Ethical Assessment of Russian Election Interference Using the Framework of Just Information Warfare

Nico Manzonelli, Joseph Zuccarelli

3 May 2022

Introduction

Traditionally speaking, U.S. military doctrine has revolved around four fundamental domains of warfare: land, air, sea, and space. However, in 2010, the U.S. military officially announced the addition of a fifth war domain–cyberspace [1]. The Department of Defense defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" [2]. Over the past decade, the expansion of cyberspace forced military leaders to consider the ability to control, disrupt or manipulate an adversary's informational infrastructure equally important to traditional measures of military strength. Information and communication technologies continually prove to be a useful and convenient technology for waging war, which has led to a revolution in military affairs. This revolution is not solely affecting military leaders, as ethicists and policymakers alike are now being forced to consider how traditional ethical theories can be adapted to address the novelties of this new phenomenon.

In the following article, we use a relatively new ethical framework known as Just Information Warfare (JIW) to assess Russian tactics used to interfere with the 2016 U.S. presidential election. First, we properly define information warfare and describe how concepts from Just War Theory and Information Ethics are merged to create JIW. Next, we provide background concerning our chosen case study–Russian election interference–and analyze the case through the lens of JIW. Finally, we offer up three key takeaways from our work.

Just Information Warfare

Information Warfare

Information warfare (IW) is defined as the use of information and communication technologies devoted to breaching an adversary's informational infrastructure in order to either disrupt it or obtain relevant data concerning the adversary's resources, military strategies, etc [3]. This type of warfare is different from traditional warfare in several respects. Traditionally, war is a necessarily violent phenomenon that involves the sacrifice of human lives and damage to both military and civilian infrastructures. On the other hand, IW enables entities to inflict damage upon an opponent without exerting physical force or violence. Traditional warfare concerns human beings and physical objects, while IW involves artificial and non-physical entities alongside human beings and physical objects. Although the lack of violence and overall non-destructive nature of IW seems to make it desirable from an ethical and political perspective, the disruptive nature of IW can severely damage contemporary information societies and potentially lead to dangerous outcomes. Consider the follwoing examples from the past decade.

In June 2015, the US Office of Personnel Management (OPM) indicated that it had been the victim of one of the largest breaches of government data in US history. The breach compromised extremely sensitive Standard Form 86 documents (SF 86 – Questionnaire for National Security Positions) that are used in the background investigations of prospective federal government employees. These documents include various forms of personally identifiable information such as Social Security numbers, names, dates and places of birth, and addresses. In total, OPM estimated that approximately 21.5 million records from the database were affected by the breach. The overwhelming consensus is that the breach was carried out by state-sponsored hackers working on behalf of the Chinese government. The motive behind the breach remains unclear, yet it is assumed that those involved intended to compile a database of American government employees using the data obtained in the attack [4].

In February 2022, Russia launched a full-scale ground invasion of its western neighbor–the country of Ukraine. Although this conflict has now escalated to the level of physical violence that is typically associated with traditional warfare, there is a history of evidence of Russian-led IW operations aimed at shaping the outcome of the dispute. Prior to the invasion, Russia carried out a long-running propaganda campaign on Russian state media outlets and Kremlin-backed accounts online to cast Ukrainians as Nazis and the perpetrators of genocide against Russian-speakers in eastern Ukraine. The purpose of this misinformation campaign was twofold–to justify the ground invasion of the Ukraine and cast NATO-affiliated countries as aggressors in the conflict [5, 6].

Just War Theory

Ethical analyses of war are typically developed following three main paradigms: Just War Theory (JWT), Pacifism, or Realism. JWT is an ethical framework studied by military leaders, ethicists, theologians, and policymakers that deals with the justification of 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") and *jus in bello* ("right conduct in war"). The former set of principles concerns the morality of going to war, while the latter set of principles concerns the morality of conduct within a war [7]. The following two paragraphs outline each set of principles.

Jus ad bellum typically comprises the following six principles: just cause, legitimate authority, right intention, reasonable prospects of success, proportionality, and last resort. 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 an excuse to achieve some wrongful end. Reasonable prospects of success requires that the entity waging war is reasonably likely to achieve its aims. Proportionality indicates that the expected benefits of waging war must exceed its expected evils or harms. Finally, last resort requires that there is no less harmful avenue to achieve the established just cause [8].

Jus in bello typically comprises the following three principles: discrimination, proportionality, and necessity. Discrimination requires that those involved in the conduct of war must always properly distinguish between military objectives and civilians, and intentionally attack only military objectives. Proportionality indicates that combatants must ensure the harm caused to civilians is not excessive in relation to the military advantage achieved by an act of war. Finally, necessity refers to the fact that combatants must always use the least harmful means feasible when carrying out an act of war [8].

JWT is as old as warfare itself, yet as the nature of warfare has evolved, the application of the principles outlined by JWT has become less clear. This problem mainly arises because JWT focuses on the use of force and violent physical warfare. As previously indicated, the cyber domain is virtual and enables for IW to involve abstract entities. This property of IW severely complicates pivotal concepts defined in JWT such as harm, target, and attack. Discussions of this problem are plentiful in the extant literature [9]. In the following two sections we detail one philosophers approach and proposed solution.

Information Ethics

Information Ethics (IE) is a macro-ethics that enables the analysis of ethical issues by endorsing an informational perspective. This approach follows from the consideration that internet and communication technologies have radically changed the informational context in which moral issues arise, requiring us to rethink the foundations upon which our traditional ethical positions are based [10]. Under IE, the moral value of an entity is determined by its contribution to the enrichment and flourishing of the informational environment. This environment, referred to as the *infosphere*, includes all existing things, physical or non-physical, and the relations occurring between them. The blooming of the infosphere is to be considered the ultimate good, while its corruption or destruction is to be considered the ultimate evil. Any form of corruption or destruction of an informational entity is referred to as *entropy* [11].

Using the two key terms outlined in the previous paragraph, IE outlines four principles for evaluating individuals contributions to the information environment [12]. These four principles are defined as follows:

(i) Entropy ought not to be caused in the infosphere (null law);

(ii) Entropy ought to be prevented in the infosphere;

(iii) Entropy ought to be removed from the infosphere;

(iv) The flourishing of informational entities as well as of the whole infosphere ought to be promoted by preserving, cultivating, and enriching their properties.

Each principle is fairly straightforward. Merging these principles with those outlined by JWT leads us to the final ethical theory discussed in this paper–Just Information Warfare.

Just Information Warfare

Just Information Warfare (JIW) is an ethical framework that merges JWT with IE to establish the necessary and sufficient criteria for evaluating instances of IW [13]. This criteria is defined as follows:

(i) IW ought to be waged only against those entities that endanger or disrupt the well-being of the infosphere;

(ii) IW ought to be waged to preserve the well-being of the infosphere;

(iii) IW ought not to be waged to promote the well-being of the infosphere.

The first principle prescribes the condition under which the decision to resort to IW is morally just. Under this principle, any entity that endangers or disrupts the well-being of the infosphere forfeits its basic rights to exist and flourish within the infosphere and makes itself an illicit target. This principle enables inhabitants of the infosphere to adequately discriminate between proper and improper targets of IW.

The second principle gives other inhabitants of the infosphere a moral obligation to prevent any entity that has made itself an illicit target from causing more evil within the infosphere. In other words, other inhabitants of the infosphere are within their rights to wage IW to re-establish the status quo within the infosphere and repair any damage caused by a malicious entity. Under this principle, IW should fulfill a similar role as police forces in democratic states (i.e., it should only be used as an active measure to reduce or prevent instances of evil within the infosphere).

The third and final principle indicates that IW is never justly waged when the end goal is to improve the well-being of the infosphere. Under the theory of IE, IW is understood as a form of disruption. Therefore, by definition, IW is never to be considered desirable nor a vehicle for fostering the prosperity of the infosphere. Instead, IW is only to be considered a necessary evil used to fight something even more undesirable–the uncontrolled increase of entropy within the infosphere.

One important caveat is necessary–any instance in which an entity wages IW must comply with the principle of *proportionality.* Although we cannot think of proportionality in the exact same context as outlined by JWT, the logic is very similar. In waging IW, the endorsed means must be sufficient to impede the progress of the malicious entity, yet these means must not generate more entropy than the amount aimed at removing in the first place [13].

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 is often considered one of the greatest upsets in U.S. election history. Beyond this point, the 2016 U.S. presidential election is also remembered as a significant instance of Russian election interference. Since 2016, details of the Russian interference efforts have come out in drips and drabs, with information revealed in memorandums released by intelligence agencies, court documents filed by Special Counsel Robert Mueller, testimony from Trump associates in court and investigative news reports [14, 15, 16]. In 2020 the Senate Intelligence Committee released its final report, a nearly one-thousand page document that details Russia's aggressive IW tactics used to influence the outcome of the election [17]. The U.S. intelligence community ultimately came to the conclusion that the Russian interference centered around three goals: to damage the Clinton campaign, to boost the Trump Campaign, and to sow distrust in American democracy overall. They sought to achieve these goals primarily through the use of three tactics: probing state voter databases, hacking the Democratic campaign and its committees, and spreading false propaganda on social media [18].

Although U.S. intelligence agencies concluded that no Russian hackers were able to alter actual votes during the 2016 election, there is evidence of attacks on voter registration systems in at least 21 states prior to election day. Reports indicate that the hackers stole information on approximately 500,000 voters from an unnamed state's database. This voter information included names, addresses, dates of birth, driver's license numbers, and partial Social Security numbers. It is unclear what the Russians did with the information gathered in the breach [18].

Beyond their attacks on U.S. voter registration systems, Russian hackers were also able to successfully access several restricted systems belonging to the Democratic campaign and its committees. In the months leading up to the election, hackers sent phishing emails to various Clinton campaign staffers and volunteers that appeared as Google security notifications.

Using this approach, the hackers were able to gain unauthorized access to several notable campaign members accounts, including chairman John Podesta, and steal tens of thousands of emails. After obtaining these emails, the Russians released them in the run up to election day, creating frequent 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 [18].

While the first two tactics that we've described are primarily classified as traditional cyber attacks, Russia 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 people who post comments on social media in line with the goal of the ordering party, using fake profiles) and bots (i.e., programs that send out messages automatically in response to the appearance of a keyword) on social media to spread misinformation and incite division amongst the electorate. During the months prior to election day these troll factories and bots posted controversial content concerning 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 that criticized the Clinton campaign [18].

In response to the findings on Russian election interference, the U.S. government has since taken steps to better protect against foreign IW tactics while also imposing punitive measures upon Russia. Immediately following the 2016 election, former 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 [19]. In 2018, a federal grand jury sitting in the District of Columbia indicted 12 Russian military intelligence officers for their alleged roles in interfering with the 2016 election (see Figure 1) [20]. In 2019, the U.S. 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 U.S. elections [21].

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

Analysis

Russian Actions

Analyzing Russian election interference efforts under the framework of JIW, it becomes abundantly clear that this was an instance of unjust IW due to violations of principles I and II. Recall principle one, which states that IW ought to be waged only against those entities that endanger or disrupt the well-being of the infosphere. There is no well-documented record of U.S. sponsored IW against Russia; therefore, it appears that the U.S. did not act in any way that would forfeit its rights within the infosphere and make itself an illicit target of IW. Recall principle two, which states that IW ought to be waged to preserve the well-being of the infosphere. Russian hackers introduced an enormous amount of entropy to the infosphere, as they stole sensitive U.S. voter information, leaked private campaign member emails, and created troll factories and bots to start major misinformation campaigns on social media. These entropy-increasing actions did not preserve the well-being of the infosphere in any way; they created chaos in an effort to further the Russian state's own political agenda.

U.S. Actions

Analyzing the U.S. response to the Russian election interference under the same framework, we conclude that U.S. acted in accordance with JIW, specifically principles I and II. Recall principle one, which states that IW ought to be waged only against those entities that endanger or disrupt the well-being of the infosphere. Following from the analysis included in the previous section, it is clear that Russia forfeited its basic rights with its entropy-increasing actions and made itself an illicit target of IW. The U.S., as another inhabitant of the infosphere, had a moral obligation to impede upon Russia's efforts and prevent the hacking groups from perpetrating more evil in the form of IW. U.S. leaders attempted to fulfill this obligation by taking a primarily defensive approach. Recall principle two, which states that IW ought to be waged to preserve the well-being of the infosphere. The U.S., in its response, attempted to remove the chaos caused by Russian IW tactics opposed to inciting more chaos within the infosphere. As indicated previously, the U.S. took major steps to improve election-security task forces and leveraged legal measures and economic sanctions in an effort to more effectively deter Russian IW in the form of election interference. The most recent U.S. 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 highlights three main ideas. First, traditional ethical theories or frameworks are often difficult to directly apply within the realm of cyberspace due to its unique nature. Second, election interference is becoming an increasingly popular form of IW that countries must successfully safeguard against. Third and finally, JIW is a relatively new and useful ethical tool for reasoning about instances of IW.

Cyberspace is posing unique challenges when it comes to the application of traditional ethical theories or frameworks, as discovered when attempting to reason about instances of IW through the lens of JWT. As indicated previously, IW does not often involve physical violence, which in turn makes it difficult to reason about the proportionality of IW attacks and subsequent counterattacks. IW also does not necessarily require uniformed soldiers to carry out attacks, as many countries unofficially sponsor underground hacking groups, which makes it difficult to properly discriminate between combatants and non-combatants. Attribution is another major difficulty posed by the nature of cyberspace; hackers are extremely effective in terms of disguising themselves, making it hard to even identify potential illicit targets of IW.

Given the growing complexity of cyberattacks, election interference is now an extremely relevant form of IW that countries who hold elections must develop protections against. Elections are the basis of democratic legitimacy; therefore, it is essential that the citizens of democratic nations feel fully confident in their results. We've seen that countries such as the U.S. are taking extra steps to defend against election interference, specifically through the establishment of election-security task forces. Perhaps there is also a need for improved international law that protects against foreign election interference.

When it comes to instances of IW such as election interference, JIW can serve as a new and useful tool for reasoning about their ethicality and formulating a proper response. As we found while carrying out this case study, there is no single approved solution within this space; there were other just actions that the U.S. could have taken in response to Russian election interference. Therefore, critical thinking will continue to be necessary on the part of government leaders and policymakers, which can be made easier with guidance from frameworks such as this one.

Disclaimer: The contents of this paper do not reflect the opinions or views of the United States Army. The work presented consists of our personal research and beliefs on JIW and Russian election interference.

References

[1] Charles H Hall. *Operational Art in the Fifth Domain*. Tech. rep. Naval War College Newport RI Joint Military Operations Department, 2011.

[2] William E Gortney. *Department of Defense Dictionary of Military and Associated Terms*. Tech. rep. Joint Chiefs Of Staff Washington, 2010.

[3] Edward L Waltz. *Information Warfare Principles and Operations*. Artech House, Inc., 1998.

[4] Stephanie Gootman. “OPM Hack: The Most Dangerous Threat to the Federal Government Today”. In: *Journal of Applied Security Research* 11.4 (2016), pp. 517–525.

[5] Maria Snegovaya. “Putin’s Information Warfare in Ukraine”. In: *Soviet Origins of Russia’s Hybrid Warfare’, Russia Report* 1 (2015), pp. 133–135.

[6] Jessica Brandt and Adrianna Pita. “How is Russia Conducting Cyber and Information Warfare in Ukraine?” In: *Brookings* (2022).

[7] Michael Walzer. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. Hachette UK, 2015.

[8] Seth Lazar. “War”. In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Spring 2020. Metaphysics Research Lab, Stanford University, 2020.

[9] Randall R Dipert. “The Ethics of Cyberwarfare”. In: *Journal of Military Ethics* 9.4 (2010), pp. 384–410.

[10] Luciano Floridi. “Information Ethics, its Nature and Scope”. In: *Acm Sigcas Computers and Society* 36.3 (2006), pp. 21–36.

[11] Luciano Floridi. *The Ethics of Information*. Oxford University Press, 2013.

[12] Luciano Floridi. “Information Ethics: On the Philosophical Foundation of Computer Ethics”. In: *Ethics and information technology* 1.1 (1999), pp. 33–52.

[13] Mariarosaria Taddeo. “Just Information Warfare”. In: *Topoi* 35.1 (2016), pp. 213–224.

[14] Office for the Director for National Intelligence. “Background to ”Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution”. In: (2017).

[15] et al Cole Matthew. “Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election”. In: *The Intercept* (2017).

[16] Kate Fisher. “Russian Interference in the 2016 United States Presidential Election”. In: *Plan II Honors Theses-Openly Available* (2019).

[17] “S. Rept. 116-290 - RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, VOLUMES I-V”. In: *Library of Congress* (2022).

[18] Abigail Abrams. “Here’s What We Know So Far About Russia’s 2016 Meddling”. In: *Time* (2019).

[19] Adam Goldman. “F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations”. In: *The New York Times* (2019).

[20] “RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS”. In: *FBI: Most Wanted* (2022). URL: `https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections`.

[21] Lara Jakes. “With Sanctions on Russia, U.S. Warns Against Foreign Election Meddling”. In: *The New York Times* (2019).