On the Relationship Between the Ethics and the Law of War: Cyber Operations and Sublethal Harm

Edward Barrett

Why do we need dialogue between ethical and legal perspectives on norms governing the initiation and conduct of interstate conflict? This essay will examine this question by first critiquing a legal analysis of a new form of conflict: military cyber operations. These operations possess an unusual combination of characteristics as they (1) do not involve munitions moving through space and across borders, (2) often originate from or traverse innocent third-party states, (3) can be difficult to attribute, (4) are often purveyed by nonstate actors, and (5) frequently produce effects that do not neatly coincide with legal definitions such as "uses of force." As a consequence of these unusual characteristics, experts have labored to apply to cyber operations existing legal frameworks that govern international violence. The most influential effort to date has been the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*; and while it is for the most part ethically commendable, this essay will begin by highlighting several of the manual's ethical shortcomings and will then extract general reasons why international law nevertheless must be informed by ethical analysis.

That said, the second part of the essay will affirm the importance of law for ethical analyses of justified responses to the burgeoning phenomenon of sublethal harms. While states have always used sublethal harms to weaken adversaries economically, militarily, ideologically, culturally, and politically, technological developments have magnified the regularity and effectiveness of these practices, particularly against free societies. For example, an open Internet enables the theft of intellectual property and weapons plans and the distribution of politically

Ethics & International Affairs, 31, no. 4 (2017), pp. 467–477.

doi:10.1017/S0892679417000454

destabilizing information. I will argue that responses to such attacks may include —in addition to defensive countermeasures—punishments that deter and reform, and may target "indirect participants" such as financial supporters. I will further argue that justified responses will require insights gleaned from criminal and tort law.

International Law and Cyber Operations

At the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence, and in response especially to cyber operations against Estonia in 2007, the *Tallinn Manual* was produced by a distinguished "International Group of Experts" from the legal and cybersecurity fields in order to "examine how extant legal norms applied to this 'new' form of warfare."[1] The manual's two parts roughly correspond to issues associated with, respectively, the *initiation* and the *conduct* of armed conflict—which are examined by ethicists under the rubrics of *jus ad bellum* and *jus in bello* criteria. Its treatment of the initiation of conflict includes what constitutes legally prohibited uses of force and legally justified responses (such as countermeasures); what constitutes an "armed attack," which triggers the right to defensively respond with force under the UN Charter's Article 51; the rights and responsibilities of innocent third-party states; and attribution requirements and cases of delayed attribution. Its treatment of the conduct of armed conflict—which coincides with "the law of armed conflict"—focuses on defining attacks in the cyber realm and identifying the persons and objects immune from such attacks. It should be noted that because "neither treaty application nor State practice is well developed in this field," the manual's experts decided to include their differing positions, which are often presented—and will be referred to herein—as the "majority" and "minority" views.

The manual remains the definitive work on these topics and continues to influence law and policy, and most of its conclusions are ethically sound.[2] However, because its analyses are grounded in extant legal norms without direct reference to underlying philosophically derived ethical norms, it remains an occasionally flawed treatment of the relevant issues.

To begin, the manual's purely legalistic assumptions—derived from applicable treaties and customary international law—can generate ethically problematic definitions of just cause. Functionally, Article 51's concept of armed attack and the ethical concept of just cause are the same: they define a *casus belli* to which one

may justifiably respond with lethal defensive force. But the related legal definitions of "uses of force" and "armed attacks" can—from an ethical perspective—lead to both overly permissive and overly restrictive conclusions. Following international law, the manual defines uses of force as acts "that injure or kill persons or damage or destroy objects."[3] Those of sufficient "scale and effects" are deemed armed attacks.[4] On the one hand, this framework can be too permissive vis-à-vis property. Ethically speaking, large-scale property destruction and damage do not in themselves justify lethal defensive harm; the property in question must be life-sustaining, and this prerequisite is not intrinsic to the definition of armed attack. On the other hand, this framework can be too restrictive vis-à-vis persons. From an ethical perspective, one may respond to unjustified and culpable threats to life with lethal force if necessary; the scale of death is irrelevant.[5] While legally limiting forceful responses to cases of armed attack–level fatalities might promote utility, it also might contravene the moral right of self-defense. This problem accounts for the "contrary view" of the United States following the International Court of Justice's 1986 *Nicaragua* judgment, which asserted that "any illegal use of force can qualify as an armed attack triggering the right of self-defense; there is no gravity threshold distinguishing illegal uses of force from armed attacks."[6]

In addition to being simultaneously overly permissive and restrictive, legal definitions of just cause can also be arbitrary because of the way in which judgments are made. What counts as harm sufficient to rise to the level of an armed attack is determined through practice, which in reality can mean that the definitions of stronger parties will prevail. Reliance on international law therefore does little to discourage wars initiated by the powerful in defense of "national interests" that merely support a desired standard of living. A dialogue between ethics and international law thus serves to provide necessary critiques of self-serving legal interpretations of both kinetic and cyber operations.

A second *ad bellum*-related flaw in the manual involves the relationship between culpability and just cause. In assessments of whether an armed attack has occurred, the experts were "divided over the issue of whether the effects in question must have been intended." The minority of experts asserted that espionage "unexpectedly result[ing] in significant damage" should not be considered an armed attack. On the other hand, the majority concluded that "intention is irrelevant in qualifying an operation as an armed attack and that only scale and effects matter."[7] According to their analysis, victims of unintentional grave harm would possess a right to respond in kind, if necessary. But from an ethical perspective,

the majority's position is erroneous. Culpable acts are those done intentionally, freely, and with knowledge or vincible ignorance of the relevant normative and empirical facts; and only culpable murderous acts compromise one's capacity for justice and dignity to the degree required to forfeit one's right to life and incur liability to lethal defensive harm. Although the response advocated by the manual's majority would be *excused* if the victim were unable to know that the act was unintended, the response would still not be *justified*.[8]

Third, the discussion of *ad bellum* proportionality is problematic primarily because it misunderstands the criterion, which requires that the total expected good caused by a war outweighs the total expected harm. Instead, the manual asserts that the issue at hand is "how much force . . . is permissible once force is deemed necessary" (that is, once last resort has been satisfied), and concludes that the proportionality criterion limits this amount to "that required to end the situation that has given rise to the right to act in self-defense."[9] In other words, the manual stipulates that the *ad bellum* criterion of proportionality, instead of ensuring that the goods at stake are commensurate with anticipated harms, requires one to use only a necessary amount of force to put an end to the situation. One can easily imagine a case in which this leads to massive defensive retaliation to stop a much less harmful attack. Additionally, the entire analysis is misplaced, as the imperative to use only necessary amounts of force is an *in bello* issue.

Fourth, the manual's treatment of when temporary functionality losses would qualify as a just cause is self-contradictory. Like kinetic weapons, cyber weapons can physically destroy or damage computers. But because of their potential to be transitory or reversible, cyberattacks can also merely compromise functionality. While permanent losses of functionality can create the same effect as physical destruction, temporary functionality losses are unique to cyber operations and require additional analysis. Part of the manual's discussion on functionality occurs in the *in bello* section that defines a cyberattack. Associating attacks on objects with damage or destruction, the majority asserted that interference with functionality would qualify as damage and thus constitute a use of force only if "restoration of functionality requires replacement of physical components."[10] Accordingly, a transitory or reversible loss of function not requiring the replacement of physical components would constitute neither an attack nor, by extension, a just cause. But elsewhere in the manual some experts argue that actions not resulting in physical damage would qualify as an armed attack if the ensuing negative effects were

https://doi.org/10.1017/S0892679417000454 Published online by Cambridge University Press

extensive—although others still maintain that direct "harm to persons or physical damage to property" is a precondition for an armed attack.[11] Ethically speaking, justified responses would be a function of both an attack's culpability and overall effects. Assuming culpability, a temporary loss of the functionality of a system that was not physically damaged would be a *casus belli* if the event resulted in death, for example, in the event of the temporary disabling of an air traffic control system that caused mass casualties.

Fifth, from an ethical perspective, although the manual's treatment of *in bello* proportionality is excellent, it could be improved in one way: Since civilians on both sides retain all of their rights, one should not dismiss consequences such as loss of email or banking services from collateral damage calculations.[12] Of course, such costs could be awarded relatively low values.

Sixth and finally, the manual unfortunately adopts a purely legal approach to targeting nonparticipating civilians, arguing that cyber operations that do not qualify as "uses of force"—ones that merely inconvenience—may be intentionally directed against civilian objects such as computers. Interference with functionality is permitted if physical repair or operating system reinstallation is not required.[13] Data, related or unrelated to functionality, is also targetable.[14] Large-scale email blockage also does not qualify as an attack.[15] Additionally, and as mentioned earlier, none of these harms need to be minimized or considered in collateral damage proportionality assessments. That these conclusions follow logically from their premises demonstrates the danger of purely legal approaches. From an ethical perspective, intentionally harming civilians, in addition to usually being strategically ineffective, is unjust. In peacetime or wartime, persons who have not culpably transgressed the rights of others have forfeited none of their own, and are not liable to any degree of harm—not even the inconveniences described above. Accordingly, domestic and international statutes should define these injustices as punishable crimes, and appropriate executive and legislative oversight should be implemented. And if nonparticipating civilians are to be affected by cyber operations before or during war, these effects must be minimized and weighed in the ways currently associated with, respectively, economic sanctions and dual-use objects.

With these ethical critiques in the background, I suggest four broad reasons why ethics should continue to guide the international law of cyber conflict specifically and of war more generally. First and most fundamentally, securing moral rights that are universally possessed, and that do not simply evaporate or become

https://doi.org/10.1017/S0892679417000454 Published online by Cambridge University Press

violable when "war" breaks out, is a primary *raison d'être* of international law. As Adil Haque has trenchantly argued, international humanitarian law (IHL) should not merely "aim to balance military and humanitarian considerations, permitting types of killing that generally are necessary for military victory and prohibiting types of killing that generally are not."[16] Instead, IHL should "prohibit morally unjustified killing and thereby protect human rights."[17] Second and related, the fact that the interests of the most powerful states often determine international laws and shape their interpretation requires a countervailing ethical conversation. In the post-9/11 debate over the nature and permissibility of torture, for example, ethical arguments have been crucial. Third, the fact that valid legal reasoning can recommend targeting nonparticipating civilians is unsettling and further indicates that a dialogue between ethics and law is necessary. Especially when confronting new frontiers such as the cyber realm, ethical principles must be revisited.

Fourth, although complex situations may require the laws of war to be based on a pragmatic ethical fiction, ethical analyses can highlight the moral benefits of altering such situations. For example, contemporary revisionist just war scholars rightly insist that when one warring party is in the wrong, its combatants are not the moral equals of the defending combatants. But given epistemic uncertainty and the human propensity to punish perceived wrongdoers, laws that assume the moral equality of combatants may minimize harm. Nevertheless, revisionist arguments highlight the moral imperatives to alleviate uncertainty and permit selective conscientious objection. Existing institutional proposals to mitigate uncertainty such as the one suggested by Jeff McMahan might be hobbled by practical problems, but constraints might change over time and proposals that are presently inadequate might eventually lead to successful ones.[18] And even if epistemic uncertainty remains an intractable problem, clarity about the ontological and moral status of combatants might encourage more robust efforts to explore nonlethal alternatives.

Ethically Justified Responses to Sublethal Harm

Thus far the emphasis has been on law as the handmaiden of ethics. But an emerging trend in international conflict—which includes cyber operations—will require the law's assistance in determining morally justified responses to wrongdoing. In the late 1700s, Immanuel Kant wrongly predicted that the increasing destructiveness of war would eventually encourage states to seek peace through

https://doi.org/10.1017/S0892679417000454 Published online by Cambridge University Press

global governance. Instead and increasingly, they are maximizing their relative power by continuously harming adversaries through a combination of lethal and sublethal actions that avoid crossing and even redefine the legal threshold of "cause for war."[19] The "unrestricted warfare" strategy outlined by two Chinese People's Liberation Army colonels in 1999 presaged this trend, and it is now widely recognized as a significant aspect of "hybrid" or "gray zone" conflict.[20] These tactics have typified Russian actions in its near abroad in Ukraine, Georgia, and the Baltics, and include DDoS attacks, election manipulation, and cyber theft. While the ethics of responding to lethal harm has been examined for centuries as part of the just war tradition, more work needs to be done on justified responses to sublethal harms in the international system.[21]

Victims have the moral right to defend themselves from unjustified sublethal harms. At the same time, any intentional defensive harm is justified only if the attacker has forfeited the rights affected by such harm—life, bodily integrity, freedom, property, reputation—through his wrongdoing and thus has become liable to it. Accordingly, many of the same concepts govern justified sublethal and lethal defensive harms. First, as discussed above, only culpable agents of harm are liable to sublethal defensive harm.[22] Second, agents intending to inflict sublethal harm are liable to *anticipatory* defensive harm only if actively preparing to do so. Third, because of a wrongdoer's worth as a human being, agents of sublethal harm are liable to defensive harm only when it is both effective and necessary for the defense of actual or potential victims.[23] McMahan has argued that the effectiveness requirement differentiates liability and desert; a person "can deserve to be harmed, and there can be a reason to harm him, even if harming him will not prevent or rectify any other harm."[24] Concerning necessity, if passive defenses would be effective, active defensive harm would be unjustified. Fourth, agents of sublethal harm are liable only to defensive harm that is (narrowly) proportionate. The harm done to the wrongdoer must be commensurate with the importance of the rights being defended. Framed differently and as mentioned above, the wrongdoer must have forfeited the rights that such harm would otherwise violate.

When we turn to proportionality, an important difference arises between justified responses to lethal and sublethal harms. While the concept applies to both, murderers and unjust combatants are liable to *lethal* defensive harm, but agents of sublethal harm normally are not.[25] In cases of sublethal attacks, because the unjustified harms involved are not life-threatening, the wrongdoer retains the right to life and is not liable to be defensively killed. By analogy, killing a

pickpocket, even if doing so were effective and necessary for defense from theft, would be unjustified. However, this constraint on responses to sublethal harms creates two possibilities with defensive ramifications that do not obtain for lethal defensive harms: inflicting *punitive* harm, and targeting *indirect* participants.[26] Let me explain both.

First, on the ethics of inflicting punitive harm, consider the increasingly common case of recurring cyber theft from banks. In a domestic context, many would accept that incarcerating the perpetrators is justifiable as a defensive measure to stop the cyber thief from continuing to commit the crime. But we could also argue that punitive harms, which impose hard treatment during incarceration—for the purposes of retribution, general deterrence of other would-be cyber thieves, specific deterrence to discourage the perpetrator from engaging in future cyber theft, or reform of the perpetrator—may be justifiable as well. Human rights require both that punishment serves a purpose and that it does not treat wrongdoers as means—respectively ruling out retribution/desert (no purpose) and general deterrence (wrongdoer treated as a means) as grounds for punishment. But under these prohibitions the specific deterrence and reform of the wrongdoer would remain valid consequentialist grounds for punishments, which would allow such punishments as an extremely austere standard of living and noncompensatory fines. Of course, a cyber thief's liability to these measures would require that they be not only proportionate but also effective and necessary. Apropos the relationship between ethics and law, it must be emphasized that the experience embedded in statutes, case law, and law enforcement should be the source of judgments about effectiveness and necessity vis-à-vis deterring and reforming criminals. Therefore, we cannot determine which punitive measures are ethically permissible without the law. And if justified punitive measures eventually deter or reform the cyber thief, both punitive and defensive harms would become unnecessary and the thief should be freed. Over time, precisely because of justified sublethal punitive harm, our cyber thief would become nonliable to any harm.

On the other hand, in an international context, ethically justified defensive responses to sublethal harm can be frustrating. Incarceration of the cyber thief might be impossible because of a host state's noncooperation and the inability to capture the wrongdoer through an otherwise permissible intervention. Passive defenses might prove ineffective. The sublethal defensive countermeasures to which the wrongdoers are liable might not sufficiently degrade harmful capabilities. However, because proportionate responses in these cases are sublethal,

https://doi.org/10.1017/S0892679417000454 Published online by Cambridge University Press

additional and proportionate punitive harm would be permissible if effective and necessary for the relevant purposes.[27] Given that the lack of incarceration would make reform unlikely, the purpose of such harm would be specific deterrence. Accordingly, these punitive measures would seek not to degrade harmful capabilities, but instead to mitigate malevolent intentions by harming the wrongdoer's standard of living—especially personal property and reputation. Again, the legal community's insights about effective and necessary measures will be better informed than those of philosophers. And if effective, harms with a punitive purpose will have a defensive effect, and perhaps render further harms unnecessary.

A second possibility created by this scenario is the targeting of indirectly participating civilians. The ethics and law of war rightly draw a bright line around civilians, who are at worst only indirectly responsible for unjustified lethal harms and are not liable to be killed. But indirect participants in unjustified lethal or sublethal attacks may be liable to sublethal harms, a difference that comports with criminal law. Therefore, noncooperative political leaders of the territory where a wrongdoer resides as well as civilian accomplices would surely be liable to some form of defensive and punitive sublethal harms. The combination of these countermeasures and punishments might be enough to reduce the harm and even coerce state cooperation. Determining to which harms indirect participants are liable, and relatedly which responses will defend and deter, will require deeper collaboration between ethicists and lawyers.

Conclusion

While there may be nothing completely new under the sun in the realm of security concerns, in recent years a shift in emphasis has occurred. The good news is that increasingly destructive weapons technologies have induced states to avoid periodic large-scale wars. The bad news is that enhanced abilities to weaponize communications and information systems will allow states and nonstate actors to undermine societies—especially liberal democratic societies—in myriad important ways. Although some of this activity will be lethal and may fit comfortably within existing frameworks on the ethics and law of war, certain characteristics (such as nonkinetic means, attribution challenges, and temporary functionality losses) will require careful work to apply these frameworks. As ethical shortcomings of the *Tallinn Manual* indicate, this work will require close collaboration between ethicists and lawyers. On the other hand, most of this activity will consist of

continuous sublethal harm, for which the UN Charter, IHL, and the *ad bellum* and *in bello* criteria of the just war tradition are ill-suited. Regardless of the gravity of harm, because human rights are moral rights, normative analyses of inflicting and responding to harm should be grounded in ethics and then implemented through law. Whether at peace, war, or somewhere in between, a form of legal positivism focused only on fair procedures for making laws perverts both domestic and international politics.[28]

NOTES

[1] Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013). Hereafter referred to as "the manual."
[2] For an improved version, see Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).
[3] Schmitt, *Tallinn Manual*, p. 48.
[4] Ibid., p. 55.
[5] While the manual's predominant position is that not every fatal use of force rises to the level of an armed attack (for example, see ibid., Rule 11, para. 9 and especially Rule 13, para. 7), it at one point suggests that "any use of force that injures or kills persons or damages or destroys property" is an armed attack (Rule 13, para. 5–6).
[6] Schmitt, *Tallinn Manual*, p. 47. While the *Tallinn Manual* authors rejected this contrary view, in their analysis of permissible countermeasures the minority held that "proportionate countermeasures could involve a limited degree of military force in response to circumstances below the Article 51 threshold of 'armed attack'" (Rule 9, para. 5). See also Rule 9, note 4.
[7] Schmitt, *Tallinn Manual*, p. 57.
[8] This position comports with those of David Rodin and James Brady; and contradicts that of Vinit Haksar, whose "rights-based" theory of punishment expands liability by asserting that because everyone has a claim-right not to be harmed, even unintentionally afflicted harm results in forfeiture. See David Rodin, *War and Self-Defense* (New York: Oxford University Press, 2003), pp. 779–83; James B. Brady, "A 'Rights-Based' Theory of Punishment," *Ethics* 97, no. 4 (1987), pp. 792–95; and Vinit Haksar, "Excuses and Voluntary Conduct," *Ethics* 96, no. 2 (1986), pp. 319–29.
[9] Schmitt, *Tallinn Manual*, p. 62.
[10] Ibid., p. 108.
[11] Ibid., pp. 55–56.
[12] Ibid., p. 160.
[13] Ibid., pp. 108–109.
[14] Ibid., pp. 109, 126–27. Two comments on the targetability of data. First, while the manual asserts on p. 127 that the "majority" of experts held that operations targeting data "sometimes" qualify as an attack when functionality is affected, p. 109 asserts that only a "few" experts maintained this position. Second and to their credit, a minority of the manual's experts opined that "data *per se* should be regarded as an object" and that current law prohibited the "deletion of extremely valuable and important civilian datasets," and the majority "characterized this position as *de lege ferenda*" (p. 127).
[15] Schmitt, *Tallinn Manual*, p. 109.
[16] Adil Haque, "Laws for War," in Jens David Ohlin, ed., *Theoretical Boundaries of Armed Conflict and Human Rights* (Cambridge: Cambridge University Press, 2016), p. 27. See also the chapter in this volume by David Luban, "Human Rights Thinking and the Laws of War." For a fuller treatment of Haque's argument, see his important book *Law and Morality at War* (New York: Oxford University Press, 2017).
[17] Haque, "Laws for War," p. 27.
[18] Jeff McMahan, "The Prevention of Unjust Wars," in Yitzhak Benbaji and Naomi Sussmann, eds., *Reading Walzer* (Abingdon, U.K.: Routledge, 2014). For a critique, see David Luban, "Knowing When Not to Fight," in Seth Lazar and Helen Frowe, eds., *Oxford Handbook of Ethics of War* (Oxford University Press, 2015).

[19] On threshold stretching, see Ben Connable, Jason H. Campbell, and Dan Madden, *Stretching and Exploiting Thresholds for High-Order War: How Russian, China, and Iran Are Eroding American Influence Using Time-Tested Measures Short of War* (Santa Monica, Calif.: RAND, 2016).

[20] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).

[21] Responses to relatively low-scale lethal harm have been explored under the rubric of "*jus ad vim*." See Daniel Brunstetter 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). For a critical response, see Helen Frowe, "On the Redundancy of Jus ad Vim: A Response to Daniel Brunstetter and Megan Braun," *Ethics & International Affairs* 30, no. 1 (2016). For recent work on the ethics of sublethal harm, see Michael L. Gross and Tamar Meisels, eds., *Soft War: The Ethics of Unarmed Conflict* (Cambridge: Cambridge University Press, 2017); and David Whetham, "Are We Fighting Yet? Can Traditional Just War Concepts Cope with Contemporary Conflict and the Changing Character of War?" *Monist* 99, no. 1 (2016).

[22] I realize that the relationship between culpability and liability is contested. See, for example, Rodin, *War and Self-Defense* and Jeff McMahan, *Killing in War* (New York: Oxford University Press, 2009).

[23] For an excellent analysis of whether effectiveness and necessity are preconditions to (i.e., "internal" to) liability, see Helen Frowe, *Defensive Killing* (New York: Oxford University Press, 2014), chapter 4.

[24] Jeff McMahan, "The Limits of Self-Defense," in Christian Coons and Michael Weber, eds., *The Ethics of Self-Defense* (New York: Oxford University Press, 2016), p. 192.

[25] In rare cases, such as cyber intrusions that seek to cause low-level harm as part of an existentially threatening campaign, anticipatory lethal responses might be justified.

[26] For a seminal treatment of the historical shift away from punitive war, see David Luban, "War as Punishment," *Philosophy & Public Affairs* 39, no. 4 (2011).

[27] It must be emphasized that tit-for-tat responses may be unethical. Countermeasures and punitive responses must themselves be justified.

[28] Having expanded the purpose and recipients of justified harm, it would be wise to add a cautionary note that bedevils "targeted killing" operations. While due process might not require courts or uniforms, extraordinary care must accompany the identification and treatment of liable individuals, and appropriately transparent institutional structures must be created to ensure such care.

Abstract: Why do we need dialogue between ethical and legal perspectives on norms governing the initiation and conduct of interstate conflict? This essay will examine this question by first critiquing the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which sought to apply existing legal frameworks that govern international violence to a new form of conflict. While the manual is for the most part ethically commendable, the first half of the essay will highlight several of its ethical shortcomings and will then extract general reasons why international law nevertheless must be informed by ethical analysis. The second part of the essay will affirm the importance of law for ethical analyses of justified responses to the burgeoning phenomenon of sublethal harms. While states have always used sublethal harms to weaken adversaries, technological developments have magnified the regularity and effectiveness of these practices, particularly against free societies. Responses to such attacks may include—in addition to defensive countermeasures—punishments that deter and reform, and may target "indirect participants" such as financial supporters. However, determining which responses are ethically justified will require insights gleaned from criminal and tort law.

Keywords: cyber warfare, sublethal harms, Tallinn Manual, *jus ad bellum*, *jus in bello*, international law, just war theory