Israel Law Review **48**(1) 2015, pp 81–109. © Cambridge University Press and The Faculty of Law, The Hebrew University of Jerusalem, 2015.
doi:10.1017/S0021223714000314

The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision

Michael N Schmitt[*]

This article responds to the two articles published in this journal that criticise the approach taken by the International Group of Experts (IGE) who prepared the Tallinn Manual on the International Law Applicable to Cyber Warfare. Their authors took issue with the approach of the majority of the IGE over the question of whether data qualifies as an 'object' under international humanitarian law such that, for instance, cyber operations that target civilian data violate the prohibition on attacking civilian objects. The majority of the experts took the position that the law had not advanced that far and that pre-existing law could not be definitively interpreted to encompass data within the meaning of 'objects'. In this article, the Director of the Tallinn Manual Project responds to the authors' criticism of the majority view by explaining and clarifying its reasoning.

Keywords: humanitarian law, cyber, civilian object, military objective, data

1. Introduction

The cyber operations mounted during the Russia–Ukraine and Palestine–Israel conflicts of 2014 have demonstrated the continued necessity for clarification as to how international law is to be interpreted and applied with respect to activities in cyberspace.[1] Unfortunately, the few statements that states have issued on the matter lack the granularity required to be operationally meaningful.[2]

State reticence to stake out positions with regard to cyber operations has become chronic. The cyber operations conducted against Estonia in 2007 and mounted during the international armed conflict between Georgia and Russia the following year revealed a distinct lack of forethought on the part of the international law community in general, and states in particular, as to how international law – especially the *jus ad bellum* (law governing the resort to force by states)

[*] Charles H Stockton Professor and Director, Stockton Center for the Study of International Law, United States Naval War College; Professor of Public International Law, Exeter University; Senior Fellow, NATO Cooperative Cyber Defence Center of Excellence; Fellow, Harvard Law School Program on International Law and Conflict. The author served as Director of the project that produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (n 4). The views expressed herein are those of the author in his personal capacity. schmitt@aya.yale.edu.

[1] For a call for states to do so, see Michael N Schmitt and Sean Watts, 'The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare' (forthcoming 2014) 50 *Texas International Law Journal*.

[2] As an example, NATO's September 2014 Wales Summit Declaration stated: 'Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace': NATO, Wales Summit Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales, 5 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

and *jus in bello* (international humanitarian law or IHL) – governs activities in cyberspace.[3] In response to this lacuna, the NATO Cooperative Cyber Defence Centre of Excellence, which is based in Tallinn (Estonia), commissioned a three-year research project to examine the law of cyber conflict. The project drew together an 'International Group of Experts' (IGE) which consisted of 16 renowned international law academics and practitioners working in their personal capacity (numerous experts were then serving as senior legal advisers for their governments). A team of technical advisers assisted them and observers from NATO, the United States Cyber Command and the International Committee of the Red Cross (ICRC) participated actively during the deliberations. The work of the IGE was subsequently peer reviewed by 13 international law specialists and fine-tuned based on their recommendations. In 2013, Cambridge University Press published the final product as the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[4] I served as Director of the effort.

The Tallinn Manual consists of 95 'rules' adopted unanimously by the IGE. Each rule expressed the IGE's opinion regarding the state of customary international law (including that reflected in key treaties such as the UN Charter) as of July 2012, the date of the meeting at which it adopted the final draft. The requirement for unanimity meant that the rules reflected the lowest common normative denominator. Some of the experts would have gone further, but the project's process and goals demanded a conservative approach. Consequently, the IGE sought only to identify *lex lata*; the group never intentionally roamed into the realm of *lex ferenda*.

Accompanying each of the rules is commentary that identifies its legal basis, explains its normative content, addresses practical implications thereof in the cyber context, and sets forth differing views on the scope or interpretation of the rule. The members of the IGE – all of whom had experience in advising governments, militaries or the ICRC – were acutely sensitive to the fact that they were exploring virgin territory. They therefore endeavoured to capture fully and fairly every reasonable competing perspective for consideration by the Manual's primary audience – those serving in positions requiring them to render legal advice on cyber conflict, particularly states' legal advisers. The IGE believed this approach would prove most useful to these individuals as their respective states and organisations attempted to resolve unsettled matters through the adoption of legal positions and policies, issuance of expressions of *opinio juris* and promulgation of practical guidance such as rules of engagement.

The *sine qua non* of the Tallinn Manual process was agreement on the applicability of the *jus ad bellum* and *jus in bello* to cyber operations. Consensus was quickly achieved on this point, one

[3] With regard to the conflict see Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Cooperative Cyber Defence Centre of Excellence 2010) 66–90. The international legal community began to look at the subject in the late 1990s, the first major conference being held at the United States Naval War College in 1999, the proceedings of which were published as Michael N Schmitt and Brian T O'Donnell (eds), *Computer Network Attack and International Law*, International Law Studies, vol 78 (US Naval War College 2002). However, following the events of 9/11, its attention was redirected towards issues surrounding counter-terrorism operations and the conflicts in Iraq and Afghanistan.

[4] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) (Tallinn Manual).

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

that appears to be widely accepted today.[5] With regard to IHL, the experts accordingly concurred that the extant law governed cyber weapons and cyber operations;[6] the issue was not *whether* IHL applied, but *how*. Sorting out the ways in which IHL pertained in the cyber context was obviously no easy task. Differences of opinion within the IGE were common. Thus, the commentary carefully sets out the majority and minority positions, as well as those of which the IGE was aware but were not harboured by any of the experts.[7]

The reaction of the international legal community to the Tallinn Manual, especially state legal advisers, has been favourable. Today it is widely used in ministries of defence and foreign affairs. With respect to its IHL provisions, only two issues have generated noteworthy debate – the meaning of the term 'attack', a topic addressed in passing below, and the IHL notion of 'objects', the focus of this article. Both have been the subject of debate behind closed doors during governmental discussions and in open discourse throughout academia. The question with respect to the latter is whether 'data' constitutes an object such that the IHL protection afforded to civilian objects extends to it.[8]

Significant in this regard was a conference sponsored by the ICRC and the Hebrew University of Jerusalem in November 2013 at which Mr Kubo Mačák of Exeter University and Dr Heather Harrison Dinniss of the Swedish National Defence College took issue with aspects of the Tallinn Manual's examination of whether data could be considered an 'object', as that term is understood in IHL. I spoke on the same panel and defended the IGE's work. Their presentations have matured into the articles that appear in this volume of the *Israel Law Review*. Its editors have graciously allowed me to offer a riposte. Before turning to their articles, allow me to offer a few procedural comments.

First, the precise contours of customary IHL are both indistinct and, occasionally, controversial.[9] There was nevertheless concurrence within the IGE that those aspects of Additional

[5] See, eg, NATO (n 2); Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, June 2013, UN Doc A/68/98, 24 para 19; Harold H Koh, 'International Law in Cyberspace', Address at the USCYBERCOM Inter-Agency Legal Conference, Ft Meade, Maryland, 18 September 2012, reprinted in (2012) 54 *Harvard International Law Journal Online* 1, 3–5; Advisory Council on International Affairs (the Netherlands), 'Government [of the Netherlands] Response to the AIV/CAVV Report on Cyber Warfare', http://www.aiv-advies.nl/ContentSuite/template/aiv/adv/collection_single.asp?id=1942&adv_id=3016&page=regeringsreacties&language=UK; ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', October 2011, Doc 31IC/11/5.1.2, 36–38.

[6] Tallinn Manual (n 4) r 20; In particular, they pointed to Additional Protocol I, art 36, which requires legal review of new means and methods of warfare: Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I or AP I). Logically, the obligation could exist only if such means and methods were subject to existing IHL principles and rules.

[7] For example, the US position on the equivalency of a 'use of force' and 'armed attack' under the *jus ad bellum* is reflected in the Manual, despite the fact that no members of the IGE agreed with it: Tallinn Manual (n 4) 47. For a recent confirmation of this position by the then Legal Adviser to the State Department, see Koh (n 5) 7.

[8] Data is information in electronic form. The Tallinn Manual explains that it consists of 'the basic elements that can be processed or produced by a computer': Tallinn Manual (n 4) 258.

[9] The ICRC has completed a monumental three-volume study on the subject: Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law, Vol I: Rules* (ICRC and Cambridge University Press 2005, revised 2009) (ICRC Study). Concerns of the US regarding the study were set out in John B Bellinger

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

Protocol I to the 1949 Geneva Conventions addressing the conduct of hostilities – particularly the principles and rules surrounding attacks such as distinction,[10] proportionality[11] and precautions in attack[12] – generally reflect customary international law norms binding on non-parties.[13] Therefore, my analysis in this article of the relevant provisions of Additional Protocol I applies fully to their customary law counterparts.

Second, the views set forth in this article are entirely my own and are not intended to reflect those of any other member of the IGE. To the extent that I explain how the IGE came to its conclusions, the discussion is based on my recollection of the sessions that took place over the three-year period during which the Tallinn Manual came to life.

Third, like the IGE, I will slavishly adhere to the *lex lata*. I have set out elsewhere my views on where the law might be headed,[14] but in this article I merely comment on the state of the law as of July 2012. Although I believe the law on the notion of objects will evolve with some rapidity, speculation is not my purpose here. I do realise that the majority's interpretation of objects leads to undesirable results in the sense that it opens the door to cyber operations against data that could have a significant negative impact on the civilian population. However, an *all*-inclusive treatment of data as an object would, as will be explained, be *over*-inclusive. Until states determine the appropriate balance, it would be precipitate to extend the meaning of objects to this degree.

Finally, my contribution to the *Israel Law Review* must not be interpreted as criticism of Mr Mačák or Dr Harrison Dinniss. Both are brilliant scholars and, as an aside, dear friends. However, their contributions cannot go unanswered for it is the very process of intellectual give and take that will not only preserve IHL, but allow it to evolve in positive directions.[15] Thus, I offer these thoughts in the spirit of constructive and amiable dialogue between colleagues.

---

and William J Haynes, 'A US Government Response to the International Committee of the Red Cross's Customary International Humanitarian Law Study' (2007) 89 *International Review of the Red Cross* 443. On the study, see also Susan Breau and Elizabeth Wilmshurst (eds), *Perspectives on the ICRC Study on Customary International Humanitarian Law* (Cambridge University Press 2007.

[10] AP I (n 6) art 48, operationalised as to persons and objects in arts 51 and 52 respectively. The corresponding Tallinn Manual (n 4) rule is 31. See also ICRC (n 9) rr 1 and 7; Department of the Navy & Department of Homeland Security, 'The Commander's Handbook on the Law of Naval Operations', NWP 1-14M/MCWP 5-12/COMDTPUB P5800.7A, 2007 (NWP 1-14M), para 5.3.2.

[11] AP I (n 6) arts 51(5)(b), 57(2)(a)(iii), 57(2)(b). The corresponding Tallinn Manual (n 4) rule is 51. See also ICRC (n 9) rr 14, 18–19; NWP 1-14M (n 10) para 5.3.3.

[12] AP I (n 6) art 57. The corresponding Tallinn Manual (n 4) rules are 52–58. See also ICRC Study (n 9) rr 15–20; NWP 1-14M (n 10) para 8–1. On proportionality and precautions in cyber attacks, see Eric Talbot Jensen, 'Cyber Attacks: Proportionality and Precautions in Attack' (2013) 89 *International Law Studies* 198.

[13] To illustrate, I have highlighted in the footnotes the relevant rules of the ICRC Study (n 9) and, as an example of acquiescence by a non-party state, paragraphs from the most recent US military manual, NWP 1-14M (n 10), when first encountered.

[14] Michael N Schmitt, 'The Law of Cyber Warfare: *Quo Vadis*?' (2014) 25 *Stanford Law and Policy Review* 269; Michael N Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' (forthcoming 2014) 96 *International Review of the Red Cross*.

[15] The paradigmatic example being the well-known exchange on the issue of civilian direct participation in hostilities found in the *New York University Journal of International Law and Politics* by individuals who participated in the project leading to publication of the ICRC's interpretive guidance on the subject: Nils Melzer (ed), *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009); Kenneth Watkin, 'Opportunity Lost: Organized Armed Groups and the ICRC "Direct

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

2. THE RELEVANT TEXT

In order to grasp the discussion that follows, it is useful to quote the relevant text from the Tallinn Manual. The fulcrum of debate is rule 37, which provides: 'Civilian objects shall not be made the object of cyber attacks. Computers, computer networks, and cyber infrastructure may be made the object of attack if they are military objectives'.[16] This rule derives from Article 52(1) of Additional Protocol 1: 'Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives as defined in paragraph 2'.[17] The first sentence of Article 52(2) similarly provides that '[a]ttacks shall be strictly limited to military objectives'. The ICRC's Commentary on the Additional Protocols explains that the sentence was intended to confirm the previous principle.[18] Therefore, the operative prohibition is found in Article 52(1) and not, as is often incorrectly asserted, Article 52(2).

Article 52(2) serves to define the term 'civilian' as used in Article 52(1) by negative reference to the concept of military objective, an approach adopted in the Tallinn Manual.[19] According to Rule 38,[20]

> Military objectives are those objects which by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. Military objectives may include computers, computer networks, and cyber infrastructure.

The definition in the first extracted sentence is a nearly verbatim adaptation of that found in Article 52(2), except that the Additional Protocol rendering begins with the introductory clause '[i]n so far as *objects* are concerned'.[21] As will become clear, both Mr Mačák and Dr Harrison Dinniss attribute to that clause significance in the context of data that I do not.

Neither takes issue with the Rule 38 definition of military objectives proper. Their concern focuses instead on the following brief section of the commentary to Rule 38 addressing the question of whether data is an object.[22]

Participation in Hostilities" Interpretive Guidance' (2010) 42 *New York University Journal of International Law and Politics* 641; Michael N Schmitt, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42 *New York University Journal of International Law and Politics* 697; Bill Boothby, '"And For Such Time As": The Time Dimension to Direct Participation in Hostilities' (2010) 42 *New York University Journal of International Law and Politics* 741; W Hays Parks, 'Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect' (2010) 42 *New York University Journal of International Law and Politics* 769; Nils Melzer, 'Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities' (2010) 42 *New York University Journal of International Law and Politics* 831.

[16] Tallinn Manual (n 4) 124.

[17] See also ICRC Study (n 9) r 7; NWP 1-14M (n 10) paras 5.3.2, 8.1 and 8.2.

[18] Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC 1987) (ICRC Commentary), para 2014.

[19] Tallinn Manual (n 4) 125. On military objectives, see Agnieszka Jachec-Neale, *The Concept of Military Objectives in International Law and Targeting Practice* (Routledge forthcoming 2015).

[20] Tallinn Manual (n 4) 125. See also ICRC Study (n 9) r 8; NWP 1-14M (n 10) para 8.2.

[21] Emphasis added.

[22] Tallinn Manual (n 4) 127.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

> The majority of the International Group of Experts agreed that the law of armed conflict notion of object should not be interpreted as including data. Data is intangible and therefore neither falls within the 'ordinary meaning' of the term object[23] nor comports with the explanation of it offered in the ICRC Additional Protocols Commentary. Nevertheless, as noted in the Commentary to Rule 30, a cyber operation targeting data may, in the view of the majority of the Experts, sometimes qualify as an attack when the operation affects the functionality of computers or other cyber systems. A minority of the Experts was of the opinion that, for the purposes of targeting, data per se should be regarded as an object. In their view, failure to do so would mean that even the deletion of extremely valuable and important civilian datasets would potentially escape the regulatory reach of the law of armed conflict, thereby contradicting the customary premise of that law that the civilian population shall enjoy general protection from the effects of hostilities, as reflected in Article 48 of Additional Protocol I. For these Experts, the key factor, based on the underlying object and purpose of Article 52 of Additional Protocol I, is one of severity, not nature of harm. The majority characterized this position as *de lege ferenda*.

The reference to the ICRC Commentary built on an earlier observation in the Tallinn Manual commentary that '[t]he meaning of the term "object" is essential to understanding this and other Rules found in the Manual. An "object" is characterized in the ICRC Additional Protocol Commentary as something "visible and tangible"'.[24]

As will become apparent, critics of the majority approach sometimes conflate the legal meaning of the term 'attack' as used in Rule 37 and that of 'object' – the issue at hand with regard to data. The meaning of attack is central to the conduct of hostilities in cyberspace because the IGE took the position that only cyber operations that qualify as attacks in the IHL sense are subject to the Tallinn Manual rules that make reference to 'attacks'. Accordingly, the IGE took care to employ the term 'cyber attack' in its rules and commentary only when a 'cyber operation' satisfied its definition of the term contained in Rule 30: 'A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[25]

The commentary accompanying Rule 30 elaborates on the relationship between the notion of attack and operations against data.[26]

> Although the Rule is limited to operations against individuals or physical objects, the limitation should not be understood as excluding cyber operations against data (which are non-physical entities) from the ambit of the term attack. Whenever an attack on data results in the injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the 'object of attack' and the operation therefore qualifies as an attack. Further, as discussed below, an operation against data upon which the functionality of physical objects relies can sometimes constitute an attack.

[23] Vienna Convention on the Law of Treaties (entered into force 27 January 1980) 1155 UNTS 331 (VCLT), art 31(1).
[24] ICRC Commentary (n 18) para 2008.
[25] Tallinn Manual (n 4) 106 r 30.
[26] ibid 107–08.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

Some members of the IGE expressed unease with the apparent exclusion of cyber operations targeting (as distinct from 'attacking') data that might be detrimental to the civilian population, but not destructive or injurious. Various views surfaced on the issue, as explained in the commentary.[27]

> Within the International Group of Experts, there was extensive discussion about whether interference by cyber means with the functionality of an object constitutes damage or destruction for the purposes of this Rule. Although some Experts were of the opinion that it does not, the majority of them were of the view that interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components. Consider a cyber operation that is directed against the computer-based control system of an electrical distribution grid. The operation causes the grid to cease operating. In order to restore distribution, either the control system or vital components thereof must be replaced. The cyber operation is an attack. Those Experts taking this position were split over the issue of whether the 'damage' requirement is met in situations where functionality can be restored by reinstalling the operating system.
>
> A few Experts went so far as to suggest that interference with functionality that necessitates data restoration, while not requiring physical replacement of components or reinstallation of the operating system, qualifies as an attack. For these Experts, it is immaterial how an object is disabled; the object's loss of usability constitutes the requisite damage.
>
> The International Group of Experts discussed the characterization of a cyber operation that does not cause the type of damage set forth above, but which results in large-scale adverse consequences, such as blocking email communications throughout the country (as distinct from damaging the system on which transmission relies). The majority of the Experts took the position that, although there might be logic in characterizing such activities as an attack, the law of armed conflict does not presently extend this far. A minority took the position that should an armed conflict involving such cyber operations break out, the international community would generally regard them as attack. All Experts agreed, however, that relevant provisions of the law of armed conflict that address situations other than attack, such as the prohibition on collective punishment (Rule 85), apply to these operations.
>
> It should be noted that a cyber operation might not result in the requisite harm to the object of the operation, but cause foreseeable collateral damage at the level set forth in this Rule. Such an operation amounts to an attack to which the relevant law of armed conflict applies, particularly that regarding proportionality (Rule 51).

A brief comment is merited before replying to the two articles. Both Dr Harrison Dinniss and Mr Mačák sometimes speak of a Tallinn Manual position. The only such positions are with respect to the rules themselves (because they required unanimity) or in those instances when the commentary offers but a single interpretation of a rule. Styling other aspects of the Manual as such risks attributing views to members of the IGE who did not hold them and, in some cases, vigorously disputed them. In fact, what both authors do is to contest a *majority* position. That said, it happens to be my position, so let me turn to their points.

[27] ibid 108–09.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

3. A Reply to Mr Mačák

Mr Mačák begins by pointing to the '[i]n so far as objects are concerned' introductory clause in the definition of military objective in Article 52(2), drawing the conclusion that the Tallinn Manual commentary's exclusion of the clause seems to limit the term to objects, and is therefore inconsistent with state practice. This is not the case. The commentary expressly notes that the limitation is solely for the Manual's own purposes and was adopted simply because the analysis used to determine when individuals are targetable differs from that which applies to objects.[28] In fact, I accept the ICRC Commentary's observation that '[i]t should be noted that the definition is limited to objects but it is clear that members of the armed forces are military objectives …'.[29] However, the relevant question is not whether the IHL term 'military objectives' includes items other than objects (which it does), but instead whether data constitutes an object as that term appears in Article 52(1), its customary law equivalent, and the Tallinn Manual's derivative Rule 37.

This minor deviation complete, Mr Mačák turns to the issue at hand – data. He points to the following single sentence in the commentary apparently to conclude that the majority based its exclusion of data as an object on an essentially textual analysis: 'Data is intangible and therefore neither falls within the "ordinary meaning" of the term object nor comports with the explanation of it offered in the ICRC Additional Protocols Commentary'[30] (which characterises an object as an entity that is 'visible and tangible'). As he notes, the sole supporting footnote to the sentence in the Tallinn Manual commentary cites Article 31(1) of the Vienna Convention on the Law of Treaties.[31] In a footnote of his own, Mr Mačák observes that Article 31 also 'endorses the contextual (or systematic) method, and the teleological (or functional) method'.

This was a point that the IGE fully understood. Indeed, its citation of Article 31(1) suffices to encompass all three methods of interpretation: 'A treaty shall be interpreted in good faith in accordance with the ordinary meaning [textual] to be given to the terms of the treaty in their context [contextual] and in the light of its object and purpose [teleological]'.[32] In fact, the IGE

[28] ibid 126. Mr Mačák discusses 'locations' in his article, but no member of the IGE disputed the interpretation by which a location was encompassed in the meaning of the term 'object' since, after all, that is the plain meaning of the art 52(2) text. Note that locations are visible and tangible, the classic example being a mountain pass through which enemy forces intend to pass. On qualification of cyber targets by location, see Tallinn Manual (n 4) 128.
[29] ICRC Commentary (n 18) para 2017.
[30] Tallinn Manual (n 4) 127. Professor Marco Sassòli has observed that '[o]nly a material, tangible thing can be a target': Marco Sassòli, 'Legitimate Targets of Attacks under International Humanitarian Law' (2003) International Humanitarian Law Research Initiative Working Paper, January 2003, 2.
[31] The Tallinn Manual clearly explains its use of citation in the introduction, an explanation that in part accounts for the sole citation: Tallinn Manual (n 4) 7–9.
[32] VCLT (n 23) art 31(1). On art 31, see Jean-Marc Sorel and Valerie Bore-Eveno, 'Article 31' in Olivier Corten and Pierre Klein (eds), *The Vienna Conventions on the Law of Treaties: A Commentary* (Oxford University Press 2011) 804. As they note, '[i]t is thus fairly obvious that the text of Article 31 is a true example of a compromise: a compromise between the defenders of textual interpretation, of subjective interpretation based on the parties' intention, and of end-focused or teleological interpretation which attempts to extract those meanings from the text which might be intended beyond the formulation used': ibid 808. See also David S Jonas and Thomas N Saunders, 'The Object and Purpose of a Treaty: Three Interpretive Methods' (2010) 43 *Vanderbilt Journal of*

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

regularly took context and object and purpose into consideration. For instance, the term 'cyber context' appears in the Manual 50 times, while 'object and purpose' does so on eight occasions. Moreover, the reference to the ICRC Commentary's 'visible and tangible' text comports with the invitation in Article 32 of the Vienna Convention to consider 'supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of Article 31, or to determine the meaning when the interpretation of a treaty provision according to Article 31' remains 'ambiguous or obscure'.[33]

Mr Mačák next addresses whether the minority view set forth in the Tallinn Manual's commentary is, as characterised by the majority, a position *de lege ferenda*. As his starting point, he opines that I (and the Tallinn Manual) take the position that 'a putative interpretation of the law would be rejected as merely *de lege ferenda* if it was not grounded in relevant state practice and *opinio juris*', and asserts that it is 'not an appropriate standard for the interpretation of international law'. That is not my position. On the contrary, I agree that such an approach would be inappropriate, as would, to my knowledge, every member of the IGE.

To take a simple but telling example, Article 36 of Additional Protocol I requires a review of new weapons, means and methods of warfare.[34] Since they are new, there is little state practice and seldom much *opinio juris* against which to gauge their lawfulness. This does not preclude the interpretation of existing norms in light of the new weapon's intended use in order to comply with the Article 36 review requirement. Had my position been that state practice and *opinio juris* must attend any novel interpretation or application of IHL, the Tallinn Manual project itself would have been stillborn. Negligible state practice was available vis-à-vis the vast majority of the rules we crafted or the often differing interpretations thereof found in the commentary. That state practice which did exist was often classified and therefore inaccessible to most members of the IGE. Although the group was operating in this relative vacuum of state practice and *opinio juris*, it nevertheless was able to agree unanimously on the text of a wide array of rules.

This is not to say that the IGE operated precipitously. On the contrary, it took a very conservative approach. As noted in the introduction to the Manual, 'because State cyber practice and publicly available expressions of *opinio juris* are sparse, it is sometimes difficult to definitively conclude that any cyber-specific customary international law norm exists'.[35] In no case did the IGE conclude that a cyber-unique customary law norm – that is, a 'new' norm – had crystallised. This being so, Mr Mačák's use of the United Kingdom's assertion that a norm permitting humanitarian intervention had emerged is a *non sequitur*, except as an illustration that the line

Transnational Law 565, 577–81. Moreover, with respect to the IGE's citation of only art 31(1), the remaining paragraphs of the article serve primarily to supplement and expound on the first.

[33] Vienna Convention (n 22) art 32(a). On art 32, see Yves le Bouthillier, 'Article 32' in Olivier Corten and Pierre Klein (eds), *The Vienna Conventions on the Law of Treaties: A Commentary* (Oxford University Press 2011) 841.

[34] AP I (n 6) art 36. See also NWP 1-14M (n 10) para 5.3.4 (albeit limited to reviews of weapons). The IGE agreed that the reference to 'means' in the article was customary in nature, but did not agree on the character of the requirement to review methods of warfare: Tallinn Manual (n 4) 153–54.

[35] Tallinn Manual (n 4) 5.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

between *lex lata* and *lex ferenda* is horribly indistinct. This very truism lay at the heart of the IGE's conservatism, as evidenced not only by its insistence on including every reasonable interpretive viewpoint in the commentary, but also by its intentionally broad articulation of the unanimously agreed upon rules.

Rather than propounding new norms, the entire project focused on the interpretation of established norms. In this regard, all members of the IGE agreed that context mattered. Like Mr Mačák, we rejected the premise reflected in Sir Gerald Fitzmaurice's 'principle of contemporaneity' that international law can be somehow trapped in time.[36] The fact that states participating in the drafting of a relevant treaty failed to contemplate cyber operations was never an insurmountable obstacle to interpreting and applying its provisions.

To be fair, members of the IGE approached the task at hand from a variety of interpretive perspectives. Some were traditional positivists, while others – like myself (a New Havenist 'light') – leaned towards a policy-oriented approach. Yet, the group concurred that to retain valence, IHL has to be interpreted in light of the environment in which it is to be applied. Doing so with sensitivity to the object and purpose of IHL in general, and its individual principles and rules in particular, was similarly deemed crucial. In our view, IHL's dominant object and purpose is to delicately balance military necessity and humanitarian concerns.[37] Since the balance is continuously influenced by contemporary reality and values, interpretation shifts – and appropriately so – over time.[38]

Whenever the degree of uncertainty regarding interpretation and application in a particular situation proved significant, the IGE applied a rebuttable presumption in favour of not finding *lex lata*. In our view, it was for states, rather than the IGE, to make the interpretive leap. We were fearful that charges of going too far in particular instances would undermine the credibility, and therefore the utility, of the entire work. In any event, our decision to cite all reasonable interpretive stances in the commentary relieved us of the need to make such leaps.

Broadly speaking, three interpretive and applicative situations presented themselves. At one end of the spectrum lay those cases in which the advent of cyber warfare posed no interpretive dilemma. For instance, all members of the IGE agreed that a lethal or physically injurious cyber operation is an 'attack' in IHL terms and that one directed at civilians who are not directly participating in the hostilities is unlawful.[39] The fact that there have been no known civilian casualties resulting from cyber operations during an armed conflict did not detain the group in arriving at this conclusion. In the IGE's opinion, Rule 37's prohibition of such cyber operations is clearly *lex lata* despite the absence of practice or state expressions of concurrence in the interpretation; it

[36] Gerald Fitzmaurice, 'The Law and Procedure of the International Court of Justice 1951–54: Treaty Interpretation and Other Treaty Points' (1957) 33 *British Year Book of International Law* 203, 212.
[37] On the issue, see Michael N Schmitt, 'Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance' (2010) 50 *Virginia Journal of International Law* 795.
[38] For instance, all new weapons are subject to the rule that they must be discriminate, but advances in precision have rendered the international community's understanding of what it means to be discriminate more demanding: see generally, Christopher Markham and Michael N Schmitt, 'Precision Air Warfare and the Law of Armed Conflict' (2013) 89 *International Law Studies* 669.
[39] Tallinn Manual (n 4) r 32.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

is consistent with the plain text of the IHL norm and analogous previous practice with respect to other new methods and means of warfare. What is more, the rule in no way skews the contemporary balance between military necessity and humanitarian considerations.

This simple illustration (there are many more) illustrates the inaccuracy of Mr Mačák's contention that the IGE, or at least the majority thereof, was of the view that equating 'the absence of relevant state practice and *opinio juris* in support of a certain interpretation with the incorrectness of such interpretation under *lex lata* would be a step too far'. We did not, again to use his words, 'substitute the dearth of state practice for proper treaty interpretation'. On the contrary, it was our willingness to find *lex lata* when state practice and/or *opinio juris* were absent that we feared would draw criticism.

Mr Mačák seems to suggest that the majority was erratic in this regard, citing its position on organised armed groups in contradistinction to the aforementioned cautious approach to data as an object. The notion of 'organised armed group' is a crucial one in IHL. The existence of a non-international armed conflict depends on hostilities at a particular level of intensity between an organised armed group and a state, or between two or more such groups.[40] Furthermore, members of an organised armed group are targetable by different criteria from individuals who, although civilians, have directly participated in hostilities.[41]

The majority of the IGE (note that the composition of 'the majority' varied from case to case) concluded that 'the failure of members of the group physically to meet does not alone preclude it from having the requisite degree of organization'.[42] This conclusion was neither ungrounded nor radical. There is widespread practice of treating online groups as a single entity, both during peacetime and armed conflict, as recently exemplified by Anonymous and the Syrian Electronic Army respectively. Moreover, the majority, among whom I number myself, was restrained in qualifying online groups as organised. We excluded collections of individuals acting *collaboratively* (as in the case of many of the cyber attacks against Estonia in 2007 and Georgia in 2008), as distinct from *cooperatively*. The example used in the commentary was similarly narrow: 'a distinct online group with a leadership structure that coordinates its activities by, for instance, allocating specified cyber targets among themselves, sharing attack tools, conducting cyber vulnerability assessments, and doing cyber damage assessment to determine whether "reattack" is required'.[43] The majority went on to question whether such a group could satisfy the purported

[40] The International Criminal Tribunal for the former Yugoslavia, in a well-accepted characterisation, has described non-international armed conflict as 'protracted armed violence between governmental authorities and organized armed groups or between such groups within a State': ICTY, *Prosecutor v Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-AR72, Appeals Chamber, 2 October 1995, [70]. On the question of organised armed groups in the cyber context see Tallinn Manual (n 4) 88–90. See also Michael N Schmitt, 'Classification of Cyber Conflict' (2013) 89 *International Law Studies* 233, 245–48.

[41] On the targetability of members of an organised armed group, see Melzer (n 15) 70–73 (regarding the temporal scope of protection). Some controversy exists surrounding the ICRC's assertion that to qualify as a member of an organised armed group, the individual concerned must have a 'continuous combat function' therein: Tallinn Manual (n 4) 116–17. For my views on the subject, see Michael N Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis' (2010) 1 *Harvard National Security Journal* 5, 21–24.

[42] Tallinn Manual (n 4) 89.

[43] ibid 89.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

criterion of being capable of implementing and enforcing IHL.[44] Furthermore, even if 'organised', the practical impact of the majority's position is tempered by the fact that the group in question would still have to be 'armed'[45] and, in the case of classification of the conflict as a non-international armed conflict, engage in activities crossing the requisite level of intensity.[46] The IGE's restraint in this case accords with that which the majority took in the case of data.

At the opposite end of the spectrum were circumstances so remote from those self-evidently encompassed by an existing norm that its application in the cyber context could not be justified through contextual interpretation and/or by its object and purpose. In such cases, either a new norm or a dramatically new interpretation of the existing norm would have to emerge to address such situations. The former requires sufficient state practice and *opinio juris* to say the norm has crystallised, whereas the latter would only take hold once general acceptance as to the purported interpretation has coalesced. As an example, it has long been understood that the mere causation of civilian inconvenience does not qualify a military operation as an attack, nor does civilian inconvenience play into proportionality assessments or trigger the requirement to take precautions in attack to avoid collateral damage.[47] Thus, a cyber operation directed against a dual military/civilian use server that results in temporary interference with civilian email communications would not, on that basis alone, require consideration of that effect. Any assertion to the contrary plainly represents *lex ferenda*, at least for the present.

Between these two extremes lie situations in which: (i) the contextual applicability of a norm is not self-evident; (ii) there is some state practice and/or *opinio juris*, but not enough to definitively conclude that a new norm has emerged; or (iii) it is unclear that a particular interpretation in the cyber context is now generally accepted by states. In light of the relative paucity of practice or *opinio juris*, the issue of data fell into this category, as reflected in the differences of opinion within the IGE over its treatment.

Mr Mačák attributes excessive impermeability to the majority position, but it is more accurate to say that its adherents found themselves unable to comfortably aver that an interpretation by which the term 'object' includes data is manifestly self-evident. Therefore, its members agreed that state practice, *opinio juris*, or some other indication that the view had attained traction among states was needed before interpreting it as such vis-à-vis the prohibition on attacking objects, the rule of proportionality and the requirement to take precautions in attack. This position did not mean that members of the majority believed data should not be protected, or that it would not be so protected in the future. It simply signalled fidelity to our commitment to express *lex lata*, and no more, in the Tallinn Manual.

[44] ibid 89–90.

[45] See discussion in Tallinn Manual (n 4) 88: '… a group is armed if it has the capacity of undertaking cyber attacks' (r 30)); Schmitt (n 40) 248–49.

[46] See discussion in Tallinn Manual (n 4) 88; Schmitt (n 40) 248–49.

[47] Tallinn Manual (n 4) 160. For an identical conclusion beyond the context of cyber operations, see *HPCR Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press 2013) commentary accompanying r 14.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

In this regard, the definition of objects in the ICRC Commentary as something 'visible and tangible' did inform the majority's deliberations. However, despite the concern of both authors, at no point (on any issue) did the IGE deem itself bound by the ICRC Commentary. Albeit highly respected and influential (and extremely useful in our work), the Commentary is not binding as a matter of law. Additionally, it was produced well before computers came of age on the battlefield and, therefore, did not preclude reasonable contextual application of the respective Additional Protocol principles and rules to cyber operations.

Mr Mačák correctly notes that the visible and tangible reference was proffered to differentiate those objects meant to be protected by Article 52(1) of the Protocol from the general aims, goals or purposes of a military operation. For example, a strike on an electrical grid supplying energy to enemy forces, an object that qualifies as a military objective, must be distinguished from the desire to disrupt enemy command and control, which is the goal of the operation but not a military objective in the IHL sense. This is a distinction the IGE did not miss, but that did not detract from the fact that those who drafted the Article understood objects as those entities that were visible and tangible and used these characteristics to limit the Article's reach. The drafting history also includes a discussion of objects that references 'inanimate objects', which would further support this conclusion.[48] The point is that although the 'visible and tangible' comment influenced the IGE's deliberations (as well it should have[49]), it was not dispositive.

In the majority's view, a more influential factor was that certain military operations directed at civilian populations are currently commonplace.[50] For instance, psychological operations are

[48] Statement of US Representative, 'Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts', Geneva, 7 February 1975, CDDH/III/SR.15, vol XIV, 119. Professor Yoram Dinstein has noted that '[t]he noun "objects", used in the definition, clearly encompasses material and tangible things. However, the phrase "military objectives" is certainly not limited to inanimate objects, and it is wrong to suggest that the Protocol's language fails to cover enemy military personnel. To be on the safe side, the framers of Article 52(2) added the (otherwise superfluous) words "[i]n so far as objects are concerned," underscoring that not only inanimate objects constitute military objectives. Human beings can categorically come within the ambit of military objectives. Indeed, human beings are not the only living creatures that do. Certain types of animals – cavalry horses and pack mules in particular – can also be legitimate targets': Yoram Dinstein, 'Legitimate Military Objectives under the Current Jus in Bello' (2002) 78 *International Law Studies* 140, 142–43. Thus, he views objects as material, tangible and inanimate, but accepts, as did the IGE, that humans can also qualify as military objectives, albeit by different criteria. See also Yoram Dinstein, *The Conduct of Hostilities in International Armed Conflict* (2nd edn, Cambridge University Press 2010) 92 ('Since the noun "objects" intrinsically relates to material and tangible things, the definition must be regarded as confined to inanimate objects').

[49] Report of the International Law Commission on the Work of the Second Part of Its Seventh Session (1966) 2 *Yearbook of the International Law Commission* 169, 220, UN Doc A/6309/Rev 1 ('the text must be presumed to be the authentic expression of the intentions of the parties' and 'the starting point of interpretation is the elucidation of the meaning of the text, not an investigation *ab initio* into the intentions of the parties').

[50] Psychological operations are especially useful in counter-insurgency, stability and counter-terrorism operations. According to NATO, 'in complex political and social contexts where the will of the indigenous population becomes the metaphorical vital ground (i.e. it must be retained or controlled for success), there is a requirement to influence and shape perceptions through the judicious fusion of both physical and psychological means': NATO, 'Allied Joint Doctrine', December 2010, AJP-01 (D), 2–10. See also, generally, NATO, 'Allied Joint Doctrine for Civil-Military Cooperation', February 2013, AJP-3.4.9; NATO, 'Allied Joint Doctrine for Psychological Operations', October 2007, AJP-3.10.1(A). It should be cautioned that psychological operations, despite their generally negative image, may have such humanitarian purposes as exhorting the population to refrain

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

often designed to influence the attitudes and behaviour of the enemy's civilian population. This can be done, for example, by jamming the enemy civilian leadership's public television transmissions. No one would argue that such operations were *attacks* on a civilian *object*.

If those same messages were posted online, deleting or altering the video file could disrupt their use. The consequences of treating the file as an object would be significant, for the data would qualify as a *civilian* object; it would make no effective contribution to military action and its destruction would not offer a definite military advantage.[51] Moreover, the operation would qualify as an attack because a civilian object would be damaged (altered) or deleted (destroyed). Thus, the operation would amount to an unlawful attack on a civilian object. It did not seem congruent to countenance the jamming, but disallow a cyber operation with the same impact on the civilian population solely on the basis that data was affected.

In light of such outcomes, the majority was unprepared to treat data as an object, at least until evidence surfaces that states are willing, or even likely, to adopt the position. Although its members were acutely aware that the destruction of some civilian data could generate serious consequences, they were not ready to confidently claim that the military necessity/humanitarian considerations balance had been so transformed by this reality that a new interpretation of data was required. Reduced to basics, the majority believed the simple extension of the notion of objects to data would be, at least at present, overbroad. The closest the IGE came to this position was acceptance of the premise that if harm to data has a physically destructive or injurious consequence, it qualifies as an 'attack' and would be encompassed in the prohibition on attacking civilian objects, the proportionality rule and the precautions in attack requirement. In the case of the prohibition, the 'object of attack' would be the entity affected, not the data; as to proportionality and precautions, the collateral damage would be that resulting from harm to the data, not the harm to the data itself.[52]

To summarise, a methodical reading of the Tallinn Manual in its entirety establishes that the IGE rejected the notion of contemporaneity, interpreted the extant law in context, carefully considered the object and purpose of IHL and understood that IHL norms evolve over time. The group recognised, in the words of the Israeli Supreme Court, that 'new reality at times requires new interpretation. Rules developed against the background of a reality which has changed *must take on a dynamic interpretation* which adapts them, in the framework of accepted interpretational rules, to the new reality'.[53] Thus, in the absence of evidence signalling the emergence of a new norm or reinterpretation of the notion of object by states, Mr Mačák's disagreement with the majority position boils down to a difference of opinion as to whether the issue fell within the

from participating in war crimes, crimes against humanity or genocide; allow the unimpeded transit of humanitarian assistance; respect the work of non-governmental organisations; provide objective news; and warn the civilian population to stay away from areas where combat is likely to occur.

[51] AP I (n 6) art 52(2).

[52] Tallinn Manual (n 4) 108.

[53] HCJ 769/02, *Public Committee Against Torture in Israel and Palestinian Society for the Protection of Human Rights and the Environment v Israel and Others* ILDC 597 (IL 2006) [2006], para 28.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

first category described above – that in which the applicability of a norm in the cyber context is self-evident in light of the changed circumstances – or not.

Allow me to comment on his position. To begin with, the precise issue is not, as he puts it, to 'interpret the term "object" in Article 52(2) in light of present day conditions' – that is, to define it by reference to the prerequisites for an object to qualify as a military objective. It is how to define the term as it appears in Article 52(1), which contains the operative prohibition on attacking civilian objects. Article 52(2) has little direct bearing on whether a target *is* an object. Instead, it imposes a further requirement that objects qualify as military objectives before they may be lawfully attacked.

With respect to defining the term 'object', Mr Mačák first points to translation discrepancies in the six authentic languages, noting that in two – French and Spanish – the term '*un bien*' may be translated into English as 'a good' or 'a property', and that in the Francophone world the legal term includes both tangible and intangible property. However, this argument ignores the full text of the ICRC Commentary on the issue.

> The English text uses the word 'objects', which means 'something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing'. The French text uses the word 'biens', which means 'chose tangible, susceptible d'appropriation'.
>
> *It is clear that in both English and French the word means something that is visible and tangible.*[54]

As is apparent, the authors of the ICRC Commentary – who include native French speakers who were involved in the Diplomatic Conference that drafted the treaty – considered the French text and were comfortable with the 'visible and tangible' rendering of 'object'.

Mr Mačák next contends that the term 'object' in the Additional Protocol section relating to attacks 'means something that may become the target of attacks. It must thus be something susceptible to "destruction, capture, or neutralization"' – a phrase drawn from Article 52(2)'s definition of military objective. Presumably this logic is based in part on that paragraph's introductory proviso that only military objectives may be attacked. He asserts that data fits this description.

This approach reverses the correct chain of legal analysis. Enemy morale may be 'destroyed'. Enemy radio and phone transmissions may be 'captured'. Enemy command and control capability may be 'neutralised'. However, the fact that targeting them 'make[s] an effective contribution to military action and [their] total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage' does not render them objects.[55]

Proper analysis starts with determining whether a target is an object. This is why the issue of data as an object is fundamental. Only if it is an object (which I believe it is not) does the requirement for the second step arise – determining whether the operation qualifies as an attack. If the

[54] ICRC Commentary (n 18) paras 2007–08 (emphasis added).
[55] AP I (n 6) art 52(2); Tallinn Manual (n 4) r 38.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

data (object) in question is destroyed (deleted) or damaged (altered), the operation is logically an attack because damage and destruction are conditions precedent to qualification as an attack.[56] Once this threshold is crossed, it is necessary to establish whether the data (the object of attack) is a military objective, which is assessed in part by whether its 'destruction, capture, or neutralisation, in the circumstances ruling at the time, offers a definite military advantage'.[57] Accordingly, the fact that data may be deleted (destroyed) or altered (damaged) is not in itself determinative as a matter of law; it must qualify as an object before such consequences have a normative effect.[58]

Continuing his analysis, Mr Mačák highlights the discussion of psychological operations that appears in my writings.[59] Similar analysis can be found in the Tallinn Manual commentary, and the subject was in part engaged above.[60] He contends that I have 'argued that destruction of data without physical consequences is more akin to psychological operations' and therefore he queries 'is computer data analogous to abstract notions such as population morale or to "tangible" things such as a bridge?'. However, I was addressing a different issue – qualification of cyber operations as 'attacks' under IHL – not the character of data.

As noted in the introduction, a major debate – unresolved during the Tallinn Manual process – surrounds the legal scope of the term 'attack', a critical matter because many of IHL's 'conduct of hostilities' prohibitions are framed in terms of 'attack', including that at issue here.[61] Article 49(1) of Additional Protocol I defines attacks as 'acts of violence against the adversary, whether in offence or defence'.[62] The IGE agreed that the definition extends to acts that are not in themselves violent (as in the case of cyber operations) but which nevertheless produce violent consequences.[63] Therefore, the group unanimously agreed that, at a minimum, 'a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[64] The majority further took the position that damage

[56] AP I (n 6) art 49; Tallinn Manual (n 4) r 30: the Manual does not address this issue head on because of the majority view that data does not qualify as an object.
[57] AP I (n 6) art 52(2).
[58] For a general discussion of the process of contemporary targeting from a legal perspective, see Michael N Schmitt and Eric Widmar, '"On Target": Precision and Balance in the Contemporary Law of Targeting' (forthcoming 2014) 7 *Journal of National Security Law and Policy*. See also William H Boothby, *The Law of Targeting* (Oxford University Press 2012); Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Brill 2009). On targeting practices generally, see US Chairman of the Joint Chiefs of Staff, 'Joint Publication 3-60, Joint Targeting', 31 January 2013.
[59] He cites Michael N Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 *International Law Studies* 89, 92–96; Schmitt, '*Quo Vadis*' (n 14) 298.
[60] Tallinn Manual (n 4) 106, 112.
[61] See, eg, AP I (n 6) arts 51, 52, 54–58. For my views on this issue, see Schmitt, 'Rewired Warfare' (n 14); Michael N Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (Cooperative Cyber Defence Centre of Excellence 2012) 283, 289–93. See also Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 *International Review of the Red Cross* 533, 556–60; ICRC (n 5) 37–38.
[62] See also ICRC Study (n 9) 4.
[63] Tallinn Manual (n 4) 106–107.
[64] ibid r 30.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

included the notion of interference with the functionality of an object that necessitates repair, even if the object is not physically affected.[65]

A key issue in this debate is the meaning of the term 'violence' in Article 49(1); the specific question is whether non-destructive or non-injurious consequences can nevertheless amount to the type of violence envisaged by the Article. My references to psychological operations were made in this context: 'operations aimed at the civilian population are not uncommon during armed conflict, the paradigmatic example being psychological operations, which are generally deemed lawful unless they cause physical harm or human suffering'.[66] The issue raised by psychological operations is not whether data is more like morale or bridges; it is whether non-destructive or non-injurious cyber operations directed *at civilian objects or civilians* are more like psychological operations against them (not traditionally viewed as 'violent', and therefore not an *attack*) or kinetic targeting operations (clearly unlawful attacks because they are violent).

In the article he cites, written two years before completion of the Tallinn Manual, I took on the 'object' controversy without reference to psychological operations.[67]

> [O]ne unsettled issue is whether data resident in computers comprise an 'object' …
>
> No definitive answer to this question exists. It would appear overbroad to characterise all data as 'objects'. Surely a cyber operation that deletes an innocuous e-mail or temporarily disrupts a television broadcast does not amount to an unlawful attack on a civilian object. For instance, it is well settled that an operation employing electronic warfare to disrupt civilian media is lawful. It would make no sense to distinguish between such an operation and a cyber operation that destroys data to achieve precisely the same result. Absent an agreed interpretation in the cyber context, it is perhaps best to tread lightly in characterising data as an object.
>
> Generally, data should not be characterised as an object in itself. Rather, the determinative question is whether the consequences attendant to its destruction involve the requisite level of harm to protected physical objects or persons. If so, the cyber operation constitutes an unlawful attack.

My position is thus as follows. Since data is not an object, then on that basis it is not subject to the prohibition on attacking civilian objects; it is instead necessary to look to the consequences of its damage or destruction to determine whether the prohibition applies. However, as I have just noted above, I concede that if data is an object as a matter of law, the prohibition applies, albeit only if the cyber operation in question qualifies as an attack because the data has been damaged or destroyed.[68]

Mr Mačák later returns to the issue of 'attack', contending that cyber operations that destroy data would constitute an attack. As just stated, I agree that they would *if* data first qualifies as an

[65] ibid 108–09.
[66] Schmitt, 'Cyber Operations and the Jus in Bello' (n 59) 91.
[67] ibid 96.
[68] Professor Noam Lubell, cited by Mr Mačák, has been careful to make the distinction between the issues of object and attack. Although he arrives at a different result from mine, his methodological approach is valid: Noam Lubell, 'Lawful Targets in Cyber Operations? Does the Principle of Distinction Apply?' (2013) 89 *International Law Studies* 252, 261–64.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

object, but his choice of examples to demonstrate that states would treat them as attacks is unconvincing. For example, he cites the case of targeting 'critical data of a military nature, such as weapons logs, timetables for the deployment of military logistics or air traffic control information'. He argues that states would be likely to accept characterisation of the data as a legitimate military objective. In doing so, he falls into the same trap as before, for the question remains as to whether such data is an object. If so, obviously it constitutes a military objective and may be 'attacked'; but if it is not an object, it may still be 'targeted' because the prohibition on attacking civilian objects does not attach. States would be comfortable with either approach.

He also employs the example of 'essentially civilian data, such as electronic health records held at a particular hospital' that if 'clandestinely erased or altered' could endanger the lives and health of patients. Operations against such data should therefore not fall 'outside the scope of IHL'. But they do not. To begin with, the operation is an attack irrespective of the targeting of the data because of the potential foreseeable harm to patients. As the IGE noted without dissent, the requisite consequences to qualify as an attack 'include any foreseeable consequential damage, destruction, injury or death' and, accordingly, '[w]henever an attack on data results in the injury or death of individuals … those individuals … constitute the "object of attack" and the operation qualifies as an attack'.[69] Further, foreseeable *collateral* damage of the qualifying nature would also render the operation in question an attack.[70] Finally, the example is inapposite because the IGE unanimously concluded in Rule 71 that 'data that form an integral part of the operations or administration of medical units and transports must be respected and protected, and in particular may not be made the object of attack'.[71]

Mr Mačák next takes on my assertion that states would be unlikely to countenance treating data as an object because it would restrict their options, and suggests that the 'premise of [my] argument is flawed'. He analogises my example of the innocuous e-mail with a single letter (which we agree is an object) and argues that 'it is unlikely that states would, within the scope of armed conflict, engage in a military operation the sole aim of which would be to destroy one civilian letter (or one such e-mail)'. For him, the more likely scenario is an attack on a facility that qualifies as a military objective, such as a post office taken over by enemy forces. Operation of the proportionality rule would allow for the attack so long as expected collateral damage, which would include loss of the letter, is not excessive relative to the anticipated military advantage of the attack. Thus, even if an object, destruction of the letter – or the e-mail in an analogous cyber situation – would not be precluded. Therefore, states need not worry about the impact of styling data as an object.

This is unresponsive logic. The point of my argument was that there can be situations in which a state *would* want to target civilian data directly and therefore would hesitate to embrace an interpretive approach that would render it a civilian object. Examples were provided above; there are many more, including the other illustration I used in the article he refers to (extracted

[69] Tallinn Manual (n 4) 107–08.
[70] ibid 109.
[71] ibid r 71.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

above) – disrupting television broadcasts. His reference to a situation in which states would see no need to target the civilian data in question is relevant only with respect to whether the harm to that data factors into the proportionality and precautions in attack analyses. In that regard, discounting my position would have necessitated an example in which the harm to the civilian data would have altered these assessments. It is only the inclusion of such data that would concern states.

Finally, Mr Mačák turns to the matter of 'object and purpose', which, as noted, I believe must be assessed in the contemporary context. In my mind, this is the key issue. It is where he should have begun, and stopped. This is so because I agree with his observation that '[t]eleological interpretation is … an available method ... with respect to customary norms'.[72] I likewise agree with his assessment that 'the enhancement of the protection of civilians during situations of armed conflict' is the object and purpose of Article 52(2), although the better reference is Article 52(1), which contains the operative prohibition in question.

In my estimation, Mr Mačák oversimplifies the teleological interpretation of IHL. What I have noted elsewhere bears repeating here.[73]

> As the 1899 and 1907 Hague Regulations famously noted, '[t]he right of belligerents to adopt means of injuring the enemy is not unlimited.'[74] Rather, IHL represents a carefully thought out balance between the principles of military necessity and humanity. Every one of its rules constitutes a dialectical compromise between these two opposing forces.
>
> This should be unsurprising, for only states have the capacity to make international law, either by treaty or through state practice maturing into customary law. International law thus reflects the goals of those states consenting to be bound by it. In the arena of conflict, states harbour two prevailing aims. The first is an ability to pursue and safeguard vital national interests. When crafting IHL, states therefore insist that legal norms not unduly restrict their freedom of action on the battlefield, such that national interests might be affected. The principle of military necessity constitutes the IHL mechanism for safeguarding this purpose. It is not, as sometimes asserted, a limitation on military operations. Instead, the principle recognises the appropriateness of considering military factors in setting the rules of warfare.

[72] He argues that the object and purpose of AP I carries an additional degree of relevance for those states that have signed but not ratified this instrument – a category which includes, but is not limited to, the United States, citing art 18 of the Vienna Convention on the Law of Treaties. States in this position must refrain from acts that would undermine the object and purpose of the treaty. This ignores the fact that the US has, over decades, 'made its intention clear not to become a party to the treaty' and therefore is relieved of this obligation: VCLT (n 23) art 18(a). See, eg, President Ronald Reagan, 'Message to the Senate Transmitting a Protocol to the 1949 Geneva Conventions', 29 January 1987, http://www.reagan.utexas.edu/archives/speeches/1987/012987b.htm.

[73] Schmitt (n 37) 798–99.

[74] Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulation concerning the Laws and Customs of War on Land, Martens Nouveau Recueil (ser 3) 461 (entered into force 26 January 1910), art 22; Hague Convention (II) Convention with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 26 Martens Nouveau Recueil (ser 2) 949 (entered into force 4 September 1900) art 22. The principle also appears in AP I, albeit with the addition of 'methods' of warfare: AP I (n 6) art 35(1). Methods generally refer to tactics, whereas means refer to weapons.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

> Legitimate states are equally obligated to ensure the well-being of their citizenry, for the provision of 'public goods,' such as physical safety, underpins the social contract between a state and its people. The principle of humanity, which operates to protect the population (whether combatants or noncombatants) and its property, advances this imperative.

I feel compelled to make this point in response to two mirror image errors that are often made when interpreting IHL provisions. On the one hand, it is sometimes asserted that the application of IHL rules is subject to the condition of military necessity such that necessity may justify deviation therefrom, a position famously rejected in the *Hostages Case*.[75] On the other hand, IHL's incontrovertible object and purpose of tempering the suffering and destruction of warfare is frequently assessed in isolation from military necessity factors. That states carefully consider military necessity when crafting treaties or engaging in practice and expressing *opinio juris* is best illustrated by the rule of proportionality. This rule permits attacks that are expected to cause incidental harm to civilians and civilian objects so long as said harm is not excessive relative to the concrete and direct military advantage anticipated by the attacker.[76] This is so despite the fact that, for instance, the individuals harmed or otherwise affected may have nothing to do with the conflict.

Of course, Mr Mačák's concern that failure to interpret data as an object would 'greatly expand the class of permissible targets in warfare' is compelling in light of the object and purpose of protecting civilian objects, although a more precise formulation would be that cyber operations expand the practical ability to reach certain targets that exist in the form of data or that can be affected by targeting data. If the term 'object' does not include data, civilian data may be lawfully targeted despite deleterious effects on the civilian population, a reality that runs counter to humanitarian considerations. I agree.

However, one must be careful in this regard and think the matter through with normative balance. Mr Mačák cites the example of the April 2013 Syrian Electronic Army cyber operation involving a false Associated Press tweet that President Obama had been injured in a White House explosion. The tweet resulted in a significant fall on Wall Street but had no physical effects on any cyber infrastructure. He notes that '[a]ny such large-scale damage to civilian property in the physical world would certainly not escape the regulatory reach of IHL'.

In fact, the operation in question fell outside the reach of IHL because it was not associated with an armed conflict to which the United States was party. However, even had it occurred in the context of armed conflict, characterising data as an object would not have drawn the operation within the reach of IHL. While it could have been mounted by altering Associated Press data, the operation actually employed spear phishing (and a watering-hole attack)[77] to acquire the

[75] *United States v List* (*The Hostages Case*), Case No. 7 (19 February 1948), reprinted in *Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10*, Vol xi (1950) 1230, 1253–56.
[76] AP I (n 6) arts 51(5)(b), 57(2)(a)(iii), 57(2)(b).
[77] On spear phishing, see 'Spear Phishing: Scam, Not Sport', *Norton*, http://us.norton.com/spear-phishing-scam-not-sport/article. On watering-hole attacks, see 'Watering Hole Attacks', *Symantec*, https://www.symantec.com/content/en/us/about/media/pdfs/b-istr_18_watering_hole_edits.en-us.pdf.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

credentials necessary to tweet on behalf of the organisation.[78] Only in the case of altering the data would treating data as an object have rendered the operation unlawful; the phishing operation involved no data damage and thus the operation would not have qualified as a prohibited *attack*.

Even more simply, the group could have created multiple false media websites (for example, creating a website resembling that of *The New York Times* and using the domain name timesny.com instead of nytimes.com). If the websites were successfully publicised (on social media, for example) such that they would have begun to be actively shared or re-tweeted, the effects could have been just as disruptive as that which occurred. Yet, the operation would not be barred by the IHL prohibition on attacking civilian objects because no civilian data would have been affected.

Ultimately, one's position on the term 'objects' depends on a judgment call as to whether states are likely to interpret the notion as including data when they perform the balance between humanitarian considerations and military necessity that underpins all of IHL. The majority of the IGE concluded that at the present time it was premature to decide that they would. Mr Mačák merely disagrees.

Finally, Mr Mačák asserts that his interpretation 'has the additional benefit of providing clarity as to the identification of permissible military targets' and criticises the IGE's characterisation of a cyber operation against a website passing coded messages as an attack in which the military objective is the supporting cyber infrastructure. The IGE offered the example (distinguished in the commentary from a website inspiring patriotism) only to demonstrate that civilian objects engaged in cyber operations were capable of making 'an effective contribution to military action', and therefore could be converted into a military objective by the express terms of Article 52(2).[79] Yet, he dubs the characterisation 'entirely counter-intuitive and without correspondence in reality' and argues that 'any attempt to bring the website down would be likely to take the form of a denial-of-service attack'.

The characterisation is hardly counter-intuitive. Whether the data qualifies as a military objective or not, its supporting cyber infrastructure undeniably does. As to the reality of the illustration, Mr Mačák misses the fact that in light of the paucity of offensive cyber capabilities in many armed forces today, the purpose of the characterisation may be to justify a *kinetic* attack. Most importantly, and at the risk of excessive repetition, labelling data as an object provides no meaningful clarity to the identification of permissible military targets. This is because if data is an object and qualifies as a military objective, it may be attacked. If it is not an object, then such qualification is meaningless since the prohibition does not apply; it may be targeted provided a loss of functionality does not ensue. From the perspective of those planning, approving, executing or commenting on an attack, labelling data as an object provides no greater clarity than saying it is not data.

4. A REPLY TO DR HARRISON DINNISS

The criticism of the majority approach by Dr Harrison Dinniss is more linear and less theoretical than that of Mr Mačák. In great part, her approach and that of the majority lead to similar

[78] 'Trends 2014: Beyond the Breach', *Mandiant,* 4–7, http://connect.mandiant.com/m-trends_2014.
[79] Tallinn Manual (n 4) 130.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

practical results, albeit arrived at by dissimilar legal logic. This arises from her distinction between 'content-level' and 'operational-level' data. In particular, exclusion of content-level data (such as 'the text of [her] article, or the contents of medical databases, library catalogues and the like') from the ambit of the prohibition on attacking civilian objects makes sense. I agree fully with her that to the extent that 'content-level data' is protected, it is because IHL affords, as will be discussed, 'special protection' to certain entities.

Where we part ways conceptually is with respect to operational-level data (program data) – that is, the 'type of data that gives hardware its functionality and ability to perform the tasks we require'. She argues that this should be considered an object. Although a majority of the IGE rejected this view, a different majority, when considering the separate issue of qualification of a cyber operation as an attack, deemed a cyber operation that results in a system's loss of functionality and requiring replacement of physical components to be an attack.[80] Within that majority were experts, myself among them, who were of the view that attacks included situations in which 'functionality can be restored by reinstalling the operating system'.[81] Thus, whether the operation is prohibited because targeted operational-level data is a civilian object or because a civilian system is targeted in a manner that results in its loss of functionality, the operation in question is unlawful.

Dr Harrison Dinniss then turns to her assessment of the majority approach to data as an object, which she labels 'inconsistent'. She begins, like Mr Mačák, with the observation that Rule 38 on the definition of military objectives omits the phrase 'in so far as objects are concerned' that appears in Article 52(2) of Additional Protocol I. She also highlights the majority's citation of the ICRC Commentary's 'visible and tangible' text, noting – again as Mr Mačák did – that the phrase was meant to distinguish objects in the sense of Article 52 from the general aims or purposes of a military operation; it was not 'to specifically exclude intangible objects from the definition'. These points were addressed earlier and merit no further comment.

However, based on the latter distinction, Dr Harrison Dinniss maintains '[t]hus any computer program, database, system or virtual network could still qualify as a legitimate target if it meets the two-part definition set out in Article 52(2)'. This assertion is a leap of logic. The mere fact that the 'visible and tangible' text was not included to eliminate intangible entities from the scope of the term 'objects' does not mean that the prohibition on attacking objects *necessarily* encompasses entities lacking those characteristics. It merely leaves open that possibility. Moreover, as explained above, the majority considered the phrase but did not attribute determinative significance to it; like Mr Mačák, she attributes greater significance to the phrase in the majority position than did the majority itself, although in fairness to both of them a more robust discussion of the issue might have added clarity.

After brief discussion of whether data is or should be considered 'tangible' from a scientific perspective – a point on which I defer to the project's technical experts – Dr Harrison Dinniss

[80] ibid 108.
[81] ibid 109.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

makes the bold claim that 'requiring tangibility leads to a manifestly unreasonable result', and offers the following example in support of the assertion.

> To take a practical example, weapons, weapons systems and military *matériel* are perhaps the epitome of a legitimate military objective. Malware that is designed specifically to cause death, injury, destruction or damage is indisputably a weapon. Examples include Stuxnet-type code, which is intended to cause physical destruction, or even viruses such as Wiper, which destroyed the functionality of computer systems without destroying any physical components. However, by excluding intangible objects such as code from the interpretation of the definition offered by the majority of the Tallinn group, neither of these cyber weapons would constitute a legitimate military objective. It cannot be correct that one can have a weapon that is made entirely from code that does not constitute a military objective.

She continues that 'either a piece of code such as Stuxnet is a civilian object [because it is not a military objective] or, given that the problem is with the term "object" itself, it is not covered by the definition of military objectives at all'. Because the object and purpose of Additional Protocol I is 'to provide effective protection for civilians and civilian objects while enabling parties to an armed conflict to conduct effective military operations, either of those alternatives produces a manifestly unreasonable result'. Presumably, her dilemma is that the malicious code cannot be attacked when doing so would further this object and purpose.

In fact, no dilemma exists. Irrespective of the view one takes on the object issue, Stuxnet-like code is clearly targetable during an armed conflict. This is so even if the code is used to target only civilian objects.[82] If it falls within the meaning of 'object' (the IGE minority position), the code accordingly qualifies as a military objective that may be lawfully attacked. If it is not an object (the IGE majority position), the Article 52(1) prohibition on attacking civilian objects does not apply and the code may be targeted even if the operation results in destruction or damage to the code. Further strengthening the targetability of the Stuxnet code by the majority approach is the fact that there is no prohibition on targeting data by employing a military operation that does not qualify as an attack, a separate norm explored above. Interestingly, what distinguishes Dr Harrison Dinniss' approach is her concern that, at least in this case, failure to treat data as an object precludes targeting a militarily valuable entity – which it does not. Most other critics find fault with the fact that the majority interpretation leaves the door open to targeting civilian data. She seems to turn their concern on its head.

The glitch in her analysis is that she characterises the majority approach as 'insist[ing] on tangibility in the permitted targets of cyber operations'. This is the product of her focus on the concept of military objectives and the related Article 52(2) proviso that '[a]ttacks shall be limited strictly to military objectives'. However, the IGE did not adopt, as she suggests, a 'materiality requirement for objectives'. Recall that Article 52(2) merely confirms Article 52(1), the

[82] The issue of targeting civilians, civilian objects and other persons and objects arose during the deliberation over the ICRC's Interpretive Guidance. All of the experts agreed that a person who inflicts death, injury or destruction on persons or objects could qualify as a direct participant and, assuming the other two constitutive elements were met, be targeted; thus, by definition, they were a military objective: Melzer (n 15) 49–50.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

prohibition on attacking civilian objects; it was the Article 52(1) prohibition that was at issue during the IGE's deliberations. That being so, the majority was interpreting the term 'object' to determine when an entity qualifies as a civilian object protected from attack pursuant to Article 52(1), not to assess whether data qualifies as a military objective subject to attack. The distinction is a fine but essential one. The fact that an entity is not an object does not mean it may not be 'targeted'. On the contrary, it means that the prohibition on attacking civilian objects does not apply. There is no need to determine whether the target is a military objective.

This approach is consistent with the drafting history of Article 52. During the 1972 preparatory Conference of Government Experts, there was discussion about including both the mention of objects and the definition of military objects. For instance, according to the record of the Conference,[83]

> [t]hree experts proposed simply the deletion of the article on objects of a civilian character (CE/COM III/PC 22, 29 and 51) since, in their view, the concept of such objects flowed indirectly from that of military objectives (see below, Article 43). They declared that that course would be more favourable to the civilian population, for a positive definition of objects of a civilian character ran the risk of being either incomplete or open to a restrictive interpretation.

However, the reference to objects survived, thereby supporting the premise that the notion is not to be interpreted simply by reference to the definition of military objectives. Rather, the definition of military objectives is used to distinguish among objects, such that, as confirmed in the ICRC's study on customary international humanitarian law, 'only those objects that qualify as military objectives may be attacked; other objects are protected against attack'.[84]

Dr Harrison Dinniss further suggests that the majority's insistence on tangibility vis-à-vis military objectives is related to the IHL concept of attacks. In response, I suggest it is necessary to appreciate how the IGE dealt with the two distinct legal issues at hand – objects and attacks. The definition of *object* affects whether there is a prohibition on 'shooting' at data in cyberspace; it is about the *target*. By contrast, the definition of *attack* bears on whether a military operation qualifies as an attack, such that the various prohibitions on such operations apply; it is about the *operation*.[85]

These are separate issues and the IGE treated them as such. At the risk of repeating some of what has been said above, deconstruction of the text of Article 52(1) – 'Civilian objects shall not be the object of attack or of reprisals' – makes this clear. The first inquiry is whether targeted data is even the *object of attack*. For instance, if the goal of a cyber operation is to affect the

[83] ICRC, 'Conference of Government Experts on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts: Report on the Work of the Conference', Geneva, Second Session, 3 May–3 June 1972, Vol I, July 1972, para 3.128.
[84] ICRC Study (n 9) 32.
[85] Although Dr Harrison Dinniss fails to acknowledge the fact, the IGE was actually split on whether physical damage or injury is a criterion for 'attacks'. The majority view was that such consequences were, in the present state of the law, required, but extended the notion of damage to certain interference with functionality: Tallinn Manual (n 4) 108–09.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

functionality of a cyber system, it is that system which is the 'object of attack' and the analysis would relate primarily to the system, not the data. If the goal is to affect the data itself, as in an operation to encrypt data to preclude its use by the enemy, the question is whether the data qualifies as an *object*. If data is not an object, as suggested by the majority, the Article 52(1) prohibition does not apply and analysis stops. The operation may proceed. If, as asserted by the minority, the data is an object, it becomes necessary to ask whether that data is *civilian* in nature. This is done by reference to the definition of military objectives in Article 52(2). If the data satisfies the test set out therein, the operation may proceed. If not, the final question is whether the operation qualifies as an *attack*. My view is that it does if the data is damaged (deleted, altered, etc). Should damage be likely to occur, the operation would be unlawful. However, if not – as with simply blocking data transmission – the cyber operation would not be an attack and, accordingly, is not subject to the prohibitory effect of Article 52(1). The operation may be launched.

Finally, Dr Harrison Dinniss suggests that the IGE was inconsistent in its approach to the tangibility of various entities. It was so, albeit with good reason. For instance, she cites the fact that the group imposed no tangibility condition when subjecting intangible weapons, such as biological contagions, to IHL.[86] Yet, it is unclear why that would matter. There is no logical reason to suggest that the character of a means or method of warfare must track that of the object it is used to attack.[87] From an IHL perspective, she is comparing the majority approach with dissimilar aspects of IHL and asking why we took different approaches to them.

The second example is similarly flawed. She correctly notes that the IGE concluded that certain digital property, in particular digital cultural property, was protected by IHL; this was offered as further evidence of inconsistency. Putting aside her failure to note that the IGE was split on the import of the intangibility of digital cultural property, a point discussed at some length in the commentary,[88] it is correct that the group extended IHL protection to certain types of data in various circumstances. In some cases this represented the view of the IGE as a whole, while in others majority and minority views emerged. Such data included, inter alia, that related to medical care, United Nations missions, detainee correspondence, journalism, cultural property, diplomatic archives and communications, humanitarian assistance, and occupation.[89] Protection attached also to data, harm to which might have negative effects on specified protected persons, objects, or activities. Examples include installations containing dangerous forces, objects indispensable to the civilian population, and the natural environment.[90]

[86] The IGE was actually making a different point, one that dealt with the issue of whether an act involved 'violence' such that it could qualify as an 'attack'. It was not addressing the tangibility of the weapon: Tallinn Manual (n 4) 106 ('"Acts of violence" should not be understood as limited to activities that release kinetic force. This is well settled in the law of armed conflict. In this regard, note that chemical, biological, or radiological attacks do not usually have a kinetic effect on their designated target, but it is universally agreed that they constitute attacks as a matter of law').

[87] On cyber weapons, see William H Boothby, 'Methods and Means of Cyber Warfare' (2013) 89 *International Law Studies* 387.

[88] Tallinn Manual (n 4) 229–30.

[89] ibid rr 71, 74, 76, 79, 82, 84–86.

[90] ibid rr 80–81, 83.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

What has been missed in levelling the charge of inconsistency is that IHL provides *special* protection for certain objects, persons and activities that go beyond the protection from attack enjoyed by civilians and civilian objects. This protection is often framed in terms of respecting and protecting. Rule 70 is illustrative: 'Medical and religious personnel, medical units, and medical transports must be respected and protected and, in particular, may not be made the object of cyber attack'. The commentary explains:[91]

> The requirement to 'respect and protect' involves separate obligations. The duty to respect is breached by actions that impede or prevent medical or religious personnel, medical units, or medical transports from performing their medical or religious functions, or that otherwise adversely affect the humanitarian functions of medical or religious personnel, units, or transports. It includes, but is not limited to, the prohibition on attacks. For instance, this Rule prohibits altering data in the Global Positioning System of a medical helicopter in order to misdirect it, even though the operation does not qualify as an attack on a medical transport (Rule 30). Similarly, blocking the online broadcast of a religious service for combat troops is prohibited. It must be cautioned that the Rule does not extend to situations that occur only incidentally, as in the case of the overall blocking of enemy communications.
>
> By contrast, the duty to protect implies the taking of positive measures to ensure respect by others (e.g., non-state actors) for medical and religious personnel, medical units, and medical transports. For instance, the obligation would require a military force with the capability to do so to defend a hospital in an area under its control against cyber attacks by hacktivists, when and to the extent feasible.

The next rule expounds on this prohibition with respect to data: 'Computers, computer networks, and data that form an integral part of the operations or administration of medical units and transports must be respected and protected, and in particular may not be made the object of attack'.[92] As noted in the accompanying commentary,[93]

> [t]he protection set forth in this Rule derives from the broader protection to which medical personnel, units, and transports are entitled (Rule 70).
>
> …
>
> The 'data' referred to in this Rule are those that are essential for the operation of medical units and transports. Examples include data necessary for the proper use of medical equipment and data tracking the inventory of medical supplies. Personal medical data required for the treatment of individual patients is likewise protected from alteration, deletion, or any other act by cyber means that would negatively affect their care, regardless of whether such acts amount to a cyber attack.

Similarly, Rule 74(a) provides that '[a]s long as they are entitled to the protection given to civilians and civilian objects under the law of armed conflict, United Nations personnel, installations, materiel, units, and vehicles, including computers and computer networks that support United Nations operations, must be respected and protected and are not subject to cyber attack'; Rule 82

[91] ibid 205.
[92] ibid r 71.
[93] ibid 206.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

states that '[t]he parties to an armed conflict must respect and protect cultural property that may be affected by cyber operations or that is located in cyberspace'; Rule 84 notes that '[d]iplomatic archives and communications are protected from cyber operations at all times'; Rule 86 prohibits cyber operations that are 'designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance'; and Rule 87 provides that '[p]rotected persons in occupied territory must be respected and protected from the harmful effects of cyber operations', for instance by being allowed 'to transmit news of a strictly personal nature to members of their families, wherever they may be, and to receive news from them without undue delay'.[94]

Plainly, the protection afforded to data in these and the other cases is not inconsistent with either the definition of objects or that of attacks because it is *additional* to the protection of civilian objects from attack. It is irrelevant as a matter of law whether the data concerned is an object or the operation in question amounts to an attack; neither is a condition of the special protection afforded to it under IHL. Since the activities enjoy special protection, data on which those activities depend likewise enjoys protection.

The remainder of Dr Harrison Dinniss' contribution examines the requirement under Article 52(2) of the Additional Protocol for an object to make an effective contribution to military action by 'nature, location, purpose or use', as well as the extent of specificity required in defining the military objective. As the discussion does not directly impact upon the question at hand – whether data qualifies as an object – I shall not examine it here. My sole comment is with regard to her treatment of code 'forming part of the military *matériel* of the adversary … as part of an otherwise civilian object'. In her example, cyber operations are mounted against the code, thereby affecting the system's functionality. She states that

> it seems disingenuous to suggest that the attack is directed against the host system (even though it would qualify as a military objective through its dual use), where it is, in fact, more properly viewed as collateral damage in the attack against the military object embedded within. The Tallinn Manual approach to such a problem merely moves the alleged object of the attack to the nearest physical component or the recipient of the physical effect.

This analysis is perplexing. If the host system qualifies as a military objective, as she correctly acknowledges it does because it is used to store military data, it may be attacked. This is so whether the data qualifies as an object or not. Assuming, solely for the sake of analysis, that the code is an object, both the code and the host system on which it is stored are military objectives. Neither the fact that the host system performs civilian functions nor that the goal of the attacker is to destroy the data relieves the host system of its character as a military objective. Any incidental damage to other cyber infrastructure that is civilian in nature is, of course, an issue of proportionality and precautions in attack. Yet, it has never been asserted that a military objective, such as the dual-use host system, should be factored into either of these analyses. The sole exception, as acknowledged by the entire IGE, is that 'a cyber attack against a dual-use

[94] ibid 241.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

system will be unlawful whenever the individual military components thereof could have been attacked separately'.[95]

5. QUO VADIS?

In my view, the analyses of both Mr Mačák and Dr Harrison Dinniss are at times counter-normative, while their characterisation of the work of the IGE is occasionally counter-factual. Both arrive at conclusions as to the *lex lata* that I cannot but regard as *lex ferenda*. This does not detract from the importance and erudition of their contributions to the dialectical process by which the interpretation of international law, especially IHL, continuously evolves to take account of the context in which it is to be applied.[96]

I happen to believe the law will travel in the direction at which they both point. As I have noted elsewhere, the exclusion of data from the ambit of the concept of objects[97]

> is unlikely to endure. Today, the importance of data usually exceeds that of their physical manifestation. In fact, the existence of data serves to diminish the significance of corresponding physical objects. To take a simple example, most governments maintain digital copies of records for activities such as census taking, the provision of social benefits, voting, taxation, and so forth. Loss of the digitized records would be a much greater impediment to the continuation of governmental functions than would destruction of their physical equivalents; indeed, in the future there will be no 'hard copy' records. IHL will assuredly evolve to meet the shift in the relative importance of physical and virtual data.

This process will be evolutionary, not revolutionary. States are unlikely to countenance treating all (or even just operational-level) data as an object subject to the relevant IHL prohibitions. They will continue to safeguard their legal option of directing certain operations, such as psychological operations, at civilian populations even when said operations involve damage to data. Additionally, in light of military necessity concerns, they will hesitate to accept an interpretation of IHL that includes such damage in proportionality or precautions in attack calculations.

This begs the question of how the relevant normative architecture will evolve. I can only speculate.[98] Arguably, the likeliest trend will be greater focus on consequentiality, as it is that characteristic which underpins the military necessity/humanitarian considerations balance of IHL. This approach is already evident in the acceptance of the notion of functionality by a majority of the IGE vis-à-vis the meaning of the term 'attack'.

If evolution of the notion of object takes a similar vector, perhaps the concern of states regarding treating all data as objects (over inclusivity) and the countervailing concern regarding treating

[95] Tallinn Manual (n 4) 159.
[96] For instance, I have rethought my formerly rigid understanding of the term 'attack' over the past decade based on discussions that occurred during the Tallinn Manual process and elsewhere, as well as interaction with state legal advisers on the matter: Schmitt, 'Rewired Warfare' (n 14).
[97] Schmitt, '*Quo Vadis*' (n 14) 297.
[98] For a thoughtful article on the issue, see Robin Geiß and Henning Lahmann, 'Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space' (2012) 45(3) *Israel Law Review* 381.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press

none of it as such could be addressed through the emergence of a new norm based on function. For instance, data upon which 'essential civilian services' rely would qualify, thereby rendering the data a civilian object immune from attack. This would, of course, require either interpretive acrobatics or evidence of crystallisation, but the approach would better accord with the inherent military necessity/humanitarian considerations balance of IHL than either an 'all in' or 'all out'. I offer this as merely one possibility but, however the issue plays out, normative stasis is highly improbable.

https://doi.org/10.1017/S0021223714000314 Published online by Cambridge University Press