Do Ambiguities in International Humanitarian Law make Cyberattacks more Advantageous?

Preprint · September 2021

DOI: 10.13140/RG.2.2.28157.03046

1 author:

Damian Williams
University College London
22 PUBLICATIONS **3** CITATIONS

SEE PROFILE

TABLE OF CONTENTS

---

1. INTRODUCTION

Do ambiguities in international humanitarian law ('IHL') ostensibly make state use of cyberattack more advantageous than kinetic weaponry? The current legal debate is focused on whether and when existing IHL is adaptable to hostile cyber operations. Despite its rapid technological advancement, little clarity on the subject matter has come into focus. Its destructiveness and destabilising potential are nevertheless now more frequently employed as a means to amassing and increasing state power without international or domestic legal downside.[1] In fact, Joe Biden recently stated to the ODNI and the greater intelligence community that if there will be a kinetic war, "it is going to be as a consequence of a cyber breach of great consequence."[2] Ultimately, the US is designating cyber as kinetic unilaterally, declaring its use of kinetic manoeuvres against cyberattacks legal before its domestic populace. This is anathema to the historic, multilateral consensus-built treaty-making approach to regulating weapons of war that emerged out of the Second World War. Long before Biden's announcement, ambiguity prompted states to adopt a new lexicography into military policy. In 2018, the US Department of Defence designated 'cyberspace' as a contested operating domain, which has rendered geographical military sanctuary-status of the US homeland diminished, if not defeated.[3] Years prior in 2011, the DoD designated 'cyber' as a "warfighting domain."[4] This

[1] Office of the Director of National Intelligence, Annual Threat Assessment of the US Intelligence Community (9 April 2021), 20
[2] Nomaan Merchant and Alexandra Jaffe, In 1st visit to intel agency, Biden warns of cyber conflict *AP News* (McClean, 28 July 2021)
[3] Department of Defence, Summary of the 2018 National Defense Strategy of the United States of America (19 Jan 2018), 3
[4] John Arquilla, 'Twenty Years of Cyberwar' [2013] 12 Journal of Military Ethics, 80

is a clear suggestion that the US now acknowledges purely cyber operations as similarly severe in risk as kinetic operations.

It is widely known that state cyber targeting of the US has been prolific, including attacks against US military, the US Senate, CIA, administrative federal agencies, corporations, and highly visible individuals.[5] Underlying US defence policies were recently updated to advance the intragovernmental authority required to initiate offensive cyberattacks, including pre-emptive strikes against aggressor states.[6] US deliberation on its own use of cyberattack during the Libya uprising against Colonel Muammar Gaddafi in 2011 may have exposed why the US seems to be losing the cyberwar.[7] Faced with deploying air strikes to protect resistance and civilian populations, the Obama administration considered initiating a cyberattack against Libya's air defence systems to "cripple" its ability to respond. While news reports suggested that it was close, the administration decided against cyberattack due to ambiguities in IHL.[8] In this instance, kinetic warfare, such as drone or manned-craft air-strikes were not advantageous against cyberattack for its costs or effectiveness, but instead because of its established clarity on which the US could act legally. That is—the US adopted a view that the ambiguities in IHL overrode legitimate exploitation of the advantages of cyber. The ultimate means deployed were not superior or more effective, as it is suggested that air strikes were simply the next best option that did not carry with it legal uncertainty.[9] To the state unconcerned with such legal

[5] Amy Lifland, 'Cyberwar: The Future of Conflict' [2012] 33 Harvard International Review, 7
[6] Trump Administration, National Security Presidential Memorandum 13: United States Cyber Operations Policy, National Security Presidential Memoranda [18 September 2018] [unpublished]
[7] *Lifland* (n 4) 7
[8] ibid
[9] ibid

uncertainty and seeking such an advantage, it is fair to assume that a cyber approach would be quickly deployed.

In April of this year, the US Intelligence Community warned of 'acute' state use of cyber operations as a means of "national power," to "steal information, influence populations, and damage industry, including physical and digital critical infrastructure"—particularly by "Russia, China, Iran, and North Korea."[10] Increased use of cyber operations increases the probability of increasingly "destructive and disruptive cyber activity" between states;[11] and, potentially hardens subjugation of domestic populations when authoritarian regimes deploy cyber operations and surveillance against their own.[12] The ODNI hypothesises that the status quo regarding foreign cyber operations suggests vastly developed preparedness for kinetic warfare against the US.[13] The US must act unilaterally if there exists no multilateral mechanism for reproach. During the first half of 2021 alone, The Centre for Strategic & International Studies has recorded seventy-one state-promulgated cyber incidents against government agencies, defence and tech industries, and other targets resulting in economic harm greater than $1 million USD.[14]

This begs the question: why should *jus ad bellum* or *jus in bello* account for cyberattacks? Cyberwar ethically undermines conventional "constructs" of *ad bellum*;[15] attribution *beyond reasonable doubt* is exceedingly rare;[16] cyber use too readily tests the

[10] *ODNI* (n 1) 20
[11] ibid
[12] ibid
[13] ibid 21
[14] CSIS, 'Significant Cyber Incidents' (*csis.org*, 2006-2021) <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> accessed 11 July 2021
[15] *Arquilla* (n 4) 80
[16] Ibid 81

controversiality on the just- or unjustness of pre-emptive and retaliatory measures;[17] and, although pre-emptive cyberwar may carry very little "ethical downside,"[18] it offers no strategic advantage save for alerting a target of the lost element of surprise.[19] If physical force is employed along cyberattack in self-defence, the outcome could be disproportionate and unjust,[20] and could otherwise trigger permissible lethal response under existing IHL. If the battlefield is entirely contained within the cybersphere, no single state is capable of controlling the entire "virtual domain," making many believe the potential scale of cyberwar in comparison to kinetic war to be hyperbolic.[21] Also, a 'duly constituted authority' is exceedingly difficult to attribute among actors of diverse or without rank or affiliation.[22] In such a chaotic, artificial sphere where no loss of life is anticipated, state acts fall short of the illegal lethality central to IHL. In a pure cyberwar, both offensive and defensive manoeuvring may be rendered strategically unknowable by any one state and could result in little benefit. Even the 'last resort' notion of *just war* is tested, as cyberwarfare can be employed, "early, easily, . . . highly effectively [and perpetually]."[23]

Cyber has not replaced other domains of warfare but is an additional one of increasing offensive/defensive technological capability.[24] Why do scholars divide on IHL applicability to cyberwar? For some, the reasons are plain: cyber operations are too far predated by IHL's origins, and could not have been anticipated at the scale it is known now; for others, *ad bellum*

[17] Ibid 83
[18] ibid 84
[19] ibid
[20] ibid
[21] ibid
[22] ibid
[23] ibid
[24] Ibid 80

applies outcome-determinately, as its deployment may cause loss of life and when it does—it applies; for others, short sightedness during the drafting of the UN Charter, where trepidation for defining 'use of force' and 'armed attack' resulted in a charter so vague, that attempts to pigeonhole cyber into exiting *ad bellum* are intellectually incoherent; and yet others take the view that cyber's peculiar capability of rendering attribution impossible makes it exceptionally perilous, but nevertheless too cumbersome under existing IHL, as one of its basic tenets is that belligerents are ultimately identifiable. The differing views on IHL sufficiency are myriad; what follows is a legal/theoretical analysis of the debate on whether IHL can be sufficiently applied to state cyberattack or not. For the reasons set out below, I conclude that legally, use of cyberattack is more advantageous to states than kinetic weaponry.

2. INTERPRETING CYBERATTACK

State-promulgated cyberattacks have historically resulted in sublethal harm. Ethical state response turns on whether resultant harm is lethal or sublethal. State countermeasures to sublethal harm ought to fall short of lethal response and should "deter and reform" hostile cyberoperations, even where targeting of "indirect participants" is strategically necessary.[25] A unique characteristic of cyberattacks is that they have involved a mixture of state and non-state actors in their deployment.[26] In this context, non-state actors are conceptually similar to 'indirect participants', as they play peripheral, contributory roles, but nevertheless "[generally] d[o] not directly cause harm [on a state scale] and, therefore, d[o] not lead to a loss of

[25] Edward Barrett, 'On the Relationship between the Ethics and the Law of War: Cyber Operations and Sublethal Harm [2017] 31 Ethics & International Affairs, 468
[26] ibid 467

protection against direct attack."[27] Permissible sublethal targeting of indirect participants in the cyber context is predicated on an underlying principle that states have a 'moral right' to defend themselves against sublethal harm, even where falling below the justificatory threshold for self-defensive military action.[28] This principle is coupled by another: that *any* response to a perpetrator state ought to be employed in defence of "actual or potential victims," and must be undertaken in an "effective and necessary" manner.[29] Equally, response to sublethal harm must be proportionate, and will almost always require sublethal response.[30] Use of kinetic weaponry against a purely cyber incursion carries the risk of violating the proportionality norm underpinning lawful state response, though in the face of ambiguity, the US has declared a right to do so.[31] One could imagine a disproportionate kinetic response to a cyberattack that has had minimal disruptive effect; one can also imagine a sublethal cyberattack against critical infrastructure that is so vast in scale, only lethal response would provide an adequate measure of self-defence.

Cyberattack can be deployed at levels ranging from trifling nuisance to *total war*. On one hand, its stealth may make it an ideal alternative to employing diplomatic de-escalatory options.[32] On the other hand, it may facilitate just war,[33] if it is accepted that all hostilities that fall short of munitions-use or loss of life are inherently just.[34] For one, all historical retaliatory

[27] ICRC, 'Direct participation in hostilities: questions & answers' (*ICRC International Committee of the Red Cross*, 2 June 2009) <https://www.icrc.org/en/doc/resources/documents/faq/direct-participation-ihl-faq-020609.htm>
[28] *Barrett* (n 25) 469
[29] ibid 473
[30] ibid
[31] *NSPM13* (n 6) [unpublished]
[32] *Arquilla* (n 4) 80
[33] ibid
[34] Ibid 81

cyberattacks have been more disruptive than destructive and rarely characterised as disproportionate.[35] Also, while non-combatant immunity is sacrosanct, the "non-lethal nature of cyberattack" may present less of a non-combatant issue under *in bello* terms of permissible collateral damage, where the sublethal cyberattack is responded to with a similar cyberattack.[36] However, no realistic vision of cyberattack use is considered detached enough from state power, and therefore, potential state-on-state hostilities. The expectation is that cyber operations will inevitably disrupt and destruct, lead to loss of life, and potentially incapacitate victim states' ability to self-defend—just as traditional war does in the physical sphere.

The cyber domain is an open, semi-secure sphere that presently makes up the connective tissue between command and forces, diverse weapon systems, multiple theatres of combat, disparate and unreachable parts of space, etc., and even states themselves. Hence, a realistic view of the cyber domain is that it is a more recent, still emergent, dynamic, and rapidly developing domain in which state power is projected onto and recursively interconnected with. International hostilities are possible on all spheres and may escalate to munitions-use that triggers self-defence mechanisms under IHL at any time. A missing account of the 'cyber'-sphere in IHL sets a baseline advantage against kinetic war in that it facilitates sustained adversarial action without triggering international condemnation generated out of visible breach of IHL.

On one view, given states' rights, consideration ought to be focused onto novel interpretations of IHL to effectively respond to the emergent sublethal nature of warfare. These

[35] Ibid 84
[36] ibid 85

have mostly centred around responses that are either purely punitive or authorise indirect-participant targeting.[37] As there exists no individualised recourse against state-sanctioned, non-state cyber operators, a readily cognisable normative response to sublethal cyberattacks remains elusive and difficult to extrapolate from existing IHL.[38] This leaves ethical consideration confined to underdeveloped notions of appropriate response, such as debates between specific deterrence versus retribution versus general deterrence,[39] or whether sublethal indirect-participant targeting (in self-defence) may be legally permissible.[40] Given the prevalence of non-state actors in state-directed cyber operations, their targeting *is* strategic, and can be carried out discriminately. On this view, the 'bright-line' drawn around civilians under conventional IHL can be justifiably penetrated when the target calculus is based on harm that is ultimately sublethal.[41] Even targeting "noncooperative political leaders" and "civilian accomplices" may become accepted approaches to justifiably responding to sublethal cyber operations, so long as the purpose is not arbitrary, and the harm is sufficient to defend and deter, without running afoul of indirect participants' rights against lethal harm.[42]

On another view, the cybersphere was not part of Art 51 UN Charter's 'right to self-defend drafting',[43] but the semantics of the Charter were intended to apply forwardly. While the Charter does not itself address all legal questions regarding use of force and states' right to

[37] *Barrett* (n 25) 474
[38] *Arquilla* (n 4) 84
[39] *Barrett* (n 25) 475
[40] Ibid 474
[41] ibid
[42] ibid 475
[43] "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." UNTS, *Charter of the United Nations* [1945] 1 UNTS XVI, art 51

self-defend, as the ICJ opined in *Nicaragua*,[44] the Charter memorialises and substantiates customary international law inhabited by regulations that specifically apply to, *inter alia*, the use of certain weapons technologies.[45] The two—the Charter and customary international law—should be seen as "mutually supplementing each other."[46] Therefore, it is reasonable for Charter language not to appear perfectly adaptable to cyber weaponry.[47] Similarly, Article 2(4)'s 'threat or use of force'[48] must be strained to capture the idiosyncratic nature of cyberwar tactics against what has historically been associated with the gravity of harm that triggers the right to self-defend.[49] On one view, revision is ultimately required, and Articles 51 and 2(4) language ought to be widened, allowing space for a new legal framework that accounts for circumstances in which kinetic *and* non-kinetic use of force *are* justified. [50] Also, to account for when non-state actors are implicated in state-promulgated hostilities and the effect this ought to have on *that* combatant's status before humanitarian law.[51] On this view, the distinction between kinetic and non-kinetic armed attack has become somewhat blurred due to rapid technological advancement and integration between them.

An adequate framework ought to be organised based on the character of the target: either government or civilian.[52] This follows from the view that the Charter is "foundational" to

[44] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, [176]
[45] Roman Kwiecień, 'The Nicaragua Judgement and the Use of Force - 30 Years Later' [2021] 36 Polish YB Int'l L, 23
[46] *Nicaragua* (n 44) [156]
[47] Jasper Kim, 'Law of War 2.0: Cyberwar and the Limits of the UN Charter' [2011] 2 Global Policy, 322
[48] "All Members shall refrain . . . from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." *UNTS* (n 40) art 2(4)
[49] *Kim* (n 47) 322
[50] Ibid 327
[51] Ibid 326
[52] Ibid 325

contemporary IHL, requiring interpretive approaches and revision that generates greater malleability to continually adapt with the changing multi-fold characteristics of contemporary war.[53] If accepted that cyber is an extension of both the means and approach of traditional kinetic warfare, it follows that the Charter ought to recursively provide for the evolution of the law of traditional warfare.[54] It therefore ought to provide foundational background for integrating *all* future advances in weaponry, requiring certain minimal "fine-tun[ing]" towards continued clarification over time.[55] This background clarification typically provides exposition towards the establishment of the document's 'branches'—the multilateral agreements that, *inter alia*, integrate new regulatory frameworks on specific types of weapons technologies into existing international law. On this basis, current interpretation of the Charter's applicability to cyber weaponry is insufficient, but minimally so and only requires minimal revision.

3. FEASABILITY OF CHARTER REVISION

To a certain extent, all IHL doctrine is derived from foundational documents, requiring a certain level of interpretation or re-interpretation, reaffirming the 'lawful[ness]" of the basic premises that govern state-to-state relations.[56] On this view, the operationalised principle is that 'armed attack' triggers the legal right to defend, and therefore where a cyber operation causes sufficiently grave harm, that threshold has been met, triggering the right to defend and all that follows. This is the status quo and views all historic cyber operations as having fallen short of 'armed attack'. Armed attack has been described as the "threshold for the use of

[53] ibid 323
[54] ibid
[55] ibid
[56] ibid

force," which when surpassed, triggers the right to self-defence under Art 51 of the Charter.[57] The ICJ has developed its definition, considering it more severe than a 'use of force', suggesting that an use of force may not necessarily arise to an armed attack. [58] However, when it does, it is of the "gravest forms" of 'use of force'.[59] Only in the extreme, where loss of life or comparable physical destruction is certain, does the right to self-defend become triggered, and the sublethal nature of all historic cyberattacks, on this view, does not qualify.[60]

Minimal Charter revision may not prompt a course towards multilateral regulation of the use of cyber, as Charter applicability to self-defence is the *exception*—not the rule, which proponents of sufficient cyber adaptability to existing *ad bellum* claim is exemplified by the relatively diminished-harm characteristic of all historical cyberattacks. Charter revision may focus attention onto the effects cyberoperations have on interstate relations or escalatory risk short of armed attack rather than its technical and legal effects on critical infrastructure, civilian, financial market, key defensive industry, government agency, *and* military targeting. If cyberattack falls short of triggering substantive responsive rights and obligations under IHL, the space for accounting for the effects cyberattack has on these does not belong in the Charter. Its revision may make the appearance of the document being 'upgraded', but most subject matter relevant to cyberattack and its place in law governing the relations of nations will likely remain out of direct view of Charter language, if the general structure of the Charter as it is now will inform incorporation of any new provisions.

---

[57] Laurie R Blank, 'Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict' [2020] 96 Notre Dame L Rev, 253
[58] *Nicaragua* (n 44) [191], [195], [210]
[59] ibid [210]
[60] *Barrett* (n 25) 469

Thus, following on the *Nicaragua* judgement and the *lex lata*[61] of armed attack that follows, cyberattacks are likely legally insufficient to trigger the right to self-defend, as they are unlikely to be interpreted as the gravest forms of use of force. This suggests that cyberattack victim-states are struck and constrained in the availability of legal options to respond. It seems inarguable that the Charter is the appropriate document for memorialising and informing permissible hostile deployment of cyber operations, even if 'foundational' in a distantly, removed sense. With exception to "fine-tun[ing]" the Charter to designate cyber as an emergent form of 'weapon',[62] Charter language will remain inadequate for capturing changes to warfare *in toto*, even if, post-revision, accepted as an extension of traditional warfare. Rather than minor refinement, extensive textual restructuring, including delineation of the applicability of sublethal harm in warfare and the special dispensation cyber requires when interpreting and applying the Charter seems required to address the peculiar nature of hostile cyber operations. This is particularly so if seeking minimal textual adjustment to the Charter to facilitate integration of cyberoperations into international law.

4. CYBER AND KINETIC SIMILARITIES

Proponents of the view that existing *ad bellum* is sufficiently adaptable to cyber draw attention to similarities between cyber- and kinetic-weaponry, [63] as both are deployable in a manner short of an armed attack, e.g., in kinetic: the 'shot across the bow'; or, in cyber, the momentary disruption of intragovernmental communications without physically damaging or rendering equipment-assets inoperable. On the other hand, both may be employed to destroy

[61] See *Oil Platforms (Islamic Republic of Iran v United States of America)* (Judgment) [2003] ICJ Rep 161, [51]
[62] *Kim* (n 47) 323
[63] William Boothby et al, 'When Is a Cyberattack a Use of Force or an Armed Attack?' [2012] 45 Computer, 83

military/civilian assets, e.g., direct, live-munitions deployment or a cyber operation rendering defensive munitions-deployment machinery inoperable. The salient distinction is that cyber deployment apparently *must* result in "death or a significant degree of injury . . . or physical damage to property,"[64] for *ad bellum* to apply. Where a cyberattack causes death, injury, or property damage, then kinetic and/or non-kinetic response is justified, if undertaken proportionately to the extent necessary to defend.[65] The "scale and effects" necessary for a cyberattack to qualify as grave are unknown, as no historical cyberattack has risen to an 'armed attack'.[66] While these aspects are not yet settled in customary law, the extreme cyberattack that triggers the right to self-defend is yet to occur; the presumption is that if an attack of scale were to occur, the existing threshold justifying self-defence would apply.

A commonly recalled example of significant cyber-linked physical destruction comparable to kinetic weaponry occurred with the deployment of the 'Stuxnet'[67] worm, that rendered Iranian centrifuges within the Natanz nuclear facility inoperable. Equipment assets affected by 'Stuxnet' were not part of the Iranian military's open command and control, nor were there any reported deaths from the operation.[68] In fact, Stuxnet is said to have caused no "grave humanitarian consequences;"[69] was employed to "exfiltrate sensitive data;"[70] was

[64] ibid
[65] ibid
[66] ibid
[67] "A computer worm that was designed to target software and equipment comprising Siemens Corporation developed Supervisory Control and Data Acquisition (SCADA) systems." Schmitt MN, Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press 2013), 262
[68] Roger A Grimes, Stuxnet: Smarter -- and deadlier -- than the average worm, *Chief Security Officer Online* (5 October 2010)
[69] ICRC, 'Technological Challenges for the Humanitarian Legal Framework' (11th Bruges Colloquium, Bruges, 21-22 October 2010) <https://www.coleurope.eu›pdf›Collegium41> accessed 21 July 2021, 10
[70] ibid 35

deployed effectively by taking advantage of 'pre-existing' "vulnerabilities"[71] in the "Windows operating systems;"[72] gained easy systemic infiltration due to "poorly configured internal security systems (such as use of 'default passwords);"[73] targeted specific hardware configurations;[74] and is alleged to have been deployed by the Israelis or Americans, but neither have actually claimed responsibility, nor have either been ascribed confirmed attribution.[75] Of course, the *purpose* for the Stuxnet mission was likely sharply defined, and must have been intended for physical destruction that fell far short of armed attack.

Still, if 'Stuxnet' is the exemplar for a cyber operation that causes physical damage, its scale and effects hardly arise to causing death or human injury. And while Iran conceded that Stuxnet had caused property damage, it also minimised it, later claiming to have developed a 'firewall' around Natanz that would render future cyber operations impossible.[76] Iran's publicly acknowledged retribution was in the form of cyberattacks perpetrated against US institutions, including a spate of 'distributed-denial-of-service'[77] attacks against financial institutions (including JP Morgan Chase and Citigroup). These attacks temporarily blocked customer access to accounts through the institutions' web interfaces—one of the oldest and least sophisticated forms of cyberattacks still employed today.[78]

[71] ibid
[72] ibid
[73] ibid
[74] ibid
[75] ibid 44
[76] Reuters Staff, Iran builds firewall against Stuxnet computer virus: minister, *Reuters* (Dubai, 16 May 2019)
[77] Distributed-Denial-of-Service-Attack: a "technique that employs two or more computers . . . to achieve a denial of service from a single or multiple targets." *Schmitt* (n 54) 259
[78] Jim Finkle and Rick Rothacker, Exclusive: Iranian hackers target Bank of America, JPMorgan, Citi, *Reuters* (21 September 2012)

Iran's response falls dramatically short of inflicting death, human injury, or significant property damage onto the US or Israel; it also falls short of retaliation for its nuclear program being set back by years. Neither Stuxnet nor Iran's response meet the *ad bellum* thresholds for armed attack or kinetic defensive manoeuvres. Legally, the US (and/or Israel) and Iran could repeat the exercise again without escalating matters to traditional warfare. If so, then *ad bellum* cannot be characterised as having sufficiently addressed hostile cyber-operations in this instance; alternatively, cyber operations like 'Stuxnet' are considered legal. Yet no such position has ever been openly declared or even seriously argued. It is more likely that cyber operations remain out of view of *ad bellum* for falling short of the thresholds that trigger legal protections; therefore, *ad bellum* as it is understood today is insufficiently applicable to hostile cyber operations. If this is so, cyberattack is legally advantageous against more traditional deployment strategies of kinetic warfare because its legality is unaccounted for, and therefore cannot trigger *legal* response.

5. DEFINING CYBERATTACK

There exists no adequate 'armed-attack' -based means of analysis applied to hostile cyberoperations to date. The void cyberwarfare presents is in part due to the Charter's lack of definitions for 'use of force' and 'armed attack'; conventional use of these terms by states and the ICJ typically refer to "aerial bombardment, ground assault, missile strikes, and other territorial incursions."[79] Other problems stem from differing definitions of what 'cyber' actually is. Scholarly attempts to apply cyberattacks to existing IHL, pre-Tallinn, have typically employed one of three methods: an (a) instrument-based approach: whether the weapon of choice has

[79] Reese Nguyen, 'Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare' [2013] 101 California Law Review 1081

physical characteristics similar to traditional notions of military coercion; a (b) target-based approach: whether a cyberattack is perpetrated against designated critical infrastructure, and if so, arises to an 'armed attack'; and a (c) consequence-based approach: whether the totality of the effects of a cyberattack, considering the severity and immediacy of harm, arises to an 'armed attack'.[80] Ambiguity in defining cyber- and armed attack, as the literature is split between one that delineates use of computers/computer-networks as instruments of an attack and the other, where computers/networks are the targets of attack,[81] compounds the obscurity encountered when discerning cyber operations' place in contemporary warfare. The latter generates conceptual confusion by using 'cyber' to designate the object of an attack, even as it has developed to "connot[e] a mode of attack."[82]

Other usage, including that of the US DoD incorporates both the instrument- and target-based approach to describe cyberattacks as those perpetrated through the use of computers/networks against "critical cyber systems, assets, or functions."[83] This definition does not readily speak to *ad bellum* in terms of "scope, duration, and intensity," and ultimately creates additional ambiguity towards situating cyberattacks against existing IHL.[84] This leaves a gap to bridge to ascertain where IHL actually applies.[85] Under the instrument-based approach, concepts of "*ejusdem generis*"[86] and "*noscitur a sociis*"[87] may apply, prompting the conclusion that a cyberattack, fundamentally, cannot arise to a 'use of force' or an 'armed attack', because

[80] ibid 1081
[81] ibid
[82] ibid 1088
[83] ibid
[84] ibid
[85] ibid
[86] "Of the same kind, class, or nature," *Black's Law Dictionary* <https://thelawdictionary.org/>
[87] "Known by the company it keeps," *Black's Law Dictionary* <https://thelawdictionary.org/>

the weapon is essentially comprised of computer code—an element that is neither physical nor solely military-associated.[88] In order for a 'use of force' or 'armed attack' to occur, the mode of attack ought to be physical and form part of conventional military practice.[89] This is an exceedingly traditional notion of warfare that produces a "rigid and inflexible" outcome, where acts of war remain static in "1945 terms."[90]

6. AMBIGUOUS THRESHOLDS TO CUMBERSOME APPROACHES

Under the target-based approach, a bright line is drawn around "critical infrastructure," which if subject to cyberattack, automatically triggers a state's right to self-defence, including anticipatory self-defence.[91] Both the US Congress and President's Commission under the Obama administration defined critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination [thereof]."[92] This is sometimes referred to as the 'strict liability' approach, which inevitably places the analytic focus on attribution.[93] This approach seems "dangerously" [94] wide in application, as there is little consideration of the scale or severity of a cyberattack that speaks to specifically justifying response in self-defence.[95] Despite this, most "industrialised" states have adopted similar definitions out of fear of state cyber-

[88] *Nguyen* (n 79) 1118
[89] ibid
[90] ibid 1119
[91] ibid
[92] ibid
[93] ibid
[94] ibid
[95] ibid 1120

targeting.[96] Yet, as mentioned, at least 71 cyberattacks against critical infrastructure have occurred the first six months of 2021 alone, appearing so without consequence. Though already set in domestic policy, Biden publicly warned Putin that critical infrastructure is 'off-limits' from cyber targeting in the recent two-nation summit held in Geneva.[97] Russia's response is discussed further below.

The consequence-based approach looks to outcomes: where physical destruction is the result of a cyberattack—similar to that of a kinetic attack, then use of force, armed attack, and self-defence considerations apply, tending to meet each threshold.[98] Anything less, including political or economic interference will not trigger justification for response with force.[99] This approach allows for balancing the multiple qualities of a cyberattack to ascertain an appropriate, legal response.[100] Chief among these considerations is severity; to a lesser extent, immediacy, directness, invasiveness, measurability, and presumptive necessity (per Michael Schmitt).[101] Some analysts have revealed that this multifactorial approach easily gives way to argumentation, allowing for any cyberattack to be presented as arising to an armed attack or not—an approach susceptible to undue influence based on internal, non-explicit factors such as desired influence over domestic political perception.[102]

[96] Cécilia Gallais and Eric Filiol, 'Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure.' [2017] 16 Journal of Information Warfare 1, 64
[97] Vladimir Soldatkin and Humeyra Pamuk, Biden tells Putin certain cyberattacks should be 'off-limits' *Reuters* (Geneva, 16 June 2021)
[98] *Nguyen* (n 79) 1120
[99] ibid
[100] ibid
[101] ibid 1122-1123
[102] ibid

An approach that may alleviate some of these problems is basing cyberattack severity on the level of threat it presents to a state's "sovereignty, peace, and security," and drawing the line beyond which a cyberattack arises to an 'armed attack' at when it results in "irreversible disruption or physical damage to a cyber-physical system."[103] This at once puts minimal incursions out of escalatory consideration, and accounts for both the "actor and the act,"[104] the nature of the weapon, and the quality of the target.[105] Essentially, this situates cyber operation outcomes deemed "catastrophic [and] destabilizing" and threaten "peace and security" within the province of *ad bellum*.[106] This approach also seeks to account for ambiguity in the scale of a cyberattack: while a threat may potentially spread perpetually, it is not until the physical damage element is satisfied that a cyberoperation arises to a 'use of force'.[107] This also emphasises the belief held by some that only 'physical harm' arises to a level that threatens "international peace and security."[108]

Although not widely attributed to Russian intelligence, Russia's apparent response to Biden's 'off-limits' comment was to deploy cyberattacks against 1,500 worldwide businesses with strong ties to the US.[109] Claiming to bear strict adherence to international law, and frustrated by vague deliberations on a legal response by his own National Security Council, what is the Biden administration to do? Wipe out the entire Russian infrastructure? This would be disproportionate, threaten escalation, require kinetic use of force, and potentially prompt

[103] ibid 1125
[104] ibid
[105] ibid
[106] ibid 1126
[107] ibid
[108] ibid 1129
[109] Aamer Madhani and Eric Tucker, Latest hack to test Biden's vow for consequences for Russia *Associated Press News* (Washington 7 July 2021)

multilateral war—in addition to violating existing IHL. This again suggests that cyberwar as currently conceived falls below the reach of *ad bellum* as presently conceived, where it remains in a grey sphere where its legality is either ambiguous or assured.

This suggests that cyber operations provide an advantage over traditional use of kinetic warfare, as it is capable of ongoing targeting and public knowledge of state-on-state cyberattack without 'hard' attributive certainty. Victim states struggle to accurately attribute operations to state or non-state actors or to decipher whether states employ non-state actors to achieve its hostile ends.[110] In more recent instances of uncovered, covert cyberattacks, Chinese cyberoperations against the US have been alleged without attributive certainty.[111] China's response is denial: allegations that amount to nothing more than "groundless attacks," . . . "just another old trick, with nothing new in it."[112] Nothing has followed from this. This state of affairs seems easily tolerable in the aftermath of cyberattack as is known. To the calculating military strategist, it seems clear: the safer, more effective means of achieving successful, ongoing, and covert hostile warfare is cyber, which is presently governed by no multilateral agreement and a patchwork of domestic laws that suggest IHL applicability, but are in truth, uncertain and vague.

The instrument-based approach, while useful in identifying whether cyber acts bear similarities to kinetic weaponry, is foreseeably to be employed rarely, as its use for triggering application of IHL will remain of little utility until a cyberoperation directly causes loss of life—a

[110] Jennifer Jacobs, Biden Says 'Not Sure' If Russia Is Behind Latest Cyberattack *Bloomberg* (3 June 2021)
[111] Steve Holland and Doina Chiacu, U.S. and allies accuse China of global hacking spree *Reuters* (Washington 20 July 2021)
[112] Zolan Kanno-Youngs and David E. Sanger, U.S. Accuses China of Hacking Microsoft *The New York Times* (Washington 19 July 2021)

high threshold. On the other hand, the target-based approach designates certain assets as 'off-limits' and demands a full array of responses—including use of kinetic munitions. But widescale designation of infrastructure appears arbitrary in comparison to sensitive asset designation under existing IHL, as it traditionally designates certain sites on the battlefield as sacrosanct—not *everything* a state possesses. The effect this arbitrariness has on cyber targeting is unknown. If confined to a single approach of the three, the consequence-based approach, where in consideration of the totality of the circumstances, a cyberattack may be deemed to arise to the level of an armed attack or not seems the better approach of the three. It allows for creation of a sphere where it is possible for hostile cyber operations to trigger IHL illegality, or even justify kinetic response where multiple factors apply.

While these approaches may give the appearance of better defining hostile cyber operations and/or designating thresholds for IHL to apply, they do little to bridge the gap between hostile cyberoperations and IHL, particularly if there exists no consensus on the appropriate approach to apply IHL to cyber, or because attack outcomes are framed as 'sublethal' and out of view of IHL in terms of appropriate response. Despite the availability of different approaches to analysing cyber, the lack of consensus means that no scope is broadened to incorporate hostile cyber acts for IHL to apply generally; rather, more space is defined for cyberattacks to be undertaken without triggering defensive, kinetic response. By this, aggressor states may simply shrink the sphere which is deemed safe targeting via cyber means without instigating allegations of breach of international law. In other words, the task of avoiding international condemnation for clear breach of IHL may be made easier. The void that causes this uncertainty begs for instilling multilateral agreement and uniformity of laws so as to

bridge that gap. On the other hand, the status quo reinforces the existing threat of an easy to deploy, target-state confusing, and unlikely to be adjudicated form of weapon. In this regard, it nearly becomes maxim: hostile cyber acts are advantageous to kinetic, traditional attacks in terms of IHL.

7. NON-STATE ACTOR PARTICIPATION

How can *ad bellum* apply, where non-state actors enjoy safe-haven status within the aggressor states that may employ their expertise? The 'bright-line' around 'civilians'—even 'criminal' civilians in *ad bellum* and *in bello* appears circumventable when a state employs non-state actors to potentially unknowingly fulfil its hostile cyber missions. On one view, an expansion of 'armed conflict' to include non-state actors who take part in cyber operations that benefit aggressor states would make *in bello* apply.[113] The problem of applicability is compounded where non-state actor involvement is in the initiating, first-strike state cyberattack.[114] In light of this emergent quality of non-state actor involvement, *ad bellum* could be adjusted to include their acts in a "matrix of transnational use of force."[115] By recognising a changed legal status of non-state actors, the problem of attribution can potentially be somewhat alleviated with the availability of more evidence,[116] though there presently exists no known due process that considers these types of acts committed by non-state actors.

In a technological sense, it is relatively easy to hide the connection between the non-state actor and larger state cyberoperations—particularly where 'participant nodes' are

[113] Heman Faga, 'The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyberattack, and Cyber Warfare in the 21st Century' [2017] 10 Baltic Journal of Law & Politics, 24
[114] ibid
[115] ibid 25
[116] ibid

unaware of each other's roles. Further, for some, it is the current definition of cyberwarfare that does not arise to the threshold where existing *jus ad bellum* and *jus in bello* applies,[117] — not the acts themselves. How then can the expansion of armed conflict to include non-state actors *in bello*, relative to IHL sufficiency, trigger an *ad bellum* right to self-defend?[118] If no damage is incurred, criminal charges may be fitting, particularly where state participation is too remote to define, and instructions for carrying out certain acts are arguably available open source. If a state is clearly implicated in the hostile cyber acts of non-state actors, it would require some restructuring of IHL, especially as it relates to "necessity, distinction, proportionality and humanity"[119]—foundational principles that confine justifiable use of force to manners, means, and degrees of destruction designated permissible.

Expanding the definition of armed attack to include acts of non-state actors may provide for easier *ad bellum* adaptability, and ease some of the difficulty associated with cyberattack attribution. However, later problems stemming from the comingling of fair trial rights and civilian justice with military codes of conduct and IHL may surface, as both may grossly alter the nature of each, creating a cumbersome overlap too unwieldly for effective multilateral prosecution of non-state actors. This suggests that a separation between criminalisation of state conduct and the non-state actor participant may provide for a better accounting of this peculiarity of cyberattack. Without a current legal regime that sanctions it, non-state actor participation remains a successful strategy for subverting state attribution. Ease of successful attribution avoidance makes non-state actor employment in state sanctioned cyberattacks

[117] ibid
[118] ibid
[119] ibid 26

advantageous to kinetic forms of attack, given a lack of certain attribution to the actor, and therefore to the state.

For the non-state actor, the ethos for intentional participation is unknown; it may be patriotic—like citizens taking up arms against their nation's adversaries; or perhaps the grant of immunity for engaging in criminal conduct of scale is enticing. This however bears little on explaining the phenomena of increased state use of non-state actors in its cyber operations. It seems more likely their utility and ample availability to deploy attacks in a manner unsuspecting present a means separated from military domains with a high capacity for inflicting sublethal disruption and destruction. However, addressing this lacuna in the law through expanding all 'armed conflict' to include non-state actors seems too cumbersome, and desirous of drastic change to existing *in bello* to meet the challenge of adapting it recursively to the non-state actor's peculiar involvement in state cyber offenses in both *ad bellum* and *in bello*. Such an extreme suggests that the end-product will carry little resemblance to traditional IHL, as distinguishing combatants from civilians is elemental in IHL doctrine, evolving since the adoption of the first Geneva Convention ~160 years ago.

Having the cyber phenomenon render IHL a *tabula rasa* exposes a tendency for cyber subject matter to be grossly exaggerated. On a more basic, practical view of expanding 'armed attack' to include civilians, tools for actor attribution may facilitate easier state attribution and may become more readily available, but may equally make attribution *more* difficult, particularly if the norms that underpin *ad bellum* are altered in a way that gives rise to greater interpretive manipulation, and unintended loopholes far beyond that which exposes advantageous use of non-state actor status within the law. Further, civilian inclusion as

prosecution subject matter may give rise to increased scapegoating, as the next logical step for a hostile state actor is to extend avoidance of attribution through a denial of association with the implicated non-state actor.

8. EVIDENTIARY PROBLEMS

Attribution difficulty also touches on evidentiary problems inherent in IHL proceedings. On one view, treating digital evidence as 'circumstantial' may be more appropriate in proving state responsibility for cyberattack.[120] The distinction between 'public' and 'legal' attribution within context is required to meet the correct burden within international legal fora.[121] IHL proceedings require that evidence be "fully conclusive,"[122] whereas the standard adopted for informing the public is typically anything "good enough" to suggest a particular perpetrator.[123] Consequences for inaccurate attribution could be dire, as mistaken response may itself become a violation of international law.[124]

On the evidence-deficiency view, traditional *ad bellum* does apply to hostile cyber acts, but hurdles created by missing procedural standards for considering evidence creates a level of complexity that renders much of the evidence untestable.[125] Still, if the problem of attribution is overcome, and states can accurately identify an aggressor state deploying cyberattack, there is no particular reason to believe that all other ambiguity will cease. On an ethical basis, the victim state remains confined to reacting proportionately, and solely for the purpose of

[120] Sharngan Aravindakshan, 'Cyberattacks: A look at Evidentiary Thresholds in International Law' [2021] 59 Indian Journal of International Law, 285
[121] ibid
[122] ibid 290
[123] ibid 298
[124] ibid
[125] ibid

deterring further cyberattack and reforming conditions causing hostilities at their root. This still falls short of *ad bellum* applicability certainty, as the thresholds for triggering mechanisms remain unmet, adding onto reasons for making the subject matter in legal proceedings uncertain. Hence, attributing all IHL ambiguity to the issue of accurate attribution is problematic, as hurdles continue in post-attribution adjudication.

9. THE TALLINN APPROACH

The above suggests that the complexity of cyberattack, and/or its being unanticipated when existing law on the use of force was adopted has led to a scenario where a militarily acknowledged element of war appears unsuitably vague in terms of IHL.[126] The existing non-binding recommendations in *Tallinn* are all that remains, and recommends a multipronged balancing test for determining 'use of force', including: (a) severity; (b) immediacy; (c) invasiveness; (d) measurability of effects; (e) military character; and (f) state involvement.[127] If use of force criteria is met, then Tallinn recommends moving the analysis onto attribution by seeking out whether the act was carried out by an "organ of . . . [any particular] state [or states]."[128] Under the Draft Articles on Responsibility of States for Internationally Wrongful Acts, 'any' state organ may be implicated in proscribed acts regardless of its stated function.[129] The Draft Articles also extend this onto private entities, acting *ultra* or *intra vires*.[130] This however is distinct from the 'non-state actor' participant in state sanctioned cyberattack

[126] Jeff Kosseff, *Cybersecurity Law* (Wiley 2020), 415
[127] ibid 417
[128] ibid 418
[129] "The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State." UNGA, *Responsibility of States for internationally wrongful acts*, adopted 8 January 2008, A/RES/62/61, art 4(1)
[130] *Kosseff* (n 126) 418

discussed above—especially the unwitting participant, as the Draft Articles would apply once the state's or complicit non-state actor's identities are known.[131]

Under the Tallinn approach, existing international legal praxis contains adequate space for integrating and considering cyber acts and their scale and follow along the same trajectory for applying post-act duties that implicate state action. If such an act can both qualify as a 'use of force', and is attributable to a state, then the Tallinn approach is to move the legal analysis onto which acts undertaken in self-defence are justified under international law.[132] This implicates necessity and proportionality under customary legal norms—necessary to protect fundamental security interests; proportionate in scale so as to overcome or deter the existing threat.[133] Under this view, most historical state-promulgated cyberattacks fall short of justifying the use of force in response;[134] or an alternative view: that in most historical instances of cyberattacks, perpetrators have skirted IHL enforcement.

An outcome-based view of cyberattack makes inclusion of cyberwar into existing LOAC feasible for some.[135] On this view, *jus in bello* becomes the focus when a cyberattack has resulted in "physical destruction of property or death or injury of persons" at a "sufficient scale and effect," having triggered the right to respond in self-defence and engagement ensuing.[136] On this view, cyberwarfare is similar to the emergence of any other weaponised technology,[137]

[131] "An organ includes any person or entity which has that status in accordance with the internal law of the State." *UNGA* (n 126) art 4(2)
[132] *Kosseff* (n 126) 418
[133] ibid
[134] ibid
[135] Kyle Phillips, 'Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain' [2013] 70 Joint Force Quarterly, 70
[136] ibid 73
[137] ibid

and is subject to the principles of necessity, distinction, proportionality and unnecessary suffering, depending on whether a particular act can be qualified as an 'attack'.[138] Art 49 API Geneva Convention defines an attack as an "ac[t] of violence . . . whether in offense or defence."[139] Most cyber activities cannot be characterised as 'violence'.[140] Added complexity arises where civilian property is cyberattacked; if legal, only military or dual-use objects may be targeted, and only to the extent that it is militarily necessary, towards a "valid military objective."[141] In the US, this view creates difficulty towards integrating cyber into US defence policy, as most cyber infrastructure is shared by civilian and state/military organisations.[142] Proportionality is also uniquely tested,[143] as damage inflicted on a state may not be excessive in relation to the anticipated military advantage foreseen by the act.[144] Despite this complexity, the Tallinn view is that the cyber sphere is an added domain of warfare "(land, sea, air, space, and cyber)," in which the current *ad bellum* and *in bello* framework sufficiently guides military personnel to act legally.[145]

10. IN WAR

In *ad bellum*, the scale and effect of a cyber operation may inform whether a cyberattack arises to an 'armed attack'. Where this is the case, the quality and character of the 'use of force' becomes the chief consideration.[146] By implication, this was made so via the ICJ's

[138] ibid
[139] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977) 1125 UNTS 3 (Additional Protocol I) art 49
[140] *Phillips* (n 135) 70
[141] ibid 74
[142] ibid
[143] ibid
[144] ibid
[145] ibid 75
[146] ibid

Nicaragua judgment.[147] Article 2 Geneva Conventions, AP I, Common Article 3 Geneva Convention, and AP II all establish the permissible and proscribed once an 'armed attack' has occurred.[148] Instruments of international law do not limit applicability of cyberattacks where 'armed attack' is established.[149] In *in bello*, when employed in conjunction with conventional weapons, cyberattacks are part of the 'armed conflict'.[150] For this to have been justified under contemporary international law, the Tallinn approach underscores that an *ad bellum* nexus must have existed between the initiating 'armed cyberattack' (if it were executed via cyber means) for this to apply.[151] Consistent with customary law, state intent does not form part of the determination of whether such a nexus exists, or ultimately, whether an armed attack occurred.[152] Therefore, the aggressor state's 'mental state' is, to a certain degree, irrelevant in regards to whether a cyberattack justifies an *ad bellum* declaration of having been victim of an armed attack.[153]

In *in bello*, Hague Convention IV— the 'Martens Clause'[154] provides for the "law of nations" to remain operational even in face of novel scenarios not contemplated in existing law, including protections of "inhabitants and . . . belligerents."[155] This suggests that while there may exist no specific place in law where cyberweaponry is considered, the law as it stands

[147] ibid
[148] ibid
[149] ibid
[150] ibid
[151] ibid
[152] Dominic Raab, ''Armed Attack' after the Oil Platforms Case' [2004] 17 Leiden Journal of International Law, 728
[153] ibid 729
[154] ". . . in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established . . . from the laws of humanity, and the dictates of the public conscience." Convention (IV) Respecting the Laws and Customs of War on Land, 18 Oct 1907, 36 Stat. 2277, preamble ¶8
[155] Dan-Iulian Voitaşec, 'Applying International Humanitarian Law to Cyberattacks' [2015] 530 Lex ET Scientia International Journal, 130

continues to stand. Similarly, military necessity, proportionality, and humanitarian considerations remain where cyber operations arise to implicate LOAC.[156] Again, on this view, no historical use of cyber operations has arisen to an 'armed attack' under *ad bellum* alone, but its use in conjunction with kinetic attack presumes that 'armed attack' has occurred.[157] Under *in bello* legal use of cyberattack is similar, if not an extension of the use of kinetic weaponry towards achieving military aims consistent with protections within its framework.

Under *in bello*, cyberwarfare fits well as an emergent form of 'remote warfare', as there is precedent for its interpretation under international law, in a manner consistent with the "existing framework that governs the conduct of hostilities."[158] This is so when remote warfare is used, *inter alia*, for reconnaissance or destructive targeting, somewhat akin to the manner in which aerial drones are employed. On one view, failing to incorporate armed cyberattack in *in bello* interpolates needless complexity, making application of existing law to novel forms of warfare too cumbersome so as to be effective.[159] Contemporary, or traditional understanding of 'armed conflict' is that framework, and is adequate for defining armed cyberattack as a means of armed *remote* warfare and informs whether certain countermeasures are accepted legally.[160]

This view adopts the ICRC's definition of 'cyberwarfare': "operations against a computer or a computer system through a data stream, when used as means and methods of warfare in

[156] ibid
[157] ibid
[158] Anthony Cullen, 'The characterization of remote warfare under international humanitarian law' in Ohlin, Jens David (eds) *Research Handbook on Remote Warfare* (Edward Elgar Press 2017), 131-132
[159] ibid
[160] ibid

the context of an armed conflict, as defined under IHL"[161]—a mixed 'instrument-based' and 'target-based' approach. Under this view, lethal cyber operations do not present an advantage to kinetic weaponry; it complements other emergent technologies in response to increasingly complex warfare. Under traditional notions of *in bello,* such advances ought not withstand established *opinio juris*. Though there is complexity, the simplicity in effectively adapting *in bello* to use of cyberattack comes from it being deployed once armed attack has been established, and that it is deployed once the right to deploy kinetic weaponry has been declared.

However, if one were to envision elevated, destructive capabilities short of lethal harm be accounted for in *ad bellum*, to the victim state, problems with responding proportionality may be alleviated in part, as it follows that legal options to respond will too become available.[162] This could lead to new rules of engagement that would mitigate lethal cyberattack escalation.[163] Alternatively, this could limit the perceived benefits of cyberoperations, or even confine attacks to cyber-on-cyber for their lost utility due to advanced cyber-defensive capabilities. The danger with viewing pure cyber-on-cyber warfare with a laissez-faire lens is that, in the face of ineffective IHL, escalation may be rapid, possibly evolving into "unwanted conventional or nuclear war."[164] Thus, assuring that IHL account for the cybersphere is imperative.

[161] ibid 121
[162] Jonathan Lancelot, 'Cyber-diplomacy: cyberwarfare and the rules of engagement' [2020] 4 Journal of Cyber Security Technology, 242
[163] ibid
[164] ibid

While there currently exists no rules of engagement specific to cyberwar,[165] principles of *in bello* are intended in part to prevent 'perpetual war'.[166] War in 'cyberspace' may be resistant to this aim, as it is arguably beyond the jurisdiction of any one state,[167] given that its environment is 'notional', raising myriad *additional* problems against the current IHL framework: (a) war within it is disorienting and limitless; (b) it is 'lawless territory' in Westphalian terms; (c) IHL is predicated on the relative stability of the Westphalian system; (d) "psychology and technological prowess (rather than physical might)," sets the "balance of power;"[168] etc.

11. AFTER WAR

Heightened risk for "disrupt[ting] the balance of power"[169] applies to all war; escalation into "large-scale conventional war, or . . . a nuclear exchange" is always a possibility.[170] The targeting of critical infrastructure by cyberattack can bear affects in the 'physical world' similar to kinetic war.[171] While necessity and proportionality ought to inform response, at a certain point of increased instances of cyberattack, 'lethality' may follow naturally without de-escalation. Within the context of war, the place for the 'cyberattack' is in war; for others, the applicable context remains ambiguous: incomplete, incoherent definitions of what 'cyber' means seem unworkable under IHL principles.[172] If remaining inadequately defined in war, the lines where legality and illegality, or sublethality and lethality intersect may become too

[165] ibid
[166] ibid
[167] ibid
[168] ibid
[169] ibid 243
[170] ibid 250
[171] ibid
[172] ibid

unpredictable,[173] and likely contribute to policy decisions towards unilateral declaration of a right to respond kinetically. As mentioned above, the rapidly increasing incidence of cyberattack suggests there is a missing lever of statecraft, where cyber means of attack are finally focused upon, attached to relevant legal norms, and memorialised in consensus-based agreement between nations. Without this step post *in bello*, unaddressed uncertainty regarding cyber operations may lead to increasingly effective, deadlier, and more fully developed cyberweaponry.[174] Attributed to *Kant*, that diplomatic lever would "bridg[e] the needed gap" between "cyberspace, physical space, proportionality, error, and escalation,"[175] through a framework for governing nations transitioning out of war.

If it were accepted that *ad bellum* and *in bello* apply to hostile cyber operations under existing understanding, then the movement to post-hostility should come into form: *jus post bellum,* along with newly "codified legal norms" preventing future escalations to *ad bellum* and *in bello*; the cyberwar aftermath may prove so destructive, that refined or rewritten norms of warfare may also form part of the origins of the multilateral-instrument used to memorialise *post bellum*.[176] For the view that LOAC does not apply to hostile cyber operations, in the face of sublethal harm, a proponent may ask "what war?" or "what peace?"[177] In the military sphere, cyberwar has a longer history of acknowledged lethal engagement. The present lack of safeguards coupled with threats of retaliatory kinetic war suggests that the "Kantian *jus post bellum*" is a long way off from preventing the new face of war with cyber included from fully

[173] ibid
[174] ibid
[175] ibid 252
[176] ibid
[177] ibid

emerging.[178] Blind rigidity in legal interpretation could render existing law ineffective at some point.

12. TOWARDS *AFTER* WAR

As the cybersphere has had an outsized impact on all aspects of life, including state power; and has perhaps rendered war changed in a fundamental sense; malleable and contextual legal application against more integrated, evolved, and deadlier multi-use weapons technologies will be required. [179] "[T]ransition[ing] from war to peace," follows as an endpoint,[180] where a categorical moral obligation emerges: multilateral efforts ought to acknowledge, prevent, and/or mitigate diminution of all humans' freedoms.[181] Under the *Kantian* view, 'forever-war' is inevitably pre-empted through post warfare establishment of an "international juridical condition" of "perpetual peace."[182] As dependence on cyber expands towards total, global interconnectivity, threats to the cybersphere generate greater ontological insecurity, perhaps repainting the future of war; or, according to Kant's view, inevitably making the undertaking of war meaningless and needless.[183] This is immense, even baroque for Kant. It suggests that in an inevitable, *post* conflict era, the character of weaponry will carry less importance on a scale relevant to nations.

The initiating step towards a *Kantian* endpoint of war reasonably begins with weapons technology regulation and disarmament. This would entail multilateral treaty negotiation that specifically addresses the use of cyber in conflict, preferably accounting for scope of harm, state

[178] Klaus-Gerd Giesen, 'Towards a Theory of Just Cyberwar' [2013] 12 Journal of Information Warfare, 22
[179] ibid 28
[180] ibid
[181] ibid
[182] Brian Orend, 'Kant's Just War Theory' [1999] 37 Journal of History of Philosophy, 323
[183] ibid

attribution process, and non-state actor criminalisation. The UN body tasked with the "ultimate goal of . . . disarmament,"[184] is the UN Disarmament Commission—a "deliberative body . . . [that] consider[s] and mak[es] recommendations . . . [on] disarmament,"[185] to the General Assembly. The Commission is technically supported by the UN Office of Disarmament Affairs. In 2019, an Open-Ended Working Group was formed by the Office to reaffirm the UN's role in regulating "developments in information and communications technologies,"[186] consistent with its three-pillar mandate for protecting "peace and security, human rights and sustainable development."[187] The final report raises issues, *inter alia*, of critical infrastructure and independent, domestic state policing of internet usage;[188] it also endorses widening of international law to include cyber phenomena, and supports heightened state reporting of cyberattack vulnerability and multilateral protection of information and communications technologies production.[189]

This has been hailed as an achievement in consensus-building,[190] though it is worth noting that consensus-building around *any* UNDC-recommended multilateral agreement failed between 1999 and 2017.[191] Still, the effort to address offensive cyber use has been initiated, no doubt from increased incidence and escalatory potential of hostile cyberoperations. It is not

[184] UNODA, 'About Us' (*United Nations Office for Disarmament Affairs*) <https://https://www.un.org/disarmament/about/>
[185] UNODA, 'United Nations Disarmament Commission' (*United Nations Office for Disarmament Affairs*) <https://https://www.un.org/disarmament/about/>
[186] UNGA, Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report [2021] A/AC.290/2021/CRP.2, 3
[187] ibid
[188] Josh Gold, 'Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?' (*Council on Foreign Relations* 18 March 2021) <https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what>
[189] ibid
[190] ibid
[191] *UNODA* (n 184)

suggested that a working group will trigger a *Kantian* post-conflict universe, but the multilateralism and reassertion of the UN's role in regulating warfare could signal imminent, incremental consensus-building towards cyber's place in such a post-conflict future. However, the precise time for legal clarification has not arrived; we do not yet relate in a *post bellum* existence, although existing multilateral agreements and the advanced nature of the multilateral system may suggest we are slowly moving towards that direction.

13. CONCLUSIONS

Kinetic warfare will always be part of war so long as there is no *total* peace—and so will cyberoperations. Not only is kinetic weaponry deployment costlier than cyber operations, cyberoperations can be undertaken ceaselessly, without triggering defence mechanisms or accounting for civilian indirect participation under existing IHL. Further, no precedent exists for the cyberattack that arises to an armed attack, and therefore, the destructiveness of status quo cyberattack usage may remain for a time. There also exists no clear approach to interpreting cyberattack against IHL, nor is there any multilateral consensus on defining cyberattack or differentiating it from kinetic warfare under the law. On a more practical level, there is no accounting for non-state actor participation in cyberattack, nor have evidentiary problems in terms of attribution and legal proceedings been addressed. It follows from these voids that there exists no multilateral agreement establishing where use of hostile cyberoperations sits within IHL.

As a declared domain of war, cyberattack' s exponentially increased use suggests advantages over purely kinetic weaponry. The focus of this document is that it is situated against an antiquated legal regime, where the lack of accounting for the impact cyber has had

on war has made cyberoperations more legally advantageous than kinetic weaponry to states who would take advantage of ambiguous applicability of international law. 'Cyber' exposes ambiguities in existing IHL., and its historical use has been deployed at levels short of legal thresholds triggering law. With no multilateral consensus establishing the legal limits of its use, and its potential for ubiquitous integration whether on the battlefield or not, and whether sublethal or lethal, cyberattack currently remains out of view of IHL, and is therefore currently more advantageous legally than kinetic forms of weaponry.

BIBLIOGRAPHY

Treaties

Convention (IV) Respecting the Laws and Customs of War on Land (18 Oct 1907) 36 Stat. 2277

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1979) 1125 UNTS 3 (Additional Protocol I)

UNGA, *Responsibility of States for internationally wrongful acts*, adopted 8 January 2008, A/RES/62/61

UNTS, *Charter of the United Nations* [1945] 1 UNTS XVI

ICJ Caselaw

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14

Oil Platforms (Islamic Republic of Iran v United States of America) (Judgment) [2003] ICJ Rep 161

US Government

Department of Defence, Summary of the 2018 National Defense Strategy of the United States of America, 19 Jan 2018

Office of the Director of National Intelligence, Annual Threat Assessment of the US Intelligence Community, April 9, 2021

Office of the President, National Security Presidential Memorandum 13: United States Cyber Operations Policy, National Security Presidential Memoranda, 18 September 2018 [unpublished]

United Nations
UNGA, Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report [2021] A/AC.290/2021/CRP.2

ICRC
ICRC, 'Direct participation in hostilities: questions & answers' (*ICRC International Committee of the Red Cross*, 2 June 2009) <https://www.icrc.org/en/doc/resources/documents/faq/direct-participation-ihl-faq-020609.htm>

ICRC, 'Technological Challenges for the Humanitarian Legal Framework' (11th Bruges Colloquium, Bruges, 21-22 October 2010) <https://www.coleurope.eu›pdf›Collegium41> accessed 21 July 2021

Books
Kosseff, J, *Cybersecurity Law* (Wiley 2020)

Schmitt, M, Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press 2013)

Book Chapters
Cullen, A, 'The characterization of remote warfare under international humanitarian law' in Ohlin, Jens David (eds) *Research Handbook on Remote Warfare* (Edward Elgar Press 2017)

Journal Articles
Aravindakshan, S, 'Cyberattacks: A look at Evidentiary Thresholds in International Law' [2021] 59 Indian Journal of International Law 285

Arquilla, J, 'Twenty Years of Cyberwar' [2013] 12 Journal of Military Ethics 80

Barrett, E, 'On the Relationship between the Ethics and the Law of War: Cyber Operations and Sublethal Harm [2017] 31 Ethics & International Affairs 467

Blank, L, 'Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict' [2020] 96 Notre Dame L Rev 249

Boothby, W et al, 'When Is a Cyberattack a Use of Force or an Armed Attack?' [2012] 45 Computer 82

Faga, F, ‘The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyberattack, and Cyber Warfare in the 21st Century’ [2017] 10 Baltic Journal of Law & Politics 1

Gallais, C and Filiol, E, ‘Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure.’ [2017] 16 Journal of Information Warfare 64

Giesen, K-G, ‘Towards a Theory of Just Cyberwar’ [2013] 12 Journal of Information Warfare 22

Kim, J, ‘Law of War 2.0: Cyberwar and the Limits of the UN Charter’ [2011] 2 Global Policy 322
Roman Kwiecień, ‘The Nicaragua Judgement and the Use of Force - 30 Years Later’ [2021] 36 Polish YB Int'l L 21

Lancelot, J, ‘Cyber-diplomacy: cyberwarfare and the rules of engagement’ [2020] 4 Journal of Cyber Security Technology 240

Lifland, A, ‘Cyberwar: The Future of Conflict’ [2012] 33 Harvard International Review 7

Nguyen, R, ‘Navigating ‘Jus Ad Bellum’ in the Age of Cyber Warfare’ [2013] 101 California Law Review 1081

Orend, B, ‘Kant’s Just War Theory’, [1999] 37 Journal of History of Philosophy 323

Phillips, K, ‘Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain’ [2013] 70 Joint Force Quarterly 70

Raab, D, ‘‘Armed Attack’ after the Oil Platforms Case’ [2004] 17 Leiden Journal of International Law, 719–735

Voitaşec, D-J, 'Applying International Humanitarian Law to Cyberattacks' [2015] 530 Lex ET Scientia International Journal 126

Press

Finkle, J and Rothacker, R, Exclusive: Iranian hackers target Bank of America, JPMorgan, Citi, *Reuters* (21 September 2012)

Gold, J, ‘Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?’ *Council on Foreign Relations* (18 March 2021) <https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what> accessed 22 August 2021

Grimes, R, Stuxnet: Smarter -- and deadlier -- than the average worm, *Chief Security Officer Online* (5 October 2010)

Holland, S and Chiacu, D, U.S. and allies accuse China of global hacking spree *Reuters* (Washington 20 July 2021)

Jacobs, J, Biden Says 'Not Sure' If Russia Is Behind Latest Cyberattack *Bloomberg* (3 June 2021)

Kanno-Youngs, Z and Sanger, D, U.S. Accuses China of Hacking Microsoft *The New York Times* (Washington 19 July 2021)

Madhani, A and Tucker, E, Latest hack to test Biden's vow for consequences for Russia *Associated Press News* (Washington 7 July 2021)

Merchant, N and Jaffe, A, In 1st visit to intel agency, Biden warns of cyber conflict *AP News* (McClean, 28 July 2021)

Reuters Staff, Iran builds firewall against Stuxnet computer virus: minister, *Reuters* (Dubai, 16 May 2019)

Soldatkin, V, and Pamuk, H, Biden tells Putin certain cyberattacks should be 'off-limits' *Reuters* (Geneva, 16 June 2021)

Reference Websites

Black's Law Dictionary <https://thelawdictionary.org/> accessed 21 July 2021

CSIS, 'Significant Cyber Incidents' (*csis.org*, 2006-2021) <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> accessed 11 July 2021

UNODA, 'About Us' (*United Nations Office for Disarmament Affairs*) <https://https://www.un.org/disarmament/about/> accessed 22 August 2021

UNODA, 'United Nations Disarmament Commission' (*United Nations Office for Disarmament Affairs*) <https://https://www.un.org/disarmament/about/> accessed 22 August 2021