Israel Law Review **48**(1) 2015, pp 55–80. © Cambridge University Press and The Faculty of Law, The Hebrew University of Jerusalem, 2015.
doi:10.1017/S0021223714000260

Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law

Kubo Mačák[*]

This article presents the case for a progressive interpretation of the notion of military objectives in international humanitarian law (IHL), bringing computer data within the scope of this concept. The advent of cyber military operations has presented a dilemma as to the proper understanding of data in IHL. The emerging orthodoxy, represented by the 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare*, advances the argument that the intangible nature of data renders it ineligible to be an object for the purposes of the rules on targeting in IHL. This article, on the contrary, argues that because of its susceptibility to alteration and destruction, the better view is that data is an object within the meaning of this term under IHL and thus it may qualify as a military objective. The article supports this conclusion by means of a textual, systematic and teleological interpretation of the definition of military objectives found in treaty and customary law. The upshot of the analysis presented here is that data that does not meet the criteria for qualification as a military objective must be considered a civilian object, with profound implications for the protection of civilian datasets in times of armed conflict.*

Keywords: computer data, cyber, international humanitarian law, military objective, object

1. Introduction

The nature of warfare is undergoing a paradigm shift. Comparable in significance with the moments when armed contest for the first time expanded into the sea and then into the air, warfare has today irrevocably entered another domain: cyberspace.

While this latest development has opened a host of yet unresolved problems, ranging from questions of military strategy and tactics to technical matters and to issues of law, this article focuses narrowly on one significant challenge posed by this development to the applicability of international humanitarian law (IHL): namely, how do we assess, from this perspective, cyber attacks the aim of which is the destruction of electronic data without necessarily resulting in physical damage? In particular, does such data qualify as an 'object' under IHL, and may it thus be considered a military objective?

[*] Lecturer in Law, University of Exeter; DPhil Candidate (Law), Somerville College, University of Oxford; MPhil, MJur (Oxon); Mgr (Charles University, Prague); k.macak@exeter.ac.uk.
Earlier versions of this article were presented at the Law School Research Seminar at the University of Exeter on 20 November 2013 and at the 8th Annual Minerva/ICRC Conference, 'Military Objectives and Objects of War: An Uneasy Relationship', 24–25 November 2013, Minerva Center for Human Rights, The Hebrew University of Jerusalem, Israel. I am grateful to the participants for their helpful comments. I would like to express a special word of thanks to the following friends and colleagues who have read and commented on earlier drafts: Ana Beduschi, Jarrod Hepburn, Annika Jones, Mike Sanderson, Aurel Sari, Michael Schmitt and Noam Zamir. Finally, I would like to thank the anonymous reviewers for their valuable comments and suggestions. Any errors or omissions are, of course, entirely mine. All internet resources were last accessed on 15 July 2014.

The answers to these questions have significant consequences for the conduct of cyber operations in general and cyber warfare in particular. Attacks of this kind have not only been forecast and pondered over in academic literature,[1] but they have become a frequent occurrence in modern day reality.[2] One of the cornerstones of IHL is the principle of distinction, described by the International Court of Justice (ICJ) as a 'cardinal' principle of IHL.[3] It prescribes that belligerent parties must at all times distinguish between civilian objects and military objectives and direct their operations only against military objectives.[4] Does this distinction extend into the realm of cyberspace?

This article argues in favour of a broad understanding of the notion of 'object', bringing data within the scope of the rules on military objectives as codified in Additional Protocol I to the 1949 Geneva Conventions.[5] This interpretation runs against the 'emerging orthodoxy' represented by the recently published *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[6]

Accordingly, the article begins by presenting the position taken by the authors of the Tallinn Manual (Section 2). It then disposes of the possible objection that while an alternative view could be desirable, it would at best amount to a view *de lege ferenda*, but not an interpretation *de lege lata* (Section 3). It considers and rejects one possible interpretation under which data would amount to a non-object, yet it could constitute a legitimate military objective (Section 4). Finally, the article presents its case for the consideration of data as an object under IHL utilising the general rule of treaty interpretation reflected in Article 31 of the Vienna Convention on the Law of Treaties (Section 5). It will be demonstrated that this understanding is in line with the ordinary meaning of the term 'object' as understood in light of present day conditions, taking account of the context of the term in the Protocol and the object and purpose of the treaty.[7]

---

[1] See, eg, Mark R Schulman, 'Discrimination in the Law of Information Warfare' (1999) 37 *Columbia Journal of Transnational Law* 939, 964 (reversible attacks rendering systems inoperable); Herbert Lin, 'Cyber Conflict and International Humanitarian Law' (2012) 886 *International Review of the Red Cross* 515, 519 (attacks against critical military data containing deployment timetables); Michael N Schmitt, 'The Law of Cyber Warfare: *Quo Vadis*?' (2014) 25 *Stanford Law & Policy Review* 269, 297 (attacks causing the deletion of state-maintained digitised records).

[2] See, eg, *McKinnon v Government of the USA and Another* [2008] UKHL 59, per Lord Brown of Eaton-under-Heywood, [13]; 'Military Blamed after Planes Vanish from Europe Air-Traffic Control Screens', *The Guardian*, 13 June 2014 (both discussed below in Section 5.1.3); Max Fisher, 'Syrian Hackers Claim AP Hack that Tipped Stock Market by $136 Billion. Is it Terrorism?', *Washington Post*, 23 April 2013 (discussed below in Section 5.2).

[3] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Rep 226 (*Nuclear Weapons*), [78].

[4] 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), art 48; Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law, Vol I: Rules* (International Committee of the Red Cross and Cambridge University Press 2005, revised 2009) (ICRC Study), r 7.

[5] AP I, ibid.

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

[7] The analysis put forward in this article is largely in agreement with that presented in this volume by Heather Harrison Dinniss ('The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military

2. EMERGING ORTHODOXY: THE NOTION OF MILITARY OBJECTIVE DOES NOT INCLUDE DATA

The Tallinn Manual is the result of a comprehensive and rigorous endeavour that aims to identify the rules of international law applicable to cyber warfare. Produced by a group of international experts who were 'carefully selected to include legal practitioners, academics, and technical experts',[8] it purports to reflect their consensus as to the *lex lata* governing cyber conflict derived primarily from 'treaty law directly on point or sufficient state practice and *opinio juris* from which to discern precise customary international law norms'.[9] The Manual identifies a total of 95 rules belonging to general international law, the law on the use of force and IHL.

The question of the status of computer data under IHL arises in relation to the experts' interpretation of the rules on targeting in the context of cyber conflict. The relevant analysis can be found in Rule 38 and the attached commentary.[10] The rule forms part of Section 4 of Chapter 4, entitled 'Attacks against Objects', and is directly preceded by a section entitled 'Attacks against Persons'.[11] As this structure suggests, the authors distinguished between, on the one hand, rules on targeting applicable to living human beings and, on the other hand, those applying to everything else (denoted in the manual as 'objects').[12] The commentary in the Manual even appears to limit the term 'military objective' to the latter category,[13] which would, however, be at odds with much of the available state practice, according to which the term comprises individuals, objects, and often even land area.[14]

Objectives' (2015) 48(1) *Israel Law Review* 39, Sections 1 and 2). One difference relates to the scope of the concept of data. While Dinniss limits her analysis to 'operational-level data' or 'code', I argue that even what she designates as 'content-level data' should in principle be considered as an 'object' for the purposes of IHL. As will be seen in Section 5 of the present article, to do otherwise means to exclude from the ambit of IHL both data that should be seen as military objectives (such as weapons logs or military logistics data) *and* data of a clearly civilian character (such as private stock exchange or government taxation datasets). The broad understanding of the notion of 'object' proposed in this article would encompass these types of data as well.

[8] Tallinn Manual (n 6) 9.

[9] ibid 5; see also ibid 6–7 (cautioning that although the rules were agreed on by the experts on a consensual basis, the text of the commentary accompanying the individual rules did not always command the support of all the participants).

[10] ibid 134–37.

[11] ibid 124 and 113, respectively.

[12] See also ibid 106, r 30 (stating that cyber attacks may either cause 'injury or death to *persons*' or 'damage or destruction to *objects*') (emphases added).

[13] ibid 126 para 2 ('As used in this Manual, the term 'military objectives' refers only to those *objects* meeting the definition set forth in this Rule') (emphasis added). Nevertheless, this use is not entirely consistent throughout the Manual: see, eg, ibid 123 para 4 (acknowledging that an attack 'against a military objective, *including combatants*, might cause terror') (emphasis added).

[14] See, eg, Australia, *The Manual of the Law of Armed Conflict*, Australian Defence Doctrine Publication 06.4, Australian Defence Headquarters, 11 May 2006, para 5.27 ('The term "military objective" includes *combatant members* of the enemy armed forces') (emphasis added); Belgium, *Droit Pénal et Disciplinaire Militaire et Droit de la Guerre, Deuxième Partie, Droit de la Guerre*, Ecole Royale Militaire, par J. Maes, Chargé de cours, Avocat-général près la Cour Militaire, D/1983/1187/029 (1983) 27 ('Considered as military objectives are 1) Persons … 2) *Objects* … 3) *Places*') (emphasis added); Russia, Regulations on the Application of International Humanitarian Law by the Armed Forces of the Russian Federation, Ministry of Defence of the Russian Federation, Moscow, 8 August 2001, para 1 ('military objectives include units of armed forces

The Tallinn Manual transplants the wording from the Protocol into its legal definition of the term 'military objective'.[15] The relevant provision, Article 52(2) of the Protocol, which is considered today to reflect customary law,[16] reads:[17]

> Attacks shall be limited strictly to military objectives. *In so far as objects are concerned,* military objectives are limited to 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.

As rephrased by the Manual, Rule 38 states the following:

> Civilian objects are all objects that are not military objectives. 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.[18]

As expressly mentioned in the text of the rule *in fine*, tangible technological infrastructure, including computers and computer networks, is not excluded from the material scope of the rule. However, this is not the case with computer data.

As the experts tied the definition of military objectives closely to the notion of 'objects', they assigned central importance to the meaning of this term in the framework of Additional Protocol I. They cited the International Committee of the Red Cross (ICRC) Commentary on the Additional Protocols and observed that in this commentary '[a]n object is characterized ... as something "visible and tangible"'.[19] Placed against this interpretative background, data was poised to

(*personnel*, weapons and military equipment), except for medical units and medical transports') (emphasis added); United Kingdom, *The Manual of the Law of Armed Conflict*, Ministry of Defence, 1 July 2004, para 5.4.1 ('The term "military objective" includes *combatant members* of the enemy armed forces') (emphasis added); United States, JP I-04, 'Legal Support of Military Operations', 17 August 2011, https://www.fas.org/irp/doddir/dod/jp1_04.pdf, II-2 ('Military objectives are *combatants* and ... objects') (emphasis added). The military manuals referred to throughout this article are cited in the ICRC Customary IHL Database, 'Practice Relating to Rule 8: Definition of Military Objectives', http://www.icrc.org/customary-ihl/eng/docs/v2_rul_rule8_SectionA.

[15] Tallinn Manual (n 6) 125–26 para 1.

[16] ICRC Study (n 4) r 8 (considering the definition from art 52(2) AP I (n 4) to constitute a norm of customary international law applicable in both international and non-international armed conflicts); Marco Sassòli and Lindsey Cameron, 'The Protection of Civilian Objects: Current State of the Law and Issues de lege ferenda' in Natalino Ronzitti and Gabriella Venturini (eds), *The Law of Air Warfare: Contemporary Issues* (Eleven International 2006) 49–50 (concluding, on a close analysis of state practice including that of states which had not ratified AP I, that the definition provided in art 52(2) AP I is of a customary nature); Tallinn Manual (n 6) 126 para 1 and references cited therein (accepting the customary character of the definition and citing national military manuals and various compilations of international law applicable to armed conflicts).

[17] AP I (n 4) art 52(2) (emphasis added).

[18] Tallinn Manual (n 6) 125 (emphasis added).

[19] ibid 126 para 4 fn 81, citing 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* (International Committee of the Red Cross 1987) (ICRC Commentary), 633–34 paras 2007–08.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

remain outside the scope of IHL rules on targeting. The experts continued: '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'.[20] The experts did not explain what they considered to be the 'ordinary meaning' of the term 'object'. The only footnote in the whole paragraph leads to Article 31(1) of the Vienna Convention on the Law of Treaties[21] (VCLT) without further elaboration.[22] In particular, no mention is made of any of the other methods of interpretation enshrined in the VCLT.[23] A key consequence of this position is that a cyber operation targeting data would not fall within the ambit of IHL unless it were to affect the functionality of a control system resulting in the need to replace its physical components.[24]

The text, however, acknowledges the contrary position held by a 'minority' of the experts – namely that 'for the purposes of targeting, data per se should be regarded as an object'. This position is justified by the essentially teleological consideration that if data was *not* to be considered an object, the act of deletion of valuable civilian datasets would fall outside of the scope of application of IHL, thus contradicting the principle of protection of the civilian population from the effects of hostilities.[25] The relevant text concludes with a laconic observation that '[t]he majority characterised this position as *de lege ferenda*'.[26]

3. THE SIGNIFICANCE OF THE LACK OF STATE PRACTICE FOR THE DISTINCTION BETWEEN *LEX LATA* AND *LEX FERENDA*

The view promoted in this article aligns with the minority opinion among the international group of experts. It is therefore necessary to consider at this point the objection that, however desirable this interpretation might be, it would nonetheless be a position '*de lege ferenda*'.[27]

At first blush, such an objection might certainly appear formidable. In the methodological section of the study, the experts clearly confined the scope of the Tallinn Manual within the

[20] Tallinn Manual (n 6) 127 para 5 (footnote omitted).
[21] Vienna Convention on the Law of Treaties (entered into force 27 January 1980) 1155 UNTS 331 (VCLT), art 31(1) ('A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose').
[22] Tallinn Manual (n 6) 127 fn 82.
[23] See ibid 127 para 5. In addition to the textual method of interpretation, art 31 VCLT also endorses the contextual (or systematic) method, and the teleological (or functional) method. All three are applied to the present subject matter in Section 5 below. For a general discussion of the methods of interpretation embodied in art 31 see, eg, Mark E Villiger, *Commentary on the 1969 Vienna Convention on the Law of Treaties* (Martinus Nijhoff 2009) 425–41.
[24] Tallinn Manual (n 6) 108–09 para 10, 127 para 5; see also text at nn 161–169 below (considering the implications of this position).
[25] Tallinn Manual (n 6) 127 para 5; see also AP I (n 4) art 48; see further Section 5 of this article (construing the term 'object' in light of the object and purpose of AP I).
[26] Tallinn Manual (n 6) 127 para 5.
[27] cf ibid 127 para 5; see also Schmitt (n 1) 272 (admitting that in order for law to remain effective over time, it must be responsive to context, but emphasising the role played by the states in the process).

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

four corners of *lex lata*.[28] Furthermore, the chairman of the group of experts, Professor Michael Schmitt, has in his separate writing relevant to cyber conflict occasionally characterised views differing from the positions eventually embraced by the Manual as not representative of *lex lata*.[29] Both in Professor Schmitt's writing and in the methodology of the Manual, 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*.[30] It is submitted, however, that this is not an appropriate standard for the interpretation of international law.

The distinction between *lex lata* (law as it is) and *lex ferenda* (law as it ought to be) – borrowed from positivist legal theory and domestic law – sits uneasily in the unique horizontal legal framework of international law. To a much greater extent than municipal law, international law is characterised by uncertainty as to the existence, not just the interpretation, of many of its putative rules, including some of the most fundamental ones. Arguments as to their existence (dimension *lex lata*) often feature some elements of policy, desirability and progressiveness (dimension *lex ferenda*).[31]

By way of an example, we may consider the recent debate over the existence of a norm permitting humanitarian intervention in international law in respect of the ongoing Syrian conflict. Although such a norm cannot easily be deduced from the corpus of written treaty law,[32] the United Kingdom government issued a statement in August 2013 in which it seemed to consider this norm as part of customary international law.[33] It did not cite any state practice and many

[28] Tallinn Manual (n 6) 5 ('The Rules set forth in the Tallinn Manual accordingly reflect consensus among the Experts as to the applicable *lex lata*, that is, the law currently governing cyber conflict. It does not set forth *lex ferenda*, best practice, or preferred policy').

[29] See, eg, Michael N Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context Attack' (2012) *4th International Conference on Cyber Conflict* 283, 293 ('Admittedly, the conclusions reached in this article regarding the meaning of "attack" in international humanitarian law may seem unsatisfactory. Non-destructive attacks and those that do not place individuals or objects at physical risk can have severe consequences. Yet, the interpretation advanced in this article represents the extant law, that is, the *lex lata*. Assertions to the contrary are, in the author's estimation, merely *lex ferenda*') (italics in original); Michael N Schmitt, 'Cyber Operations and the *Jus in Bello*: Key Issues' in Raul A Pedrozo and Daria P Wollschlaeger (eds), *International Law Studies: Vol 87 – International Law and the Changing Character of War* (US Naval War College 2011) 104 ('Both approaches have merit, the former in its fidelity to received understandings of IHL, the latter in that it would respond to concerns that the traditional understanding is under-inclusive since it admits of highly disruptive cyber operations to which IHL would not apply. As it stands, though, the former represents *lex lata*, the latter *lex ferenda*') (italics in original).

[30] cf Tallinn Manual (n 6) 5–6 (stating that where relevant state practice and *opinio juris* were lacking, the experts were 'hesitant' to lay down the exact scope and application of a given principle of law vis-à-vis the novel situation in cyberspace); see also Schmitt (n 1) 295 (reporting, with regard to the closely related term 'attack', that the experts 'opined that, *there being no State practice on the issue*, the current law limits the term to physical harm caused to persons and tangible objects') (emphasis added).

[31] cf Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Oxford University Press 1995) 10 (stating that the understanding of international law as process put forward by the author makes the distinction between *lex lata* and *lex ferenda* less important).

[32] See, eg, Simon Chesterman, *Just War or Just Peace?: Humanitarian Intervention and International Law* (Oxford University Press 2002) 1.

[33] UK Government, 'Chemical Weapon Use by Syrian Regime: UK Government Legal Position', 29 August 2013, paras 2 and 4, https://www.gov.uk/government/publications/chemical-weapon-use-by-syrian-regime-uk-government-legal-position.

commentators were quick to point out that there was a lack of such practice at the time.[34] The UK's approach was evocative of the 1945 Truman Proclamation,[35] in which the United States famously put forward a claim known to be inconsistent with pre-existing international law with the aim of generating a *new* norm of customary international law[36] – the difference being, of course, that where the Truman-led US succeeded,[37] David Cameron's UK seems to have failed.[38]

However, irrespective of the final fate of the UK's proposition, it is interesting for our purposes to highlight what the British government *did* cite in place of the missing analysis of state practice. The UK, led by the aforementioned aim to persuade other states to ascribe to its view, included in its statement the contention that the intervention would 'alleviate the scale of the overwhelming humanitarian catastrophe in Syria'.[39] This was clearly a policy-based consideration which, if expressed in general terms, would amount to a proposition that non-consensual foreign military intervention that alleviates humanitarian disasters ought to be or is permitted by international law. Such an argument thus obviously inhabits the borderline area between *lex lata* and *lex ferenda*.[40] Indeed, one might interpret the allegedly noble purpose of the intervention as one of the requirements permitting it under the (putative) rule *lex lata*. Some have gone even further to argue that the legality of a military intervention would turn on a strategic assessment of its capacity to achieve the stated objective of improving the situation on the ground.[41] Be that as it may, this example serves to illustrate the close relationship between *lex lata* and *lex ferenda* in international law.[42]

However, it is important to bear in mind that the fact that the two dimensions do not exist in two watertight compartments does not mean that they have somehow collapsed into one single criterion of persuasiveness or have become irrelevant altogether. The aim here is rather to show that the lack of state practice in favour of one interpretation does not necessarily mean that an

[34] See, eg, Robert Booth, 'Syria: Legal Doubt Cast on British Government's Case for Intervention', *The Guardian*, 29 August 2013 ('[Dapo Akande] said there is "very little evidence of state support for this view. Indeed most states have explicitly rejected this view."').
[35] US, 'Proclamation with Respect to Natural Resources of the Subsoil and Sea Bed of the Continental Shelf', reproduced in (1946) 40 *American Journal of International Law Supplement* 45.
[36] Michael Byers, *Custom, Power and the Power of Rules: International Relations and Customary International Law* (Cambridge University Press 1999) 91.
[37] ibid 91.
[38] Nicholas Watt, Rowena Mason and Nick Hopkins, 'Blow to Cameron's authority as MPs Rule Out British Assault on Syria', *The Guardian*, 30 August 2013 (reporting that the UK Parliament voted against military engagement in Syria).
[39] UK Government (n 33) para 4.
[40] See Higgins (n 31) 10.
[41] Guglielmo Verdirame, 'The Law and Strategy of Humanitarian Intervention', *EJIL: Talk!*, 30 August 2013, http://www.ejiltalk.org/the-law-and-strategy-of-humanitarian-intervention ('The legal assessment of the intervention in Syria thus turns on a question that – in the first instance at least – strategists rather than lawyers are better placed to address: is there a military option that can improve conditions for people in Syria? Put in other terms: is there an achievable humanitarian purpose?').
[42] See Antonio Cassese and Joseph Weiler (eds), *Change and Stability in International Law-Making* (De Gruyter 1988) 66–92 (discussion of the relevance of the distinction between *lex lata* and *lex ferenda* in international law).

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

alternative interpretation should automatically prevail, as some of the writing referred to above might appear to suggest.[43]

After all, despite the unambiguously proclaimed aim to limit the scope of their scrutiny to *lex lata*,[44] even the experts arguably tread along both sides of the fuzzy line separating the two dimensions. Putting aside the notion at the centre of the present article (to which I will return shortly), we may pick another notion almost at random to demonstrate the flaw at the basis of this objection. Let us consider, for instance, the way in which the experts apply the criterion of minimum organisation to 'virtual' groups.

The Tallinn Manual discusses 'virtual' groups, or groups organised solely online, in a section concerned with the criteria for the existence of a non-international armed conflict.[45] Although the applicable treaty text, Common Article 3 of the Geneva Conventions, does not contain a specific bottom threshold, post-Cold War case law has identified two – today generally accepted – criteria of minimum intensity of hostilities and minimum organisation of the non-state conflict party.[46] The Manual also reflects and accepts this development.[47]

It then applies the criterion of 'minimum organisation' to 'virtual' groups, defined as those in which all relevant activities occur online.[48] The experts seemed reluctant to classify *any* cooperatively operating online group of individuals engaged in cyber attacks as an organised armed group for the purposes of IHL.[49] However, '[t]he majority of [experts] agreed that the failure of members of the group physically to meet does not alone preclude it from having the requisite degree of organisation'.[50] In other words, the majority of experts were willing to accept that a 'virtual' group could be an organised armed group under IHL (triggering the application of the law of non-international armed conflict).[51]

[43] See references in n 30 above and accompanying text.
[44] Tallinn Manual (n 6) 5.
[45] ibid 84 et seq, r 23 ('Characterization as non-international armed conflict').
[46] See ICTY, *Prosecutor v Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-AR72, Appeals Chamber, 2 October 1995, [70] ('[A non-international] armed conflict exists whenever there is ... *protracted* armed violence between governmental authorities and *organized* armed groups or between such groups within a State') (emphasis added), as applied in ICTY, *Prosecutor v Tadić*, Judgment, IT-94-1-T, Trial Chamber II, 7 May 1997, [562]; ICTY, *Prosecutor v Limaj, Bala and Musliu*, Judgment, IT-03-66-T, Trial Chamber II, 30 November 2005, [88]–[170]; ICTY, *Prosecutor v Haradinaj, Balaj and Brahimaj*, Judgment, IT-04-84-T, Trial Chamber I, 3 April 2008, [37]–[60] (especially at [49]: 'The criterion of protracted armed violence refers more to the *intensity* of the conflict rather than its duration') (emphasis added).
[47] Tallinn Manual (n 6) 84 para 1, 87 para 6.
[48] ibid 89 para 13.
[49] cf ibid 89 para 13 (discussing the spectrum of autonomy with regard to 'virtually' organised groups).
[50] ibid 89 para 13.
[51] ibid 89 para 13. See also ibid para 14 fn 50 and accompanying text (adding the proviso that – at least in Additional Protocol II conflicts – the group would need to have the means to implement IHL). It is noteworthy that Cordula Droege, who participated in the work of the expert group as the representative of the ICRC without a vote, reached a different conclusion. For her, the requirement of having the means to implement IHL is practically incapable of being fulfilled by a 'virtual' group. She thus concludes that such a group could not have the command and disciplinary structure necessary to constitute a party to the conflict: 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, 550–51.

The experts did not identify any state practice or *opinio juris* to bolster this interpretation. This is not surprising. After all, 'online' or 'virtual' groups engaged in cyber warfare are a novelty, which could not have been foreseen by the drafters of the Geneva Conventions in 1949 or even, in all likelihood, by the ICTY Appeals Chamber in 1995.[52] However, the absence of state practice, the likely basis of the rejection of the minority view regarding data as objects,[53] did not prove determinative in the analysis of the law applicable to 'virtual' groups.[54]

How then do we get out of this interpretative maze? The distinction between *lex lata* and *lex ferenda* is undoubtedly one worth maintaining. However, to equate 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. After all, subsequent practice of states in the application of a treaty is but one of the considerations to be taken into account in interpreting the treaty in question,[55] and its absence cannot conclusively prove one over all other possible interpretations.[56]

Technological progress by definition entails the emergence of novel concepts and categories, which are initially untied to any state practice or *opinio juris* regarding the interpretation of the concomitant legal issues. We should not substitute the dearth of state practice for proper treaty interpretation. Instead, we should assess the meaning of terms found in international treaties by reference to agreed methods of interpretation. This is what this article turns to in the remaining text.

4. ALTERNATIVE ROUTE: DATA IS NOT AN OBJECT, YET IT MAY BE A MILITARY OBJECTIVE

The experts have modified slightly the text of Article 52(2) of the Protocol without directly acknowledging so. The literal reading of the provision clearly permits the existence of military objectives which are objects, as well as those which are not. This is apparent from the limiting language at the beginning of the second sentence of the provision: '*In so far as objects are concerned*, military objectives are limited to ...'.[57] The highlighted part of the sentence allows for the existence of a class of things which are not objects, yet which should be considered military objectives. The Tallinn Manual, however, equates military objectives with objects.[58] The definition of military objectives it proposes in Rule 38 leaves out non-objects: 'Military objectives *are* those objects which ...'.[59]

[52] See n 46 above.
[53] See Tallinn Manual (n 6) 127 para 5.
[54] cf ibid 88–90 paras 11–15.
[55] See VCLT (n 21) art 31(3)(b).
[56] See further Villiger (n 23) 429–32.
[57] AP I (n 4) art 52(2), second sentence.
[58] Tallinn Manual (n 6) 126 para 3.
[59] ibid 125, r 38, second sentence.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

It thus appears possible to read data, as a matter of *lex lata,* into the undefined class of non-objects left out by the Manual, but clearly contained in Additional Protocol I. This option certainly has some superficial appeal. It would allow us to accept the requirement of visibility and tangibility in relation to 'objects' proposed by the experts. The rest of the analysis in the Manual would thus remain unaffected. Data would be intangible 'non-objects', yet potentially military objectives.

The problem with this 'alternative route' solution is twofold: (i) it is entirely inconsistent with the traditional understanding of the notion of military objectives, and (ii) it would lead to a number of further interpretive difficulties in specific situations. First, this solution undermines the traditional interpretation of the dichotomy of targets which constitute legitimate military objectives in IHL, namely persons and objects.[60] Within this understanding, Article 52(2) of the Protocol defines military objectives falling into the latter category and leaves it for its other provisions to define the former.[61] This is also how the vast majority of states interpret military objectives in their military manuals.[62]

Admittedly, for a few states, 'establishments' or 'places' form a third – ostensibly separate – category.[63] For example, the 1983 Belgian Law of War Manual categorises military objectives into '1) Persons … 2) Objects … 3) Places'.[64] Nevertheless, in spite of the different taxonomy, it would appear that this division is still consistent with the dichotomous structure of Article 52(2). 'Places' are simply a subcategory of 'objects' *largo sensu*, singled out for clarity. The Commentary by Bothe and his co-authors confirms this understanding by referring to the drafting history of Additional Protocol I: '[T]o make this interpretation unambiguously clear, several NATO countries expressed an understanding in their explanation of vote on Art. 52, that a specific *area of land* may be a military objective' if it fulfils the criteria specified in the provision

[60] See, eg, Michael Bothe, Karl Josef Partsch and Waldemar A Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff 1982) 277; ICRC Commentary (n 19) 635 para 2017; Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (2nd edn, Cambridge University Press 2010) 84–85; Gary D Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge University Press 2010) 519; see also Bothe, Partsch and Solf, ibid 285 fn 17 (attributing the reluctance on the part of the drafters to state clearly that persons may be targeted to the prevailing sentiment that doing so would not be appropriate in a humanitarian instrument). The structure of the Tallinn Manual also respects this dichotomy: Part 4 entitled 'Conduct of Hostilities' covers rules on attacks in a general section (Section 2, 'Attacks Generally'), two specific sections concerning 'Attacks against Persons' (Section 3) and 'Attacks against Objects' (Section 4), respectively: see Tallinn Manual (n 6) rr 30–40. See also text at nn 12–14 above.

[61] See, especially, AP I (n 4) arts 43 and 50, as well as Geneva Convention relative to the Treatment of Prisoners of War (entered into force 21 October 1950) 75 UNTS 135, art 4A, which distinguishes between persons who are combatants and the residual category of civilians.

[62] See ICRC, Customary IHL Database, 'Practice Relating to Rule 8: Definition of Military Objectives', section A. III, http://www.icrc.org/customary-ihl/eng/docs/v2_rul_rule8.

[63] See, eg, Belgium, *Droit Pénal et Disciplinaire Militaire et Droit de la Guerre, Deuxième Partie, Droit de la Guerre*, Ecole Royale Militaire, par J. Maes, Chargé de cours, Avocat-général près la Cour Militaire, D/1983/1187/029 (1983) 27; Benin, *Le Droit de la Guerre, III fascicules*, Forces Armées du Bénin, Ministère de la Défense Nationale (1995) Fascicule I, 12–13; Hungary, *A Hadijog, Jegyzet a Katonai, Föiskolák Hallgatói Részére*, Magyar Honvédség Szolnoki Repülötiszti Föiskola (1992) 18; Kenya, *Law of Armed Conflict, Military Basic Course (ORS)*, 4 Précis, The School of Military Police (1997) Précis No. 2, 11.

[64] Belgium, *Droit Pénal et Disciplinaire Militaire et Droit de la Guerre*, ibid 27.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

with respect to *objects*.[65] None of the other state parties objected to this interpretation, which means that we may safely assume that localities were to be considered a subclass of objects.[66] The persons–objects dichotomy, insofar as the construction of these provisions is concerned, thus appears to be correct.

This well-accepted and uncontroversial interpretation would, however, be turned upside down if data were held to belong in the 'non-object' category, until now populated only by living human beings.

Second, the 'alternative route' interpretation would consequently leave no valid criterion to assess whether a specific dataset would be a military objective. This is so because, in order to determine whether a specific object or a person is targetable in the specific circumstances, IHL sets out different legal criteria.

On the one hand, the rule for objects is spelt out in the second half of the second sentence of Article 52(2). This provision contains a two-pronged test, which requires that the *object* in question makes an effective contribution to military action and that its destruction, capture or neutralisation offers a definite military advantage.[67] Although this test is equally suitable in its application to data as it is to tangible objects (a point to which I return in the next section), it would not be available because of the interpretation of data as a *non*-object.

On the other hand, criteria which determine whether a certain person may permissibly be targeted in combat are, without hesitation, inapplicable to non-living things, whether tangible or not. It would be patently absurd to insist that the targetability of a certain dataset is assessed on the basis of its 'combatant status' or 'direct participation in hostilities'. It thus becomes clear that the association of data with other non-objects in the normative framework of the Protocol would lead to absurd results. Therefore, despite its initial appeal, the 'alternative route' solution must also be rejected.

5. PROPOSED VIEW: DATA IS AN OBJECT, *ERGO* IT MAY BE A MILITARY OBJECTIVE

The view advocated by this article is that, contrary to the conclusion reached by the experts drafting the Tallinn Manual, data may indeed be considered as an object within the meaning of Article 52(2) AP I. If this interpretation is correct, whether a particular dataset is a military objective would be considered by reference to the criteria in the second part of the second sentence of that provision.[68] In this section of the article, my aim is to expound the term 'object' in Article 52(2), using the generally accepted methods of treaty interpretation as codified in the VCLT.

[65] Bothe, Partsch and Solf (n 60) 307 (emphasis added).
[66] The understanding of areas of land as potential military objectives is shared by the Manual: see Tallinn Manual (n 6) 128 para 7. See, however, n 13 above (noting that the Manual, at least in some places, seemed to have excluded combatants from the scope of the notion of military objectives).
[67] AP I (n 4) art 52(2).
[68] See text at n 17 above for the full text of the provision.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

It is submitted that the ensuing analysis applies also, to a great extent, to the meaning of the term 'object' under customary international law. This is despite the obvious fact that *stricto sensu* the VCLT does not apply to norms of customary law.[69] The possibility that a norm exists in parallel in both treaty law and customary law is firmly established in international law.[70] Article 52(2) may safely be described as a 'fundamentally norm-creating' treaty rule of the kind that the ICJ considered in the *North Sea Continental Shelf* cases to be capable of evolving into custom.[71] Its parallel existence in customary and treaty law should thus not be in doubt.[72] It is true that the ICJ noted in *Nicaragua* that such rules, even if identical in treaty law and customary law, are nevertheless distinguishable, inter alia, by reference to the available methods of interpretation.[73] However, the differences should not be overstated. As Judge Tanaka observed in *North Sea*, '[t]he method of logical and teleological interpretation can be applied in the case of customary law as in the case of written law'.[74] As will be seen, the present analysis is in large part based precisely on these two shared methods of interpretation. Moreover, to the extent that this article relies on methods not available in respect of customary law (especially the contextual method insofar as it takes other treaty provisions into account), this should be seen as complementary in that it provides an additional reason in favour of the interpretation advocated here. In any event, this approach does not differ significantly from that undertaken by the authors of the Tallinn Manual. The experts, while describing the Article 52(2) definition as customary,[75] openly stated that they considered 'treaty law directly on point' when identifying the rules governing cyber conflict[76] and accepted that the VCLT rules on interpretation are pertinent to the analysis of the meaning of the term 'object' in international law.[77]

According to the 'general rule' of interpretation found in Article 31(1) VCLT, '[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose'. The question before us is whether the meaning of the term 'object' today extends to cover electronic data for the purposes of the definition of military objectives. Mark Villiger, the author of a detailed commentary on the VCLT, cautions that 'the various means mentioned in Article 31 are all of equal value; none are of an inferior character'.[78] Apart from the ordinary meaning of the term in question we must

[69] VCLT (n 21) art 1; see also Theodor Meron, 'The Continuing Role of Custom in the Formation of International Humanitarian Law' (1996) 90 *American Journal of International Law* 238, 246 (observing that the VCLT rules on treaty interpretation do not apply to customary law outside the treaty context).
[70] *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v US*) Merits [1986] ICJ Rep 14 (*Nicaragua*), [177]; see also VCLT (n 21) art 38.
[71] *North Sea Continental Shelf cases* (*Federal Republic of Germany v Netherlands and Denmark*) Merits [1969] ICJ Rep 3 (*North Sea*), [72].
[72] See also n 16 above (listing the authorities confirming the customary law status of the definition found in art 52(2) AP I (n 4)).
[73] *Nicaragua* (n 70) [178].
[74] *North Sea* (n 71) dissenting opinion of Judge Tanaka, [55].
[75] Tallinn Manual (n 6) 126 para 1.
[76] ibid 5.
[77] ibid 127 para 5 fn 82 (citing art 31(1) VCLT as authority for the proposition that '[d]ata is intangible and therefore [does not] fall within the "ordinary meaning" of the term object') (internal quotation marks retained).
[78] Villiger (n 23) 435.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

therefore examine, in particular, the context in which it appears and the object and purpose of the treaty.[79]

5.1. ORDINARY MEANING IN CONTEXT

As a starting point, let us recall that the authors of the Tallinn Manual based their refusal to characterise data as objects on the fact that an object must be, in their view, something 'visible and tangible'.[80] Although the Manual was completed in early 2013, these words were borrowed from the ICRC Commentary on the two Additional Protocols, published 26 years earlier.[81] Although the concept of electronic data was not unknown in 1987, it is not difficult to believe that the idea of cyber warfare did not cross the minds of the authors of the Commentary. After all, it was published two full years before Tim Berners-Lee invented the World Wide Web,[82] revolutionising the way in which information was exchanged online and laying the foundations of the modern day virtual world.

The discussion of military objectives in the ICRC Commentary was instead very much grounded in the reality of 'analog' warfare. In fact, the word 'computer' is mentioned in the Commentary only twice. First, the authors highlight (with barely concealed bewilderment) the then novel possibility of storing 'all provisions of international law applicable in case of armed conflict ... in the memory of a *computer*'.[83] Second, when discussing the requirements for identity cards under Annex I to Additional Protocol I, the authors refuse to accept that an electronic card (which could be produced, as they observe, thanks to '[c]urrent developments in *computer* information') could replace good old paper-based cards foreseen by the drafters of the Protocol.[84]

With these considerations in mind, could the authors of the Commentary then have intended to exclude data when they wrote that in order for something to be an object, it must be 'visible and tangible'? Surely not. In 1987 it was still much too soon to consider hostilities in cyberspace. So why did they include these words? 'Visible and tangible' – as opposed to what?

The authors of the Commentary provide the answer to that question only a few paragraphs below the text cited in the Tallinn Manual. They write, in relation to the term 'objective', that it is also supposed to mean 'tangible and visible things ... *and not the general objective (in the sense of aim or purpose) of a military operation*'.[85] The authors described objects and

[79] Although art 31(1) VCLT (n 21) requires in addition that the interpretation be conducted in good faith, this principle pertains primarily to the parties to the treaty, requiring them to act honestly, fairly and reasonably when they engage in treaty interpretation: Villiger (n 23) 425–26. It would thus not be appropriate to apply it to an independent academic undertaking of the present kind.
[80] Tallinn Manual (n 6) 127 para 5.
[81] ICRC Commentary (n 19) 634 para 2008.
[82] Tim Berners-Lee, 'Information Management: A Proposal', Internal Memo, CERN, March 1989, http://cds.cern.ch/record/1405411/files/ARCH-WWW-4-010.pdf.
[83] ICRC Commentary (n 19) 951 para 3347 fn 16 (emphasis added).
[84] ibid 1154 para 3970 (emphasis added).
[85] ibid 634 para 2010. The dichotomy is even more apparent in Marco Sassòli's entry on military objectives in the Max Planck Encyclopaedia of Public International Law: Marco Sassòli, 'Military Objectives' in Rüdiger Wolfrum

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

objectives as tangible to distinguish them from abstract notions such as the goals and aims of the parties to the conflict.[86] The reason behind this distinction is readily apparent. If a party's aim were to amount to a legitimate target justifying an attack by its opponent, the detailed and balanced rules on targeting would lose any sense.[87] Belligerents would gain a trump card if they wanted to pursue an attack against an object which would not meet the orthodox understanding: they could just claim they need to destroy it in order to neutralise the aim of the enemy.[88] Civilian infrastructure would thus become fair game through the back door of this too broad interpretation of the term 'objective'. However, it would be incorrect to read more into the ICRC Commentary.[89]

5.1.1. CONTEMPORANEITY

Since we cannot accept the interpretation of the term 'object' adopted by the ICRC Commentary for the purposes of our inquiry, we need to examine independently what its 'ordinary meaning' is. This raises a crucial inter-temporal aspect: is the question determined by the 'ordinary meaning' at the time of the adoption of the treaty, or may this meaning evolve over time?

If it is the former, the matter could be disposed of at this stage. If we have just accepted that the authors of the ICRC Commentary could not in 1987 have conceived of the potentiality that data would play a role in warfare, then even less could we presume that the drafters of the Protocol would have been capable of doing the same *ten years earlier*. Unfortunately, there is no provision in the VCLT that provides a simple answer. The only related draft article – Article 56 entitled 'The inter-temporal law' – was deleted from the VCLT during the *travaux préparatoires* stage.[90]

(ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2008) para 9 ('Only a material, tangible thing can be a military objective in the sense of a legitimate target for attacks. *Immaterial objectives, such as victory, or notional targets, such as civilian morale, cannot be attacked*, but only achieved or affected through attacking tangible things' (emphasis added)).

[86] cf Hague Rules of Air Warfare (drafted December 1922 – February 1923), art 24(1) (in this first definition of a military objective, the term used in place of an 'object' was, somewhat tautologically, 'objective', which may further explain the authors' need to distinguish objects from goals or aims).

[87] See also Sassòli (n 85) para 9 ('Contrary to World War II, it is today generally accepted that under existing law those things must be military objectives and that civilian objects may not be attacked for the purpose of shattering civilian morale').

[88] cf AP I (n 4) art 52(2) ('military objectives are limited to those objects ... whose total or partial destruction, capture or *neutralization*, in the circumstances ruling at the time, offers a definite military advantage' (emphasis added)).

[89] Accord Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 184–85; see also Dinniss (n 7) Section 2 (developing this point and providing further historical context).

[90] Philippe Sands and Jeffery Commission, 'Treaty, Custom and Time: Interpretation/Application?' in Malgosia Fitzmaurice, Olufemi Elias and Panos Merkouris (eds), *Treaty Interpretation and the Vienna Convention on the Law of Treaties: 30 Years On* (Martinus Nijhoff 2010) 41.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

The classic formulation of the former position comes from Judge Gerald Fitzmaurice. In his series of articles entitled 'The Law and Procedure of the International Court of Justice' he labelled it the principle of contemporaneity:[91]

> The terms of a treaty must be interpreted according to the meaning which they possessed, or which would have been attributed to them, and in the light of current linguistic usage, *at the time when the treaty was originally concluded*.

For Fitzmaurice, this principle derived from the rule that the rights of parties to a dispute, as they stood on a certain date, should be adjudged on the basis of the law as it was on that same date.[92] In relation to treaties, he added that 'it follows automatically' that a valid determination could be reached only on the basis of the contemporaneous meaning of the terms on the date on which the treaty was concluded.[93]

Although Fitzmaurice's position carried great weight at the time, it is submitted that it was already overbroad at the time of the writing and has since been superseded by the ensuing development of international legal practice. First, the principle of contemporaneity as proposed by Fitzmaurice was overbroad as it assumed, without any further analysis, that for any dispute on any point of law arising from a treaty, the appropriate reference point would be the state of law at the time of the conclusion of the treaty. This is patently not true for all conceivable situations. The original understanding of a treaty obligation may lose its meaning, become absurd or manifestly inapplicable with the passage of time, leading to the necessity to abandon the strict application of this principle in a given case. After all, earlier rulings departing from or ignoring this putative principle had already existed by the time of Fitzmaurice's writing in 1957.[94]

Second, whatever the status of the alleged principle was at that time, the following course of events undermined its claim to universal applicability. In spite of its endorsement by the International Law Commission's (ILC) Special Rapporteur on the law of treaties, Sir Humphrey Waldock, the principle was rejected by the ILC in 1964 and was not included in the final text

---

[91] Sir Gerald Fitzmaurice, 'The Law and Procedure of the International Court of Justice 1951–4: Treaty Interpretation and Other Treaty Points' (1957) 33 *British Year Book of International Law* 203, 212 (emphasis added).
[92] ibid 225.
[93] ibid 225.
[94] See, eg, *Maltass v Maltass* (1844) 1 Rob Ecc 67, 73, cited in Ian McTaggart Sinclair, 'The Principles of Treaty Interpretation and their Application by the English Courts' (1963) 12 *International and Comparative Law Quarterly* 508, 545 fn 28:

> If it be contended that, at the time of concluding the treaties, neither party thought of British subjects domiciled in Smyrna, that may perhaps be true, for little indeed was known or thought of domicile, in the legal sense of the term, in those early times; but if the words of the treaty are sufficient to cover the case, and if the object of the treaties was to apply to all British merchants, then the application to a state of circumstances not particularly contemplated, but within the general scope of the treaties, would not limit their construction.

It was suggested in later writing that in proposing the principle of contemporaneity, Fitzmaurice placed too much importance on Judge Huber's ruling in *Island of Palmas Arbitration* (1928) 2 RIAA 829, in which Huber was, however, analysing the acquisition of title to territory. In that context, the application of the principle of contemporaneity is more appropriate, but it is questionable whether it can be extrapolated as a general principle of treaty interpretation valid for all cases. See Campbell McLachlan, 'The Principle of Systemic Integration and Article 31(3)(c) of the Vienna Convention' (2005) 54 *International & Comparative Law Quarterly* 279, 289 fn 53.

of the VCLT.[95] Moreover, even the ICJ, from whose case law Fitzmaurice originally derived his principles of treaty interpretation,[96] did not subsequently apply the principle of contemporaneity without exception. In fact, in 1991, in one of a series of articles conceived as a continuation of Fitzmaurice's earlier work,[97] Hugh Thirlway concluded, again on the basis of examination of the ICJ jurisprudence, that the principle had been qualified in the following way:[98]

> Provided that, where it can be established that it was the intention of the parties that the meaning or scope of a term or expression used in the treaty should follow the development of the law, the treaty must be interpreted so as to give effect to that intention.

Returning to the subject of the present inquiry, how do we choose between Fitzmaurice's and Thirlway's understandings of contemporaneity? It is submitted that for three independent reasons, we ought to rely on this latter 'qualified' principle in interpreting the term 'object' in Article 52(2). The first reason relates to the nature of the Protocol and the term in question. As the ICJ held in the *Navigation Rights* case, if parties choose a generic term in a treaty entered into for a very long period, they should be presumed to have intended that such a term is to have an evolving meaning.[99] As we know, the Protocol is a treaty of indeterminate duration and the term in question is a generic one, supporting the use of evolutive interpretation.

Second, the object of the Protocol as a treaty providing for the protection of victims of armed conflicts[100] also supports resort to evolutive interpretation. The three most influential international human rights tribunals have established that human rights treaties are living instruments which must be interpreted in light of present day conditions.[101] It is submitted that when in doubt over whether to turn to the originalist or evolutive reading, the latter should be used with regard to multilateral treaties which are designed for the protection of individuals, a characteristic shared by the human rights treaties and the Protocol.[102]

---

[95] McLachlan, ibid 292; see further *Yearbook of the International Law Commission* 1964, vol I, 33–40 (recording the discussion of the draft Article 56 which had resulted in the rejection of the proposed text by the members of the ILC for fear that it 'might lead to misunderstanding').

[96] Fitzmaurice (n 91) 203.

[97] Hugh Thirlway, 'The Law and Procedure of the International Court of Justice 1960–1989: Part One' (1989) 60(1) *British Year Book of International Law* 1, 4.

[98] Hugh Thirlway, 'The Law and Procedure of the International Court of Justice 1960–1989: Part Three' (1991) 62(1) *British Year Book of International Law* 1, 57.

[99] *Dispute regarding Navigational and Related Rights* (*Costa Rica v Nicaragua*) Judgment [2009] ICJ Rep 213, [66] ('[W]here the parties have used generic terms in a treaty, the parties necessarily having been aware that the meaning of the terms was likely to evolve over time, and where the treaty has been entered into for a very long period or is "of continuing duration", the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning').

[100] See Section 5.2 below for a detailed analysis of the object and purpose of AP I in respect of the analysed provision.

[101] *Tyrer v United Kingdom* (1978) 2 EHRR 1, para 31; *The Right to Information on Consular Assistance in the Framework of the Guarantees of the Due Process of Law* (1999) Inter-Am Ct HR, Advisory Opinion of 1 October 1999, (Ser A) No 16, [114]; UN Human Rights Committee, *Roger Judge v Canada*, Communication No 829/1998, UN Doc CCPR/C/78/D/829/1998 (2003), para 10.3.

[102] cf *The Right to Information on Consular Assistance*, ibid [114] ('international human rights law ... has made great headway thanks to an evolutive interpretation of *international instruments of protection*') (emphasis added);

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

Third, terms of the Additional Protocol have been anything but immune to the evolutive approach so far. A number of other terms found in the Protocol have been interpreted in light of the circumstances prevalent at the time of their application. For instance, in the *Nuclear Weapons* advisory opinion, the ICJ emphasised the importance of the so-called Martens Clause enshrined in Article 1 of the Protocol[103] as means of addressing what the Court called 'the rapid evolution of military technology'.[104] It has been correctly observed that the merit of this passage in the opinion was to embrace a dynamic approach to IHL in general.[105]

As a further example, in the *Targeted Killing* case, the Israeli Supreme Court was faced with the question of when a civilian is taking a direct part in hostilities and thus loses his or her protection from attack under Article 51(3) of the Protocol. The Court unequivocally embraced an evolutive interpretation of that provision, reasoning that if the reality changes, the interpretation of previously developed rules must also evolve.[106] Although this decision has been the subject of a considerable degree of criticism, the application of the evolutive method of interpretation to the terms of Additional Protocol I has not raised specific objections.[107]

5.1.2. MODERN MEANING

It is submitted that we should interpret the term 'object' in Article 52(2) in light of present day conditions. In this respect, we may be assisted by the other authentic language versions of the Protocol[108] as well as by a closer examination of the modern reality relevant to the present subject.

First, there is a striking discrepancy dividing the six authentic language versions of Additional Protocol I into two groups. English, along with Arabic, Chinese, and Russian, are in the first

see also Stephane Jacquement, 'The Cross-Fertilization of International Humanitarian Law and International Refugee Law' (2001) 83 *International Review of the Red Cross* 651, 658 (arguing that human rights *or* the humanitarian nature of a treaty necessitates a more dynamic approach to interpretation).

[103] AP I (n 4) art 1(2) ('In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from dictates of public conscience').

[104] *Nuclear Weapons* (n 3) [78].

[105] Vincent Chetail, 'The Contribution of the International Court of Justice to International Humanitarian Law' (2003) 85 *International Review of the Red Cross* 235, 259.

[106] 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 ('[N]ew 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') (emphasis added).

[107] cf Orna Ben-Naftali and Keren Michaeli, 'Public Committee Against Torture in Israel v. Government of Israel. Case No. HCJ 769/02' (2007) 101 *American Journal of International Law* 459, 465 (criticising the *result* to which the use of evolutive interpretation had led the court, but accepting its *applicability* within the framework of AP I); see further Meagan S Wong, 'Targeted Killings and the International Legal Framework: with Particular Reference to the US Operation against Osama Bin Laden' (2012) 11 *Chinese Journal of International Law* 127, 149–51 (demonstrating that the Court's use of evolutive interpretation brought about a result that may be seen as merging the protection under IHL and under human rights law).

[108] See VCLT (n 21) art 33.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

group. These four languages use the generic word 'object' to express the term in question: 'object' in English, 'بالأعيان' in Arabic,[109] '物体' in Chinese[110] and '*объект*' in Russian.[111] However, the second group of languages, made up of French and Spanish, use a different word. Here, the word used is '*un bien*' in both French[112] and Spanish[113] (plural '*les biens*' and '*los bienes*', respectively), which translates into English literally as 'a good' or 'a property'.[114] We may put the first group aside as the words used are identical and do not shed further light on one another.

However, as far as the word '*bien*' is used, in particular in francophone legal literature, it is immediately notable that it is not limited to objects which have a physical presence in the 'real world'. On the contrary, the term '*bien*' is specifically divided in several French-speaking jurisdictions into tangible and intangible (corporeal and incorporeal) sub-categories.[115] In a different context, the majority of experts insisted that '*sensu stricto*, data does *not* qualify as property'.[116] This view was not, however, supported by any citation and it was followed by an express rejection by the minority.[117]

It is important to add that our aim here is not to transplant terms from domestic law into international law without paying due regard to their context. The fact that '*un bien*' may also conceivably exist in an intangible form is mentioned solely in order to shed more light on the meaning of the word 'object' in the English version of the Protocol.[118]

Second, I turn to the question of whether present day reality has evolved with an effect on the ordinary meaning of the term 'object'. In order to do this properly, we must not examine the term in abstract but in the context of the Protocol as such.[119] I have already stated that the remainder of the sentence in which the term 'objects' finds itself rules out the abstract meaning of the word in the sense of a goal or a purpose.[120]

---

[109] AP I (n 4) art 52(2), Arabic version, http://www1.umn.edu/humanrts/arab/b094.html.
[110] AP I (n 4) art 52(2), Chinese version, http://www.icrc.org/chi/resources/documents/misc/additional_protocol_1.htm.
[111] AP I (n 4) art 52(2), Russian version, http://www1.umn.edu/humanrts/russian/instree/Ry5pagc.html.
[112] AP I (n 4) art 52(2), French version, http://www1.umn.edu/humanrts/instree/french/y5pagcf.htm.
[113] AP I (n 4) art 52(2), Spanish version, http://www1.umn.edu/humanrts/instree/Sgenevaconvprotocol1.html.
[114] See, eg, 'bien', *Grand Dictionnaire Hachette-Oxford* (4th edn, Oxford University Press 2007) 92.
[115] See, eg, Canada, Code Civil du Québec, art 899 ('Les biens, *tant corporels qu'incorporels*, se divisent en immeubles et meubles') (in French) (emphasis added). I am grateful to Adam Mauntah and Jessica Joly for drawing my attention to this example.
[116] Tallinn Manual (n 6) 245 para 3 (emphasis added) (discussing the nature of data in the context of r 90 concerning the confiscation and requisition of property under the law of occupation).
[117] ibid ('A minority of the Experts was of the view that data *can* qualify as property') (emphasis added).
[118] cf VCLT (n 21) art 23(1) ('When a treaty has been authenticated in two or more languages, *the text is equally authoritative in each language*, unless the treaty provides or the parties agree that, in case of divergence, a particular text shall prevail') (emphasis added), and art 23(3) ('The terms of the treaty are presumed to have *the same meaning* in each authentic text') (emphasis added).
[119] Villiger (n 23) 426 ('the ordinary meaning of a term is not to be determined in the abstract but in the context of the treaty').
[120] See text at nn 85–89 above.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

The examined term appears in Section I of Part IV of the Protocol. Although the section is labelled 'General Protection against Effects of Hostilities', it also sets out the key rules on targeting during international armed conflicts.[121] The understanding of the term 'object' throughout this section generally means something that may become the target of attacks.[122] It must thus be something susceptible to 'destruction, capture or neutralization'.[123]

It is submitted that data fits this description. Even though the Tallinn Manual itself does not consider this issue further, the chairman of the group of experts has raised two different cogent objections in his writing in defence of the view found in the Manual. I will address them in turn. First, Professor Schmitt has argued that destruction of data without direct physical consequences is more akin to psychological operations, which fall outside of the scope of the rules on targeting in Additional Protocol I.[124] Second, he has claimed that if all data were treated as an object, states would have to forfeit their ability to conduct some operations with an effect on civilians. According to this argument, states would therefore not accept such a limitation.[125]

As to the first point, is computer data analogous to abstract notions such as population morale or to 'tangible' things such as a bridge? While morale may be *affected* by attacks, it is a subjective category the existence or extent of which cannot be objectively *determined*. A bridge, on the other hand, either remains unscathed, is damaged, or is no more. Its existence and condition does not depend on subjective assessment or belief.

Computer data, as generally understood today, is more akin to the latter. According to the Oxford English Dictionary, in the realm of computing data means 'the quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media'.[126] It is true that at a certain point it might be difficult to determine whether a particular dataset has been tampered with from the outside, as the attacker may conceal his or her traces. For example, although various organisations within Iran were targeted by the Stuxnet virus as early as June 2009, its existence was only discovered 13 months later.[127] However, this difficulty does not mean that the potential alteration or destruction of data in question is categorically indeterminable. Similarly, a bridge located in a place that is too remote for a belligerent to determine its current state, or even its existence, would not become a non-object for the purposes of Article 52(2) of the Protocol.

In a recent article, Noam Lubell also rejects the analogy between cyber and psychological operations, although he arrives at the same conclusion on the basis of a different line of

[121] See generally Bothe, Partsch and Solf (n 60) 274–80.
[122] ibid 285 ('So far as the term "military objectives" pertains to objects ... [a]s used in Section I of Part IV, it generally means the target of attacks').
[123] AP I (n 4) art 52(2).
[124] Schmitt (2011) (n 29) 92–96.
[125] Schmitt (n 1) 298.
[126] 'Data', Oxford English Dictionary, http://www.oxforddictionaries.com/definition/american_english/data.
[127] Symantec, 'W32.Stuxnet Dossier, version 1.4', February 2011, 2 and 7, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; ESET, 'Stuxnet under the Microscope', revision 1.31 (undated), 19, http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

argument, focusing on the notion of attack rather than object.[128] He emphasises that the nature of psychological operations is to convince and not to harm, whereas cyber operations will inevitably cause some form of harm, which may in some cases cross the threshold of attack.[129]

The present analysis is in agreement with Lubell's conclusion. However, it bears emphasising that, unlike Lubell, I am not concerned here with the required intensity of harm, only with the eligibility of certain types of object to be harmed at all. Not all types of interference with data would amount to harm in this sense: for instance, misappropriation or misuse of data might not, whereas its deletion or alteration most probably would. Nevertheless, because data is susceptible to destruction and this destruction would be objectively verifiable – even if at times, admittedly, with some or significant evidentiary difficulty – the analogy with psychological operations must be rejected at this point.[130]

The second objection relates to the supposed unwillingness on the part of states to accept the definition of data proposed here on the ground of it being overbroad. Professor Schmitt has argued that treating data as an object would mean that states would no longer be able to engage in cyber activities that have effects on the civilian population.[131] His earlier writing may provide some guidance as to the kind of activities he had in mind: 'It would appear overbroad to characterize 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'.[132] Although under a certain set of circumstances this might be the correct conclusion, it is submitted that the premise of the argument is flawed.

For greater clarity, let us consider instead the example of the 'innocuous e-mail', but in relation to an equally innocuous *letter*, one written on paper and sealed in an envelope rather than

[128] Noam Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' (2012) 89 *International Law Studies* 252, 260 ff; see also AP I (n 4) art 49 and Tallinn Manual (n 6) 106, r 30.
[129] Lubell, ibid 263–64.
[130] See also ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', October 2011, 36, http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-102-en.pdf (defining 'cyber operations' as 'operations against or via a computer or a computer system through a data stream [with the aim] to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system'); US Joint Chiefs of Staff, 'Information Operations', Joint Publication 3–13,13 February 2006, GL-5, http://www.information-retrieval.info/docs/jp3_13.pdf (defining 'computer network attack' as '[a]ctions taken through the use of computer networks to disrupt, deny, degrade, *or destroy* information resident in computers and computer networks, or the computers and networks themselves') (emphasis added). These references confirm that both the NGO tasked with the guardianship of IHL and the leading state in the area of cyber warfare adopt the same view of computer data as an object susceptible to destruction by cyber operations as that embraced in the present article. It should be noted that the definition has since been revoked in the new version of the US joint publication. However, press reports following the release of classified documents by the whistleblower, Edward Snowden, indicate that the same conception of offensive cyber operations was integrated in a US presidential directive: see further US Joint Chiefs of Staff, 'Information Operations', Joint Publication 3–13, 27 November 2012, GL-3, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (confirming the removal of the definition of 'computer network attack'); Barton Gellman and Ellen Nakashima, 'U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show', *Washington Post*, 30 August 2013 (reporting a presidential directive issued in October 2012, which defines 'offensive cyber-operations as activities intended "to manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves"').
[131] Schmitt (n 1) 298.
[132] Schmitt (2011) (n 29) 96.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

stored as computer data. As the (somewhat loaded) qualifying adjective 'innocuous' suggests, the letter's destruction per se would indeed probably not be lawful under IHL. This would, however, not be the consequence of the letter not being an *object*. Rather, its destruction would probably be unlawful as the letter would not be a *military objective* in that it fails to meet the criteria in Article 52(2) – namely the dual consideration of whether it makes an effective contribution to the military action of one conflict party and whether its destruction would offer a definite military advantage for the other.

It is, however, unlikely that states would, within the scope of an armed conflict,[133] engage in a military operation the sole aim of which would be to destroy one civilian letter (or one such email). Such an outcome would in virtually all conceivable situations be the consequence of a larger operation targeting, say, the post office building overtaken by the military forces of the enemy. In this case, if an attack on the post office-cum-military outpost occasioned the destruction of letters stored in the building, their destruction might nevertheless be lawful by the operation of the rule of proportionality. On this basis, an attack may be expected to cause incidental damage to civilian objects and yet be lawful as long as this damage is not excessive in relation to the concrete and direct military advantage anticipated.[134] The same considerations would apply to the electronic equivalent of the innocuous civilian letter. Admittedly, its destruction in isolation would most probably fail to meet the criteria of lawfulness under IHL. However, as long as it is an incidental effect of an otherwise lawful military operation compliant with the principle of proportionality, the fact that the email was deleted would not amount to an unlawful attack.[135]

The extant architecture of IHL thus appears to be satisfactory and should not diverge from the expectations of states. Their capacity to engage in cyber operations occasioning the destruction of data, as long as those operations complied with the applicable rules of IHL, would remain unimpeded. Moreover, as stated above, psychological operations (whether 'cyber' or not in nature) would remain beyond the reach of IHL. In sum, it is hoped that this analysis serves to alleviate, to some extent, the concern that states would not be willing to accept the interpretation proposed here.

5.1.3. NORMATIVE CONTEXT

What remains to be assessed at this point is the correlation of the proposed interpretation with the normative framework of which the interpreted provision forms a part – in other words, the broader context surrounding the term 'object'. Do the provisions of Section I of Part IV of the Protocol presume that an 'attack' against an object would have to entail the use of physical or kinetic force, rendering the proposed interpretation meaningless?[136] Professor Schmitt has persuasively shown that even though the definition of 'attack' in Article 49 of the Protocol is

[133] Otherwise IHL would not apply at all.
[134] AP I (n 4) arts 51(5)(b), 57(2)(a)(ii), 57(2)(b); ICRC Study (n 4) r 14.
[135] See further Dinniss (n 89) 185–93 (detailing how the fulfilment of these conditions may be assessed with regard to objects understood in the sense advocated in this article).
[136] cf ICRC Commentary (n 19) 603 para 1880 ('the term "attack" means "combat action"'); Bothe, Partsch and Solf (n 60) 289 ('[t]he term "acts of violence" denotes physical force').

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

'instrumentality-based', the rest of the section takes a 'consequence-based' approach when operationalising the term.[137] In other words, even though attacks were originally defined as 'acts of violence' in the Protocol, they can, '[t]hrough the process of induction',[138] 'be redefined as operations that result in, or if unsuccessful were originally expected to result in, death or injury of individuals or destruction or damage of objects'.[139] The use of physical force is not a *sine qua non* of an attack under the terms of the Protocol. Further, and here I part ways with Professor Schmitt's interpretation, cyber operations that aim to destroy data fit this consequence-based approach. Let us consider two examples to shed more light on this proposition.

First, an attack of this sort may target critical data of a military nature, such as weapons logs,[140] timetables for the deployment of military logistics[141] or air traffic control information.[142] Their destruction would not entail the use of physical force and yet it would fit the dual considerations of Article 52(2). Such data makes an effective contribution to the military action of one party; in fact, its military action would be inextricably bound to and based on this particular dataset. Its destruction would, therefore, also offer a definite military advantage to the opposing party. In this example, data is a legitimate military objective; it is submitted that it would probably also be accepted as such by states.

Second, an attack might target essentially civilian data such as electronic health records held at a particular hospital. If this data were to be clandestinely erased or altered, the lives and health of patients in the hospital would be endangered.[143] This data does not, of course, meet the criteria of a military objective; its destruction would rather affect the integrity of a civilian object (the data itself) and the safety of the civilian population (the patients in the hospital). The Commentary by Bothe and his co-authors extrapolates these two considerations as attributes of 'attacks' bringing them within the scope of the Protocol.[144]

---

[137] Schmitt (2012) (n 29) 291.

[138] In light of the same author's prescription regarding the need for state practice and *opinio juris* to support a novel interpretation (see n 29 above), it is somewhat surprising that here this method of induction is seen as satisfactory without any state practice and/or *opinio juris* being advanced in favour of the proposed redefinition. Nonetheless, the present writer agrees with the tenor of the argument in Schmitt's piece; in fact, it could be argued that it shows that an interpretation may be convincing even in the face of the lack of corresponding state practice.

[139] Schmitt (2012) (n 29) 291.

[140] cf *McKinnon v Government of the USA* (n 2) Lord Brown of Eaton-under-Heywood, [13] (summarising that the appellant in the case allegedly deleted logs from computers at US Naval Weapons Station Earle, which had contained data on identity, location, physical condition, staffing and battle readiness of US Navy ships).

[141] Herbert Lin, 'Cyber Conflict and International Humanitarian Law' (2012) 886 *International Review of the Red Cross* 515, 519.

[142] 'Military Blamed after Planes Vanish from Europe Air-Traffic Control Screens', *The Guardian*, 13 June 2014 (reporting the claim of the Slovak authorities that an 'electronic warfare exercise' run by NATO caused dozens of aircrafts to disappear from the air-traffic control radar system).

[143] David Francis, 'The Coming Cyber Attack that Could Ruin Your Life', *The Fiscal Times*, 11 March 2013 (warning that changed data may be deadly when doctors prescribe unnecessary drugs or order irrelevant procedures on its basis).

[144] Bothe, Partsch and Solf (n 60) 288 ('[the term "attacks"] applies to those aspects of military operations which most directly affect *the safety of the civilian population* and *the integrity of civilian objects*') (emphases added), cited with approval in Schmitt (2012) (n 29) 291 fn 36.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

Both of these examples share the fact that the direct consequence of the attacks considered would be solely the destruction of data. For the Tallinn Manual, such attacks would normally fall outside the scope of IHL[145] unless, in addition, they were to interfere with the functionality of the control system to an extent requiring the replacement of physical components.[146] However, in neither of the examples considered would such interference be necessary or even useful to achieve the aims of the attacker. Still, as we have seen, assessing such attacks would entail making determinations expressed in the Protocol's rules on targeting. It is therefore submitted that, taking present day conditions into consideration, the proposed interpretation of data as an object better fits the context of the interpreted provision.

5.2. OBJECT AND PURPOSE

Finally, we need to examine the possible interpretations of the term 'object' with regard to the object and purpose of Additional Protocol I. Not only is the recourse to teleological interpretation mandated by the VCLT, but its importance is further underlined by the fact that the Protocol is a multilateral treaty of humanitarian import. For treaties of this nature, examining the object and purpose is particularly important and may even prevail over the intentions of the parties.[147]

Teleological interpretation is also an available method of interpretation with respect to customary norms.[148] It is submitted that the *telos* of a treaty rule of a norm-creating character carries over into customary international law in the event of its evolution into custom.[149] In addition, the analysis of the object and purpose of the Protocol 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.[150] According to the accepted rules of treaty-making, such states are bound to refrain from acts that would undermine the object and purpose of the treaty in question.[151]

Although a treaty may have several objects and purposes,[152] it would hardly be doubted that one of the main ones if not *the* object and purpose of Additional Protocol I is to improve the

[145] The experts, apparently aware of some of the undesirable consequences of this position, built in a patchwork of solutions for the protection of some ostensibly civilian uses of data. With respect to the above-mentioned example of personal medical records, r 71 prohibits the making of medical data 'the object of attack'. This is an apparent contradiction with the interpretation of data as a non-object, interference with which is not considered an attack for the purposes of IHL. The Manual seems to tacitly acknowledge as much but it just states pragmatically (and without any further explanation or citation) that '[p]ersonal 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*': see Tallinn Manual (n 6) 206 (emphasis added). The outcome is to be commended, but the process of reasoning used is, unfortunately, strained and self-contradictory.

[146] See Tallinn Manual, ibid 108–09 para 10.

[147] Villiger (n 23) 427–28.

[148] *North Sea* (n 71) dissenting opinion of Judge Tanaka, [55]; see also text at nn 73–77 above.

[149] See text at n 71 above (asserting that art 52(2) AP I (n 4) is such a rule).

[150] Other signatories are Iran and Pakistan, http://www.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesSign&xp_treatySelected=470.

[151] VCLT (n 21) art 18.

[152] Villiger (n 23) 427.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

protection of victims of armed conflicts over and above that provided by the four Geneva Conventions: the title of the Protocol states that it relates 'to the Protection of Victims of International Armed Conflicts'.[153] Its Preamble refers to the goal of enhancing the protection as something the state parties considered necessary.[154] The ICRC Commentary states expressly that this was the object and purpose of the Protocol[155] and the same position has been taken for granted by academia[156] and international jurisprudence.[157]

The rules in Part IV of Additional Protocol I focus specifically on civilians as a subcategory of victims of armed conflicts.[158] We may thus infer that the object and purpose of Article 52(2) and its normative context is the enhancement of the protection of civilians during situations of armed conflict.[159] Of the two potential interpretations, we must thus choose the one which better serves the identified object and purpose of the Protocol.[160]

The interpretation propounded in the Tallinn Manual removes data from the scope of IHL unless its destruction entails the loss of functionality of physical infrastructure (computers and networks) carrying the data in question.[161] In addition, the experts only considered an interference with functionality to qualify as damage if restoration of functionality requires replacement of physical components.[162] What this means is that many targets whose physical equivalents are firmly protected by IHL from enemy combat action would be considered fair game as long as the effects of the attack remain confined to cyberspace. This is, unfortunately, not just a fanciful comment without any real support in the field. Cordula Droege sums up the literature which puts forward the view that the availability of cyber operations expands the list of legitimate targets as even attacks on objects which are prohibited in the physical world might now be considered legal.[163]

---

[153] AP I (n 4) title ('Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)').

[154] AP I (n 4) Preamble, para 3 ('Believing it necessary ... to reaffirm and develop the provisions protecting the victims of armed conflicts and to supplement measures intended to reinforce their application').

[155] ICRC Commentary (n 19) 1064 para 3685 ('[It] may be hoped for ... that the possibility of making reservations will facilitate the universal acceptance of the Protocol without adversely affecting *its object and purpose*, which *is to improve the protection provided by the Conventions to the victims of international armed conflicts*') (emphasis added).

[156] See, eg, Elmar Rauch, *The Protocol Additional to the Geneva Conventions for the Protection of Victims of International Armed Conflicts and the United Nations Convention on the Law of the Sea* (Duncker & Humblot 1984) 58; Joakim Dungel and Shannon Ghadiri, 'The Temporal Scope of Command Responsibility Revisited: Why Commanders Have a Duty to Prevent Crimes Committed after the Cessation of Effective Control' (2010) 17(1) *UC Davis Journal of International Law & Policy* 1, 17.

[157] See, eg, ICTY, *Prosecutor v Blagojević and Jokić*, Judgment, IT-02-60-A, Appeals Chamber, 9 May 2007, [281]; ICTY, *Prosecutor v Orić*, Judgment, IT-03-68-A, Appeals Chamber, 3 July 2008, [19].

[158] See AP I (n 4) title of Part IV ('Civilian Population').

[159] See also Frits Kalshoven, 'Bombardment: From "Brussels 1874" to "Sarajevo 2003"' in Frits Kalshoven (ed), *Reflections on the Law of War* (Martinus Nijhoff 2007) 448; Frits Kalshoven, 'Belligerent Reprisals Revisited' in Kalshoven, ibid 777 ('general protection of the civilian population ... is one of the major "objects and purposes" of the Protocol').

[160] VCLT (n 21) art 31(1); see further Villiger (n 23) 427–28.

[161] Tallinn Manual (n 6) 127 para 5.

[162] ibid 108–09 para 10.

[163] Droege (n 51) 561 and references in fns 89–92.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press

For illustration, let us consider the real-world example of the attack on the official Twitter account of Associated Press in April 2013. A group of Syrian hackers known as the Syrian Electronic Army published a fake tweet announcing explosions in the White House and injury to the US President. The effects were immediate and momentous: the Dow Jones Industrial Average index of the New York Stock Exchange dropped with the effect of erasing $136 billion of equity market value.[164] It should be highlighted that all of this occurred without any effect on physical objects, whether the servers of Twitter or the stock exchange, or the internet infrastructure carrying the data in question. Although the consequences of this particular attack were short-lived, it highlights the extent of damage that can be caused by means of cyber operations. Any such large-scale damage to civilian property in the physical world would certainly not escape the regulatory reach of IHL. Many other hypothetical examples of this kind abound.[165]

The interpretation of data as non-object would thus greatly expand the class of permissible targets in warfare. It is submitted that this expansion would go against the object and purpose of Additional Protocol I as it would expose the civilian population to additional danger instead of providing it with protection. The general principle of IHL that the right of belligerents to adopt means of injuring the enemy is not unlimited[166] further supports a restrictive interpretation of the notion of military objectives.[167] Because anything[168] that is not an object cannot qualify as a military objective, we should therefore interpret the term 'object' broadly in order to achieve the aim underlying the rules on targeting. Accordingly, data should, also on the analysis of the object and purpose of the Protocol, be considered an 'object' in this context.[169]

This interpretation has the additional benefit of providing clarity as to the identification of permissible military targets in cyber warfare. For example, bringing down a website used solely for military purposes would clearly qualify as an attack on a military objective under IHL. The Tallinn Manual recognises that such a cyberspace-confined object, using the example of 'a website passing coded messages to resistance forces behind enemy lines', would be making an effective contribution to military action.[170] However, because of its approach, it is forced to maintain a

[164] Fisher (n 2).
[165] See, eg, Schmitt (n 1) 297 (highlighting the importance of digital records for the functioning of modern-day governments with regard to census taking, the provision of social benefits, voting and taxation).
[166] See 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; Respect for Human Rights in Armed Conflicts, UNGA Res 2444 (XXIII), 19 December 1968, UN Doc A/7433 (1968), para 1(a); see also AP I (n 4) art 35(1) (restating the principle using a slightly different formulation). In his seminal work on the law of targeting, Professor Boothby describes this principle as 'one of the most fundamental customary principles of the law of armed conflict': William H Boothby, *The Law of Targeting* (Oxford University Press 2012) 58.
[167] cf ICRC Commentary (n 19) 404 para 1418 (noting that the distinction between military objectives and civilian objects in art 52(2) AP I (n 4) serves 'precisely' the goal of preventing unnecessary suffering).
[168] The use of the word 'any*thing*' is deliberate here as persons may certainly qualify as military objectives: see text at nn 60–62 above.
[169] See also Tallinn Manual (n 6) 127 para 5 (rejecting the position of the minority of experts according to whom the view of the majority contradicts the principle of protection of the civilian population from the effects of hostilities as it makes IHL inapplicable to acts of deletion of valuable civilian datasets).
[170] ibid 130 para 13.

strained reasoning that the military objective in this case would not be the website itself, but 'the cyber *infrastructure supporting the website*'.[171] This is entirely counter-intuitive and without correspondence in reality, where any attempt to bring the website down would be likely to take the form of a denial-of-service attack and would certainly not have any consequences in physical space, and even less would it demand the replacement of physical components.[172]

6. CONCLUSION

To interpret the law without due regard to the changes in reality is to risk its reduction into irrelevance. The Tallinn Manual is therefore a very valuable contribution to the interpretation of international law with regard to the novel challenges posed by cyber warfare. Nevertheless, it is the contention of this article that in one narrow aspect the Manual has not succeeded in this aim.

This article has put forward the view that, in spite of the dearth of state practice on the matter, the concept of military objectives in IHL should properly be construed to include computer data. It has been argued that data is an 'object' for the purposes of the IHL rules on targeting. The interpretation proposed by this article is openly evolutive in character. This is, however, the rule rather than an exception in this area.

After all, the 1982 Commentary by Bothe and his co-authors had already observed with a degree of foresight that 'in the dynamic circumstances of armed conflict, objects which may have been military objectives yesterday may no longer be such today *and vice versa*'.[173] This prediction has been confirmed repeatedly since the Commentary was published – for example, although back in 1982 drones belonged to the realm of science-fiction,[174] today they are considered to be standard military objectives.[175]

The rapid development of information technology in the decades following the adoption of Additional Protocol I has entailed an unprecedented challenge for IHL. Both civilian life and military operations depend to a growing degree on information and activities confined to cyberspace, with little to no ramifications in the physical world. If the law of armed conflict is to retain its relevance, it ought to reflect this change. That is why, it is submitted, in 2015 computer data are objects under international humanitarian law.

[171] ibid (emphasis added).
[172] cf ibid 108–09 para 10 (stating that the majority view among the experts was that a cyber operation would qualify as an attack only if it interfered with the functionality of an object to the extent that its restoration would require the replacement of physical components); see also text at nn 161–163 above.
[173] Bothe, Partsch and Solf (n 60) 326 (emphasis added).
[174] See, eg, Frank Herbert, *The Great Dune Trilogy* (Gollancz 1979) 64–65 (describing the 'hunter-seeker', a floating remote-controlled device used to kill the target by injection of a lethal poison).
[175] Humanitarian Policy and Conflict Research, 'Manual on International Law Applicable to Air and Missile Warfare', Bern, 15 May 2009, r 22(a), http://ihlresearch.org/amw/HPCR%20Manual.pdf.

https://doi.org/10.1017/S0021223714000260 Published online by Cambridge University Press