MÜHF-HAD Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi • Cilt 27, Sayı 2, Aralık 2021, ISSN: 2529-0142, ss. 1298-1313 • DOI:10.33433/maruhad.994306

ARAŞTIRMA MAKALESİ
RESEARCH ARTICLE

Changing Notion Of Object And Targeting Data Under The Law Of Armed Conflict

Değişen Nesne Kavramı Ve Silahlı Çatışma Hukukunda Verilerin Hedef Alınması

Yunus Emre Gül*

ABSTRACT

The notion of an object is changing by being taken small steps. Although, there is an ambiguity whether 'data' is an object or not under the law of armed conflict, the qualification of it will be discussed from different perspectives in this article. While the lex lata position does not accept data as an object by the impact of textual interpretation, the lex ferenda position approaches differently and regards data as an 'object' by taking teleological interpretation into consideration. As a last point of view, it will be demonstrated that state practice seems to progress towards the latter approach by giving examples from official documents prepared by states and international organisations. At this point, it will be demonstrated in this article that data is not an object, but it evolves towards being accepted as an object.
Keywords: Data, the notion of object, law of armed conflict, state practice.

ÖZ

Nesne kavramı, küçük adımlar atılarak değişmektedir. Her ne kadar Silahlı Çatışma Hukuku kapsamında 'veri'nin nesne olup olmadığı üzerinde bir belirsizlik olsa da söz konusu terimin niteliği farklı perspektiflerden bu makalede tartışılacaktır. Olan hukuku (lex lata) temel alan bakış açısı lafzi yorum metodunun etkisiyle 'veri'yi nesne olarak kabul etmezken olması gereken hukuku (lex ferenda) temel alan bakış açısı farklı bir şekilde yaklaşmakta ve teleolojik yorum metodunu dikkate alarak 'veri'yi nesne olarak kabul etmektedir. Son bir bakış açısı olarak, devletler ve uluslararası kuruluşlar tarafından hazırlanan resmî belgelerden örnekler verilerek, devlet uygulamasının ikinci yaklaşıma doğru ilerlediği gösterilecektir. Bu noktada, bu makalede verinin nesne olduğu değil, nesne olarak kabul edilmeye doğru evrildiği ispatlanacaktır.
Anahtar Kelimeler: Veri, nesne kavramı, silahlı çatışma hukuku, devlet uygulaması.

* Ph.D. Candidate at the University of Bonn Department of Law, ORCID: 0000-0002-8701-2236.

Sorumlu Yazar/Correspondence Author: Yunus Emre Gül
E-posta/E-mail: yunus.gul@uni-bonn.de
Geliş Tarihi/Received: 12.09.2021 **Kabul Tarihi/Accepted:** 22.11.2021

INTRODUCTION

In the 21st century, human beings have become more technology-reliant than ever. Although it brings many benefits, it cannot be denied that there are many drawbacks too. One of them is that people store almost all of their information in their computers as 'data', which can be defined as 'the basic element that can be processed or produced by a computer to convey information'.[1] Nevertheless, data is not under the protection of the law of armed conflict (LOAC) when current state practices are taken into account.

There are two prominent opinions in today's LOAC regarding data. While one approach does not accept data as an object by focusing on textual interpretation, another school of thought acknowledges its status as an object by taking teleological interpretation into account. At this point, although it is not a binding document, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (the 'Tallinn Manual') which is prepared by the International Group of Experts (the 'Experts') represents a good example in which two prominent approaches present their arguments in order to support their positions. While the majority of the Experts did not accept data as an 'object' since its 'ordinary meaning' necessitates being 'tangible' and 'visible',[2] the minority adopted the different notion and regarded data as an 'object' by focusing on the protection of civilians. [3] In this regard, while the former position accepts targeting and deleting GPS data as an 'attack' if it occurs tangible consequences such as 'death, injury, damage, destruction', according to the latter position, mere deletion of it suffices to accept it as an 'attack' even if there are not any physical effects. Even though the former position is accepted as *lex lata*, the latter position still is regarded as *lex ferenda* since state practices favour the former position today.[4]

The importance of the discussion is related to the application of the principle of distinction while conducting cyber operations against data. If data is not accepted as an object, almost all civilian data becomes vulnerable to cyber operations. For example, it is stated in the fourth report prepared by Duncan Hollis regarding practices of American States on cyber operations that there is no member of Organization of American States (OAS) who 'took the position that civilian data is directly subject to the principle of distinction in armed conflict'.[5] Nonetheless, only some of them such as Chile and Guyana takes the effects of cyber operations targeting data into consideration, and bans those operations which result in harmful consequences against the civilian population without touching upon the status of data in the LOAC.[6]

1 Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) Glossary p.564.

2 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC 1987) para 2008.

3 Schmitt, *Tallinn Manual* (n 2) rule 100 cmt. para. 6-7.

4 Michael N Schmitt, 'The Notion of "Objects" during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision' (2015) 48 Israel Law Review 81, 84; Michael N Schmitt, 'The Law of Cyber Warfare: Quo Vadis' (2014) 25 Stan. L. & Pol'y Rev. 269, 296.

5 Duncan B. Hollis, *International Law and State Cyber Operations: Improving Transparency*, OEA/Ser.Q, CJI/doc 603/20 (5 March 2020), p. 16.

6 Ibid.

On the other hand, both *lex lata* and *lex ferenda* positions have their own drawbacks. When data is not accepted as an object, the position becomes underinclusive since data is at the center of civilian life in the modern world. However, the contrary position is overinclusive, since it converts lawful actions in international law such as cyber espionage into unlawful acts. Therefore, there is no clear-cut answer to the status of data today. In line with this, after questioning those two stances, the present author further introduces that some recent developments strengthen the *lex ferenda* position despite the continuing prevalence of the present *lex lata*.

1. FROM THE PERSPECTIVE OF LEX LATA

Whilst some traces can be found in 1907 Hague Regulations about military objective,[7] it is properly defined in 1923 Hague Aerial Warfare Rules as 'an objective whereof the total or partial destruction would constitute an obvious military advantage for the belligerent'.[8] However its first binding regulation was accomplished by Additional Protocol I to the Geneva Conventions (1977).[9] While civilian objects are defined as those objects which 'are not military objectives' in article 52(1) of the AP – I, the second paragraph of the article defines military objectives as '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'.[10] Hence, there are two criteria in order to regard an objective as 'military'; an effective contribution and a military advantage.

Nature of object 'comprises all objects directly used by the armed forces'.[11] In other words, it reflects the fundamental character of the object.[12] Also, another type of object may make an effective contribution to military action due to its location. [13] This type of object is a lawful target because of having 'special importance to military operations'.[14] When it comes to the purpose criterion, it is related to the 'intended future use of an object'.[15] It takes 'the enemy's intent' into consideration, and if there is reliable information that the intended use of the object is to serve military aims, then

7 *See* Hague Convention IX of 1907 Concerning Bombardment by Naval Forces in Time of War Article 2.

8 Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare (December 1922 – February 1923) art 24(1).

9 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (hereinafter 'AP-I').

10 AP-I art 52(2).

11 Sandoz, Swinarski and Zimmermann (n 3) para 2020.

12 HPCR Manual on International Law Applicable to Air and Missile Warfare (Bern, 15 May 2009) art. 22(a) (hereinafter 'HPCR Manual')

13 Sandoz, Swinarski and Zimmermann (n 3) para 2021.

14 *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare* (Program on Humanitarian Policy and Conflict Research at Harvard University 2010) 107.

15 Sandoz, Swinarski and Zimmermann (n 3) para 2022.

the object will be deemed a lawful target.[16] Use is related to the present function of the object.[17] All these criteria have a common ground which is to be an 'object' in order to be qualified as a military objective.

In the Official Commentary on Additional Protocols prepared by the International Committee of the Red Cross (ICRC), an object is defined as '*something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing*' by giving reference to Oxford Dictionary which dates back to 1970.[18] Though the technology was not at today's level at that time, and functions of computers were much more inferior, 'data' was not accepted as an 'object' by the majority of the Experts since it '*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 1987 Commentary*'.[19] Thus, from their perspective, the 'ordinary meaning' of an object necessitates a relationship with something that is 'tangible' and 'visible'.[20] Although it can be claimed that own wording of the AP – I does not establish any rule in terms of interpreting 'object' limited to tangible things, it also does not state anything in terms of disregarding intangible things within the meaning of military objective too, and from this perspective, every intangible thing can be ruled as an 'object' and the definition may change according to every interpreter. [21] In this respect, it is important to determine state practices in order to avoid uncertainty. Nevertheless, state practices neither render 'data' as an 'object' nor regard mere deletion or alteration of data as 'attack'. [22]

Whilst data cannot be accepted as an 'object' *per se*, if cyber operations against data result in violent consequences, then they may perfectly fall within the ambit of 'attack'. At this point, it is important to clarify the difference between cyber operation and cyber attack. While the former can be defined as 'the employment of cyber capabilities to achieve objectives in or through cyberspace',[23] the latter is 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[24] For this reason, a cyber operation should reach a certain level of violence in order to be defined as a cyber attack such as damage or destruction to objects. Accordingly, if 'data' is not accepted as an object, then merely targeting it will never reach that level even if large amounts of data are deleted or destroyed.

Even though the majority of the Experts do not recognize data as an 'object', most members of this position admit that 'a cyber operation targeting data may sometimes qualify as an attack when the

16 *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare* (n 15) 107.

17 Sandoz, Swinarski and Zimmermann (n 3) para 2022.

18 ibid 2007.

19 Schmitt, *Tallinn Manual* (n 2) Rule 100 Cmt. para.6.

20 Sandoz, Swinarski and Zimmermann (n 3) para 2008.

21 Elizabeth Mavropoulou, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' (2015) 4 Journal of Law & Cyber Warfare 23, 49.

22 Schmitt, *Tallinn Manual* (n 1) Rule 83 Cmt. para.8; Heather A. Harrison Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives' (2015) 48 Israel Law Review 39, 42.

23 Schmitt, *Tallinn Manual* (n 2) Glossary 564.

24 ibid Rule 92.

operation affects the functionality of cyber infrastructure or results in other consequences that would qualify the cyber operation in question as an attack', whereas some of them still do not accept even if the operation affects the functionality of the infrastructure.[25] However, the interference with the functionality should result in the 'replacement of physical components' in order to fall ambit of an attack.[26] Although 'other consequences' are not clarified in the Manual, they still do not include non-tangible results, since they refer to objects which are under special protection.[27] Thus, it is important to occur violent consequences in the physical world to accept cyber operation as an attack. Lubell criticizes the stance of the majority since the replacement can be done in an hour but incapacitating a system may continue for days without giving any physical harm.[28] However, he still seems to agree with the majority while arguing the difference between cyber operation and cyber attack and calling those 'designed to damage data' as 'cyber operations'.[29]

Conducting an operation against data which affects the functionality of cyber infrastructure may reach the level of attack, but it still does not open a door for interpreting data as an object since the 'object of attack' is the functionality of this system, not data per se.[30] Hence, cyber operations that solely have an impact on 'data' are not prohibited under the LOAC. Nevertheless, they should not be regarded as completely lawful because they may fall in the ambit of other branches of International Law, and be regarded as illegal. As stated by the International Court of Justice,

> '*There can be no doubt that, as a general rule, a particular act may be perfectly lawful under one body of legal rules and unlawful under another. Thus it cannot be excluded in principle that an act carried out during an armed conflict and lawful under international humanitarian law can at the same time constitute a violation by the State in question of some other international obligation incumbent upon it.*' [31]

Therefore, it is always possible that these operations may be unlawful under human rights law or jus ad bellum.

25 ibid Rule 100 Cmt. para.6.

26 ibid Rule 92 Cmt. para.10.

27 Tim McCormack, 'International Humanitarian Law and the Targeting of Data' (2018) 94 International Law Studies 222, 226.

28 Noam Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' (2013) 89 International Law Studies 252, 266.

29 ibid 259.

30 Schmitt, 'The Notion of "Objects" during Cyber Operations' (n 5) 104–105.

31 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v. Serbia) (Judgment)* [2015] ICJ Rep para. 474.

2. FROM THE PERSPECTIVE OF LEX FERENDA

Treating 'data' as an 'object' was defended by two prominent scholars in the doctrine; Kubo Macak[32] and Heather Harrison Dinniss[33]. However, while Macak accepts all data as a new way of understanding of 'object', Dinniss makes differentiation and only accepts 'operational data' to fit into this category. The difference between them is that the 'destruction of operational-level data or code will result in loss of functionality of the system, whereas similar destruction of content-level data will leave the system intact, albeit with corrupted or missing data'.[34] Even though they have different understanding on that issue, both of those writers emphasize that the Commentary had been prepared even before the world wide web was invented, and they try to expand the notion of an object by teleological interpretation.[35] Additionally, they argue that the Commentary did not include 'intangible' things into the notion of an object since the concern was related to the targeting civilian morale and 'the general objective (in the sense of aim or purpose) of a military operation'.[36] However, the beginning of the sentence in the Commentary is that 'there is however no doubt that in this article both the English and French texts intended tangible and visible things by the word "objective"'.[37] Thus, there is no uncertainty about the intent of authors: a thing should be 'tangible' and 'visible' in order to be deemed as an 'object'.

According to the minority position in Tallinn Manual, some data which 'is "essential" to the well-being of the civilian population' should be regarded as an 'object' by considering the possible significant consequences of targeting them.[38] In line with this minority position, ICRC states in its challenge report that

> '*Moreover, data have become an essential component of the digital domain and a cornerstone of life in many societies. However, different views exist on whether civilian data should be considered as civilian objects and therefore be protected under IHL principles and rules governing the conduct of hostilities. In the ICRC's view, the conclusion that deleting or tampering with essential civilian data would not be prohibited by IHL in today's ever more data-reliant world seems difficult to reconcile with the object and purpose of this body of law. Put simply, the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them*'.[39]

32 Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 Israel Law Review 55.

33 Dinniss (n 23).

34 ibid 41–42.

35 ibid 43; Mačák (n 33) 67. Also see Ido Kilovaty, 'Virtual Violence-Disruptive Cyberspace Operations as Attacks under International Humanitarian Law' (2016) 23 Mich. Telecomm. & Tech. L. Rev. 113, 141.

36 Dinniss (n 23) 44; Mačák (n 33) 68 n.87; Lubell (n 29) 268; Sandoz, Swinarski and Zimmermann (n 3) para 2010. Also see Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, 'Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' [2020] International Review of the Red Cross 1, 32.

37 Sandoz, Swinarski and Zimmermann (n 3) para 2010.

38 Schmitt, *Tallinn Manual* (n 2) Rule 100 Cmt. para.6.

39 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts'

From the perspective of the present author, the traces of ICRC position could be followed back to the Commentary in which it was advised to military legal advisers to do appropriate documentation, [40] and, was noted that 'in some armies all provisions of international law applicable in case of armed conflict have been stored in the memory of a computer. A staff which has a terminal can thus instantly find all legal provisions applicable to a given problem'.[41] Even if the Commentary was prepared in 1987, the authors did not see any difference between documentation as a hard copy or storing in the computer as data. Lubell emphasizes this point by arguing that

> '*The reference to "visible and tangible" is not part of the Protocol definition, but rather the understanding given to it at a particular point in time and in a specific context. These must be examined more closely to see whether the same reasoning applies to our current situation. At the time of drafting it is unlikely that the drafters would have considered the possibility of data destruction separate from physical damage. Destroying data at the time would have meant physically damaging the storage method, such as the paper files. Today, however, it is perfectly possible to destroy vast quantities of vital data without physically destroying the computers on which they are stored. To place this in context, it raises the question whether a kinetic attack that results in the setting on fire of five hundred mailbags is any more harmful than a cyber operation that permanently deletes five million e-mails. This is a scenario that could hardly have been contemplated when the Commentary made the reference to objects being "visible and tangible." Looking beyond this specific phrase into the explanation surrounding its use further reveals why it might not exclude data*.'[42]

Liivoja&McCormack approach this issue in a similar manner by explaining that

> '*Permanent destruction of data can have significant ramifications, even though falling short of physical violence. For example, wiping out the data in the entire State's banking system or patent database by means of a computer virus may have far more deleterious consequences than the physical destruction of a single data centre. Yet, under the Manual, the former would be an attack only if it can be demonstrated that some physical injury occurred, whereas the second is undoubtedly an attack*.'[43]

Although authors of the Commentary were aware of technological developments, it is stated that

(ICRC2019)21<https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf?fbclid=IwAR3ksX7qBnQd61yJFgKqYlAhRKF3VPh9sFFhIZaQB2hNzxqAhksEjJJ83HM>. Also *see* Daragh Murray, *Practitioners' Guide to Human Rights Law in Armed Conflict* (Oxford University Press 2016) 307–308.

40 Sandoz, Swinarski and Zimmermann (n 3) para 3347.

41 ibid 3347 note 16.

42 Lubell (n 29) 267.

43 Rain Liivoja and Tim McCormack, 'Law in the Virtual Battlespace: The Tallin Manual and the Jus in Bello', *Yearbook of International Humanitarian Law*, vol 15 (Springer 2014) 53.

> '*Current developments in computer information processing systems make it possible to produce very small identity cards for military use ("electronic dog tags"). Neither this type of identity card, nor the type used for bank cards or to restrict access to high-security areas, nor again the type of identity card which is based on biometric techniques, can replace the identity card provided for in the Conventions and the Protocol, 3 which can be manufactured without recourse to sophisticated techniques and contains information comprehensible to everybody, everywhere.*'[44]

Hence, they did not accept to replace 'identity card' with electronic means despite the fact that they were ready to accept renovations. These dilemmas make it harder to guess the way of interpretation of authors and apply it to present conditions.

By referring to Schmitt's consequence-based approach, which regards an operation as an 'attack' by taking its severe consequences into consideration, Macak presents two examples in order to treat data as an object.[45] First, military critical data which makes an effective contribution to the enemy's war-fighting capacity is a legitimate target from the perspective of states. Second, targeting and deleting essential civilian data may adversely affect the well-being of the civilian population. Dinniss approaches this issue from a different standpoint. According to her, some cyber weapons may cause severe consequences, and if they are not accepted as an object since they are 'made entirely from code', there is a danger not accepting these cyber weapons as legitimate military objectives.[46] Also, she argues that it is more sensible to target military data in a dual-use system by accepting is as an 'object' rather than conducting an attack against the whole system by considering the minimization of civilian harm.[47] Although the argumentation is different, they both try to reach a conclusion that targeting data may have significant effects in today's world, and it is more appropriate to interpret 'object' by comprising data. [48]

On the other hand, two issues should be clarified. First, it is important not to legitimize the argument by confusing the principle of distinction and proportionality or precautions. After the object is determined as a 'lawful target', the latter will come into the scene. Therefore, the initial step is to determine whether the objective is a lawful target or not. The significance of this determination is that if the data is deemed as an object at the first step, then deleting (destroying) or altering (damaging) it will fall within the ambit of attack.[49] At this point it will be prohibited because civilian objects may not be the subject to attack according to article 51 of the AP – I, however, if it is not accepted as an object in the first step, then mere deletion or alteration of it does not fall within the prohibition. Dinniss's point already accepts it as an attack, and it becomes easier to accept 'data' as an object while making argumentation by starting from the last point. However, the problem starts at the first step in

44 ibid 3970.

45 Mačák (n 33) 76.

46 Dinniss (n 23) 44–45.

47 ibid 51.

48 Mačák (n 33) 77; Dinniss (n 23) 45.

49 Schmitt, 'The Notion of "Objects" during Cyber Operations' (n 5) 96.

order to qualify data as an object. Therefore, if it is not accepted as an 'object', it does not make any sense to comment on neither proportionality nor precautions.[50]

Secondly, not accepting data as an object does not exclude it from the ambit of targetable military objectives. If data contributes war-fighting or war-supporting capability of an enemy, then it will be accepted as a lawful target. This can be seen in Peru's response to Improving Transparency Project in which it was proposed to regard certain types of data as military objectives.[51] Moreover, according to the long-established but debatable practice of the USA, if it also contributes to the war-sustaining capability of a belligerent party, it may be rendered as a lawful target too since

> '*[C]yber operations against an enemy's financial system could directly impede its ability to sustain the conflict. Indeed, they likely would do so with greater effect than kinetic or cyber attacks on oil or other resources that indirectly provide the war effort's economic foundation*'.[52]

However, this position is not generally adhered by scholars since destroying war-sustaining objects is too remote in terms of adversely affecting the military action of the enemy.[53] Whilst the general position does not regard war-sustaining objects as a lawful target, the situation becomes too problematic when it comes targeting the financial assets of terrorist organizations.[54] However, there is no doubt that everything which makes an effective contribution to the military capacity of an enemy can be subject to an attack.

While both Dinniss' and Macak's arguments try to indicate that even if non-physical consequences of cyber operations against data may have severe effects on society, the missing point is that severity of foreseeable consequences already determines an operation as 'attack'.[55] When a cyber operation that targets data results in (or at least foresees) a certain level of violence, it will be qualified as a cyber attack.[56] Also, the Manual does not exclude every operation which does not have kinetic consequences. For instance, there are some instances where kinetic consequences do not occur but the operation can be determined as an attack such as chemical and biological attacks or cyber operations

50 Jeffrey Biller and Michael N Schmitt, 'Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare' (2019) 95 International Law Studies 179, 181–182.

51 Duncan B. Hollis, *International Law and State Cyber Operations: Improving Transparency*, OEA/Ser.Q, CJI/doc 615/20 (7 August 2020), pp. 27-28.

52 Michael Schmitt and Tim Mauer, 'Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?' (*Just Security*) <https://www.justsecurity.org/44411/protecting-financial-data-cyberspace-precedent-progress-cyber-norms/> accessed 4 April 2020.

53 Schmitt, *Tallinn Manual* (n 2) Rule 100 Cmt. para.18-19.

54 Kenneth Watkin, 'Sustaining the War Effort: Targeting Islamic State Oil Facilities' (*Just Security*) <https://www.justsecurity.org/15890/sustaining-war-effort-targeting-islamic-state-oil-facilities/> accessed 4 April 2020; Daphné Richemond-Barak, 'Is Money a Legitimate Target?' (*Just Security*) <https://www.justsecurity.org/29255/money-legitimate-target/> accessed 4 April 2020; Charlie Dunlap, 'The Loyola Conference and the Evolving Definition of Military Objective' (*Lawfire*) <https://sites.duke.edu/lawfire/2016/02/14/the-loyola-conference-and-the-evolving-definition-of-military-objective/> accessed 4 April 2020.

55 Schmitt, 'The Notion of "Objects" during Cyber Operations' 98.

56 Schmitt, *Tallinn Manual* (n 2) Rule 92 Cmt. para.6.

that cause severe mental suffering.[57] Hence, if the consequences of the operation is severe enough, it is already accepted as a cyber attack and subject to the LOAC. Moreover, if a cyber operation is designed to give rise to a certain level of violence, it is enough to accept it as an 'attack' even if it does not give rise to any violence. Therefore, it is not true to assume that all operations which do not result in physical consequences, cannot be regarded as attack. However, accepting an operation as 'attack' does not automatically render the target as an 'object'.

Actually, there is just one consequence of not accepting data as an 'object' which is that there is no illegality to target civilian data by cyber operations in terms of mere deletion or alteration since directing operations against civilian persons or objects are regarded as legitimate under the LOAC.[58] Nevertheless, if the door is opened in terms of rendering non-physical consequences within the ambit of LOAC, it may be possible to finish the argument by stating that 'any inconvenience to civilians is prohibited'.[59]

On the other hand, it should be noted that a cyber operation against data may be subject to the LOAC if it is part of a whole attack. For example, a cyber operation may be conducted by an adverse party in order to collect information about the system and prepare an attack that will come after it. In this vein, the attack will be evaluated as a whole, and an operation which represents the beginning of the attack will be subject to the LOAC.[60] Even though the situation is the same for those cyber operations that disrupt or neutralize the system, some academicians accept these results as an 'attack'. According to Dormann, article 52(2) of AP – I regards not only destruction but also neutralization of the object in terms of gaining the military advantage, so a cyber operation that neutralizes the military objective can be accepted as a cyber attack.[61] Nonetheless, the problem in Dormann's definition is that if an adverse party intends to conduct a cyber attack resulted in violent consequences, then it will be important to evaluate whether the objective is military or not. [62] Furthermore, the term 'military objective' is not only used in the AP – I in the context of attacks, but also discussed in article 48 and 51(7) of the Protocol in a broader context by referring all types of military operations. [63] Droege looks from a different perspective and states that if a cyber operation which disrupts 'the functioning of objects without physical damage or destruction, even if the disruption is temporary' should be

57 ibid Rule 92 Cmt. para.8; Michael N Schmitt and Chad E Highfill, 'Invisible Injuries: Concussive Effects and International Humanitarian Law' (2018) 9 Harvard National Security Journal 72; Michael N Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (IEEE 2012) 290.

58 US Department of Defence, *Law of War Manual* (2015) 1022; McCormack (n 28) 238; Michael N Schmitt, 'Wired Warfare: Computer Network Attack and Jus in Bello' (2002) 84 International Review of the Red Cross 365, 395.

59 Lubell (n 29) 262.

60 Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 131–132.

61 Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks' 6 <https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf> accessed 3 April 2020. In his last article written together with Laurent Gisel and Tilman Rodenhäuser, his position continued to be defended. See Gisel, Rodenhäuser and Dörmann (n 37) 27. Also see Robin Geiss, 'The Conduct of Hostilities in and via Cyberspace', *Proceedings of the ASIL Annual Meeting* (Cambridge University Press 2010) 373.

62 Michael N Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 International Law Studies 89, 95.

63 Dinniss (n 60) 198.

regarded as an 'attack' since, *inter alia*, there is no difference whether making a civilian object useless by giving it physical damage or not.[64] Although this broader understanding seems sensible when there are some instances in which there is no difference for an attacker to gain the same advantage either by neutralizing or disrupting rather than attacking to military object, the weakness of the argument is that not every cyber operation which contributes to the military position of the belligerent party may be qualified as an attack. [65] Therefore, the determination should be based on whether the intention of the perpetrator is to conduct an attack or operation. Also, such positions seem to be over-inclusive when state practices are considered since those operations which do not have physical consequences by disruption or interference are not prohibited in the LOAC.[66]

3. A STEP FORWARD TOWARD AN EVOLVING LEX FERENDA

On the other side of the coin, some important developments happened. While it is not clearly stated that data is an object, the *lex ferenda* position has started to find its place in statements of states with regards to cyberspace. For instance, while declaring its position on cyberspace,

> '*a deliberate offensive or malicious action carried out via cyberspace and intended to cause damage (in terms of availability, integrity or confidentiality) to data or the systems that treat them, which may consequently harm the activities for which they are the medium*'

is regarded as cyber attack by France.[67] Before this definition was announced, the importance of 'the confidentiality, availability, and integrity of data' was also stated in the US Department of Defence Cyber Strategy without clearing the stance on what are the consequences of having an impact by cyber operations on such kind of data.[68] The uniqueness of the French perspective is that it does not matter whether conducting an operation against data has an impact on the functionality of the system or not in order to accept it as a cyber attack, if the operation affects 'availability, integrity or confidentiality' of data, and emerges that 'the targeted equipment or systems no longer provide the service for which they were implemented'.[69] Even if there is no clear understanding on accepting data as an object, the statement clearly goes beyond the *lex lata* because of not requiring physical consequences and accepting civilian data as 'protected objects' though it is intangible.[70]

64 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, 558–559. Also see Dieter Fleck, 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual' (2013) 18 Journal of Conflict and Security Law 331, 341; Kilovaty (n 36).

65 William H Boothby, *The Law of Targeting* (Oxford University Press 2012) 383.

66 US Department of Defence (n 58) 1022; Schmitt, '"Attack" as a Term of Art in International Law' (n 57) 289; Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (n 62) 95.

67 Ministère des Armées, 'International Law Applied to Operations in Cyberspace' 13, 18 <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf> accessed 4 April 2020.

68 'The Department of Defense Cyber Strategy' (The Department of Defense 2015) 1. (hereinafter 'DOD Cyber Strategy')

69 Ministère des Armées (n 67) 13.

70 ibid 15; UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications

In addition to France's statement, the approach of Australian Government is not limited to those operations which result in violent consequences while accepting cyber operation as an attack. In their cyber engagement strategy, cyber attack is defined as

> '*a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity*'.[71]

In this respect, it can be argued that there is not any clear reference to data unlike France's approach, and the definition still requires an effect that reaches some level of threshold in order to accept an act as a cyber attack. However, putting 'information' into definition may be held as an indication of accepting those operations which occur non-kinetical results as an attack. In the same vein, this approach is also adopted by Germany who defined cyber attacks as 'an act or action initiated in or through cyberspace to cause harmful effects on communication, information or other electronic systems, on the information that is stored, processed or transmitted on these systems or on physical objects or persons' in its very recent position paper on the application of international law in cyber space.[72] Therefore, it seems rational to define an attack by considering non-kinetical threat and broaden it by comprising non-kinetical results. The same approach can also be found in the DOD Cyber Strategy which calls not only destructive but also disruptive and manipulative acts as a cyber attack.[73] Hence, when all these documents are taken into account, it seems possible that the definition of a cyber attack will be broadened in the future, and this broader approach will end with accepting data as an 'object'.

As the last point, it is worth mentioning that Carnegie Endowment for International Peace has presented recently the idea of protecting the integrity of financial data by taking aspirations from two documents which are the 2015 United Nationals General Assembly Resolution and the G20 Summit Communiqué. While the former recommends states taking measures including 'a repository of national laws and policies for the protection of data',[74] the latter encourages G20 States to 'promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT'.[75] By considering these documents, it was proposed to the G20 States that 'a State must

in the Context of International Security' UN Doc A/74/120 (24 June 2019), p.23; Michael Schmitt, 'France's Major Statement on International Law and Cyber: An Assessment' (*Just Security*, 16 September 2019) <https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/> accessed 4 April 2020.

71 'International Security & Cyberspace – Australia's International Cyber Engagement Strategy' <https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/part_4_international_security_and_cyberspace.html> accessed 21 April 2020.

72 Germany, 'On the Application of International Law in Cyberspace' 8, <https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 19 March 2021.

73 'The Department of Defense Cyber Strategy' (n 63) 2, 7, 9. However, there is no consistency in the document since cyber attacks are also used by considering their significant consequences as similar to the Tallinn Manual. *See* ibid 5, 6, 14.

74 UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/70/174 (22 July 2015) para.16(d)(i).

75 'G20 Finance Communiqué' (18 March 2017) <http://www.g20.utoronto.ca/2017/170318-finance-en.html> accessed 4

not conduct or knowingly support any activity that intentionally manipulates the integrity of financial institutions' data and algorithms wherever they are stored or when in transit'.[76] The logical background of this proposal, in which the manipulation of the data integrity of financial institutions is prohibited by using the analogy of counterfeiting currency, is related to the devastating effects of such an incident on the global economy due to the fact that the results of conducting cyber operations against such data cannot be limited by boundaries unlike other sectors such as oil and gas, and even if only one financial institution is targetted, the chain of events may end with the global shock in the entire international system.[77] Although the proposal was not adhered by any state explicitly, and opinio juris has not changed in terms of treating any kind of data as an 'object', it is an important milestone that indicates a need to change because of the data dependency of the world economic system. International law always make a progress according to the necessities of states, and it is quite possible that the issue will be held completely different in the future.

CONCLUSION

Today, people do not need to store information by written documents, but to store them as digital data. From *lex lata* point of view, data cannot be held as an 'object' by considering the ordinary meaning of it that is stated in the Commentary on the Additional Protocols even if some type of data remains protected, and targeting civilian data in a way that not to occur death, injury, damage, destruction is not illegal *per se* according to the LOAC.

From *lex ferenda* point of view, 'data' can be regarded as an 'object' due to technological advancements compared to the time of preparation of the Commentary, and the possible consequences of targeting it in our 'data-reliant' world. From this perspective, those intangible things which cannot be included within the ambit of objects are civilians morale and the general aim of an operation. Therefore, data should be regarded as an object by taking humanitarian purposes of the LOAC in line with teleological interpretation.

The notion of lawful targets has already started to change but it still has not reached a level to regard 'data' as an 'object' yet. At this point, it is not appropriate to interpret data by approaching the issue in a manner that if authors of the Commentary lived today, they would accept data as an object. It is a sensitive issue when other branches of international law are taken into account, and states are not only reluctant to put their positions forward clearly but also change the status of data. Thus, political interests lying behind keeping data as an ambiguous issue determine approaches of states rather than legal reasons.

On the other hand, some initial steps which may broaden the notion of *lex lata* have taken place in recent years by international organizations. It is also obvious that cyber positions of some states

April 2020.

76 Tim Maurer, Ariel Levite and George Perkovich, 'Toward A Global Norm Against Manipulating the Integrity of Financial Data' (Carnegie Endowment for International Peace 2017) 4.

77 ibid 6, 7.

such as France and Germany challenge this notion even if neither these positions nor statements of those international organizations still do not reach the level in which the status of data has clearly changed. Therefore, in this article, how the situation makes progress is tried to be explained rather than adhering neither *lex lata* nor *lex ferenda* positions. Although the current situation bothers all civilians including the present author, we should be aware of the fact that law is evolving, and today's *lex ferenda* point will be tomorrow's *lex lata* as happened in the past.

BIBLIOGRAPHY

I. Primary Sources

Treaties, Manuals

Hague Convention IX of 1907 Concerning Bombardment by Naval Forces in Time of War

HPCR Manual on International Law Applicable to Air and Missile Warfare (Bern, 15 May 2009)

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3

Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare (December 1922 – February 1923)

Schmitt MN, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)

US Department of Defence, *Law of War Manual* (2015)

Cases

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v. Serbia) (Judgment) [2015] ICJ Rep 3

United Nations Documents

UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/74/120 (24 June 2019)

UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/70/174 (22 July 2015)

States' Cyber Strategy Documents

Germany, 'On the Application of International Law in Cyberspace' <https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 19 March 2021

'International Security & Cyberspace – Australia's International Cyber Engagement Strategy' <https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/part_4_international_security_and_cyberspace.html> accessed 20 April 2020

Ministère des Armées, 'International Law Applied to Operations in Cyberspace' <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf> accessed 4 April 2020

'The Department of Defense Cyber Strategy' (The Department of Defense 2015)

Secondary Sources

Books, Book Chapters, Articles

Biller J and Schmitt MN, 'Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare' (2019) 95 International Law Studies 179

Boothby WH, *The Law of Targeting* (Oxford University Press 2012)

Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare (Program on Humanitarian Policy and Conflict Research at Harvard University 2010)

Dinniss HAH, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives' (2015) 48 Israel Law Review 39

Dinniss HH, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012)

Dörmann K, 'Applicability of the Additional Protocols to Computer Network Attacks' <https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf> accessed 3 April 2020

Droege C, 'Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 International Review of the Red Cross 533

Fleck D, 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual' (2013) 18 Journal of Conflict and Security Law 331

Geiss R, 'The Conduct of Hostilities in and via Cyberspace', *Proceedings of the ASIL Annual Meeting* (Cambridge University Press 2010)

Gisel L, Rodenhäuser T and Dörmann K, 'Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' [2020] International Review of the Red Cross 1

Hollis, DB, *International Law and State Cyber Operations: Improving Transparency*, OEA/Ser.Q, CJI/doc 603/20 (5 March 2020)

——, *International Law and State Cyber Operations: Improving Transparency*, OEA/Ser.Q, CJI/doc 615/20 (7 August 2020)

Kilovaty I, 'Virtual Violence-Disruptive Cyberspace Operations as Attacks under International Humanitarian Law' (2016) 23 Mich. Telecomm. & Tech. L. Rev. 113

Lubell N, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' (2013) 89 International Law Studies 252

Mačák K, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 Israel Law Review 55

Maurer T, Levite A and Perkovich G, 'Toward A Global Norm Against Manipulating the Integrity of Financial Data' (Carnegie Endowment for International Peace 2017)

Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' (2015) 4 Journal of Law & Cyber Warfare 23

McCormack T, 'International Humanitarian Law and the Targeting of Data' (2018) 94 International Law Studies 222

Murray D, *Practitioners' Guide to Human Rights Law in Armed Conflict* (Oxford University Press 2016)

Sandoz Y, Swinarski C and Zimmermann B (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC 1987)

Schmitt MN, 'Wired Warfare: Computer Network Attack and Jus in Bello' (2002) 84 International Review of the Red Cross 365

——, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 International Law Studies 89

——, '"Attack" as a Term of Art in International Law: The Cyber Operations Context' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT* (IEEE 2012)

——, 'The Law of Cyber Warfare: Quo Vadis' (2014) 25 Stan. L. & Pol'y Rev. 269

——, 'The Notion of "Objects" during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision' (2015) 48 Israel Law Review 81

Schmitt MN and Highfill CE, 'Invisible Injuries: Concussive Effects and International Humanitarian Law' (2018) 9 Harvard National Security Journal 72

Online Documents

Dunlap C, 'The Loyola Conference and the Evolving Definition of Military Objective' (*Lawfire*) <https://sites.duke.edu/lawfire/2016/02/14/the-loyola-conference-and-the-evolving-definition-of-military-objective/> accessed 4 April 2020

'G20 Finance Communiqué' (18 March 2017) <http://www.g20.utoronto.ca/2017/170318-finance-en.html> accessed 4 April 2020

'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (ICRC 2019)<https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf?fbclid=IwAR3ksX7qBnQd61yJFgKqYlAhRKF3VPh9sFFhIZaQB2hNzxqAhksEjJJ83HM>

Richemond-Barak D, 'Is Money a Legitimate Target?' (*Just Security*) <https://www.justsecurity.org/29255/money-legitimate-target/> accessed 4 April 2020

Schmitt M, 'France's Major Statement on International Law and Cyber: An Assessment' (*Just Security*, 16 September 2019) <https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/> accessed 4 April 2020

Schmitt M and Mauer T, 'Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?' (*Just Security*) <https://www.justsecurity.org/44411/protecting-financial-data-cyberspace-precedent-progress-cyber-norms/> accessed 4 April 2020

Watkin K, 'Sustaining the War Effort: Targeting Islamic State Oil Facilities' (*Just Security*) <https://www.justsecurity.org/15890/sustaining-war-effort-targeting-islamic-state-oil-facilities/> accessed 4 April 2020