Ethical Implications of Cyber Warfare in Large-Scale Combat Operations

by Glen W. Thompson

Ethical implications of war are an essential part of the Untied States. George Washington, as Commander in Chief of the Continental Army, agreed with his British adversary that the Revolutionary War would be "carried on agreeable to the rules which humanity formed." During the Civil War, President Lincoln approved a set of "Instructions for the Government of Armies of the United States in the Field."[1] Since the inception of the Unites States, rules, instructions, ethics, and laws governed the way we go to war.

Cyberwarfare operations is not a future threat—it is a clear and present danger. Former Secretary of Defense Robert Gates argued in 2011, "Cyberspace and its associated technologies offer unprecedented opportunities to the U.S. and are vital to our Nation's security, and by extension, to all aspects of military operations."[2] Gates argued that cyberspace and its associated technologies were vital to our nation's security in 2011, and they are more of a threat today than they were back then. As technology expands, cyber warfare is increasingly used in large-scale combat operations. This paper considers the ethical implications of cyber warfare in large-scale combat operations.

In 2005, the Department of Defense (DoD) recognized cyberspace as the fifth operational domain, a move that brought cyber operations from a largely supporting effort into an operational space equal to the land, sea, air, and space domains.[3] Cyberspace is an operational domain. It shares the same importance as land, sea, and air. This paper uses the DOD cyberspace definition in *Joint Publication (JP) 1-02, DOD Dictionary of Military and Associated Terms*: "cyberspace is 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."[4] U.S. Army Cyber Command was established in 2010 to defend our nations cyberspace. Army Cyber Command carries the values and fighting spirit into today's missions in the cyber domain.[5]

Cyberspace is an operational domain which conducts missions in cyberspace. The three main cyberspace missions are offensive cyberspace operations, defensive cyberspace operations, Department of Defense Information Network. The Executive Summary in the *Joint Publication 3-12, Cyber Space Operations* states, "These three mission types comprehensively cover the activities of the cyberspace forces. The successful execution of cyber operations requires integration and synchronization of these missions."[6] Cyberspace missions are offensive and defensive.

Cyberspace missions are tasked by the Joint Staff, combatant commands, United States Cyber Command, the service cyberspace component commands, and combat support agencies. They establish a framework for the employment of cyberspace forces and capabilities. The Army is a profession ran buy trusted professionals. According to *Army Doctrine Publication 6-22*, chapter 1, the Army Ethic "is a set of enduring moral principles, values, beliefs, and laws that guide the Army profession and create the culture of trust essential to Army professionals in the conduct of missions, performance of duty, and all aspects of life."[7] The Army has legal and moral foundations to make decisions based on. The U.S. Constitution, executive orders, law of land warfare, and rules of engagement to name a few. Just War Theory and the Law of Armed Conflict provide some framework for assessing the moral justification of cyber warfare.

Just War Theory

The ethic of just war is rooted in Western philosophy. It comes from practices of ancient Greeks fighting other Greeks. According to Roland Bainton in his book, *Christian Attitudes toward War and Peace*, "Just War was commonly accepted well before Plato and Aristotle (428-398 BC).[8] Later Ambrose, Augustine, and Thomas Aquinas continue to build on the theory. The Just War Theory is framed by two questions: (1) "When is going to war justified?" and (2) "How should justified war be conducted?" There are eight principles before going to war (*jus ad bellum*), and seven principles while fighting justly in war (*jus in bello*). It would be prudent for all echelons of leadership to consult the just war tradition before engaging in large-scale combat operations when using cyberspace missions.

Total Military Insight published an article, "Understanding Just War Theory: Ethical Frameworks for Conflict." The editorial team concluded that legitimate authority, just cause, right intention, proportionality, and last resort ensure ethical conduct in cyberspace missions.[9] Although Just War Theory has been around for millennia, it is as relevant today as it was since originated.

Law of Armed Conflict

Another framework to access the moral justification of cyber warfare is the Law of Armed Conflict. According to *Field Manual 3-0*, paragraph 1-46, Law of Armed Conflict can be defined as an "extensive joint combat operations in terms of scope and size of forces committed. Conducted as a campaign aimed at achieving operational and strategic objectives. Typically involves operations by multiple corps and divisions. Typically includes substantial forces from the joint and multinational teams and often includes both conventional and irregular forces on both sides."[10] During large-scale combat operations, commanders must select the best course of action to accomplish cyberspace missions. The best course of action must first be ethical, effective, and then efficient.

Commanders must run cyberspace missions through military necessity. The cyberspace mission must be directed at a legitimate military objective. The cyberspace mission must not be towards civilian objectives and protected property and protected places. Cyberspace missions must be proportionate to minimize civilian death, injury, and property damage. Cyberspace missions must comply with the Laws of War Armed Conflict and international laws. Ultimately, cyberspace missions must be fought honorably. There must be fairness in offense and defense, mutual respect between our adversaries, and war fought in good faith.

In addition to domestic law, cyberspace missions can interfere with international law. There must be framework for responsible war during cyberspace missions in large-scale combat operations. We will examine International Humanitarian Law (IHN), the Cyber defense National Atlantic Treaty Organization (NATO), and the United Nations Charter.

International Humanitarian Law (IHL)

It is common knowledge that cyberspace missions have become a reality in large-scale combat operations. We will see some examples of the ethical implications of cyber warfare from the Russia's invasion in Ukraine. The International Committee of the Red Cross is concerned of the increasing use of cyber operations during large-scale combat operations. The international humanitarian laws cyber operations coincide with the laws of armed conflict. There are cyber capabilities that qualify as weapons and are by nature indiscriminate and are prohibited.[11] They focus on military necessity, distinction, proportionality, unnecessary suffering, and honor.

The International Committee of the Red Cross (ICRC) limits cyberspace missions during armed conflicts just as any other weapon, means and methods of warfare. There is potential human cost of cyberspace missions. The ICRC states that it is possible for "belligerents to infiltrate a system and collect, exfiltrate, modify, encrypt, or destroy data. A variety of "targets" in the real world can be disrupted, altered, or damaged, such as industries, infrastructures, telecommunications, transport, or governmental and financial systems."[12] Cyberspace missions can expose services that can bring harm to civilians and noncombatants. The ICRC highlighted eight rules to keep cyber operations ethical: 1) do not direct cyber operations against civilian objects; 2) do not use malware

or other tools that spread automatically and damage military objectives and civilian objects indiscriminately; 3) when planning a cyber operation against a military objective, do everything feasible to avoid or minimize the effects your operation may have on civilians; 4) do not conduct any cyber operation against medical and humanitarian facilities; 5) do not conduct any cyber operations against objects indispensable to the survival of the population or that can release dangerous forces; 6) do not make threats of violence to spread terror among the civilian population; 7) do not incite violations of international humanitarian law; 8) comply with these rules even if the enemy does not. Ethical implications abound.

National Atlantic Treaty Organization (NATO)

It is wise for any nation ready to execute cyber operations to abide with international law. NATO and their allies have been working to defend its networks against the growing sophistication of the cyber threats they face. At the 2016 NATO Summit in Warsaw, allied heads of state and government reaffirmed NATO's defensive mandate and recognized cyberspace as a domain of operations in which NATO must defend itself.[13] Since 2002, NATO has been protecting its communications and information systems. After the cyber-attacks against Estonia, NATO approved its first Policy on Cyber Defense in 2008. NATO has held multiple day cyber conferences to discuss cyber collaboration and create policies to achieve defense objectives. NATO has held summits creating policies to defend against and counter the full spectrum of cyber threats. In 2024, the NATO Summit was held in Washington, D.C., the "Allies agreed to establish the NATO Integrated Cyber Defense Centre to enhance protection, situational awareness, and the implementation of cyberspace as an operational domain."[14] They have gone to great lengths to bring together decision-makers across the political, military, and technical levels so that no one violates any of the policies.

United Nations Charter 2.4

According to the research report from the General Assemble First Committee Cyber Warfare and Article 2.4 of the United Nations Charter written by the chair, Nika Engelen, "cyber warfare creates chaos. It also violates the territorial integrity and sovereignty of states, and therefore also the United Nations Charter, specifically article 2.4, which is a severe violation of international law."[15] In essence, article 2.4 of the UN Charter prohibits the use of force against the territorial integrity or political independence of any state.

These principles aim to ensure that cyber warfare is conducted in a manner that respects the law of armed conflict and international law. This helps to minimize harm to civilian and civilian infrastructure. A violation to anyone of these laws can break lasting peace between nations. Cyberwarfare fought unjustly can have long-term consequences, making it difficult to ensure peace and stability.

It is required that commanders request a legal review before employing cyber weapons and cyber weapon systems. It states in the *Commander's Handbook on the Law of Land Warfare* that "prior to fielding or deploying any weapon system, including non-lethal weapons, cyber weapons and cyber weapons systems, DOD requires the legal review of the acquisition or procurement be reviewed to ensure compliance with all applicable U.S. domestic law and international law, international agreements, customary international law."[16] Commanders must receive a legal review by an attorney authorized by the Military Department so that there would not be any ethical implications from cyber operations.

Command and control need to be established at all levels. There must be command and control for global and multinational cyber operations. Also, there must be command and control for cyber operations supporting combatant commanders that work with U.S. Army Cyber Command. The command and control must be nested with the Unified Command Plan, National Military Strategy, the Department of Defense Cyber Strategy, and the Department of Defense for Operating in the Information Environment. There are many ethical and legal implications if command and control is not established while executing cyberspace operations.

Ethical Implications

There are ethical and legal implications if one is not following the laws and policies both domestically and internationally. The ethical implications of cyber warfare in large-scale combat operations are far-reaching if not

fought justly. This last section addresses the law of war and cyber operations from Just War Theory and Russia's cyber operations in Ukraine.

Ethical Implications and Just War Theory

The updated 2023 Department of Defense *Law of War Manual* is the authority of lawful and unlawful practices to keep war ethical and legal. Some examples of cyber operations include, "operations that use computer to disrupt, deny, degrade, or destroy information resident in computers and computer networks. Ethical and lawful cyber operations may include reconnaissance (e.g., mapping a network), seizure of supporting positions (e.g., securing access to key network systems or nodes), and pre-emplacement of capabilities or weapons (e.g., implanting cyber access tools or malicious code).

Cyber Operations and *Jus Ad Bellum*

The *Law of War Manual* lists several issues under the law of war governing the resort of force. There must be legal and moral reasons to go to war. There are several examples to legally and justifiably engage in a war or an armed conflict. The first issue of cyber operations includes triggering a nuclear plant meltdown. This could lead to horrific consequences. Civilians could lose their lives, environmental damage, and long-term health effects. The second issue, opening a dam. This could lead to flooding, destruction of civilian homes and infrastructures. This too could lead to a significant loss of life. The third issue presented for cyber operations, disabling air traffic control. This could result in airplane crashes which could endanger many civilian lives.[17]

Cyber Operations and *Jus in Bello*

Again, the *Law of War Manual* makes distinctions that set legal and moral rules that govern how two militaries fight justly in combat. One example, a cyberattack that would destroy enemy computer systems could not be directed against civilian infrastructure (e.g., stock exchange, banking systems, and universities). Another example, cyber operations must be necessary to achieve a legitimate military objective and would be unnecessary to attack nonmilitary objectives. Cyber operations must avoid causing unnecessary suffering or harm to civilians.[18]

Russia's cyber operations in Ukraine

Russia has been executing cyber operations in Ukraine since 2014.[19] In 2015, Russian hackers targeted Ukraine's power grid, causing widespread blackouts. This attack disrupted electricity supply to hundreds of thousands of people and demonstrated the potential for cyber operations causing significant harm to civilian infrastructures. There were many more cyber-attacks between 2016 and 2021. Public institutions, banks, postal services, newspapers, transport infrastructure and businesses were impacted.

According to the European Parliament, in 2017, NotPetya malware hit the Chornobyl nuclear power plant and close to 13,000 devices used by public institutions, were hit. The malware had a global impact, affecting sixty-five countries and about 50,000 systems, including European and US companies, FedEx, Maersk and Merck, and inflicting a loss of over U.S. $10 billion.[20]

Conclusion

The ethical implications of not following the laws of war are significant. Clear policies and guidelines for the use of cyber operations must be flowed. International cooperation develops a common ground for the use of cyber operations. There are many ethical implications reported from Russia's cyber operations in Ukraine. Principles of distinction and proportionality have been undermined. Cyber operations can violate international law and ethical principles. Some implications can cause civilian harm when not executed ethically. There could be an erosion of ethical and moral standards resulting in desensitization and loss of credibility. Cycles of violence can provoke retaliation and escalation. Global stability is at risk when one undermines international order which could cause future violations.

Endnotes

1 Department of Defense *Law of War Manual*. June 2015 (Updated July 2023), iii.

2 *Joint Publication 3-12*, *Cyberspace Operations,* 08 June 2018, 1-1.

3 U.S. Joint Chiefs of Staff. *Capstone Concept for Joint Operations*, Joint Publication ver 2.0 (Washington, DC: U.S. Joint Chiefs of Staff, August, 2005), 7.

4 *Joint Publication (JP) 1-02. Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (as amended 30 September 2010), 118.

5 *Our History | U.S. Army Cyber Command. n.d.* www.arcyber.army.mil. https://www.arcyber.army.mil/About/History/.

6 *Joint Publication 3-12. Cyberspace Operations,* 08 June 2018, vii.

7 *Army Doctrine Publication 6-22. Army Leadership*, 1-44.

8 Bainton, Roland H. 2008. *Christian Attitudes toward War and Peace*. Wipf and Stock Publishers, 49.

9 Team, E. (2024, July 5). *Understanding Just War Theory: Ethical Frameworks for Conflict – Total Military Insight*. The Insurance Universe. https://totalmilitaryinsight.com/just-war-theory-2/

10 *FM 3-0. U.S. Army Operations*. October 2022, 1-46.

11 "ICRC Position Paper: International Humanitarian Law and Cyber Operations during Armed Conflicts." 2020. International Review of the Red Cross. March 2020. https://international-review.icrc.org/articles/ihl-and-cyber-operations-during-armed-conflicts-913#footnoteref10_t5rqyoe.

12 International Committee Red Cross. *International Humanitarian Law and Cyber Operations during Armed Conflicts*, November 2019; available at, https://safe.menlosecurity.com/doc/docview/viewer/docNCFC3682AC36784b6801e3e6f69290b639e333aaf263246a25ed11846c5d6b986c61a86f829a9

13 NATO. 2024. "Cyber Defence." NATO. July 30, 2024. Https://www.nato.int/cps/en/natohq/topics_78170.htm.

14 Ibid.

15 2025. Menlosecurity.com. 2025. https://safe.menlosecurity.com/doc/docview/viewer/docN3E883271578F494a64a9ff758b86ae71034c1598ef4baf06730833cb4958f549e27fd7f61324.

16 *Field Manual 6-27/MCTP11-10C. The Commander's Handbook on the Law of Land Warfare*, 07 AUG 2019, 2-33.

17 Department of Defense. *Law of War Manuel*, 1036.

18 Roscini, Marco*, The Applicability of the jus in bello to Cyber Operations*, *Cyber Operations and the Use of Force in International Law* (Oxford, 2014; online edn, Oxford Academic, 16 Apr. 2014), https://doi.org/10.1093/acprof:oso/9780199655014.003.0003.

19 Przetacznik with Tarpova, *Russia's War on Ukraine: Timeline of Cyber-attacks*, June 2022, https://safe.menlosecurity.com/doc/docview/viewer/docNF37E9E586D781b1756e47f7c021b0e95f0d158f5e17a6e4d31557462824f3b42ea65c5f3ea3c.

20 Ibid.