "How a Cyber Attack Transformed Estonia," *BBC News*, 17 April 2017. https://www.bbc.com/news/39655415.

[58] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 50–51. https://doi.org/10.5038/1944-0472.4.2.3.

[59] Davis, "Hackers Take Down the Most Wired Country in Europe."

[60] Davis, "Hackers Take Down the Most Wired Country in Europe"; McGuinness, "How a Cyber Attack Transformed Estonia…"; Herzog, "Revisiting the Estonian…," 50-51.

[61] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe."

[62] Davis, "Hackers Take Down the Most Wired Country in Europe"; Herzog, "Revisiting the Estonian…," 61.

to run precisely two weeks as a show of force.[63] As technology and influence mediums evolve, so too have Russian strategies to employ these burgeoning capabilities. Russian influence operations have insidiously morphed from "overt to covert, physical to digital, conventional to asymmetric", yet have successfully retained the characteristic of deniability.[64] These expanding capabilities lack fidelity and are "ripe with potential unintended consequences"; notwithstanding, what Russia loses in precision, they gain in freedom of movement and the ability to escape attribution.[65]

The complexity of the operational environment is a key enabler in Russian influence operations; this environment provides Russian hackers an opportune medium to exact surgical exploitation, and then vanish into the ether.[66] By disseminating information with relative ease, operators are able to sow disinformation and create discontent within the US and its allies. Therefore, America's "political discourse [is] a ripe target for disinformation efforts" because it is an opportunity space. Russia can use freedom of speech within the US as a mechanism to exploit and impart their will — discrediting Western governments while causing confusion and discord.[67] However, without a clear deterrence plan, Russian meddling will continue unabated. Therefore, the US must identify and employ threshold limits and proportionate retaliation actions to dissuade Russian aggressions because they are gaining an edge.[68] Circumstances for the West are further complicated by Russia's ever-evolving tactics and masterful use of statecraft to

---

[63] Davis, "Hackers Take Down the Most Wired Country in Europe".
[64] Polyakova, "The Future of Political Warfare…," 2.
[65] *Ibid.*
[66] Bergmann, "War by Other Means…," 13.
[67] *Ibid.,* 4.
[68] Andy Greenberg, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure'," *Wired*, 9 May 2017, https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

achieve their desired end states. Consequently, the US and its allies must recognize the immediacy of the situation and develop proactive strategies to mitigate Russian influence and regain information and cyber dominance.

HOW CAN THE US NOT ONLY MITIGATE RUSSIAN INFLUENCE IN THE CYBER DOMAIN, BUT GAIN THE ADVANTAGE?

Hardening US and Allied infrastructure, systems, and strategies through enhanced, public, and private cooperation

Recent empirical data has suggested that Russian cyber-attacks "represent the paramount threat to U.S. critical infrastructure".[69] Russia has shown, without question, the formidability of their cyber and information warfare capabilities against the West. Moreover, by maintaining a continuous and persistent presence in the cyber and information spaces, they are able to attack US and allied systems and infrastructure with impunity. Admittedly, the West has inadvertently enabled these activities by failing to adequately harden their infrastructure, systems, and strategies. Conversely, the US has limitedly used cyber attacks in response to Russian provocation. The US's fear is that a proportionate information or cyber attack against Russia could lead to reprisal and subsequent escalation.[70] Further, the US and its allies are "reluctant to respond to such aggression by Russia with counterattacks, partly for fear that the United States' infrastructure [is] more vulnerable."[71] The threat to key systems and infrastructure is further exacerbated by increased globalization, interconnectedness, and reliance on cyberspace; thus, introducing "the potential risk for malicious cyber activity to result in

---

[69] Isaac R. Porche III, "Fighting and Winning the Undeclared Cyber War (PDF) ," RAND (blog), 24 June 2019, https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html.

[70] David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, 15 June 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

[71] *Ibid.*

direct physical consequences" with little recourse.[72]

To counter Russian activities, the US and its counterparts must, "clearly articulate sectors that it believes should be off limits to a cyberattack and warn that if these sectors are deemed to be under attack — such as interference in an election or an attack on critical infrastructure — the United States will respond forcefully."[73] Nevertheless, "lines in the sand" alone will not stop Russian influence. Instead, there must be a unified call to arms amongst the US and its allies for increased global transparency among social media companies and private corporations.[74] By increasing communication with the civilian sector, the US and allied governments gain necessary intelligence, tactics, techniques and procedures used by hackers that could potentially thwart future attacks.[75] Moreover, mitigation of Russian influence is incumbent upon collective, integrated global action in areas of defense, security, and intelligence, if the West intends on "frustrating [Russian] efforts, precluding their options while expanding our own, and forcing them to confront conflict under adverse conditions."[76] Consequently, the West cannot successfully implement a strategy that mitigates Russian influence operations — let alone gain an advantage — if they are unable to determine attribution.

The complex nature of cyberspace allows bad actors to manipulate the West —

---

[72] The Department of Homeland Security, *DHS Cybersecurity Strategy (PDF)* (Washington, DC: U.S. Government Printing Office, 4 April 2019): 2, https://dod.defense.gov/ Portals/1/Documents/ pubs/2018-National-Defense-Strategy-Summary.pdf

[73] Bergmann, "War by Other Means…", 28.

[74] Paris Martineau, "Russia's Disinformation War Is Just Getting Started," *Wired*, 8 October 2019, https://www.wired.com/story/russias-disinformation-war-is-just-getting-started/.

[75] *Ibid.*

[76] The United States Department of Defense. *Summary of the 2018 National Defense Strategy of the United States of America (PDF)* (Washington, DC: U.S. Government Printing Office, 2018): 5, https://dod.defense.gov/Portals/1/Documents/ pubs/2018-National-Defense-Strategy-Summary.pdf; Isaac R. Porche III, "Fighting and Winning the Undeclared Cyber War," RAND (blog), 24 June 2019, https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html.

free of attribution. Therefore, in order to adequately protect and respond to attacks, the US and its allies must know where the attacks are originating from. A task made infinitely more difficult by its inherent need for concerted global coordination, all dependent upon capable and competent domestic security, dedicated lines of communication, and buy-in from the military, political and private sectors.[77] If the US and its allies want to increase communication with the private sector, they will need a reliable and capable system for timely information sharing.[78] Latency in cyber or information operations means the difference between controlling the narrative or reacting.

Due to the nebulous and seemingly unbounded nature of cyberspace, no one country or corporation can single-handedly regulate this space. Instead, to counteract malicious actors in this domain, there must be a unified international effort toward the establishment of cyberspace norms and acceptable behaviors.[79] Additionally, the international community must extend beyond diplomats and tacticians and include a high degree of interoperability and collaboration with private sector companies like Google, Facebook, and Twitter to best secure the space.[80] The same aspects of cyberspace that prove difficult for the West to protect against exploitation, grant Russia their competitive advantages. By and large, combatting influence operations through hardening of US and allied systems and infrastructure is a complex problem requiring a global unity of effort externally and a whole-of-nation response internally.

---

[77] The Select Committee on Intelligence of the United States Senate, *Disinformation: A Primer in Russian…,* 8; Brands, "Paradoxes of the Gray Zone (PDF)," 8.

[78] Polyakova, "The Future of Political Warfare…," 15.

[79] The Department of Homeland Security, *DHS Cybersecurity Strategy (PDF)*, 4; Polyakova, "The Future of Political Warfare…," 15.

[80] Polyakova, "The Future of Political Warfare…," 15.

Coordinated whole-of-nation responses containing a confluence of statecraft, diplomacy, and military responses

The US could potentially react to Russian influence with a whole-of-nation response. They could initially call on congressional support to increase sanctions on Russia's government and its oligarchs as a means of striking funding avenues.[81] Similarly, legislative and political support could be garnered from Congress and the Senate to help create norms, regulations, and global support.[82] Moreover, integration and coordination must extend beyond the legislators and include the "U.S. State Department, the Defense Department, the Treasury Department, and the intelligence community", as well as, private sector companies like Google and Facebook.[83] By enhancing private sector coordination and diplomatic and law enforcement responses, the US is able to combat the threat while maintaining legal and ethical standards.[84] Russian influence operations represent a significant threat to the US, its infrastructure, and way of life; therefore, to combat this existential threat requires the political, military, and private sectors acting in concert along delineated lines of operations— whose actions are steeped in intelligence.[85]

For effective intelligence and counterintelligence gathering against near-peer adversaries, the US must increase its manpower and subsequently refocus and rebalance their priorities between counterterrorism and influence operations to effectively maintain

---

[81] Bergmann, "War by Other Means…", 24.
[82] *Ibid.,* 27.
[83] Chivvis*, Understanding Russian "Hybrid Warfare"…,* 8.
[84] Joseph Marks, "The Cybersecurity 202: U.S. Should Counter Russia and China Hacking with Its Own Influence Operations, Think Tank Says," *The Washington Post*, 1 February 2019. https://www.washingtonpost.com/news/ powerpost/paloma/the-cybersecurity-202/2019/02/01/the-cybersecurity-202-u-s-should-counter-russia-and-china-hacking-with-its-own-influence-operations-think-tank-says/5c5341331b326b29c3778d3d/.
[85] Chivvis*, Understanding Russian "Hybrid Warfare"…,* 8.

a competitive advantage.[86] However, the strength, timeliness, and responsiveness garnered through intelligence collection demands integration and collaboration between US and allied agencies.[87]

Lastly, the US and its allies require refined deterrence strategies against Russian influence operations to effectively compete and gain the advantage. To retain the advantage in the operational environment, US and allied strategies should superimpose overt and covert cyber operations with political action — delineating firm "lines in the sand" and encroachment consequences.[88] Again, effective deterrence requires a concerted whole-of-nation approach that incorporates active and overt information operations — aimed at dissuading Russian aggression publicly and gaining the informational advantage.[89] A potential deterrence measure could be a pre-existing capability — offensive cyber operations.

Increased US and Allied Offensive Cyber Operations to gain the strategic advantage and deter further aggression

As aforementioned, Russia's intent is quite clear — to subvert Western ideals through unregulated, and unattributable means. By not targeting hardened structures or physical infrastructure, the Kremlin can attack "intangible dimensions" such as political and social harmony and erode at "the health and stability of democracies."[90] Therefore, if the US and its allies are to improve deterrence, detection, and counter disinformation,

---

[86] Bergmann, "War by Other Means…", 27.

[87] Stacie L. Pettyjohn and Becca Wasser, *Competing in the Gray Zone: Russian Tactics…*, 44; Chivvis, *Understanding Russian "Hybrid Warfare"…,* 9.

[88] Polyakova, "The Future of Political Warfare…," 18.

[89] Julian E. Barnes, "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attacks," *The New York Times*, 13 July 2018, https://www.nytimes. com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html.

[90] Morris, *Gaining Competitive Advantage in the Gray Zone*…, 3.

they need to gain the strategic advantage in the information and cyber domains.[91] Traditionally, the US and its allies have relied on cyber as a means of defending key infrastructure, monitoring bad actors, and gathering necessary intelligence about their would-be digital assailants. The US's choice to defend cyberspace, vice go on the offensive, stems from fears of potential escalation. However, the US should not be so quick to dismiss offensive cyber operations as they offer options for retaliation against Russian influencers — if nested in strategic purpose.[92]

Cyberspace offers the US and its allies an opportunity space for proactive vice reactive engagement and exploitation. Additionally, in its application of preventive and retaliatory cyber pressure against Russian influence operations, the US demonstrates its resolve and ability to respond in kind.[93] Offensive cyber operations offer the West a mechanism to target support networks and quickly exact retribution against Russian provocations. For example, the US is currently examining the feasibility of targeting "senior leadership, oligarchs, and Russian elites" with offensive cyber and information operations.[94] If they chose to target these key figures, the US could put pressure on the individuals themselves, disrupt funding avenues, and dissuade future operations.

However, the application of offensive cyber operations carries significant potential for unanticipated escalation with Russia. Thus, offensive cyber operations must be part of a comprehensive approach, tempering its "military, diplomatic, and economic

---

[91] Bergmann, "War by Other Means…", 27.

[92] Bergmann, "War by Other Means…", 23.

[93] Seth G. Jones, "Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare," (Center for Strategic and International Studies, October 2018): 9, https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.

[94] Ellen Nakashima, "U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election," *The Washington Post*, 25 December 2019, https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/ 12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.

aspects" with risk versus gain. Additionally, for strategic deterrence to occur by, with, or through offensive cyber operations, the US and its allies need a unified and congruent end state.[95] To achieve these end states, cyber attacks must not be applied indiscriminately, but with strategic purpose — akin to the use of precision munitions in achieving a decisive advantage.[96]

The end state is simple, "to make cyberspace more peaceful rather than simply to punch back in anger"; thus, the employment of offensive cyber operations must be well calculated and applied tactfully based on risk of escalation.[97] It is no surprise that "Russia will continue to target the United States at home and abroad until the U.S. government implements a more aggressive offensive information campaign."[98] Offensive cyber operations may not be the panacea to Russian aggression, but they are an option available to the US and its allies. The West does not have the luxury of "sitting on its laurels", but must continue to make progress in countering the ever-growing and omnipresent threat of Russian influence. The solutions sets are out there, but must be cultivated through global coordination — beginning internally, through whole-of-nation synthesis.

CONCLUSION

It is evident that Russia is consistently and persistently expanding its influence operations in the information and cyber domains and more importantly, that the US and its allies can do more to counter these actions — beginning with the divergence of Russian strategies. These disparate theories and naming conventions are highly

---

[95] Morris, *Gaining Competitive Advantage in the Gray Zone*…, xiii; David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, 15 June 2019.

[96] Morris, *Gaining Competitive Advantage in the Gray Zone*…, xiii.

[97] Joseph Marks, "The Cybersecurity 202: U.S. Should Counter Russia and China Hacking with Its Own Influence Operations, Think Tank Says," *The Washington Post*, 1 February 2019.

[98] Jones, "Going on the Offensive…," 9.

problematic and take focus away from tenable mitigation strategies. It is evident that terms like ‘hybrid warfare’, ‘gray zone’ operations, and ‘NGW’ unnecessarily add confusion, do little to clarify Russia’s activities, and obfuscate solution sets. Therefore, to begin formulating viable solutions, the US and its allies must agree on a what exactly Russia is doing in the influence space. More emphasis should be given to Russia’s growing proficiency in discrediting and debilitating Western influence through political, diplomatic, economic, and military means — not what name to call it.

Additionally, using these buzzwords interchangeably leads strategists down a dangerous path of flawed assumptions and ill-conceived conceptualizations of Russia’s activities. What is necessary is a collective understanding of how Russia achieves strategic influence. It follows that key infrastructure hardening and concerted global response are mutually dependent on a shared understanding of how Russia achieves influence dominance. Technology has continued to evolve, yet Russian intentions have remained somewhat constant. Russia has and will continue to rely on combinations of national strengths and statecraft to accomplish their strategic objectives; however, they have focused the bulk of their efforts within the information and cyber domains.

Consequently, it is incumbent upon the US and its allies to coordinate their efforts and develop a coherent, sustainable, and measurable strategy to not only mitigate Russian influence operations, but gain the advantage. The necessary strategies must begin with internal US coordination consisting of a whole-of-nation response to Russian influence operations. Once the US is able to increase transparency and coordination between the private, political, and military sectors, the fight can then be expanded externally. The overarching theme for a successful mitigating strategy requires global unification of

purpose and economy of effort. Lastly, all options against the Russian influence campaign — such as offensive cyber operations — must remain on the table as available responses; notwithstanding, the determination to use these options must not fail to consider the risk of escalation.

By and large, Russia's strategic intentions and goals have remained seemingly constant since the close of the Cold War. What has changed is Russia's medium of choice — cyberspace. To fight and win in cyberspace, the US and its allies must be appropriately poised and prepared to apply offensive cyber operations against Russia. However, in order to cultivate these capabilities, the West must improve information sharing and transparency, if they are to successfully work through political, social, and legal constraints and restraints. Thus, it is incumbent on the US and its allies to expedite collective developments concerning cyber rules of engagement, targeting, and proportionality to respond quickly and maintain the ethical high ground.

Time is fleeting.

BIBLIOGRAPHY

Adamsky, Dmitry. "Cross-Domain Coercion: The Current Russian Art of Strategy (PDF)." *IFRI Security Studies*, November 2015. https://www.ifri.org/sites/default-/files/atoms/files/pp54adamsky.pdf.

Allison, George. "Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack Say GCHQ." *UK Defence Journal*, 14 February 2018. https://ukd-efencejournal.org.uk/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack-say-gchq/.

"Average and Peak Power – A Tutorial - University of Oregon." Accessed 19 January 2020. http://hank.uoregon.edu/experiments/modelocked-fiberlaser/20063.pdf.

Bartles, Charles K. "Getting Gerasimov Right (PDF)." Research Gate. *Military Review*, January 2016. 30-37. https://www.researchgate.net/publication/329933852_Getting_Gerasimov_Right.

Barnes, Julian E. "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attacks." *The New York Times*, 13 July 2018. https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html.

Barno, David, and Nora Bensahel. "Fighting and Winning in the 'Gray Zone.'" War on the Rocks, 10 August 2015. https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/.

Bergmann, Max, and Carolyn Kenney. "War by Other Means: Russian Active Measures and the Weaponization of Information (PDF)." The Moscow Project, 6 June 2017. https://themoscowproject.org/reports/war-means-russian-active-measures-weaponization-information/.

Boston, Scott, and Dara Massicot. "How Russia's Military Has Evolved." RAND Corporation, 7 December 2017. https://www.rand.org/pubs/perspectives/PE231.html.

Brands, Hal. "Paradoxes of the Gray Zone." Foreign Policy Research Institute, 5 February 2016. https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

Charap, Samuel. "The Ghost of Hybrid War." *Survival* 57, no. 6 (2 November 2015): 51–58. https://doi.org/10.1080/00396338.2015.1116147.

Cheever, Erik. "The Unit Impulse Function." Unit Impulse Function. Accessed 19 January 2020. http://lpsa.swarthmore.edu/BackGround/ImpulseFunc/ImpFunc.html.

Chivvis, Christopher S. *Understanding Russian "Hybrid Warfare" And What Can Be Done About It*. Santa Monica, CA: RAND Corporation, 2017.

Codevilla, Angelo M. "Tools of Statecraft: Diplomacy and War." Foreign Policy Research Institute, 15 January 2008. https://www.fpri.org/article/2008/01/tools-of-statecraft-diplomacy-and-war/.

Connell, Mary Ellen, and Ryan Evans. "Russia's 'Ambiguous Warfare' and Implications for the U.S Marine Corps (PDF)." CNA, May 2015. https://www.cna.org/CNA_files/PDF/DOP-2015-U-010447-Final.pdf.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired*. 5 June 2017. https://www.wired.com/2007/08/ff-estonia/.

The Department of Homeland Security. *DHS Cybersecurity Strategy (PDF)*. Washington, DC: U.S. Government Printing Office, 4 April 2019. https://dod.defense.gov/Portals/1/Documents/ pubs/2018-National-Defense-Strategy-Summary.pdf

Galeotti, Mark. "The Mythical 'Gerasimov Doctrine' and the Language of Threat." *Critical Studies on Security* 7, no. 2 (27 February 2018): 157–61. https://doi.org/10.1080/21624887.2018.1441623.

Galeotti, Mark. "Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe." ECFR.EU. Accessed 19 January 2020. https://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

"The 'Gerasimov Doctrine' and Russian Non-Linear War." In Moscow's Shadows, 17 September 2017. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Gerasimov, Valery. "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations." trans. Robert Coalson. *Military-Industrial Kurier*, 27 February 2013, accessed 4 April 2020. https://jmc.msu.edu/50th/download/21-conflict.pdf.

Greenberg, Andy. "The NSA Confirms It: Russia Hacked French Election 'Infrastructure.'" *Wired*. 9 May 2017. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/.

Grigas, Agnia. "How Soft Power Works: Russian Passportization and Compatriot Policies Paved Way for Crimean Annexation and War in Donbas." Atlantic Council, 29 August 2019. https://www.atlanticcouncil.org/blogs/ukrainealert/how-soft-power-works-russian-passportization-and-compatriot-policies-paved-way-for-crimean-annexation-and-war-in-donbas/.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49–60. https://doi.org/10.5038/1944-0472.4.2.3.

Higgins, Andrew. "Russian Money Suspected Behind Fracking Protests." *The New York Times*. 1 December 2014. https://www.nytimes.co-m/2014/12/01/world/russian-money-suspected-behind-fracking-protests.html.

Holland, Emily, and Rebecca Friedman Lissner. “Countering Russian Influence in the Balkans.” Lawfare, 31 October 2019. https://www.lawfareblog.com/countering-russian-influence-balkans.

Jones, Seth G., “Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare.” Center for Strategic and International Studies, October 2018. https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.

Kofman, Michael, and Matthew Rojansky. “A Closer Look at Russia’s ‘Hybrid War.’” Wilson Center. Wilson Center, April 2015. https://www.wilsoncenter.org/sites/default/files/7-KENNAN CABLE-ROJANSKY KOFMAN.pdf.

Kofman, Michael. “Russian Hybrid Warfare and Other Dark Arts.” War on the Rocks, 11 March 2016. https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

Lee, Dave. “The Tactics of a Russian Troll Farm.” *BBC News*. 16 February 2018. https://www.bbc.com/news/technology-43093390.

Losh, Jack, and Sebastien Rabas. “Putin's Angels: The Bikers Battling for Russia in Ukraine.” *The Guardian*, 29 January 2016. https://www.theguardian.com/world/2016/jan/29/russian-biker-gang-in-ukraine-night-wolves-putin.

Lutsevych, Orysia. “Agents of the Russian World: Proxy Groups in the Contested Neighbourhood.” *Chatham House*, April 2016. https://www.chathamhouse.org/publication/agents-russian-world-proxy-groups-contested-neighbourhood.

Marks, Joseph. “The Cybersecurity 202: U.S. Should Counter Russia and China Hacking with Its Own Influence Operations, Think Tank Says.” *The Washington Post*, 1 February 2019. https://www.washingtonpost.com/news/ powerpost/paloma/the-cybersecurity-202/2019/02/01/the-cybersecurity-202-u-s-should-counter-russia-and-china-hacking-with-its-own-influence-operations-think-tank-says/5c5341331b326b29c3778d3d/.

Martineau, Paris. “Russia's Disinformation War Is Just Getting Started.” *Wired*. 8 October 2019. https://www.wired.com/story/russias-disinformation-war-is-just-getting-started/.

McGuinness, Damien. “How a Cyber Attack Transformed Estonia.” *BBC News*, 17 April 2017. https://www.bbc.com/news/39655415.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. Santa Monica, CA: RAND Corporation, 2019.

Nahzi, Fron. “The West Cannot Sit by While Russia Exploits Social Media with Disinformation.” TheHill. The Hill, 26 December 2019. https://thehill.com/opinion/international/475797-the-west-cannot-sit-by-while-russia-exploits-social-media-with.

Nakashima, Ellen. "U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election." *The Washington Post*, 25 December 2019. https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.

Ng, Nicole, and Eugene Rumer. "The West Fears Russia's Hybrid Warfare. They're Missing the Bigger Picture." Carnegie Endowment for International Peace, 3 July 2019. https://carnegieendowment.org/2019/07/03/west-fears-russia-s-hybrid-warfare.-they-re-missing-bigger-picture-pub-79412.

Paul, Christopher, and Miriam Matthews. "Russia's 'Firehose of Falsehood' Propaganda Model." RAND Corporation, 11 July 2016. https://www.rand.org/pubs/perspectives/PE198.html.

Pettyjohn, Stacie L., and Becca Wasser. *Competing in the Gray Zone: Russian Tactics and Western Responses*. Santa Monica, CA: RAND Corporation, 2020.

Polyakova, Alina, and Spencer P. Boyer. "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition (PDF)." Brookings Institute, March 2018. https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf.

Pomerantsev, Peter. "We Need to Rethink the 'Information War' with Russia." *Time*, 9 November 2019. https://time.com/5722805/rethink-information-war-russia/.

Porche III, Isaac R. "Fighting and Winning the Undeclared Cyber War." RAND (blog), 24 June 2019. https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html.

"President Trump China Strategy: Death by A Thousand Paper Cuts..." The Last Refuge, 27 November 2019. https://theconservativetreehouse.com/2019/11/27/president-trump-china-strategy-death-by-a-thousand-paper-cuts/.

Renz, Bettina. "Russia and 'Hybrid Warfare.'" *Contemporary Politics* 22, no. 3 (2016): 283–300. https://doi.org/10.1080/13569775.2016.1201316.

Rosenberg, Matthew, Nicole Perlroth, and David E. Sanger. "'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020." *The New York Times*, 10 January 2020. https://www.nytimes.com/2020/01/10/us-/politics/russia-hacking-disinformation-election.html.

Sanger, David E., and Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power Grid." *The New York Times*, 15 June 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

The Select Committee on Intelligence of the United States Senate. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns Panel II*. Washington, DC: U.S. Government Printing Office, 30 March 2017. https://www.intelligence.senate.gov/sites/default/-files/hearings/S Hrg 115-40 Pt 2.pdf.

Shackelford, Scott J., Michael Sulmeyer, Amanda N. Craig Deckard, Ben Buchanan, and Brian Micic. "From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do about It." University of Nebraska - Lincoln, 2017. https://digitalcommons .unl.edu/nlr/vol96/iss2/5/.

Shlapak, David A. "The Russian Challenge." RAND Corporation, 4 June 2018. https://www.rand.org/pubs/perspectives/PE250.html.

"SMA TRADOC White Paper- Russian Strategic Intentions." NSI, May 2019. https://nsiteam.com/sma-white-paper-russian-strategic-intentions/.

Spalkova, Veronika. "Influence of Russian Disinformation Operations: Specific Examples in Data and Numbers." Kremlin Watch Report. Accessed 19 January 2020. https://www.europeanvalues.net/wp-content/uploads/2019/02/Influence-of-Russian-Disinformation-Operations-Specific-examples-in-data-and-numbers.pdf.

Stanley-Becker, Isaac. "Russian Disinformation Network Is Said to Have Helped Spread Smear of U.S. Ambassador to Ukraine." *The Washington Post*, 17 December 2019. https://www.washingtonpost.com/technology/2019/12/17-/russian-disinformation-network-said-have-helped-spread-smear-us-ambassador-ukraine/.

The United States Department of Defense. *Summary of the 2018 National Defense Strategy of the United States of America (PDF).* Washington, DC: U.S. Government Printing Office, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Webb, Jonathan. "Death by A Thousand Cuts: How Micro-Risks Can Cost Your Business." *Forbes*, 28 June 2017. https://www.forbes.com/sites/jwebb/2017/06/28/death-by-a-thousand-cuts-how-micro-risks-can-cost-your-business/.