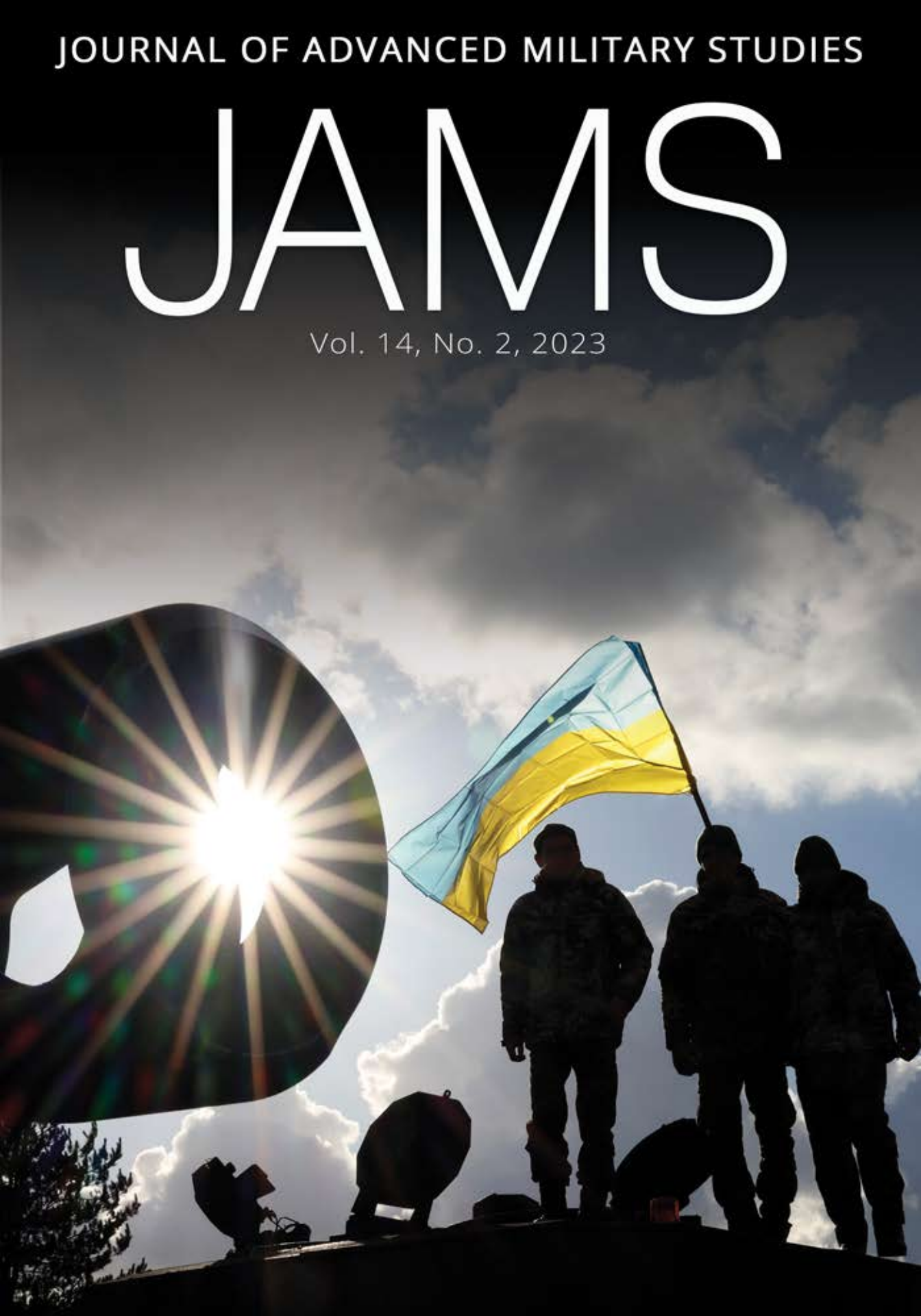
JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

Vol. 14, No. 2, 2023



MARINE CORPS UNIVERSITY
BGen Maura M. Hennigan, USMC
President

Col Mark R. Reid, USMC
Chief of Staff

SgtMaj Stephen J. Lutz, USMC
Sergeant Major of MCU

EDITORIAL STAFF
Ms. Angela J. Anderson
Director, MCU Press

Mr. Jason Gosnell
Managing Editor/Deputy Director

Ms. Stephani L. Miller
Manuscript Editor

Mr. Christopher N. Blaker
Manuscript Editor

ADVISORY BOARD
Dr. Rebecca J. Johnson
Provost
Marine Corps University

Col Mary H. Reinwald, USMC (Ret)
Editor, *Leatherneck Magazine*

Col Christopher Woodbridge, USMC (Ret)
Editor, *Marine Corps Gazette*

Col Jon Sachrison, USMC (Ret)
COO, MCU Foundation

SCHOOLHOUSE DIRECTORS
Colonel Greg Poland, USMC
School of Advanced Warfare

Colonel James W. Lively, USMC
Expeditionary Warfare School

Colonel Brian Sharp, USMC
Marine Corps War College

Colonel Andrew R. Winthrop, USMC
Command and Staff College

Journal of Advanced Military Studies
(Print) ISSN 2770-2596
(Online) ISSN 2770-260X

DISCLAIMER

The views expressed in the articles and reviews in this journal are solely those of the authors. They do not necessarily reflect the opinions of the organizations for which they work, Marine Corps University, the U.S. Marine Corps, the Department of the Navy, or the U.S. government. When necessary, errata will be published immediately following the book reviews. MCUP products are published under a Creative Commons NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) license.

Established in 2008, MCU Press is an open access publisher that recognizes the importance of an open dialogue between scholars, policy makers, analysts, and military leaders and of crossing civilian-military boundaries to advance knowledge and solve problems. To that end, MCUP launched the *Journal of Advanced Military Studies* (JAMS) to provide a forum for interdisciplinary discussion of national security and international relations issues and how they have an impact on the Department of Defense, the Department of the Navy, and the U.S. Marine Corps directly and indirectly. JAMS is published biannually, with occasional special issues that highlight key topics of interest.

ARTICLE SUBMISSIONS

The editors are looking for academic articles in the areas of international relations, geopolitical issues, national security and policy, and cybersecurity. To submit an article or to learn more about our submission guidelines, please email MCU_Press@usmcu.edu.

BOOK REVIEWS

Send an email with a brief description of your interests to MCU_Press@usmcu.edu.

SUBSCRIPTIONS

Subscriptions to JAMS are free. To join our subscription list or to obtain back issues of the journal, send your mailing address to MCU_Press@usmcu.edu.

ADDRESS CHANGE

Send address updates to MCU_Press@usmcu.edu to maintain uninterrupted delivery.

INDEXING

The journal is indexed by ProjectMUSE, Scopus, ScienceOpen, EBSCO, ProQuest, Elsevier, OCLC ArticleFirst, Defense Technical Information Center, Journal Seek, IBZ Online, British Library System, Lancaster Index to Defense and International Security Literature, and AU Library Index to Military Periodicals.

FREELY AVAILABLE AT
WWW.USMCU.EDU/MCUPRESS

Contents

Vol. 14, No. 2

BOOK REVIEWS

The Ethical Character of Russia's Offensive Cyber Operations in Ukraine
Testing the Principle of Double Effect

Lieutenant Ian A. Clark, USN

Abstract: Cyber weapons have the potential to achieve strategic military aims in a manner that reduces physical harm, but they can also be used to enhance and expand the lethality of conventional weapons and tactics. When designed to collect private data, cyber weapons can facilitate assassination, kidnapping, torture, and other severe violations of human rights and international law. Russia's invasion of Ukraine is not the first time that cyber weapons have been deployed for military purposes; however, it is likely the first example of cyber warfare tactics being deployed in a sustained and strategically significant manner in the context of conventional war. To assess the ethical character of Russia's offensive cyber operations against Ukraine, it is helpful to leverage the principle of double effect, which enables a more precise evaluation of the relationship between the intentions that motivate an act and the effects of the act once it has been taken. Drawing on this principle, this article argues that Russia's offensive cyber operations in Ukraine represent an unjust use of force and proposes ways of enhancing the ethical character of cyber warfare in future conflicts.
Keywords: cyber warfare, cyber ethics, Vulkan Files, virtue ethics, just war, principle of double effect

Within minutes of President Vladimir Putin's announcement on 24 February 2022 that Russia was to commence hostilities in Ukraine, explosions could be heard in major Ukrainian cities. Simultaneously, military vehicles and personnel crossed the Ukrainian border.[1] While Moscow sought to downplay the significance of its actions by referring to them

Lt Ian Clark is a chaplain in the United States Navy, currently serving with the United States Marine Corps. He is a PhD candidate in theological ethics at the University of Aberdeen, where his research explores the ethical dimensions of emerging military technologies. https://orcid.org/0009-0009-9325-0239.

simply as a "special military operation," it was clear that Russia had initiated a war of aggression against Ukraine.[2] Russia's attacks, however, were not simply kinetic in nature. Silently, and away from the news cameras, another invasion was also taking place in the domain of cyberspace. In concert with conventional forces, teams of hackers were busy assaulting communications satellites, critical infrastructure, media outlets, financial institutions, and more. Many of these cyberattacks commenced well before the start of physical hostilities and have continued to proliferate in the months since the invasion began.[3] While much has been said and written about the ethics of Russia's wider invasion, this article seeks to explore distinctly the ethical character of Russia's offensive cyber warfare operations against Ukraine.

According to the principles of many ethical systems, assessing the ethical character of an action requires an evaluation of its underlying intentions. To conduct such an evaluation, one might find it helpful to turn to the works of Thomas Aquinas, the medieval theologian and philosopher on whose work much of the contemporary just war theory is built.[4] Beyond his specific comments on war, which this article will also address, Aquinas addresses the ethical use of force more broadly. On the question of whether it is licit to kill in self-defense, Aquinas remarks that "nothing prohibits one act from having two effects, of which only one is within the [agent's] intention, while the other is outside of the [agent's] intention (praeter intentionem)." Aquinas goes on to note that "moral acts are of a particular kind based on what is intended and not according to what is outside the intention."[5] For Aquinas, then, the moral character of an act is rooted in its intention: even if the act produces some adverse outcomes (such as the death or injury of another), it can still be considered morally just if the action is undertaken with a morally right intention (for example, protecting one's own life).[6] While it is customary to understand Aquinas's conclusions as barring intentional killing, Gregory M. Reichberg, a noted scholar of Aquinas, suggests that Aquinas may have sought to differentiate instead between "killing as a means and killing as an end." Within this reading of Aquinas, it is possible to suggest that killing may be an intentional outcome of an action so long as the force that caused that death is "necessary and proportionate" to the threat.[7] Whether one considers killing in a localized manner (such as the killing of an armed intruder in a home) or at the aggregate level (such as a military killing in war), it seems clear that, for Aquinas, what is ethically central is the intention that one has for the end state of a situation.

Aquinas's logic, which has come to be known as the "principle (or doctrine) of double effect," has had vast implications not just in terms of examining cases of self-defense but also regarding how other violent or harmful acts are evaluated, including acts of harm, which occur in the context of armed conflict.[8] Applying this analysis tool to the context of war is not without criticism.[9] The classical just war tradition, for example, takes considerable interest in the effects of military action: militaries must certainly have the right intentions for waging war (*jus ad bellum*) but, significantly, must also conduct themselves in

a restrained manner while prosecuting the war (*jus in bello*).[10] For professional militaries, unintended but foreseen harms need to be carefully considered. Nonetheless, the principle of double effect cannot simply be rejected as incompatible with just war, and it has been used with significant effect in the ethical evaluation of conflict.[11] Michael Walzer, for instance, employs it extensively within his classic work *Just and Unjust Wars*. However, he proposes a slight modification—or perhaps clarification—to Aquinas's argument by suggesting that the double effects of an act (the positive and negative outcomes) are defensible only if they are the product of a *double intention*:

1) like Aquinas, one's intention needs to be a "good" or moral outcome, while
2) the foreseeable evil must be reduced to the fullest extent possible.[12]

This article will apply Walzer's slightly revised rendering of Aquinas's argument by suggesting that an ethical assessment of Russia's offensive cyber operations requires an examination of both their intentions and their desire to reduce harm. This nuance is important generally, but especially so in the context of cyber warfare, as military action in the cyber domain has a particular capacity to be carried out in a manner that minimizes human suffering when compared with conventional arms.

The Vulkan Files: Shedding Light on Russia's Cyber Capabilities

At the end of March 2023, the German magazine *Der Spiegel*, in conjunction with global journalistic partners, published an extensive body of reporting based on a yearlong analysis of documentation leaked by someone with access to critical files maintained by NTC Vulkan, an information technology consulting firm based in Russia. Publicly, Vulkan boasts corporate relationships with well-known firms such as IBM and Toyota Bank. However, according to *Der Spiegel*'s analysis, the firm

> is home to programmers and hackers with a sinister mission: sowing chaos and causing destruction. For example: Paralyzing the computer systems of an airport so that the tower can no longer communicate with planes. Or triggering train derailments using a software program that deactivates all safety controls. Or interrupting power supplies.[13]

It is no secret that Russia has made cyber warfare a central component of its overall warfighting strategy in Ukraine. According to analysis by Microsoft, Russian cyberattacks against Ukraine have been "destructive and relentless" and often utilized in a manner "likely aimed at undermining Ukraine's political will and ability to continue the fight, while facilitating collection of intelligence that could provide tactical or strategic advantages to Russian forces."[14] This reality aligns to the reported efforts being undertaken at Vulkan on behalf of Russian security and defense agencies where tools were developed relating to "all aspects

of modern-day cyber warfare, ranging from censorship and the manipulation of social media content to attacks on critical infrastructure," including a system code named Amezit, which was designed to gain control over electronic communications within specific geographic regions such as the Donbas or Crimea. The leaked documentation also indicated that Vulkan was charged with training personnel on deploying cyber weapons "to execute attacks on critical infrastructure," including rail, aviation, shipping, electricity, and water. Additionally, the files demonstrated that linkages exist between Vulkan and notorious hacker collectives such as Sandworm and Cozy Bear, both of which have been responsible for considerable cyberattacks, including attacks against the United States.[15] As the scholar George Lucas reminds us, "cyber weapons and tactics [that are] designed to attack civilians and civilian (noncombatant) targets" are "illegal, and decidedly immoral, in the conventional case."[16]

Has Real World Harm Been Caused?

Designing cyber weapons capable of inflicting significant damage on an adversary is one thing. It is another for them to be deployed successfully in war. The current conflict between Russia and Ukraine is not the first time one nation has deployed cyber weapons against another.[17] For example, Russia is believed to have launched a significant and far-reaching distributed denial of service attack against Estonia in 2007 and used similar tactics during their short war with Georgia the following year.[18] Arguably the most famous example of cyber warfare was the deployment of the Stuxnet computer worm, which was purportedly developed in a joint Israeli-American venture and deployed against the Islamic Republic of Iran's nuclear program. Discovered in 2010, Stuxnet's deployment resulted in physical damage to Iran's nuclear infrastructure.[19] Nonetheless, the current conflict between Russia and Ukraine is the "first major conflict involving large-scale cyber operations."[20] Like other aspects of Russia's war, these cyber operations have been largely ineffective. Having previous experience with Russian cyberattacks, Ukraine was well-prepared defensively, and the nation was "assisted in its cyber defense by friendly countries and private actors with whom it had developed cooperative relationships before the conflict," a reality that underscores the vital link between defense in the cyber domain and the "soft power" of Ukraine's relationship with "allies, global tech firms, and networks of information security researchers." All of this enabled Ukraine to "mobilize defenses unavailable to others."[21] It is possible also to suggest, as some have, that Russia has demonstrated some restraint in the cyber domain in order to limit the risk of "spillover effects," which "might in turn expand the conflict beyond its kinetic geographic boundaries," a risk that can materialize "much faster and more widely in the cyber domain."[22]

Nonetheless, suggesting that Russia's cyber operations have failed to generate real-world harm would be wrong. In March 2023, for example, the Human Rights Center at the University of California Berkeley law school filed a communication with the International Criminal Court (ICC) regarding "cy-

ber war crimes" committed by Russian personnel against Ukraine. Adopting a broad definition of "violence," which includes the means of an operation and its effects, the communication alleges significant violent practices often directed against civilians and critical infrastructure such as Ukraine's power grid. The complaint states bluntly, "Russian cyber forces have committed serious crimes against victims who suffered real harm."[23]

Ukraine has made similar claims of cyber war crimes. Victor Zhora, chief digital transformation officer at the State Service of Special Communication and Information Protection, has claimed that Russia has launched cyberattacks on Ukrainian thermal energy facilities while simultaniously attacking those facilities with lethal weapons. Zhora notes that similiarly coordinated attacks have been carried out against energy production facilities in the cities of Odesa, Lviv, and Mykolaiv. Each of these attacks used cyber weapons to expand the harm caused by conventional attacks to degrade "data services, IT infrastructure, power grids, telecommunications, and critical infrastructure." Zhora notes that all of these resources and utilities are relied on by noncombatant citizens. In addition, Zhora has claimed that Russia has used "filtration procedures" to access private data owned by noncombatants. This data has been utilized to determine whether individuals were involved in military or political service. In some cases, this illegally seized information was used to capture, kill, or torture those individuals.[24]

A Just Intent?

While the revelations about Russia's offensive cyber operations are startling, they are not surprising. It has long been known that Russia has been investing in and utilizing offensive cyber capabilities.[25] It is equally valid that many of the ambitions behind the Russian cyber weapon program (degrading critical infrastructure and supply channels, undermining command and control capabilities, and exhausting the civilian population) are not unique to the cyber environment.[26] Throughout the history of war, seemingly all nations have sought these same aims through conventional arms and tactics. One could find similar examples in nearly every conflict, modern or ancient.

Not only are these actions common in warfare, but a case can be made that cyber weapons, as a less destructive and less lethal alternative to conventional arms, are morally preferable to the kinetic alternative. In a chapter titled "Moral Cyber Weapons," Dorothy Denning and Bradley Strawser thoughtfully noted that "under certain conditions, [the use of cyber weapons] can actually become morally obligatory. When these conditions are satisfied, states not only have the morally permissible option of using cyber weapons, but a moral duty to do so." They go on to argue that

> states are morally obliged to use cyber weapons in place of kinetic weapons for a just attack whenever doing so does not result in a significant loss of capability. The reason for this moral obligation is that cyber weapons reduce both the risk to one's own (putatively just) military

> and the harm to one's adversary and non-combatants. Overall, cyber weapons are more humane, less destructive, and less risky than kinetic weapons for achieving certain military effects.[27]

Arguments like those made by Denning and Strawser are essential. However, they assume an "either/or" approach to weapon selection wherein states select the weapon system that provides the least lethal means of securing mission accomplishment. A different reality has materialized since Denning and Strawser's work was initially published. Within this new reality, states have tended toward using cyber weapons not as a means of de-escalation or harm reduction but, instead, as a means of supplementing and enhancing the efficacy of conventional attacks. This has been demonstrated in combat, especially in the contemporary Russia-Ukraine conflict, as well as in wargaming, where "substitutive cyber operations play a much more limited role in players' strategies."[28] Modern conflict integrates warfighting capabilities from across all domains, and wargamers are increasingly aware of this reality.

The rise of multidomain warfare, including the cyber domain, has understandably generated considerable interest from major corporations in the technology industry, which are increasingly vital industrial partners for militaries. For example, in the Ukrainian context, Microsoft has provided extensive analysis related to the threats faced by Ukraine's cyber infrastructure. In their determination, Russia has extensively linked its cyber operations and kinetic operations. They note,

> We observed that cyber and kinetic military operations appeared to be directed toward similar military objectives. Threat activity groups often targeted the same sectors or geographic locations around the same time as kinetic military events. Analysis of Microsoft signals with open-source kinetic attack data shows high concentrations of malicious network activity frequently overlapped with high-intensity fighting during the first six plus weeks of the invasion.[29]

Such trends have continued, and while many cyberattacks have lacked destructive capability or have been otherwise thwarted by Ukrainian cyber defenses, they have continued to be used to enhance and expand the destructive potential of Russia's conventional weapons and tactics.

For Russia, the strategy of using cyber operations alongside rather than as a substitute for conventional weapons and tactics should not be surprising. In 2013, for instance, General Valery Gerasimov, then the chief of the General Staff of the Russian Federation Armed Forces, wrote in the military journal *Military-Industrial Kurier* that the "rules of war have changed" and that nonmilitary actions were increasingly critical in achieving strategic success by way of destabilizing an adversary's population. Nonetheless, General Gerasimov notes that the success of these nonmilitary actions "is supplemented by military means of a concealed character, including carrying out actions of informational

conflict."[30] Thus, one can readily conclude that Russia, for at least a decade, has been cultivating a strategy where cyber operations (informational conflict) are seen as a supplement to more lethal forms of military engagement.

Alternative approaches do exist. Understanding cyber weapons as being a potentially morally preferable option to conventional arms can be demonstrated through historical case studies. Consider the Stuxnet computer worm, which caused Iranian nuclear centrifuges to self-destruct. As Lucas points out, Stuxnet was designed to comply with all applicable humanitarian constraints in international law; it only targeted military hardware, did not kill or injure anyone, and resulted in no collateral damage.[31] Additionally, its deployment did not lead to armed conflict, demonstrating that cyber weapons can be utilized as a strategic deterrence tool. Stuxnet demonstrates that an ethical cyber warfare strategy is possible while further underscoring how Russia has intentionally chosen to avoid such a strategy. As Ariel Levite points out in a working paper for the Carnegie Endowment for International Peace, "What sets these operations apart is primarily the Russian willingness to cause extensive collateral damage during its operation, contrasted against the United States' exceptional caution to avoid doing so."[32]

The Principle of Double Effect

Jus ad bellum principles require a state to have a just cause if its wider warfighting efforts are to be considered just.[33] Examples of a just cause include self-defense against an armed attack, supporting an ally, or intervening in dire humanitarian emergencies.[34] In the case of Russia's invasion of Ukraine, the United Nations General Assembly has overwhelmingly condemned Russia's actions as lacking a just cause.[35] Arguably, this renders any military activity conducted by Russia unjust (save, perhaps, for lifesaving efforts). However, even if it were to be assumed that Russia's cause was just—or that it might be just—the essential question that must be asked regarding cyber warfare is this: Is Russia utilizing cyberattacks as a means of reducing the harm experienced by their adversary? This question returns us to our initial "double intention" criteria for assessing this issue through the lens of the principle of double effect.

As Denning and Strawser point out, it is quite possible that a state could use cyber capabilities to answer this question in the affirmative, even while engaging in multidomain warfare.[36] One can imagine a moral actor concerned principally with strategic mission accomplishment while significantly reducing harm to people and property, as was the case with Stuxnet. If this were Russia's ambition, one could see that the principle of double effect could validate the morality of Russia's use of cyber weapons. After all, while some harm might be done to civilians, that harm would ultimately be in pursuit of resolving hostilities less destructively, leading to fewer deaths and reducing the death and destruction associated with war. Such a dual intention would broadly satisfy the ethical standards set forth by the principle of double effect in the context of armed conflict.

This, however, does not appear to be Russia's intent. Far from seeking to reduce harm, Russia's use of cyber weapons appears designed to enhance and expand the lethality of its military's conventional weapons and tactics. For example, Russia's most notable success in the conflict to date in cyberspace was its effective disruption of Viasat satellite services immediately preceding its land invasion, an apparent attempt to undermine communications systems on which the Ukrainian armed forces relied for command-and-control purposes. However, while this attack seems to have fallen short of its broadest goals, it is also apparent that it and other cyber operations conducted before the invasion were not designed to deter hostilities but to better enable them.[37] The intent of this cyberattack seems clear: Russia's aim was not to reduce harm but to expand its ability to make war through more violent and destructive means. This tactic appears to be part of a broader strategy for cyber operations as opposed to isolated cases of malfeasance.

Like previous versions, Russia's most recent 2021 *National Security Strategy* makes limited reference to military ethics and does not provide a moral theory that constrains or guides military activity.[38] It does, however, give much greater priority to the information domain than previous versions, suggesting that "the retention and multiplication of traditional Russian spiritual-moral values" are "the foundation of Russian society" and that some of the greatest threats to these "spiritual-moral values" comes vis-à-vis the cyber domain.[39] It is clear that the Russian Federation seeks to justify an expansion of military activity in this domain by linking it not only to national security but also to national identity and values. At the same time, the *National Security Strategy* does indicate prioritization of "quality of life" and the "wellbeing of Russian nationals" as key goals and guides.[40] While Ukraine, and the wider international community, would strongly disagree with the suggestion that Ukrainians are "Russian nationals," this is indeed a claim that Russia itself has made. Russia has used this as justification for its invasion. President Vladimir Putin, for instance, has regularly referred to Russians and Ukrainians as "one people."[41] In a 2019 interview, President Putin claimed, "I believe that Russians and Ukrainians are one people . . . one nation, in fact."[42] If Russia genuinely believed this to be true, any attack on the Ukrainian people or their infrastructure would seem to conflict with the nation's stated ethical and moral intention of protecting the wellbeing of Russian nationals within their defense strategy. There is a glaring inconsistency between Russia's political and moral rhetoric.

It is true that the notion of "intent" can be somewhat nebulous, which is why Just War criteria also demands consideration of specified and permissable just causes.[43] One might suggest that every nation that has ever gone to war has done so because they believed, from their unique perspective, that their cause was just. Those on the receiving end of military action rarely agree. How, then, can outside parties assess the intent of another? In the case of Russia, we can take their public statements seriously. Russia has made several public statements about its intentions behind invading Ukraine. President Putin, for instance,

has spoken of the threat of the North Atlantic Treaty Organization's (NATO) expansion into the former Soviet bloc, as well as baseless claims of genocide against ethnic Russians and a desire to "denazify" Ukraine, which he addressed when announcing the start of his "special military operation" on the morning of 24 February 2022.[44] While we may acknowledge that there will always be some asymmetric knowledge on this account, it is also important to note that the principle of double effect demands harmony between intent and its corresponding acts. Thus, the principle can be examined in reverse. If we cannot fully understand one party's intent, we can examine their actions and decide whether they have any reasonable connection to the pursuit of justice and peace. In *Ethics and Cyber Warfare,* George Lucas makes space for "an impartial court of public opinion" in determining the legitimacy of cyber vigilantism.[45] This suggests that public perception has a valid role in assessing a given reality's ethical character. A similar logic can be applied here: if this connection cannot be reasonably determined, then we can reasonably conclude that the intention that motivated the action is unjust and, as such, the military action fails to satisfy the principle of double effect.

Let us return to Aquinas's initial example of one who kills in self-defense. For him, the actor's intention is the central locus in judging an act's morality. One can be confronted with two dead bodies: one killed by someone defending themselves and another killed in anger. While the result is the same in both circumstances, only the former can be considered a just act because the intent was not the evil of death but the goodness of self-preservation. However, Aquinas also notes that "an act proceeding from a good intention may be rendered illicit if it is out of proportion to the end."[46] In other words, the harm that is caused must not be excessive or needless. If one needs to kill to defend one's life, so be it. However, if one can defend one's life with other-than-lethal force, all the better. In that case, killing would be unjust because the intention becomes to kill rather than simply do what is necessary to preserve one's life. In this, we can see that Aquinas and Walzer's view of the principle of double effect are well aligned: it is not merely enough to possess a right intention, but one must also fight for that right intention in a manner that does not artificially amplify or justify excessive force.[47] To borrow the language of the International Committee of the Red Cross, it is prohibited to use "means and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering."[48] While this prohibition has generally not yet been extended to cyber weapons, it does provide a particular moral direction about how any instruments of war can be ethically and legally utilized. Such a determination of whether an outcome is "superfluous" or "unnecessary" depends on reconciling those actions to a just intent and reconciling them to what is both necessary and proportionate to realize that intent.

Russia's cyber operations against Ukraine continually fail to satisfy even these basic ethical principles. Whether one examines Russia's cyber warfare strategy through the lens of the court of public opinion, leaked documentation,

or simply by referencing the real-world effects of its actions, the conclusion must be made that Russia's intention for its cyber warfare program is not the deterrence of conflict or the minimization of harm in war, but rather to enhance the lethal and destructive force of their conventional military power while, simultaneously, expanding the war's adverse impacts on noncombatants.

Just Cause and Military Necessity

As previously indicated, the principle of double effect does not always neatly fit within the just war tradition, despite both being derived in large part from the work of Aquinas. This is likely because Aquinas's comments on killing in self-defense imagine a singular individual, while his remarks on war envision the work of a public authority. Aquinas draws a vital distinction between private self-defense and the use of force by representative governments.[49] Nonetheless, their conceptual linkage centers on a shared desire for peace. Just as an individual who needs to defend themselves does not desire to harm another person, the goal of states should be to avoid conflict and, if that is not possible, to achieve victory in a manner that limits war's harmful effects, primarily on noncombatants.

The principle of double effect informs the just war tradition, particularly as it relates to the *jus ad bellum* principle of just cause and the *jus in bello* principle of necessity, both of which are cornerstone elements of the just war tradition. Carefully considering the principle of double effect enables political and military leaders to reflect on their true intentions in carrying out armed conflict and, secondarily, to consider what is necessary to realize that intention.

Interestingly, within his *Summa Theologiae*, Aquinas differentiates between a "just cause" and a "proper intention." His assessment of the former is brief, simply saying that "those who are attacked deserve to be attacked on account of some fault." For some additional depth, he quotes Augustine who wrote (in his *Quaestiones in Heptateuchum*) that just wars "avenge wrongs" when another city or state "has to be punished either for refusing to make amends for what was done unjustly by its subjects or to restore what was wrongly taken." Thus, we can conclude that within the works of Aquinas, a just cause for war can only be a response to harm caused by another party. By contrast, Aquinas explains that a "proper intention" is either the advancement of the good in the world or the avoidance of evil. Quoting Augustine again (in his *On the Words of the Lord*), Aquinas shares that a just war should be "carried on with a zeal for peace, that evil be restrained and the good assisted."[50] In this manner, Aquinas concedes that a war can be prosecuted with a just cause (correction of injustice) and still be morally illicit if the ambition of the military response is vengeance, cruelty, lust for power, and other immoral motivations. This distinction, while nuanced, helps assess Russia's offensive cyber operations in Ukraine because it reveals an essential truth: even if one were to take seriously Russia's claim that their cause is just, it could also be said that their warfighting enterprise remains illicit because their intentions are so ethically distorted.

Regarding military necessity, the principle of double effect requires that any harmful or destructive actions must be in pursuit of a right intention (the restoration of peace) instead of being pursued for their own purposes (the desire to kill or harm). Referencing the English philosopher Henry Sidgwick, Walzer notes that it is not permissible to do "any mischief which does not tend materially to the end [of victory], nor any mischief of which the conduciveness to the end is slight in comparison with the amount of mischief."[51] Said another way, a target is deemed a military necessity—and thus a just target—if and only if striking it is clearly purposeful in relation to achieving the just intention or goal. It is clear, then, that Russia's offensive cyber operations against Ukraine fail to meet these standards.

Conclusion and Application

Russia's invasion of Ukraine has been characterized by egregious breaches of military ethics and human decency, many related to indiscriminate targeting or intentional attacks on civilians. Compared to destroyed apartment buildings, sexual violence, torture, and ruined hospitals, Russia's military activity in cyberspace may seem relatively minor, especially when one considers that they have not been as effective as they were designed to be.[52] Nonetheless, Russia's cyber operations have been extensive, and the nation has long sought to develop disruptive cyber capabilities intended to have an outsized impact on civilian infrastructure and amplify the effects of conventional weapons and tactics. Ukraine and others have suggested that Russia's cyber activity is at least complicit in aiding war crimes.

As the Vulkan leaks have demonstrated, there is a growing potential for cyber operations to bring about significant harm to civilian populations, as well as a genuine appetite for such harm to be realized. The Russia-Ukraine conflict may be the first major conflict that leveraged large-scale cyber operations, but it will not be the last.[53] Countries worldwide, including the United States, are investing in offensive and defensive cyber capabilities, and it is reasonable to assume that cyber will play an ever-expanding role in future conflicts.[54] This is especially true as an increasing share of the world becomes connected to the internet and as the Internet of Things continues to proliferate.[55]

Learning from Russia's ethical failures in the cyber domain, those who desire to fight with honor would do well to remain focused on both their intentions and the effects of their corresponding actions. Ethics demands that war be waged for just purposes, but it also demands that the actions that states take in war—including those taken in cyberspace—be done with the right intentions and in a way that seeks to minimize harm. Cyber weapons do have the potential to achieve these goals while helping nations fight well. However, as Russia has demonstrated, they can also amplify violence, adversely impact noncombatants, and degrade targets that are not of military necessity. Such actions must be avoided in future conflicts. The United States recently released a public fact sheet on the 2023 Department of Defense cyber strategy that concludes with

these words: "With a robust and integrated cyber capability, the Department will work to deter conflict where it can and prevail where it must."[56] This guiding ethos conforms well to the principle of double effect: the stated mission is to deter conflict and minimize harm. However, if it must engage in conflict in the cyber domain, the United States will prevail in accordance with a just intent.

Endnotes

1. Jim Garamone, "Russian Forces in Initial Phase of Invasion of Ukraine, Official Says," DOD News, 24 February 2022.
2. T. D. Gill, "The *Jus ad Bellum* and Russia's 'Special Military Operation' in Ukraine," *Journal of International Peacekeeping* 25, no. 2 (2022): 121–27, https://doi.org/10.1163/18754112-25020002.
3. Cynthia Brumfield, "Russia-Linked Cyberattacks on Ukraine: A Timeline," CSO, 24 August 2022l.
4. The just war theory refers to a body of historical and contemporary ethical, theological, and legal principles related to justifications for war (commonly discussed in its Latin form, *jus ad bellum*) and appropriate military conduct within war (*jus in bello*). Many of these principles have become codified within the laws of armed conflict. The Internet Encyclopedia of Philosophy, accessed 17 June 2023, neatly summarizes the core principles of *jus ad bellum* as "having just cause, being a last resort, being declared by a proper authority, possessing right intention, having a reasonable chance of success, and the end being proportional to the means used." *Jus in bello* principles, by contrast, help to establish ethical norms around target legitimacy and the levels and types of force that can be morally applied. Increasingly, some scholars are pointing to a third category of the just war theory that addresses moral responsibilities following the cessation of hostilities (known as *jus post bellum*).
5. Frederick Christian Bauerschmidt, "Homicide," in *The Essential* Summa Theologiae, 2d ed. (Grand Rapids, MI: Baker Academic, 2021), 228–32.
6. David Whetham and George R. Lucas, *The Relevance of the Just War Tradition to Cyber Warfare*, 1st ed. (Abington, UK: Routledge, 2015), 164–65.
7. Gregory M. Reichberg, *Thomas Aquinas on War and Peace* (Cambridge, UK: Cambridge University Press, 2016), 173–85, https://doi.org/10.1017/CBO9781139095884.
8. Whetham and Lucas, *The Relevance of the Just War Tradition to Cyber Warfare*, 164–65.
9. Eduardo Rivera-López, "The Limited (But Relevant) Role of the Doctrine of Double Effect in the Just War Theory," *Ethics and Global Politics* 10, no. 1 (2017): 117–39, https://doi.org/10.1080/16544951.2017.1396181.
10. Whetham and Lucas, *The Relevance of the Just War Tradition to Cyber Warfare,* 161–64.
11. Whetham and Lucas, *The Relevance of the Just War Tradition to Cyber Warfare*, 164–65; and Rivera-López, "The Limited (But Relevant) Role of the Doctrine of Double Effect," 117–18.
12. Michael Walzer, *Just and Unjust Wars*, 5th ed. (New York: Basic Books, 2015), 156.
13. Nikolai Antoniadis et al., "A Look Inside Putin's Secret Plans for Cyber-Warfare," *Der Spiegel*, 30 March 2023.
14. *An Overview of Russia's Cyberattack Activity in Ukraine* (Redmond, WA: Microsoft, 2022).
15. Antoniadis et al., "A Look Inside Putin's Secret Plans for Cyber-Warfare."
16. George Lucas, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare* (New York, NY: Oxford University Press, 2016), 26.
17. Richard Stiennon, *A Short History of Cyber Warfare*, 1st ed. (Abington, UK: Routledge, 2015), 7–32.
18. Stiennon, *A Short History of Cyber Warfare*, 7.
19. Stiennon, *A Short History of Cyber Warfare*, 20–22. While no nation has formally claimed responsibility for Stuxnet, it has been widely attributed to a collaborative ef-

fort between the United States and Israel called "Operation Olympic Games" within academic and technical literature. For further information, see Josh Fruhlinger, "Stuxnet Explained: The First Known Cyberweapon," CSO Online, 31 August 2022. Fruhlinger notes that "it's now widely accepted that Stuxnet was created by the intelligence agencies of the United States and Israel."

20. James Andrew Lewis, "Cyber War and Ukraine," Center for Strategic and International Studies, 16 June 2022.
21. Patrick Howell O'Neill, "The Propaganda War Has Eclipsed Cyberwar in Ukraine," *MIT Technology Review*, 2 March 2022. It is important to note that Ukraine, too, has sought to develop coordinated "cyber resistance groups" comprised of hackers within and outside of Ukraine. In some cases, these groups have expressed a desire to attack Russian power grids and railroads, although there is no proof that such attacks have been carried out. See *An Overview of Russia's Cyberattack Activity in Ukraine*; and Jason Healey, "Ukrainian Cyber War Confirms the Lesson: Cyber Power Requires Soft Power," Council on Foreign Relations, 4 April 2023.
22. Ariel (Eli) Levite, *Integrating Cyber into Warfighting: Some Early Takeaways from the Ukraine Conflict* (Washington, DC: Carnegie Endowment for International Peace, 2023), 16.
23. "Ukraine Symposium—Accountability for Cyber War Crimes," Lieber Institute, West Point, 14 April 2023.
24. Shannon Van Sant, "Kyiv Argues Russian Cyberattacks Could Be War Crimes," *Politico*, 9 January 2023.
25. Stiennon, *A Short History of Cyber Warfare*, 17–20.
26. *Strategy*, Marine Corps Doctrinal Publication 1 (Washington, DC: Headquarters Marine Corps, 1997), 83–89.
27. Dorothy E. Denning and Bradley J. Strawser, "Moral Cyber Weapons," in *The Ethics of Information Warfare*, ed. Luciano Floridi and Mariarosaria Taddeo (Cham, Switzerland: Springer Cham), 85–103.
28. Jacquelyn Schneider, Benjamin Schechter, and Rachael Shaffer, "A Lot of Cyber Fizzle But Not a Lot of Bang: Evidence about the Use of Cyber Operations from Wargames," *Journal of Global Security Studies* 7, no. 2 (March 2022): 1–19, https://doi.org/10.1093/jogss/ogac005.
29. *An Overview of Russia's Cyberattack Activity in Ukraine*.
30. Valery Gerasimov, trans. Robert Coalson, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review* (January–February 2016).
31. Lucas, *Ethics and Cyber Warfare,* 59.
32. Levite, *Integrating Cyber into Warfighting*, 9.
33. Whetham, and Lucas, *The Relevance of the Just War Tradition to Cyber Warfare*, 162.
34. Whetham, and Lucas, *The Relevance of the Just War Tradition to Cyber Warfare*, 162.
35. George Wright, "Ukraine War: UN Condemns Russian Invasion Ahead of Anniversary," BBC, accessed 8 July 2023.
36. Denning and Strawser, "Moral Cyber Weapons," 89. Denning and Strawser's paper principally relates to the moral obligation of militaries to select weapons that enable mission accomplishment while simultaneously minimizing unnecessary harm. They write, "The just war tradition demands that we avoid unnecessary harm to the extent possible in the prosecution of a just war. If some of the harm of war may be avoidable by using cyber weapons instead of kinetic weapons, it seems that the just war tradition would demand that we so use cyber-weapons, where possible."
37. In an effort to mitigate similar attacks, the U.S. Department of Defense awarded SpaceX a contract to provide Starlink satellite internet to Ukraine. In so doing, the Pentagon noted "the critical nature of these systems" and stated that "satellite communications constitute a vital layer in Ukraine's overall communications network." Amanda Macias and Michael Sheetz, "Pentagon Awards SpaceX with Ukraine Contract for Starlink Satellite Internet," CNBC, accessed 23 July 2023; and Lewis, "Cyber War and Ukraine."

38. "The President Approved the National Security Strategy," Kremlin, 2 July 2021; and Nils Terje Lunde, "Asymmetric Ethics?: Russian and Western Perceptions of War," in *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe*, ed. Janne Haaland Matlary and Tormod Heier (Cham, Switzerland: Palgrave Macmillan Cham), https://doi.org/10.1007/978-3-319-32530-9_11.
39. Julian Cooper, "Russia's Updated National Security Strategy," NATO Defense College, 19 July 2021.
40. Elizabeth Buchanan, "Russia's 2021 National Security Strategy: Cool Change Forecasted for the Polar Regions," Royal United Services Institute for Defence and Security Studies (RUSI), 14 July 2021.
41. Andrew Wilson, "Russia and Ukraine: 'One People' as Putin Claims?," RUSI, 23 December 2021.
42. "Putin: Russians, Ukrainians Are 'One People'," Associated Press, 20 July 2019.
43. By definition, *intent* refers to a yet-unrealized but desired military end state. For instance, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 notes that "the first requirement is to establish what we want to accomplish, why, and how." This "first requirement" is the "clearly identified concept and intent." This statement that intent must be "clearly identified" is a helpful reminder that Just War criteria requires more than simply believing one's cause to be just. Instead, reasonable grounds must exist for believing it is just in relation to specified and permissible causes. As the principle of double effect makes clear, intent is a vital consideration for determining the moral status of an action that yields more than one effect. However, for a warfighting effort to be compatible with the broader Just War tradition, intention must be clearly linked with other defined jus ad bellum principles.
44. Max Fisher, "Putin's Case for War, Annotated," *New York Times*, 24 February 2022.
45. Lucas, *Ethics and Cyber Warfare*, 23.
46. Bauerschmidt, "Homicide."
47. Reichberg, *Thomas Aquinas on War and Peace*, 175; and Walzer, *Just and Unjust Wars*, 56.
48. St. Petersburg Declaration of 1868, "Practice relating to Rule 70. Weapons of a Nature to Cause Superfluous Injury or Unnecessary Suffering," International Humanitarian Law Databases, accessed 21 July 2022.
49. Reichberg, *Thomas Aquinas on War and Peace*, 176.
50. Frederick Christian Bauerschmidt, "War," in *The Essential* Summa Theologiae*: A Reader and Commentary*, 2d. ed. (Grand Rapids, MI: Baker Academic, 2021), 216–20.
51. Walzer, *Just and Unjust Wars*, 128–29.
52. Lewis, "Cyber War and Ukraine."
53. Lewis, "Cyber War and Ukraine."
54. "Fact Sheet: 2023 DoD Cyber Strategy," Department of Defense, accessed 29 May 2023.
55. "Measuring Digital Development: Facts and Figures 2021," International Telecommunication Union, accessed 21 July 2023, 1–2. As of 2021, 63 percent of the world's population used the internet. Between 2020 and 2021, the share of the global population using the internet grew by 5.8 percent, which the agency reports as "in line with pre-crisis rates" (a significant uptick was noted at the onset of the Covid-19 pandemic).
56. "Fact Sheet."