The Ethics of Cyber War in Ukraine:
A Consideration of the Ethics of Small-Scale Conflict without Arms.

By CH (MAJ) Robert Cox
Regimental Chaplain and Ethics Instructor
U.S. Army Signal School
Cyber Center of Excellence
Fort Gordon, GA

Prepared for the Combined Arms Center Ethics Symposium
April 2023

Abstract: The cyber-attacks attributed to Russia against Ukraine before and during the current Russian war against Ukraine are unjust. That assertion is based on the simple consideration that the cyber operations were part of a larger war. And that war fails the principles of *jus ad bellum* and *jus en bello*. This paper will seek to answer whether those types of attacks are properly considered cyber war by examining the nature and even existence of cyber war as a legitimate category. The paper will argue that cyber operations fall into the category of soft war or gray zone operations. The paper will also consider the sufficiency of the current rules and morals required to regulate and inform cyber operation ethics. The principle of *Jus Ad Vim* will be introduced to enhance ethical consideration of cyber-attacks short of war.

Introduction

At the end of the large-scale Crimean War in 1856, Britain, France, and other nations created a concise piece of international maritime law, the Paris Declaration Respecting Maritime Law.[1] The intent of this declaration was, in part, to abolish privateering as an acceptable action and privateers as acceptable actors in Naval warfare. Privateering was a long-used form of naval hybrid war. A privateer was a private citizen in a privately owned warship. The warship was also called a privateer. The State authorized the citizen to seize, attack, or otherwise target the interests of an enemy state, including private commercial interests.[2] Pirates and privateers were

[1] ICRC Database. "Treaties, States Parties and Commentaries, Declaration Respecting Maritime Law. Paris, 16 April 1856". https://ihl-databases.icrc.org/en/ihl-treaties/paris-decl-1856?activeTab=default (Last accessed on 03.04.2023)

[2] The Editors of Encyclopedia Britannica. "Privateer." Encyclopedia Britannica, February

difficult to distinguish. They conducted the same category of actions, seizing and attacking. Pirates lacked authorization and freely targeted anything, making them criminals. Privateers could be considered state-sponsored pirates who had a level of legitimacy. As such, the category of privateers clouded legitimate combatants, actions, and targets.

The Paris Declaration is presented to introduce a point for reasoning from analogy, shaping the thoughts about cyber war and cyber-attacks on Ukraine. Professor George Lucas describes our current state,

> *It seems for the moment that in the cyber domain, we dwell virtually in a lawless frontier, a state of nature, in which the most unscrupulous and effective cyber warriors do as they wish, and (to paraphrase Thucydides) the weaker and more vulnerable desperately seek the best bargain they can get.*[3]

Lucas' description could also apply to the age of pirates and privateers. Apart from the geographical and geopolitical parallels in Crimea, there is now as then uncertainty about the nature of the actions, actors, and targets. For instance, was targeting a neutral ship carrying goods from an enemy country legitimate? A current analogy could be a hacktivist targeting a neutral country's bank that manages enemy finances. Then there is agency and the nature of the action. A cyber-attack conducted by an opportunist for private gain would be analogous to piracy and thus criminal. Is the same action made legitimate if done by an agent of the State to achieve operational objectives in support

---

27, 2023. https://www.britannica.com/technology/privateer

[3] George Lucas, "Evolution of Norms in Cyberwarfare" in Justice at the Margins of War: The Ethics of Espionage and Gray Zone Operations. ed. Edward Barrett (Annapolis: Naval Institute Press, 2022) 137

of strategic aims? The Paris Declaration stated that its purpose was to clear up such uncertainty,

> That the uncertainty of the law and of the duties in such a matter, gives rise to differences of opinion between neutrals and belligerents, which may occasion serious difficulties and even conflicts.[4]

The Paris Declaration reduced confusion by arguably ending state-sponsored pirating. It also shows the potential of international law to bring clarity to the hybrid edge of war, at least historically, in the sea domain. The recent calls for international law and policy on cyberwarfare is a call for certainty and restraint parallel to the conditions of the Paris Declaration.[5]

What is Cyber War?

The definition of cyber war, or more formally, categorizing the ontological nature of actions in cyberspace, is essential in making ethical determinations.[6] The nature of the action will dictate the relevant rules and help to determine if just war theory correctly applies to this category of actions. International consensus on law or policy is hampered by the conflation of terms and disagreement on the essence of cyber actions. Dr. Randal Dipert, one of the first to write on the ethics of cyber warfare, reflected that "Cyberattack technology is more like an idea than like a physical thing (or person)."[7] In

---

[4] ICRC Database. "Treaties, States Parties and Commentaries, Declaration Respecting Maritime Law. Paris, 16 April 1856".

[5] Andy Greenberg, *Sandworm: A New Era in Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Doubleday: New York) 293. This was a central theme of Greenberg's and also Dipert's. Randal R. Dipert. "Ethics of Cyberwarfare." Journal of Military Ethics 9, 4 (2010): 384-410. George Lucas addresses the need in both *Ethics and Cyberwarfare* and "The Evolution of Norms in Cyberwarfare."

[6] Cameran Ashraf, 274; James A. Lewis. "Cyber War and Ukraine." Center for Strategic and International Studies. (2022)

[7] Randal R. Dipert. "Ethics of Cyberwarfare." Journal of Military Ethics 9, 4 (2010): 384-410

his article, *Cyber War and Ukraine,* James Lewis's passing comment, "the term [cyber war] itself makes little sense."[8] Difficulties arise when "cyber war" is used as a popular non-technical term like "war on poverty."[9] Some authors use the term 'cyber warfare' as a distinct term from cyber war, and others use the terms interchangeably. Several analysts deny the existence of cyber war as a distinct category of war.

Consider if the actions of modern privateers or state-sponsored hacktivists could be placed in the category of acts of war.[10] Note that an affirmative answer, hacktivists can conduct acts of war, would be significant. Not all would agree. But that affirmation does not require the concomitant existence of cyber war. The cyber theorist could affirm that a long-established category of actors, such as spies, mercenaries, privateers, and partisans, can use computers, networks, and related cyberinfrastructure to do their work. It could be asserted that the computer doesn't constitute a substantive change to the nature of their work. If their work was an act of war before computers, it remains so now. If it wasn't an act of war before computers, conducting it in cyberspace doesn't categorically change that. By extension, conducting an action in cyberspace also wouldn't change the ethical assessment of the action.

At one end of the spectrum of thought on cyber war is Professor Thomas Rid, who argued that cyber war doesn't exist.[11] At the other end of the spectrum is former

---

[8] James A. Lewis, "Cyber War and Ukraine" Center for Strategic and International Studies (2022): 1

[9] George Lucas, *Ethics of Cyberwarfare* (Oxford: Oxford University Press, 2017) 27

[10] Ibid

[11] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (Oct 2012): 5

Counterterrorism Czar Richard A. Clarke, who titled his book *Cyber War: the next threat to National Security and What to Do about it*[12].

Professor Cameran Ashraf, an authority in public policy and humanitarian law, sets the stage for doing what could be considered practical ontology in his article, "Defining Cyberwar: towards a definitional framework." He categorizes and describes the components that could constitute a concept of cyber war. His framework involves three themes that account for five different variables.[13]

Ashraf identifies the themes, Alarmist, Skeptic, and Realist, representing different schools of thought on cyber war. Alarmists, like Clark, assert that cyber warfare exists. They focus on the threat of cyber war fought in the cyber domain, causing real-world harm. Skeptics, like Rid, are not convinced cyber war exists as a distinct concept or category of conflict. Skeptics consider cyber war an ontological error or categorical fallacy. Skeptics see cyber actions as equivalent to sabotage, espionage, and propaganda done on a computer.[14] Realists hold the middle ground. They acknowledge the threat of attacks in cyberspace and so aren't skeptics. But the realists focus on defining cyber action and the other variables in and through the existing international legal framework grounds them from being alarmists.

---

[12] R.A Clarke, R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*. Harper Collins. (2010)

[13] Ashraf, "Defining Cyberwar," 276

[14] Rid, "Cyber War Will Not Take Place," 5

The strength of Ashraf's framework is in the variables he identifies as actions, actors, effects, geography, and targets. With the variables, Ashraf has given scholars and analysts a standard lens to evaluate cyber war and its ethical implications.

Scholars would use the action variable to determine what cyber actions rise to the level of war. Actions such as cyber vandalism and reversible attacks would be actions below the level of war. Actors determine who are valid combatants and who bears responsibility or moral agency. The developing consensus is that identifying the actor enables evaluating the act.[15] In the case of a state acting against another state, the actions are evaluated on a scale sliding from competition through conflict to war. If the actor is an individual or non-state organization, the actions are evaluated on a scale of competition to crime. The developing consensus is that states should bear a level of responsibility for the actions of the criminal actors in their territory.

The analyst would use the effects variable to discuss the outcomes of the action, intended and unintended. Singer and Friedman identify the effects of a cyber-attack as the primary legal justification for determining if the attack was an act of war.[16] An act of war would require casualties and or physical destruction. In May 2020, Israel narrowly avoided a cyber-attack on a desalination plant. The attack would have had devastating effects had they not countered it. Yigal Unna, then the head of Israel's National Cyber

---

[15] Ashraf, "Defining Cyberwar," 276

[16] Peter W. Singer, Allan Friedman, *Cybersecurity and Cyberwar: What Everyone needs to know* (New York: OUP 2014), 134

Directorate, declared the attack “cyber war” due to its intended effect to do significant real-world damage.[17]

Ashraf used the geography variable to describe how various scholars philosophically conceived of cyberspace. The views range from cyberspace being part of the state's sovereign territory to a separate proxy domain. Unna considered the cyber-attack on the water plant an attack on and in Israel's sovereign territory. The US Department of Defense defines cyberspace as a global domain of interconnected hardware, software, and data.[18] Brad Smith at Microsoft comments,

> The internet’s global pathways mean that cyber activities erase much of the longstanding protection provided by borders, walls, and oceans. And the internet itself, unlike land, sea, and the air, is a human creation that relies on a combination of public and private-sector ownership, operation, and protection.[19]

The geography of cyber actions, like Dipert’s description of a cyber-attack, is more of an idea than a physical place.

The target of a cyber-attack helps to define the idea of cyber war and identify the school of thought. The alarmist views critical infrastructure like the Israeli water plant as targets of cyber war. The skeptic views data, IT systems, or low-level targets as the usual and likely attacks. The problem with building a case for cyber war based on targeting is that targeting suffers from deficiency or excess. That is, espionage done on

---

[17] Aron Heller, “Israeli cyber chief: Major attack on water systems thwarted,” APNEWS.com May 28, 2020 https://apnews.com/article/63c081ec091f4c1e3f438ee35243efe0

[18] Catherine A Theohary, “Defense Primer: Cyberspace Operations,” Congressional Research Service In Focus, IF10537. https://crsreports.congress.gov

[19] Brad Smith, “Forward,” Microsoft. “*Defending Ukraine: early lessons from the Cyber War”.* (Redmond: Microsoft Corporation, 2022): 1

cyber systems doesn't rise to the level of an act of war. And the destruction of crucial infrastructure exceeds cyber war and goes to the level of terrorism or a war crime.

Determining the variables becomes essential in the assessment of a cyber operation. Consider this extreme hypothetical: the attributed actor was a state-sponsored Iranian team. The action was to infect Israeli cloud files stored in European data centers. The target was essential civilian infrastructure. The extreme effect was to achieve political ends by creating chaos through real-world devastation. A cyber expert such as Yigal Unna would call such an instance cyber war. But it takes the aggregate of those variables to reach a full assessment. Even in the aggregate, such an extreme attack, as mentioned above, is closer to terrorism or sabotage than armed conflict.

Another very real but extreme example is the 2017 NotPetya attack on Ukraine. The state actors were Russian GRU members of unit 74455, also known as the Sandworm team.[20] The intended targets were Ukrainian power, transportation, and financial infrastructure. The problem was that the effects spread well beyond the intended political end of crippling Ukraine on their national holiday. The effects spread across Europe, famously crippling the Maersk shipping conglomerate and causing billions in worldwide damages.[21] The fallout for Russia was the destruction of trust with European countries and rounds of more sanctions. The criminal charges and indictments against six Russian GRU members are important for this discussion.[22] The

---

[20] Greenberg, *Sandworm,* 269

[21] Ibid

[22] U.S District Court, Western District of Pennsylvania. *United States v. YURIY SERGEYEVICH ANDRIENKO, et al*. Criminal Case 20-316. (Oct 15, 2020)

U.S. declared the actors to be criminals. Cyber law expert Matthew McCabe describes how the attack fell short of war.[23] The effects were financially devastating but with no physical damage or casualties that are requirements for war. The victims were dispersed geographically, unrelated to any military ends. NotPetya, as an action, was disconnected from the military use of force. It was devastating but not war. It was more closely related to vandalism and propaganda. If it is not war, the Just War theory is not helpful.

In "The Evolution of Norms in Cyber Warfare," George Lucas suggests that the categories of soft war and unarmed conflict are his preferred designations for the actions of cyber warfare.[24] He also adopts grey war or grey zone operations as an appropriate category for understanding cyber warfare. Grey war would include espionage and actions of statecraft that fall just below conflict in the competition-to-conflict continuum. He says, "there seems to be no question whatsoever that cyber conflict resides at the center of whatever that grey zone otherwise designates."[25] Actions like Stuxnet would seem to fall in this category.[26] Lucas also coined the term state-sponsored hacktivism calling it the "new face of warfare in the twenty-first century."[27] State-sponsored hacktivists engage in irregular and unconventional warfare.

---

[23] Matthew P. McCabe, "Perspective: NotPetya was not Cyber 'War'" MarshMcLenna, (AUG 2018) https://www.marshmclennan.com/insights/publications/2018/aug/notpetya-was-not-cyber-war.html (accessed April 13, 2023)

[24] Lucas, "The Evolution of Norms in Cyber Warfare," 129

[25] Ibid, 130

[26] Lucas, *Ethics and Cyber warfare, 33*

[27] Lucas, *Ethics and Cyberwarfare*, 11

Some state-sponsored hacktivists are cyber privateers or freelance hackers working for the state. For others, like unit 74455, the devolving pattern is for state-sponsored hacktivists to be regular military forces posing as and acting like criminals. The units pose as criminal or vigilante groups to exploit cyber-attack attribution problems. This pattern counters the Alarmist prediction that military units would advance up the scale to devastating broad sweeping real-world attacks. The trend is for states to conduct cyber operations in the grey zone while devolving into the arena of actions once performed by criminals, vigilantes, and vandals rather than escalate into full acts of war.

Do the Principals of Just War apply?

If ethics is a combination of moral principles and external laws,[28] the question is, what is the law? For the last decade, there has been a debate over the insufficiency of international humanitarian law and laws of armed conflict to address the cyber actions of one state against another. The general presupposition has been that the current law is insufficient and new international agreements must be created.[29] That presupposition motivated writing the *Tallinn Manual on the International Law Applicable to Cyberwarfare* and the *Tallinn Manual 2.0*.[30] These works, in what Ashraf might call a Realist theme, try to demonstrate how current international law applies to cyber warfare and cyber operations. They do this partly by arguing from analogy, showing that international law speaks to cyber operations. The first manual applied the laws of armed

---

[28] Lucas, *Ethics and Cyberwarfare*, 40 - Chapter two introduces this theme which is repeated throughout the book. *See also:* Department of the Army, APD 6-22, The Army Leadership and the Profession. (Washington, DC: Government Printing Office, July 2019) 1-6

[29] See note 5 above.

[30] Michael N Schmitt,and Liis Vihul eds. *Tallinn Manual 2.0: The international law applicable to cyber operations.* (Cambridge: Cambridge Univsersity Press, 2017)

conflict to extreme cyber warfare. It demonstrated that the cyber-attacks which result in real-world damage fall under the parameters of the law. Lucas' evaluation is that the first Tallinn manual failed practically and philosophically. It drew analogies between cyber actions and existing crimes but did not bring clarity. It raised as many questions as it answered. Philosophically the declarative legal positivism of the manual ignores the need for international consensus.[31] Or, as Walzer states, "The lawyers have constructed a paper world, which fails at crucial points to correspond to the world the rest of us live in."[32] The Tallinn manuals showed that international law speaks to cyber warfare. But they unintentionally demonstrated the insufficiency of current international law to address the range of activity in cyber warfare.

The Budapest Convention on Cybercrime in 2001 and the second additional protocol of 2022 are examples of building international law through international moral consensus on cyber activity.[33] This is the kind of consensus needed for effective and applicable international law to clarify and regulate cyber warfare. The Paris Declaration of 1856 was similarly built on an international consensus. But the consensus wasn't built quickly. Privateers had been used in one fashion or another since the 1250s.[34] Hopefully, developing a consensus on cyber warfare will take less than 600 years.

---

[31] Lucas, Ethics and Cyberwarfare, 76

[32] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (Basic Books: New York, 2015), XXV

[33] Council of Europe, "Details of Treaty No. 185"

[34] Britannica, "Privateer."

The current international law on cyber warfare needs clarity. While the law is a necessary but insufficient guide, it still functions. Cases are being built now using international law to bring charges of war crimes against Russia to the International Criminal Court. The range of charges includes cyber warfare crimes.[35]

It is not that cyber operators don't have laws or that the law is completely ineffective. There are abundant Federal laws and US government rules and regulations that apply to DOD cyber operators and their peers in other agencies. The list of laws, rules, and policies is complex enough that the DOD created a helpful color-coded cybersecurity policy chart.[36] The chart has well over a hundred policies, rules, and regulations for cyber security operators.

The laws of war are most helpful when considering cyber actions as part of a multidomain operation during large-scale combat operations. When combined with combat operations, the full range of the moral force of Just War theory and the rule of international convention applies to the design and execution of cyber actions as part of the operation.

In addition to improving international law, there is potential for improvements to the moral theory of Just War that speaks to the non-extreme grey war actions. The Just War theory traditionally has two primary principles *jus ad bellum* and *jus in bello*. Michael Walzer introduced the concept of *jus ad vim*, the just use of force, or the use of

---

[35] Andy Greenberg, "The Case for War Crimes Charges Against Russian's Sandworm Hackers," *Wired*, May 2022

[36] Cybersecurity & Information Systems Information Analysis Center, "The DOD Cybersecurity Policy Chart 13MAR23," https://csias.org/csiac.org/resources/the-dodocybersecurity-policy-chart (Acessed 4APR 23)

force short of war, to the Just War discussion.[37] Jus ad vim applies to cyber operations by informing responses of limited use of force to grey zone conflicts that are short of jus ad bellum. Jus ad vim would add moral constraints to grey zone espionage and statecraft. It would relieve the pressure to tolerate cyber intrusions, cyber vandalism, and other minor conflicts that violate sovereignty but are short of a cause for war. Professor Daniel Brunstetter and ethicist Megan Braun developed principles for *jus ad vim* as: Just cause and last resort, Proportionality, the probability of Escalation, and Maximizing the rights of others through right intention and legitimate authority.[38] These principles build on Waltzer's concept and clarify when using force is morally allowed while maintaining moral restraint. These moral principles could inform international conventions but also require international affirmation and the force of law.

The recent Russian cyber-attacks since the February 2022 invasion of Ukraine have been muted in their effectiveness at achieving a military outcome and far less effective than in 2014.[39] After the initial flurry, Russian attacks have been fewer in number. The attacks that have happened are coordinated with kinetic actions but not always successfully. The Microsoft Report, "Defending Ukraine: Early Lesson from the cyber war," explains that the muted effectiveness of Russian cyber actions is due to several factors, such as the robust cyber defense Ukraine developed through years of

---

[37] Walzer, *Just and Unjust Wars, 2006, ix-xviii*

[38] Daniel Brunstetter and Megan Bran, "From Jus ad Bellum to Jus ad Vim: recalibrating our understanding of the Moral Use of Force," *Ethics and International Affairs* 27, no. 1 (2013)

[39] Lewis, "Cyber War" 1

experience.[40] It is also due to Ukraine developing strategic public and private partnerships. As the war has progressed, Russia has focused on using cyber-attacks as part of a combined attack with conventional kinetic use of force.[41] That tactic is one of the best operational uses of cyber-attacks and their effects. In doing so, the cyber-attacks now are less a violation of the laws of war and Just War principles than before the war. But they are still part of an unjust war, and so are unjust actions.

Conclusion:

At its extreme, independent cyber warfare actions can rise to the level of the use of force with effects commensurate to those of armed conflict. That level is easily achieved if the cyber action is part of a well-planned and coordinated multidomain operation. But the standard role of cyber warfare is in grey zone operations. State-sponsored hacktivists as a category of cyber actors is troubling. State-sponsored hacktivists tend to adopt actions considered criminal if done by a private organization or individual. International Law and the moral principles of Just War speak to all the variables of cyber warfare, but the principles are often insufficient. An international consensus and the development of specific laws clarifying and restraining cyber war are needed. In addition, the principle of *jus ad vim*, the use of force short of war, is a guide for the moral use of force in the grey zone conflict short of war.

---

[40] Microsoft. "*Defending Ukraine: early lessons from the Cyber War".* (Redmond: Microsoft Corporation, 2022):7-8

[41] Microsoft, "Defending Ukraine" 8

Bibliography

Ashraf, Cameran. "Defining cyberwar: towards a definitional framework." *Defense & Security Analysis*, 2021: 274-294.

Britannica, T. Editors of Encyclopedia. "Privateer." Encyclopedia Britannica, February 27, 2023.https://www.britannica.com/technology/privateer.

Brunstetter, Daniel, and Megan Braun. “From Jus Ad Bellum to Jus Ad Vim: Recalibrating Our Understanding of the Moral Use of Force.” *Ethics & International Affairs* 27, no. 1 (2013): 87–106. doi:10.1017/S0892679412000792.

Clarke, R. A., & Knake, R. *Cyber War: The Next Threat to National Security and What to Do About It*. Harper Collins, 2010.

Dipert, Randall R. "The Ethics of Cyberwarfare." *Journal of Military Ethics* (Routledge) 9, no. 4 (2010): 384-410.

Dubik, James M. *Just War Reconsidered: Strategy, Ethics, Theory.* Lexington: University Press of Kentucky, 2016.

Finlay, Christopher J. "Just War, Cyber War, and the Concept of Violence." *Philos. Technol.*, no. 31 (2018): 357-377.

French, Shannon E. *The Code of the Warrior.* New York: Rowan & Littlefield, 2017.
Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremiln's Most Dangerous Hackers.* New York: Doubleday, 2019.

Lewis, James A. “*Cyber War and Ukraine.”* Center for Strategic and International Studies, 2022.

Limnell, Jarno. "The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainin War." *International Journal of Cyber-Security and Digital Forensics*, 2015: 521-531.

Lucas, George. *Ethics and Cyber Warfare.* Oxford: Oxford University Press, 2017.

Lucas, George. "The Evolution of Norms in Cyberwar." In *Justice at the Margins of War*, by Edward Barrett, 129-144. Annapolis, MD: Naval Institute Press, 2021.

Martin, P.E.C. *Cyber Warfare Schools of Thought: Bridging the Epistemological/Ontological Divide.* JCSP 41, Toronto: Canadian Forces College, 2015.

Maschmeyer, Lennart, and Myriam Dunn Cavelty. "Goodbye Cyberwar: Ukraine as Reality Check." *CSS Policy Perspectives* 10, no. 3 (2022): 1-5.

Microsoft. Defending Ukraine: early lessons from the Cyber War. Redmond: Microsoft Corporation, 2022.

Nato Review, “Cyberwar- does it exist?” 13 June 2013https://youtu.be/OuZpqlCI1Wo (Last accessed on 04.08.2023)

Rid, Thomas. “Cyber War Will Not Take Place.” Journal of Strategic Studies 35, no.1 (2012), 5-32 DOI: 10.1080/01402390.2011.608939

Schmitt, Michael N. , and Liis Vihul. Tallinn Manual 2.0: The international law applicable to cyber operations. Edited by Michael N. Schmitt, & Liis Vihul. Cambridge: Cambridge University Press, 2017.

US, Department of the Army, FM 3-12, Cyberspace Operations and Electromagnetic Warfare. Washington, DC: Government Printing Office, August 2021.