THE CYBER DEFENSE REVIEW

Ethical Assessment of Russian Election Interference

Using the Framework of Just Information Warfare

Second Lieutenant Joseph Zuccarelli
Second Lieutenant Nico Manzonelli

ABSTRACT

The consistent development of information and communication technologies poses new ethical challenges for military leaders and policymakers in the fifth domain of warfare–cyberspace. This article engages a relatively new ethical framework known as Just Information Warfare (JIW) to assess one of the highest profile instances of information warfare in recent years–Russian interference in the 2016 US presidential election. First, we define information warfare and describe how concepts from two well-known ethical theories–Just War Theory and Information Ethics–merge to create JIW. Next, we analyze Russian military officers' 2016 election interference efforts and the corresponding US response through a JIW lens. Finally, we offer three key takeaways from our analysis that warrant further thought.

INTRODUCTION

US military doctrine revolved around four fundamental domains of warfare, land, air, sea, and space, until 2010 when cyberspace, a fifth domain, was officially added.[1] The Department of Defense (DoD) defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers."[2] Over the past decade, the expansion of cyberspace has forced military leaders to consider the ability to control, disrupt, or manipulate an adversary's informational infrastructure as important as traditional measures of military strength. Information and communication technologies

Joseph Zuccarelli, a Draper Laboratory Scholar pursuing his MS in Data Science at Harvard University, recently graduated from the United States Military Academy with a Mathematical Sciences major and a Cyber Security minor. While pursuing his undergraduate degree, Joseph worked as a Senior Writing Fellow in the West Point Writing Program and focused his undergraduate studies on researching applied mathematics and technical communication. His internship experience includes work with the Florida Panthers sports analytics team studying National Hockey League data. Joseph is a U.S. Army Second Lieutenant and will serve in the Cyber branch following completion of his studies at Harvard. joseph_zuccarelli@g.harvard.edu

increasingly prove to be useful technologies for waging war and are revolutionizing military affairs. In addition to military leaders, ethicists and policymakers also are now compelled to consider how to apply or adapt traditional ethical theories to this fifth domain.

INFORMATION WARFARE

Information Warfare (IW), properly defined, entails the use of information and communication technologies to breach an adversary's informational infrastructure in order either to disrupt it, or to obtain relevant data concerning the adversary's resources, military strategies, etc.[3] IW differs from traditional warfare in basic respects. Traditional warfare is necessarily violent and involves the sacrifice of human lives and kinetic damage to both military and civilian infrastructures. In contrast, IW enables entities to damage and degrade adversaries without physical force or violence. While traditional warfare is generally limited to human beings and physical objects, IW introduces two new dimensions: artificial and non-physical entities. Although the lack of violence and the overall non-destructive nature of IW seems to make it desirable from an ethical and political perspective, IW's disruptive nature can severely damage contemporary societies' information infrastructure and lead to dangerous outcomes. Consider the following examples from the past decade.

In June 2015, the US Office of Personnel Management (OPM) suffered one of the largest breaches of government data in US history after a data breach compromised an estimated 21.5 million records. Among the compromised records were highly sensitive Standard Form 86s (SF 86 – Questionnaire for National Security Positions), which are used to document background investigations of prospective US government employees and include personally identifiable information like Social Security numbers, names, birthdates, places of birth, and addresses. While the motive behind the breach remains unclear, the overwhelming consensus

Nico Manzonelli, a MIT Lincoln Laboratory Military Fellow working in the Cyber Security and Information Sciences Division, is pursuing his MS in Data Science at Harvard University. A recent graduate from the United States Military Academy with a BS in Systems Engineering, Nico served as a Senior Writing Fellow in the West Point Writing Program and competed on Army's varsity wrestling team. In his undergraduate studies, he focused his research on data visualization, analytics, and natural language processing. His internship experience includes working with the National Basketball Association's Technology and Products Division. Nico is a U.S. Army Second Lieutenant and will serve in the Cyber branch following completion of his studies at Harvard. nicomanzonelli@g.harvard.edu

is that Chinese government-sponsored hackers presumably carried out the attack to compile a database of US government employees.[4]

In February 2022, Russia launched a full-scale ground invasion of Ukraine. Although this ongoing conflict entails the typical physical violence associated with traditional warfare, Russian-led IW operations aim to influence public opinion and damage Ukraine's information infrastructure via cyberattacks. Prior to invasion, Russia conducted a long-running misinformation campaign using state-sponsored media outlets and Kremlin-backed online personas to cast Ukrainians as the perpetrators of genocide against Russian speakers in eastern Ukraine. The twofold purpose of said misinformation campaign was to justify the invasion of Ukraine and to paint NATO-affiliated countries as aggressors in the conflict.[5] In addition to their misinformation campaign, Russia coupled cyber and kinetic military operations for their initial invasion and continue to coordinate cyberattacks to steal information and degrade Ukrainian capabilities.[6]

JUST WAR THEORY

Ethical analyses of war typically follow three main paradigms: Just War Theory (JWT), Pacifism, or Realism. JWT is an ethical framework studied by military leaders, ethicists, theologians, and policymakers that focuses on providing justifications for how and why wars are fought. Rather than use the framework to justify "good" military actions, JWT often serves as a structured method for assessing the morality of actions in war. Traditional JWT is divided into two sets of principles: *jus ad bellum* ("right to go to war")—the morality of initiating war, and *jus in bello* ("right conduct in war"), which focuses on the morality of conduct within a war,[7] as more fully described in the next two paragraphs.

Jus ad bellum typically consists of the following six principles: just cause, legitimate authority, right intention, reasonable prospects of success, proportionality, and last resort.[8] Just cause requires that the reason for going to war must be justified (e.g., self-defense). Legitimate authority indicates that only duly constituted public authorities are allowed to wage war. Right intention refers to the fact that the entity waging war must actually intend to achieve the established just cause, rather than use it as a pretext for achieving a wrongful end. Reasonable prospects of success requires that the entity waging war must have some reasonable probability of success. Proportionality indicates that the expected benefits of waging war must exceed its expected evils or harms. The sixth and final principle, last resort, requires that there is no less-harmful avenue to achieve the established just cause other than war.[9]

Jus in bello includes three basic principles: discrimination, proportionality, and necessity.[10] Discrimination requires that those involved in the conduct of war must always properly distinguish between military objectives and civilians, and limit attacks to military objectives. Proportionality requires combatants to ensure that collateral harm to civilians is not excessive in relation to the military advantage achieved by any act of war. Finally, necessity requires combatants to always use the least harmful means feasible in order to achieve any otherwise just military objective.[11]

As the nature of warfare has evolved to include IW, applying JWT principles to modern conflicts has become increasingly difficult. This issue mainly arises because JWT typically focuses on the use of force in physically violent warfare, and not the cyber domain, where IW engages abstract entities. The unconventional nonviolent property of IW complicates core JWT concepts such as harm, target, and attack. This challenge is widely discussed in existing literature.[12] The following two sections detail how philosophers address the shortcomings of JWT by introducing two additional ethical frameworks.

INFORMATION ETHICS

Information Ethics (IE) is an ethical approach that enables the analysis of moral issues from an informational perspective. IE follows from the consideration that internet and communication technologies have radically changed the context in which moral issues arise, requiring us to rethink the foundations upon which our traditional ethical positions are based.[13] Under IE, the moral value of an entity is determined by its contribution to the enrichment of the information environment. This environment, also referred to as the infosphere, includes all existing things, physical or non-physical, and the relations occurring among them.[14] If the infosphere seems all-encompassing, that’s because it is. While biocentric ethics are based on the moral value of life and the negative value of suffering, IE is concerned with the moral value of existence.[15] In practice, this implies that the information environment includes a person, a person’s computer, and the data on said computer and thus all have moral standing. The blooming or enrichment of the infosphere is considered the ultimate good, while its corruption or destruction is considered the ultimate evil. Any form of corruption or destruction of an entity in the information environment is referred to as entropy.[16]

Using the key terms defined in the previous paragraph, IE outlines four principles for evaluating individuals' contributions to the information environment.[17] These four principles are defined as follows:

1. Entropy should not be caused in the infosphere (null law);
2. Entropy should be prevented in the infosphere;
3. Entropy should be removed from the infosphere;
4. The flourishing of informational entities and of the whole infosphere should be promoted by preserving, cultivating, and enriching their properties.

These principles are fairly straightforward, which, when merged with those outlined by JWT, bring us to the final ethical theory discussed in this article–Just Information Warfare (JIW).

JUST INFORMATION WARFARE

As an ethical framework, JIW merges concepts from JWT with IE to establish necessary and sufficient criteria for waging IW.[18] JIW hinges on the following three principles defined below:

1. IW should be waged solely against entities that endanger or disrupt the well-being of the infosphere;
2. IW should be waged to preserve the well-being of the infosphere;
3. IW should not be waged solely to promote the well-being of the infosphere.

Adhering to the first principle renders the decision to resort to IW morally just. Under this principle, any entity that endangers or disrupts the well-being of the infosphere forfeits its basic rights to flourish or even exist within the infosphere and renders itself a morally just target under JIW. This principle empowers actors in the information environment to discriminate justly between proper and improper IW targets.[19]

The second principle gives other actors in the information environment a moral obligation to prevent any malicious actor from causing more entropy within the infosphere. In other words, IW waged to reestablish the status quo or mend a damaged infosphere is morally just under JIW. Under this principle, nation-state actors conducting IW should only be used as an active measure to reduce or prevent instances of entropy within the infosphere.[20]

The third and final principle indicates that IW waged to improve the prosperity of the information environment is never just. Under the theory of IE, IW is understood as a form of disruption. Therefore, by definition, IW is never desirable and should not be used a vehicle to foster the infosphere's prosperity. Instead, IW is only to be considered a necessary evil used to combat the uncontrolled increase of entropy within the infosphere.[21]

It is important to underscore that any actor waging IW must adhere to the principle of proportionality, which may differ from but logically tracts the concept of proportionality in the context of JWT. In both JWT and JIW, proportionality implies that the means of conducting warfare must not cause more harm than the military actions addressed or corrected through an instance of warfare.[22] However, while measuring relative use of force and collateral damage is more straightforward in traditional conflict, defining comparative entropy in the information environment is nuanced and beyond the scope of our analysis.

CASE STUDY: RUSSIAN 2016 ELECTION INTERFERENCE

Background

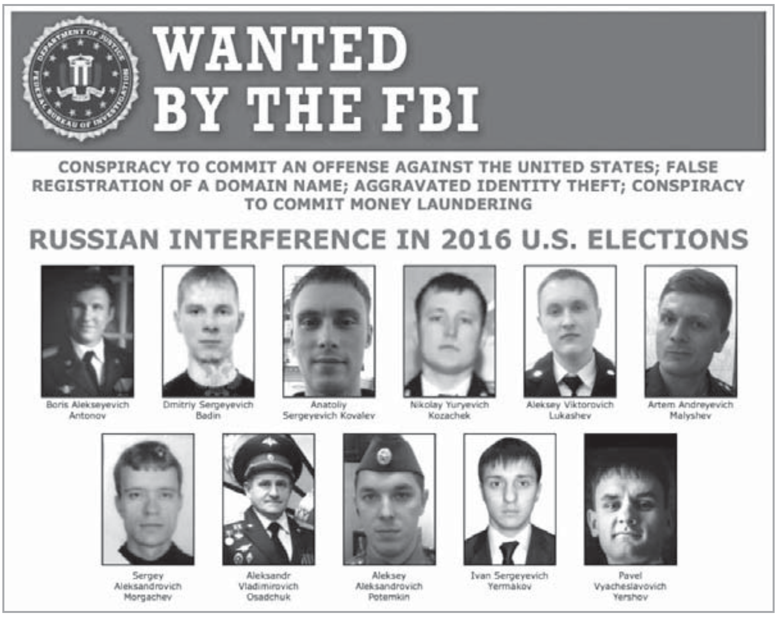
In 2016, the Republican ticket of Donald Trump and Mike Pence defeated the Democratic ticket of Hillary Clinton and Tim Kaine in what many consider one of the greatest upsets in US election history. Beyond this point, the 2016 US presidential election was also a significant instance of Russian election interference. Since 2016, details of Russian interference efforts have come out in drips and drabs, with information revealed in memoranda released by intelligence agencies, court documents filed by Special Counsel Robert Mueller, testimony from Trump associates, and investigative news reports.[23] In 2020, the Senate Intelligence Committee released its final report, a nearly 1000-page document that details Russia's aggressive IW tactics used to influence the outcome of the election.[24] The US Intelligence Community (IC) ultimately concluded that the Russian interference centered around three goals: damage the Clinton campaign, boost the Trump campaign, and sow distrust in American democracy overall. To accomplish their goals, Russian IW efforts focused on three basic tactics: probing state voter databases, hacking the Democratic campaign and its committees, and spreading false propaganda on social media.[25]

The IC concluded Russian hackers did not alter actual votes during the 2016 election, but evidence suggested pre-election attacks on voter registration systems in at least 21 states. Reports indicate that the hackers stole information on approximately 500,000 voters from an unnamed state's database, to include names, addresses, birthdates, driver's license numbers, and partial Social Security numbers. It remains unclear what the Russians did with this compromised information.[26]

Beyond their attacks on US voter registration systems, Russian hackers also successfully accessed several restricted Democratic campaign systems by sending phishing emails to various Clinton campaign staffers and volunteers. Camouflaged as Google security notifications, phishing allowed the hackers to access several notable campaign members' accounts, including chairman John Podesta, and steal tens of thousands of emails. The emails were then released during the run-up to election day to create repeated negative news cycles for the Clinton campaign. The hackers also used very similar tactics to attack the Democratic Congressional Campaign Committee and the Democratic National Committee.[27]

While the first two tactics described above are considered as traditional cyber-attacks, Russians also utilized digital influence operations to interfere with the election. As one of the more subtle IW approaches, Russian hackers developed troll factories (i.e., entities employing personas who post comments on social media reinforcing misinformation) and bots (i.e., programs that send out messages automatically in response to the appearance of a keyword) that incite division among the electorate. Prior to the election, Russia employed troll factories and bots to post controversial content divisively covering topics such as the Black Lives Matter movement, immigration, and gun control. There is also evidence of Russian groups buying and frequently posting political ads derisive of the Clinton campaign.[28]

In response to the findings on Russian election interference, the US government has taken steps to protect against foreign IW tactics and imposed punitive measures upon Russia. Immediately following the 2016 election, then Director of National Intelligence Dan Coats led the expansion and permanent establishment of "election-security task forces" at the FBI, DHS, NSA, and U.S. Cyber Command (USCYBERCOM).[29] In 2018, a federal grand jury indicted 12 Russian military intelligence officers for interfering with the 2016 election (see Figure 1).[30]



WANTED
BY THE FBI

CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS

Boris Alekseyevich Antonov

Dmitriy Sergeyevich Badin

Anatoliy Sergeyevich Kovalev

Nikolay Yuryevich Kozachek

Aleksey Viktorovich Lukashev

Artem Andreyevich Malyshev

Sergey Aleksandrovich Morgachev

Aleksandr Vladimirovich Osadchuk

Aleksey Aleksandrovich Potemkin

Ivan Sergeyevich Yermakov

Pavel Vyacheslavovich Yershov

Figure 1: Russian Officers Wanted by the FBI[31]

In 2019, the US issued economic sanctions against Russians involved with the Internet Research Agency, an organization that manipulates social media for misinformation purposes, as a warning against foreign interference in US elections.[32]

ANALYSIS

Russian Actions

When analyzing Russian election interference efforts from a JIW perspective, this clearly was an instance of unjust IW due to violations of principles I and II. Again, principle I limits just acts of IW to only those directed at entities that endanger or disrupt the well-being of the infosphere. There is no documented record of US-sponsored IW against Russia; the US has never acted tantamount to forfeit its rights within the infosphere, thereby targeting the 2016 election was morally unjust under JIW. Furthermore, principle II dictates that actors in the information environment only wage IW in order to preserve the infosphere's well-being. Having stolen sensitive US voter information, Russian hackers introduced an enormous amount of entropy to the infosphere. Additionally, by leaking campaign members' private emails and spreading major misinformation campaigns via bots or troll factories, Russian actions clearly disrupted the information environment. Such entropy-increasing actions seriously undermined the well-being of the infosphere and created chaos so as to further Russia's political agenda, which further qualifies Russian election interference as an unjust instance of IW.

US Actions

By analyzing the US response to the Russian election interference under the same framework, we conclude that US actions comported with JIW. Russia clearly forfeited its basic (i.e., principle I) rights in the infosphere, thereby exposing itself as a just target of IW. Indeed,the US, as a significant actor within the information environment, was morally obligated to counter Russia's efforts and prevent state-sponsored hackers from further perpetrating entropy in the form of IW. US leaders fulfilled this obligation by taking a defensive approach to IW. Consistent with principle II, the US response sought to reduce Russian IW-caused chaos within the infosphere, specifically with major steps to improve election-security and leveraging legal measures or economic sanctions to more effectively deter Russian IW. The most recent US presidential election perhaps serves as evidence that these efforts are working, as there were no major findings of successful IW attacks.

CONCLUSIONS

Ultimately, our work suggests three main takeaways. First, traditional ethical theories or frameworks do not often apply directly to the cyberspace realm. Second, election interference is becoming an IW vulnerability that democratic countries must safeguard against. Third, JIW provides a relatively new and useful ethical tool for analyzing instances of IW.

Analyzing IW through the lens of JWT confirms that cyberspace poses unique challenges in applying traditional ethical frameworks. As previously indicated, IW seldom involves physical violence, which renders gaging the proportionality of IW attacks and subsequent counterattacks more challenging. IW can include but does not require attack by uniformed soldiers, and countries often unofficially sponsor underground hacking groups, blurring the line between combatants and non-combatants. Attribution poses yet another hurdle in cyberspace warfare; hackers are extremely effective in terms of disguising themselves, making it hard even to identify potential targets of counter-IW.

Given the growing complexity of cyber-attacks, election interference is now an extremely relevant form of IW that countries must protect against. Elections form the basis of democratic legitimacy; therefore, it is essential that the citizens of democratic nations feel fully confident in their results. Countries such as the US are taking extra steps to defend against election interference, specifically by establishing election-security task forces. There also is a need to ensure that international law is kept current with the increasingly sophisticated technology that facilitates foreign election interference.

Indeed, JIW can serve as a useful tool for gaging the ethics of waging IW. Through using JIW to analyze the election interference and corresponding responses, we reveal that many ethical solutions exist in this space. For instance, the US could have undertaken other just actions in response to Russian election interference. The JIW framework is one helpful tool for government leaders and policymakers, who must continue to consider moral justifications for IW when enforcing international law.

DISCLAIMER

Views expressed here are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. Charles H. Hall, "Operational Art in the Fifth Domain," Naval War College, Newport RI, Joint Military Operations Department (2011), https://apps.dtic.mil/sti/pdfs/ADA546255.pdf.
2. William E. Gortney, *Department of Defense Dictionary of Military and Associated Terms* (Washington D.C.: Joint Chiefs of Staff, 2010), https://apps.dtic.mil/sti/pdfs/AD1024397.pdf.
3. Edward L. Waltz, *Information Warfare Principles and Operations* (Norwood, Massachusetts: Artech House, Inc., 1998).
4. Stephanie Gootman, "OPM Hack: The Most Dangerous Threat to the Federal Government Today," *Journal of Applied Security Research,* vol. 11, no. 4 (2016), 517-525, https://www.tandfonline.com/doi/full/10.1080/19361610.2016.1211876.
5. Maria Snegovaya, "Putin's Information Warfare in Ukraine," *Soviet Origins of Russia's Hybrid Warfare, Russia Report*, No. 1 (2015), 133-135, https://www.jstor.org/stable/pdf/resrep07921.1.pdf; Jessica Brandt and Adrianna Pita, "How Is Russia Conducting Cyber and Information Warfare in Ukraine?" Brookings (March 3, 2022), https://www.brookings.edu/podcast-episode/how-is-russia-conducting-cyber-and-information-warfare-in-ukraine/.
6. "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft* (2020), 6-7, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.
7. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 2015).
8. Seth Lazar, "War," *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta, ed. (2020), https://plato.stanford.edu/entries/war/#toc.
9. Ibid.
10. Ibid.
11. Ibid.
12. Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics,* vol. 9, no. 4 (2010), 384-410, https://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404.
13. Luciano Floridi, "Information Ethics, Its Nature and Scope," *SIGCAS Computers and Society*, vol. 36, no. 3 (2006), 21-36, https://dl.acm.org/doi/abs/10.1145/1195716.1195719.
14. Ibid.
15. Ibid.
16. Luciano Floridi, *The Ethics of Information* (Oxford, United Kingdom: Oxford University Press, 2013).
17. Luciano Floridi, "Information Ethics: On the Philosophical Foundation of Computer Ethics," *Ethics and Information Technology*, vol. 1, no. 1 (1999), 33-52, https://link.springer.com/article/10.1023/A:1010018611096.
18. Mariarosaria Taddeo, "Just Information Warfare," *Topoi*, vol. 35, no. 1 (2016), 213-224, https://link.springer.com/article/10.1007/s11245-014-9245-8.
19. Ibid.
20. Ibid.
21. Ibid.
22. Ibid.
23. Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution" (2017), https://www.dni.gov/files/documents/ICA201701 .pdf; Matthew Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *The Intercept* (June 5, 2017), https://theintercept.com /2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/; Kate Fisher, "Russian Interference in the 2016 United States Presidential Election," *Plan II Honors Thesis*—The University of Texas at Austin (2019), https:// repositories.lib.utexas.edu/handle/2152/75445.
24. "S. Rept. 116-290 - Russian Active Measures Campaigns and Interference in the 2016 US Election, Volumes I-V," Library of Congress (2022), https://www.congress.gov/116/crpt/srpt290/CRPT-116srpt290.pdf.
25. Abigail Abrams, "Here's What We Know So Far About Russia's 2016 Meddling," *Time* (April 18, 2019), https://time.com/5565991/russia-influence-2016-election.

NOTES

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Adam Goldman, "F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations," *The New York Times* (April 26, 2019),

https://www.nytimes.com/2019/04/26/us/politics/fbi-russian-election-interference.html.

[30] "Russian Interference in 2016 US Elections," *FBI: Most Wanted* (2022), https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections.

[31] Ibid.

[32] Lara Jakes, "With Sanctions on Russia, US Warns Against Foreign Election Meddling," *The New York Times* (September 30, 2019), https://www.nytimes.com/2019/09/30/us/politics/us-russia-sanctions-election-meddling.html.